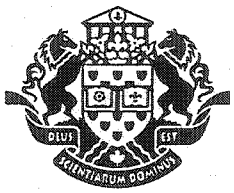


Université d'Ottawa · University of Ottawa

Université d'Ottawa · University of Ottawa

FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

YUAN, Wenhui Frank

AUTEUR DE LA THÈSE - AUTHOR OF THESIS

M.A.Sc. (Electrical Engineering)

GRADE - DEGREE

School of Information Technology and Engineering

FACULTÉ, ÉCOLE, DÉPARTEMENT - FACULTY, SCHOOL, DEPARTMENT

TITRE DE LA THÈSE - TITLE OF THE THESIS

Transparent Service for IP Roaming

D. Ionescu

DIRECTEUR DE LA THÈSE - THESIS SUPERVISOR

EXAMINATEURS DE LA THÈSE - THESIS EXAMINERS

V. Groza

I. Lambadaris

J.-M. De Koninck, Ph.D.

LE DOYEN DE LA FACULTÉ DES ÉTUDES SUPÉRIEURES ET POSTDOCTORALES

SIGNATURE

DEAN OF THE FACULTY OF GRADUATE AND POSTDOCTORAL STUDIES

Transparent Service

For IP Roaming

By

Wenhui (Frank) Yuan

A thesis submitted to the
School of Graduate Studies and Research
In partial fulfillment of the requirements for the degree of

Masters of Applied Science

Ottawa-Carleton Institute for Electrical Engineering
Department of Electrical Engineering
Faculty of Engineering
University of Ottawa
August 2002

Your file Votre référence
ISBN: 0-612-90361-3
Our file Notre référence
ISBN: 0-612-90361-3

Abstract

In this thesis, the requirements of mobile networking and transparent service are discussed. A survey of existing technologies for IP roaming is provided. IETF Mobile IP is the most favorable solution available today. However Mobile IP has some limitations: a) It does not provide transparent service to mobile hosts, i.e. it requires modifications to IP stack in mobile hosts; b) It is targeted to the wireless mobile hosts in carrier markets, which brings much unnecessary complexity for the enterprise environment, especially for semi-mobile hosts. c) The handoff of Mobile IP introduces service disruption to IP traffic. To address the issues, a new framework and suite of protocols are proposed. The solution is termed Roaming IP. Roaming IP is targeted for roaming service in enterprise networks which have both semi and full-mobile hosts. To achieve the goals of transparency, fast handoff and simplicity, some novel ideas are used in Roaming IP: Roaming ARP, Roaming ping, Local Service Name Resolution, Roaming directory, Roaming motion detection and two-phase handoff. In the second half of the thesis, an architecture and implementation of Roaming IP is presented. Lastly, experiment results, conclusions and areas of future study are provided.

Acknowledgments

I would like to thank my supervisor, Dr. Dan Ionescu, for his guidance, encouragement, optimism and support throughout my research. His ability to set goals and challenge one to achieve them is responsible for the complexity of this thesis.

I have a special thank-you to my beloved wife Xuan Zhou for her understanding and support throughout my research.

Table of Contents

List of figures

List of Tables

Glossary of Terms

AH	Away Host
AP	Access Point
API	Application Programming Interface
ARP	Address Resolution Protocol
CGI	Common Gateway Interface
CH	Correspondent Host
CLI	Command Line Interface
CPU	Central Processing Unit
C-RS	Client to Roaming Server
DHCP	Dynamic Host Configuration Protocol
DM	Directory Management Module
DN	Distinguished Name
DNS	Domain Name Service
ECS	Eager Cell Switching
FSM	Finite State Machine
FTP	File Transfer Protocol
GRE	General Routing Encapsulation
GRS	Guest Roaming Server
HRS	Home Roaming Server
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IAPP	Inter-Access Point Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IP v4	IP version 4
ICMP	Internet Control Management Protocol
IGMP	Internet Group Management Protocol
ITU	International Telecom Union
LAN	Local Area Network
LCS	Lazy Cell Switching
LDAP	Light Weight Directory Access Protocol
LNI	Local Network Interface
LSNRP	Local Service Name Resolution Protocol
LSR	Loose Source Route
LSRIP	Loose Source Route IP
MAC	Medium Access Control
MAS	Mobile Access Stations
MBG	Mobile IP Border Gateway
MR	Mobile Router
MH	Mobile Host

MIP	Mobile IP
MPLS	Multi Protocol Label Switching
MR	Mobile Router
MTU	Maximum Transmit Unit
NF	Not Fragment
OSI	Open System Interconnect
OSPF	Open Shortest Path First
PC	Personal Computer
PDU	Protocol Data Unit
PM	Pattern Matching
QCOUNT	Question Count
QoS	Quality of Service
RBMoM	Range-Based Mobile Multicast
RFC	Request For Comments
RH	Roaming Host
RIP	Routing Information Protocol
ROMIP	Mobile IP with Route Optimization
RS	Roaming Server
RSM	Roaming Service Management
RS-RS	Roaming Server to Roaming Server
SNA	System Network Architecture
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
TCP-MD	TCP-Motion Detection
TCP-R	TCP-Registration
TFTP	Trivial File Transfer Protocol
TIP	Temporary IP
TTCP	Test TCP
TTL	Time To Live
UI	User Interface
URL	Uniform Resource Locator
VIP	Virtual IP
WWW	World Wide Web

Chapter 1 Introduction

In the last several years, the Internet has experienced an explosive growth. There are hundreds of millions of computers connected to the Internet. Network applications such as Email, WWW and streaming audio/video become part of daily life. According to Internet Software Consortium [1], the number of internet host is 109,574,429 in Jan 2001. By Jan 2002, the number had increased to 147,344,723. Network connection to the Internet is a necessity. In companies, schools and governments, all computers are connected together with an internal network then connected to the Internet. Computer networks are an essential part of the infrastructure. Meanwhile, with the advance of computing technology, portable and mobile computing devices have become a reality. This trend stimulates the demand of mobile computing. The great success of palmtop devices and fast growth of laptop computer use fully demonstrate this demand. According to the IDC [2], laptop computer accounts for more than 25% of global computer revenue in 2001. The shipment of laptop computers increased 8.6% while desktop decreased 4.4% in 2001. In the next three years, the growth rate of laptop computer is forecasted in the double digits while desktop in only single digit.

The strong demand for network access and mobility brings a new challenge to provide network connection anywhere, anytime, giving rise to the need for mobile networking technology.

It is well know knowledge that when computers communicate with each other through the network, they need to follow certain protocols. The TCP/IP protocol suite[3] defined by IETF in early 1980s provides inter-working between different computers. It is the standard protocol suite used in the Internet. With the huge success of the Internet, TCP/IP became the mostly used networking protocol suite and the standard of internetworking. Our research of mobile networking focuses on the TCP/IP protocol. In the scope of our

research and this thesis, mobile networking service is mobile networking service with IP. The term "mobile networking service" is interchangeable with "IP roaming service".

In this thesis, Roaming IP is proposed to provide transparent service for IP roaming in enterprise networks. This begins with an introduction of mobile networking service and its requirements on networking protocols, followed by a brief discussion of the transparent service of mobile networking. Current research and solutions to provide roaming service with IP protocol is examined. Next, it is followed by a definition and implementation of the Roaming IP. Finally, results of experiments and conclusions are provided.

1.1 Mobile networking Service

The goal of mobile networking is to provide ubiquitous network access to users. People want to stay connected to the Internet while on the move. In the public data network, connection to the Internet is provided through the wireless infrastructure. People can browse the web or download files from Internet as long as they are in the service areas, even when they are in a moving car or train. In the enterprise network, people move around in the company with their laptop computers between offices and meeting rooms. Connection to the enterprise network is provided by wired or wireless medium. The following is an example of mobile networking service in an enterprise network. Wired and wireless Access Points are installed at all locations of the company. A laptop computer stays connected to the Internet when it roams around.

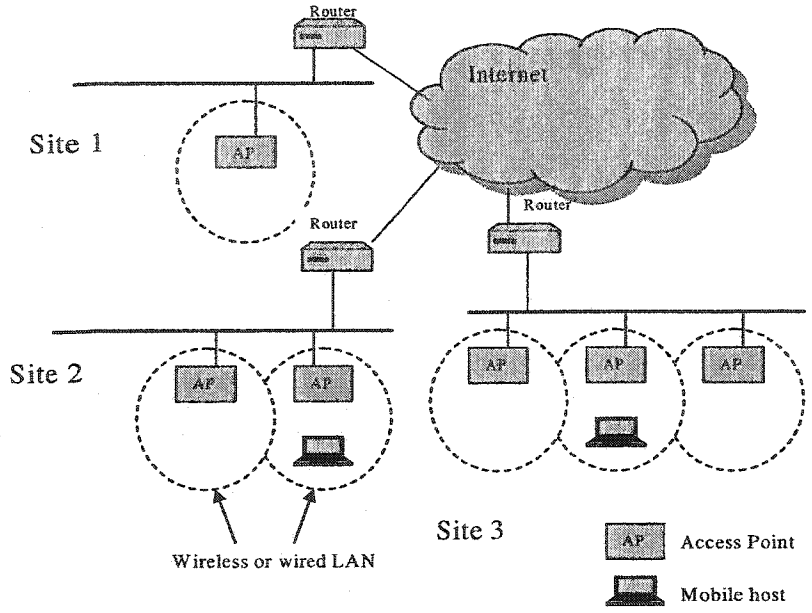


Figure 1 Wireless mobile networking

Based on the level of mobility and portability, mobile networking service can be divided into two categories: semi-mobile and full-mobile. With semi-mobile service, a mobile host stays stationary when receiving or sending traffic. When there is no network activity, the mobile host roams freely to different locations. It regains access to the network in the new location where it moves. But the mobile host does not receive or send data packets when it's moving. Semi-mobile service is common in enterprise networks. Users carry laptop computers to different locations like office and meeting rooms. There is no need to access the network during the move. The laptop is re-connected to the network after the user gets to the new location.

With full-mobile service, a mobile host stays connected to the network when it is stationary or moving, even moving across the boundary of different service areas. Full-mobile service provides more freedom to users than semi-mobile service.

1.1.1 Requirements of Mobile service to network protocols

Mobile networking service has non-traditional requirements, necessitating modifications to existing network protocols. Exceptions in the TCP/IP protocol stack include the

application and transport layer because they are location-independent. Moving locations does not have an impact on them as long as lower layers continue to provide required service. Therefore, there is no need to modify application and transport layers for mobile networking.

Mobile networking has bigger implication to the network (OSI model layer 3) and link layer (OSI model layer 2). To provide link layer service on the move, traditional wired technology does not work any more. A new link layer based on wireless technology is necessary. With mobile networking a mobile node changes its point of attachment to the network. Traditional network layer protocol may not be able to correctly deliver data packets any more. The focus of this research is to enable network layer for Mobile networking.

With semi-mobile services, a mobile host stays stationary during network connection. Both wired and wireless link layer technology satisfy the requirement. A mobile host can move into different service domains (routing subnets). Modifications to the network layer are required to route packets correctly after a roaming host moves into a different subnet.

With full-mobile services, a mobile host keeps network connection during the move. A wireless link layer protocol is required. A mobile host may move into different subnets. A new mechanism needs to be introduced in the network layer to deliver packets correctly. The mobile host also needs to maintain communications with the network when crossing the boundary of service domains. A protocol between the service stations is required to handle the handoff.

In this research, the Roaming IP solution provides both semi-mobile and full-mobile service.

1.1.2 Transparent mobile networking service

To provide mobile networking service, it is necessary to enhance the current IP protocol. The enhancement can be done on the fixed nodes like routers or on the mobile hosts. There are tens of millions of mobile hosts (e.g. laptop computers) deployed today. They are the users of mobile networking service. It is a big advantage if no change is required on the mobile hosts to access the service.

A transparent mobile networking service is a solution that does not require changes of IP protocol stack in the mobile hosts. Existing IPv4 hosts can access the service without any hardware or software modification.

1.2 Objectives, layout and Contributions of the thesis

1.2.1 Objectives

In this thesis, current research and solutions are examined to provide roaming service with IP. Since current solutions do not provide transparent service to mobile hosts, a new solution termed Roaming IP is proposed to provide transparent service for mobile networking with IP. A further objective is to present an implementation of the Roaming IP protocol and results of experiments. Finally a conclusion and areas of future study are provided.

1.2.2 Layout

In chapter 1, a brief introduction of mobile networking is given. Then the requirements of mobile networking are briefly discussed.

Chapter 2 will provide an analysis on the limitations of conventional IP in a mobile networking environment. We present technologies available today to provide mobile networking. For each solution, a brief description, advantages and limitations are given. Mobile IP is given the most attention because of its popularity. The research results of Mobile IP are discussed. Finally the limitations of Mobile IP are highlighted.

The Roaming IP solution is defined in chapter 3. Protocols and operations of Roaming IP are covered in detail. First, an introduction and terminology definition of Roaming IP is provided. Second, the requirements of Roaming IP are discussed. The definitions of operations, procedures and message formats follow.

In chapter 4, the handoff solution for Roaming IP is presented. The limitations of handoff with mobile IP and related research are discussed. Then the solution for Roaming IP to achieve fast and smooth handoff is proposed. Lastly, an analysis of the performance is provided.

Chapter 5 describes the management information of Roaming IP. A directory service is presented to manage Roaming IP.

In chapter 6, the system architecture and an implementation of roaming IP are presented. Components and implementations of roaming server are described.

Experiments are carried out to check the effectiveness and performance of Roaming IP protocol in chapter 7.

In chapter 8, a conclusion and areas of future study are provided.

1.2.3 Contributions

The major contribution of this thesis is to propose a new solution (Roaming IP) that provides transparent IP roaming service. An implementation of Roaming IP is also presented.

Roaming IP is an end to end solution for mobile networking. It provides complete transparency to mobile hosts. There is no change required on the mobile host to access mobile networking service. Roaming IP also provides a fast and smooth handoff solution. The following are ideas adopted to define Roaming IP:

- Local Service Name Resolution (LSNR).
- Roaming host detection
- Roaming ping
- Roaming server to server protocol
- Roaming host movement detection
- Two-phase service switchover
- Directory service for Roaming IP

In the thesis, an implementation of Roaming IP is presented. The implementation has the following benefits:

- Use an architecture that is flexible for future expansion
- Use third party software to speed up research
- Use Standard C and portable 3rd party libraries to maintain portability
- Give considerations to the ease of use and development

Chapter 2 Mobile networking with IP

In this chapter, limitations of IP version 4 in mobile networking are analyzed. Surveys are provided for current solutions that enable mobile networking with IP v4. A brief description of each solution is presented. The advantages and limitations are also discussed.

2.1 IP version 4 in mobile networking

2.1.1 Introduction to TCP/IP protocol

TCP/IP is often understood to mean the protocol suite used in the Internet TCP/IP, not only IP [4] (the specific protocol for interconnecting separate networks) and TCP [5] (which provides reliable data transport). TCP/IP is a 4-layer system, with each layer responsible for a specific task. The four layers, from higher to lower, are application layer, transport layer, network layer, and link layer. [3] The following diagram illustrates the relationship of different layers.

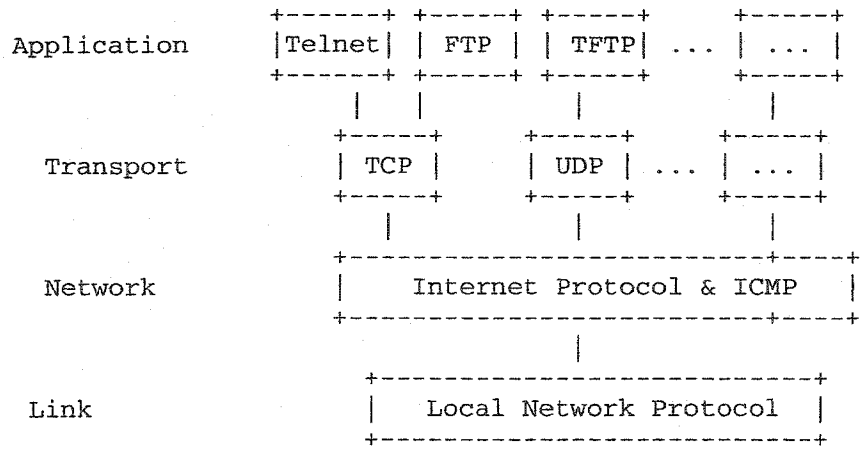


Figure 2 Protocol Relationships in TCP/IP

The *application layer* handles the details of the particular application, such as FTP, TELNET, HTTP and so on.

The *transport layer* provides an end to end connection between two applications on different nodes. It accepts data from one end point (the application layer), passes the data to the network layer. It relies on the network layer to deliver the data to the remote network node. Then the transport layer passes the data to the correct end point on the remote node. In the TCP/IP protocol suite, there are two different transport layer protocols: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol). TCP provides reliable transport service with acknowledgement and flow control while UDP provides only raw data delivery without guarantee.

The *network layer* handles the movement of packets around the network. Every node in an internet is assigned an IP address. TCP/IP network layer includes IP (Internet Protocol), ICMP [7] (Internet Control Message Protocol) and IGMP [8] (Internet Group Management Protocol), where IP is the core protocol and ICMP and IGMP are auxiliary protocols. IP address is a key component of Internet Protocol. All internet hosts are uniquely identified by IP addresses. Normally all nodes in the same local network are grouped together to form a subnet. Then subnets are interconnected by routers. Routers transfer data packets across different subnets.

The *link layer* provides raw data delivery service that is free of transmission errors to the network layer. It also provides address scheme and mechanism to deliver raw data packets to the correct network node. The link layer is responsible for communication between two nodes that are directly connected. Every node has an address used by the link layer, called *link layer address* (or MAC address for Ethernet link).

2.1.2 Packet delivery of IP Version 4

Internet protocol is the network layer in the TCP/IP stack. "The function or purpose of Internet Protocol is to move datagrams through an interconnected set of networks. This is done by passing the datagrams from one internet module to another until the destination is reached" [4]. Internet modules reside on the all networking computers and gateways

that connect different local networks together. There are currently two different versions of IP, version 4 and version 6. Since the majority of Internet hosts are running IP v4, the focus of this research is on IP v4. IP data packet delivery and its limitations in mobile networking will be examined.

Consider how data packets are transmitted from one application to another across the Internet. In figure 3, Node A is connected to the local network 1, Node B is connected to local network 2. Local network 1 and 2 are interconnected by a gateway, router C. Both network 1 and 2 are Ethernet. Node A has one network interface in local network 1, the MAC address is mac_a. Node B has one network interface in local network 2, the MAC address is mac_b. Router C has two network interfaces in both local networks, the MAC addresses are mac_c1 and mac_c2 respectively.

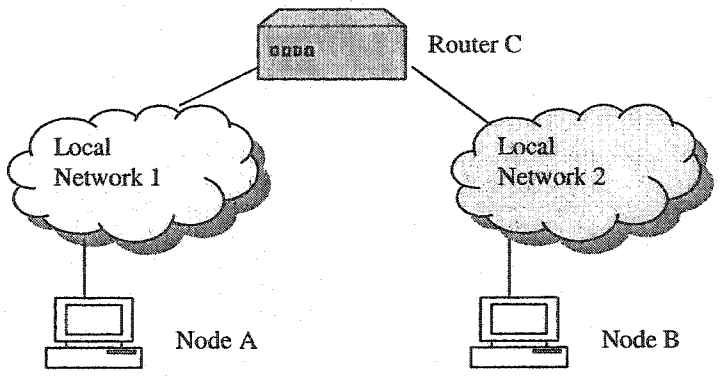


Figure 3 An IP networking example

In figure 4, components in the hosts are depicted. Application A is running on node A, application B is running on node B. Application A needs to send data to application B.

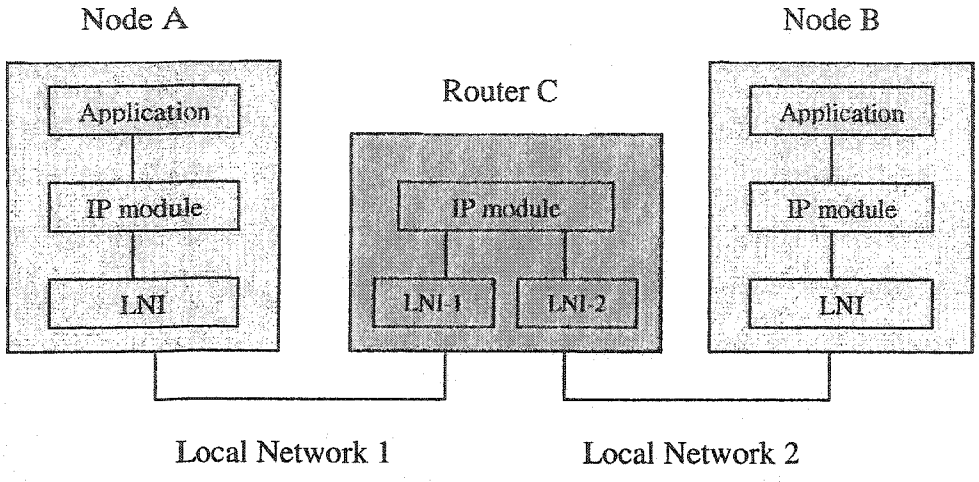


Figure 4 An example of network applications

Application A prepares data and calls an API provided by the local IP module to send the data. IP destination address and other parameters are passed with the call.

The IP module on node A creates an IP data packet by filling in the IP header information and attaching the data from application A. Then the module determines the local network address (MAC address) of next node that the packet should be sent to. The procedure is called address resolution. ARP (Address Resolution Protocol) [6]is used for this purpose. In this case destination IP is resolved to mac_c1. The IP module sends the IP packet to the local network interface LNI. The local network interface creates an Ethernet data packet by filling in the Ethernet header and attaching the IP packet. The destination address in the Ethernet header is set to mac_c1. Then it sends the packet out to the network.

The Ethernet packet is sent to Router C's network interface in network 1. In router C, The local network interface strips the Ethernet header and passes the IP packet to the IP module. The IP module checks the destination IP address against its routing rules to decide where to send the packets. This exercise is called routing. Routing rules are set up statically or dynamically by routing protocols like RIP[9] and OSPF[10]. In this case, the IP module decides to send the packet out via interface 2 in local network 2. The IP

module uses ARP to get the local network address of the next hop. The destination IP is resolved to node B mac_b. The IP module passes the IP packet to local network interface 2 with mac_b. Local network interface 2 on router C creates an Ethernet header, attaches the IP packet, then sends the packet out to local network 2.

The Ethernet packet arrives at the local network interface of node B. In node B, The network interface strips the Ethernet header and relays the IP packet to the local IP module. The IP module finds out that the packet is destined to local node. It strips off the IP header and delivers the data to application B, the final destination.

2.1.3 Limitation of IP protocol in mobile networking

As discussed, there are two critical operations to move data packets correctly: address resolution and routing. Address resolution decides the correct next node in a local network, while routing decides the correct next subnet in an interconnected network. The IP address is key in address resolution and routing.

All nodes in the Internet are uniquely identified by an assigned IP address. Normally, all nodes in the same local network are assigned IP addresses with the same address prefix and put in the same subnet. They have the same sub-network address, the same subnet mask and different node address. This makes routing in the Internet housing millions of nodes a possibility. Routing rules are summarized into a subnetwork address stead of individual node addresses, which decreases the number of routing rules by several orders of magnitude. But this also implies that the IP address of a node is associated with its location or its point of physical attachment to the Internet. All nodes that are connected to the same local network belong to the same subnet and their IP addresses have the same subnetwork prefix.

In IP version 4, because routing rules are mostly based on subnets, IP packets destined to an IP host are always delivered to a router attached to the home subnet initially. Then the packets are passed to the final destination by a router attached in the home subnet. Since

the IP host moves away from the home subnet, the packets are still sent to the router in home subnet. Because the IP host is not in the home subnet any more, the router drops all packets and sends ICMP messages "destination unreachable" back to the originator. After moving into a new location, an IP host is not able to send packets to other network nodes with its original IP address as a source address since the router in the guest network does not relay its packets to the Internet.

In conclusion, existing IP version 4 can not deliver IP packets in both directions for a host that roams away from its home subnet. In IP v4, the IP address of a host represents both the identification of the host and the location of its home network connection. The IP address specifies the IP subnet that a host can attach to, limiting the host to that network. Due to this limitation, IP version 4 doesn't satisfy the requirements of mobile networking. To provide mobile networking service, IP version 4 needs to be enhanced and new protocols need to be developed.

2.2 Current solutions of Mobile networking

The analysis provided in previous sections illustrates that the fundamental requirement of mobile networking to the networking layer is to provide reachability of a mobile host in the network. That is to say, to guarantee the delivery of packets from a mobile node to the network and packets from the network to a mobile node after the mobile node is attached to the network from a new location. If full-mobile service is required, another requirement is to provide smooth transition when mobile host moves across the boundary of different routing subnets.

In the last several years, mobile networking solutions attract much attention from both the research community and telecommunication industry. Considerable effort has been put into the research of mobile networking and significant results have been achieved. The proposals and research are discussed in the following sections.

2.2.1 Node specific route

As discussed, data packets are forwarded by routers across the Internet. Routers use rules stored in routing tables to decide how to route a packet. Routing rules are typically provisioned manually or computed by routing protocols like RIP[9] or OSPF[10]. The "node specific route" solution resolves reachability problem by changing the routing table of routers in the network. A mobile host keeps the same IP address when it moves to different service areas (IP subnets). When a mobile host moves into a new IP subnet, a node specific route is injected into the router of the new location. Then the node specific route is flooded to the rest of network. Based on the node specific routing rule for the mobile host, all data packets destined to the mobile host are delivered to the new location instead of the home network. A node specific route is described in routing protocols. With today's router, a node specific route can only be configured manually. Dynamic configuration would require new protocols be developed.

The advantages of this solution are:

- Its transparency to mobile hosts. There is no need to change the protocol running on roaming host.
- It doesn't change the efficiency in packet forwarding comparing to traditional IP. Data packets are always routed via optimal path. There is no need to do packet redirection from the home network.

The disadvantages of "node specific route" solution are:

- It's not scalable. Depending on the size of the network, the time to flood the node specific route can be very long. For each mobile host, a new route needs to be injected into the routing table. The number of node specific routes may be too big for routers to handle.
- It uses extra network resource to update node specific routes. The updating of node specific route is frequent when the mobile node is on the move, new route needs to be updated every time the node is moved.

Mainly due to its limit on scalability, the "node specific route" solution doesn't attract significant acceptance from the research community.

2.2.2 DHCP and Dynamic DNS

The "DHCP and Dynamic DNS" solution doesn't address the reachability problem directly. Instead it circumvents the problem by providing a constant name for a mobile host regardless of its location. Network hosts that need to communicate with a mobile host use the domain name [11][12] of the mobile host instead of an IP address. When a mobile host moves to a guest network, it obtains a new IP address from the local DHCP [13]server. Then the domain name entry of the mobile host will be updated in the domain name servers. Dynamic DNS[14][15] is defined for this purpose. The mobile host's domain name is resolved into the new IP address. The new IP address belongs to the guest subnet. The roaming host is able to communicate with other nodes in the network as a regular node.

The advantages of this solution are:

- There is no need to change IP stack on either roaming hosts or routers
- There are standards and implementations available.

The disadvantages are:

- It takes time to obtain a new IP address and update the domain name entries. A mobile host is not reachable until the update is finished.
- Some applications need to have a fixed IP address due to security reason. This solution doesn't work for those applications.
- Network connection cannot be maintained when changing service domains because the IP address is changed. Handoff service cannot be provided without changing the protocol layers above IP layer 3.
- Applications need to restart after the change of IP address. It's not convenient.
- It requires applications on other computers interacting with the mobile host to do name lookups every time the mobile host moves.

"An End-to-End Approach to Host Mobility"[16] presents a design and implementation of end-to-end architecture for mobile networking based on DHCP and dynamic DNS. In the proposal, the authors tried to provide handoff service by making modifications to the TCP layer and applications. Implementation of such a scheme in real network is impractical because of the cost associated with changing applications.

2.2.3 Mobility over a logical network

This is a solution described in [17]. The solution addresses mobile computers via a new "logical network" which has no direct relationship with any other existing wired network. The topology of the logical network is maintained by tracking the movements of mobile computers. A new entity, MC (mobile router) is introduced in the solution. The MC serves as the router for the logical network. All data packets destined to a mobile host is always routed to the MC. Then the MC redirects the packets to the router of the sub-network in which the mobile host resides. Finally, the router forwards the packets to the mobile host. The author provided high-level description of the idea, but did not detail protocol definition or implementation.

2.2.4 VIP

The VIP (Virtual IP) solution is discussed in [18][19][20]. In the proposal, mobile networking is called migration-transparent service. The authors proposed two new network layer services to provide host mobility: Migration-transparent host addressing and Migration-transparent packet delivery.

In VIP, every host is assigned two IP addresses: one physical IP or TIP (Temporary IP) and one virtual IP. Only the virtual IP is visible to the transport layer, i.e. the host is addressed with the virtual IP. When the mobile host changes location, it gains a new physical IP while maintaining the same virtual IP. The physical IP is related to location and the virtual IP is location-independent.

To provide migration-transparent packet delivery, a cache mechanism is used for address resolution from VIP to TIP. Each router or host holds a cache for address resolution. The address resolution is done either at the source node or the intermediate routers. If the source node does not have an entry in the cache for a destination, it makes TIP equal to VIP. The packet will be delivered to the home network unless one of the intermediate routers has an entry of the address resolution. In this case, the real TIP will be set and the packet is delivered to the destination in its new location directly. If the packet is delivered to the home network, the router there is able to do the right resolution and forward the packet to the right location. When the packet travels along the path, a cache entry is on each intermediate node using the information embedded in the packet. When a host moves to new location, all cache entries are not valid any more. A special message is broadcasted in the network to delete those entries. Because the delete message is not reliable, timers are required to delete invalid entries.

The big advantage of VIP is that: when there are many intermediate routers that support VIP protocol, the routing path of packets is optimized.

There are several serious limitations of VIP:

- Updating the address translation caches is very costly. VIP has a scalability problem.
- VIP uses an IP option to carry the protocol information. But many routers do not support the option.
- VIP needs many extra IP addresses in foreign network

2.2.5 LSRIP

The LSRIP (Loose Source Route IP) solution is discussed in [21] [22]. The LSRIP scheme uses an existing IP option to address reachability issues for mobile hosts. Mobile hosts use the same IP address regardless of its physical location. In the home network, a mobile router is introduced to keep track of the location of each mobile host. In the foreign network, Mobile Access Stations (MASs) provide connections to mobile hosts. The packets destined to the mobile host arrive in the home network and are picked up by

the MR. The MR inserts a LSR option into the packet with the transit node set to the MAS. The LSR capable routers will deliver the packet to the MAS. Lastly the MAS forward the packet to the mobile host. When the mobile host replies to the source, it inserts the LSR option in all outgoing packets specifying the MAS as a transit router. The path between the mobile host and the correspondent node is recorded in the LSR option. When the correspondent node receives the packet, it reverses the recorded route and inserts it to all packets destined to the mobile host. All packets take the optimal route.

The disadvantages of LSRIP are:

- The dependency on Internet Hosts' ability to perform route reversal which is not supported by the majority of hosts.
- LSR option is poorly or not supported by routers.

2.2.6 IETF-Mobile IP

After early experiments with mobile networking solutions, the Internet Engineering Task Force (IETF) set up a Mobile IP working group to propose a standard for mobile networking. Mobile IP protocol resulted from the initiative. Mobile IP is composed of multiple protocols to address different aspects of mobile networking. Mobile IP addresses the reachability of mobile hosts, handoffs and optimization of packet delivery. With Mobile IP, a mobile host does not change IP address when it moves into different IP subnets. A mobile host can maintain communication session when moves across the boundary of different service area (routing subnets). Mobile IP makes the change of location transparent to applications above IP layer. The IP protocol on the mobile host needs to be enhanced, but there is no change required for applications above IP.

The mobile IP protocol resolves reachability problem by introducing two new entities: home agent and foreign agent. The home agent is "a router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home, and maintains location information for the mobile node".[23] The foreign agent is "a router on a mobile node's visited network which provides routing services to the mobile node while registered. The foreign agent de-tunnels and delivers datagrams to the

mobile node that were tunneled by the mobile node's home agent". [23]The mobile host has a "care-of" address when it is in a foreign network. The care-of address is either the IP address of the foreign agent or a local address that the mobile host attains in the foreign network. As illustrated in figure 5, the home agent attracts all data packets destined to the mobile host. All data packets are delivered to the home network of the mobile host regardless of the mobile host's locations. The home agent takes appropriate action for the delivery of data packets to the mobile host based on "binding" information. A "binding" is the association between a mobile node and its care-of address. The binding information is updated on the home agent every time the roaming host moves into different foreign subnet. Data packets attracted by the home agent are encapsulated in a new IP header with destination of the foreign agent. The packets are passed to the foreign agent through regular IP routing. The foreign agent strips the outer IP header. It then delivers data packets to the mobile host.

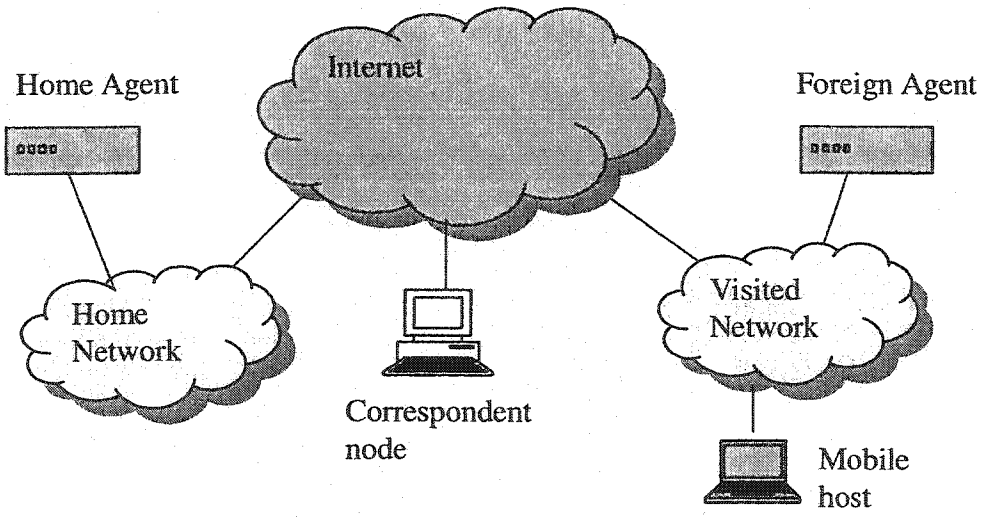


Figure 5 IETF-Mobile IP

The key documents describing mobile IP are: IP mobility Support[23], IP encapsulation within IP[24] and Minimal Encapsulations within IP [25]. IP Mobility Support is the base protocol and is primarily concerned with the maintenance of mobility bindings. IP Encapsulation within IP solves problem of packet delivery from the home agent to the

foreign agent. Minimal Encapsulation is another approach of packet encapsulation, which reduces the IP header size in encapsulated packets.

2.2.7 Research of Mobile IP

Since the introduction of mobile IP, it became the most popular solution of IP roaming. Many papers on mobile networking are devoted to mobile IP.

There are proposals that introduce new features into Mobile IP. In [26], the author proposed an extension to the DHCP protocol to allow a mobile host to obtain a home IP address instead of a foreign IP when it's in visited subnet. This enables the employment of an actual foreign agent on each subnet. Actual foreign agents provide service with better performance. In [27], the authors present a fault-tolerant protocol using checkpoint and receiver-based pessimistic message logging techniques. In [28] [29], the authors propose schemes to provide multicast service for mobile host.

Mobile IP is targeted to wireless mobile hosts in public carrier environment where, it is critical to have smooth handoff. This requirement has fueled research into the handoff performance of Mobile IP. In [31], the authors studied the performance of Mobile IP handoff. They did performance test for two different movement detections: Lazy cell switching and Eager cell switching. The handoff delays are 2.5 and 0.5 seconds respectively. In [34], the author proposed to use a single protocol for both link layer (within IP subnet) and IP layer (across IP subnet) handoffs within a local domain. The advantage of the proposal is to eliminate IP encapsulation, triangular routing, overhead and latency caused by interfacing of link and IP layer handoff management. In [35], the author proposed two schemes TCP-MD and TCP-R, modifying TCP to improve the handoff performance. In [36] [39] [40], The authors propose packet buffering to improve handoff performance. Foreign agents buffer packets and send them to the new foreign location when a mobile host moves. In [75] [76] [39], the authors propose a hierarchical mobility management scheme to exploit the locality of mobile hosts' movement to change regular handoff to a more efficient local handoff.

In Mobile IP, All packets are routed to the home agent. The home agent then tunnels the packets to the real location of a mobile host. Since this redirection uses a sub-optimal route, there is a requirement to optimize the routing. In [32], the authors propose the use of Mobile IP Border gateways (MBGs) to optimize the routing for Mobile IP. The advantage of the proposal is avoiding changes on CH (Correspondent Host). The MBG will route packets directly to the mobile host instead of the home agent. In [33], the authors propose a new scheme that the mobile host also obtains a virtual home IP. There is no triangle route problem while communicating with the new IP address. In [74], the authors presented performance result of MIP (Mobile IP) and ROMIP (Mobile IP with route optimization). The conclusions are: If the rate of birth and death of sessions are high, MIP performs better than ROMIP. Large session duration better exploits the benefit of ROMIP. The performance behavior depends on traffic pattern.

2.3 Limitations of Mobile IP and solution overview

With all the efforts from the networking industry and research community, Mobile IP has become mature. It is the preferable solution for wireless mobile networking. However, there are a few drawbacks that limit the application of Mobile IP in other areas like providing semi-mobile services in enterprise networks.

Mobile IP does not provide transparent service for IP roaming. Mobile IP is targeted to the new generation of wireless mobile host. It is assumed that new networking protocol can be implemented on mobile hosts. This means a software even a hardware upgrade is required on the current mobile hosts (i.e. Laptops). Development and deployment of new networking protocol to existing tens of millions of laptop computers is an expensive exercise.

In Mobile IP, much of the complexity is put on the mobile hosts. This, in general, is not preferable because mobile hosts are sensitive to power consumption which comes with the complexity of software.

Mobile IP is designed for wireless mobile hosts in the public carrier environment. The complexity is necessary for handling the challenging environment in public cellular network. But for roaming hosts in the enterprise environment, especially for semi-mobile hosts, Mobile IP is too complicated and too expensive.

The other drawback of mobile IP is the time of handoff is so long that it causes service disruption for TCP traffic which is discussed in detail in chapter 4.

This thesis proposes a new framework and associated protocol suite to overcome the limitations previously described. The solution is named Roaming IP. Roaming IP provides transparent mobile networking service with IP v4. Roaming IP does not introduce changes to the network protocol of mobile hosts. From a mobile host's perspective, it sees only regular IP data packets and handles those packets following regular IP protocol. All complexity of mobile networking resides on the nodes that provide roaming service, i.e. roaming servers. In Roaming IP, a fast handoff service is defined.

The biggest challenge of Roaming IP is to maintain complete transparency to roaming hosts. No change is allowed in the roaming host. To accomplish that, roaming servers have to use the same packet formats to communicate with mobile hosts. Moreover, roaming servers have to make handling of packets appear the same as regular IP v4 to roaming hosts. From the perspective of a roaming server, message formats are the same as regular IP v4, but there is new meaning associated with those packets. The way to interpret and handle those packets is changed or enhanced to support roaming IP service. For example, ARP request messages are used to do address resolution in regular IP. In roaming IP, the same message is also used for tracking mobile hosts.

Like Mobile IP, Roaming IP enables mobile nodes to move from one IP subnet to another without changing IP address. Roaming IP addresses "macro" mobility management, i.e.

Layer 3 mobility. The "micro" mobility management like handoff amongst wireless transceivers is provided at OSI layer 2, the link layer.

The Roaming IP framework will be able to re-use the research results from Mobile IP.

Chapter 3 Roaming IP

3.1 Introduction

Roaming IP is the solution to provide transparent service for IP roaming service. It differentiates itself from Mobile IP by providing complete transparent to mobile hosts. There is no change (neither hardware nor software) required on mobile hosts for the mobile networking service. Roaming IP is applicable to all hosts running in the IP v4 network today.

Roaming IP protocol needs to satisfy the following requirements:

- There is no need to change the TCP/IP stack on roaming hosts. The roaming is completely transparent to applications on the roaming host.
- A roaming host is able to communicate with other nodes after changing its point of attachment to the network without changing IP address
- A roaming host is able to communicate with other non-roaming hosts.
- Roaming IP place no additional requirement on the assignment of IP address.

Roaming IP is defined on the following assumptions:

- Mobile hosts will not change the point of attachment to the Internet more than once a second. This is the same as Mobile IP.
- A roaming server does not need to be the router in the subnet. It makes the problem even more challenging to solve. But it provides more flexibility and practicality.
- The security is handled by other layer just like conventional IP V4.

Previously discussed, IP version 4 is designed with the implicit assumption that Internet hosts are statically attached to the physical network. The IP address is associated with the

physical location of the network connection. A data packet destined to a host is always delivered to the home network that can be identified by the IP address of the host. This means that a host is no longer reachable if not attached to its home network. To maintain mobile hosts' ability to communicate when changing points of attachment to network, Roaming IP introduces new entities: guest and home roaming servers. Roaming IP provides several services: registration, packet delivery, management and handoff. Roaming IP solution is composed of the following protocols: Roaming ping, roaming ARP, local service name resolution protocol and roaming server to roaming server protocol.

3.2 Roaming IP terminology

The following terms are used to describe the roaming IP framework and protocol.

Roaming Host (RH)

A computing node that needs to access the network while changing its point of attachment. A roaming host does not change its IP address when it moves from one sub network to another. It continues to communicate with other Internet hosts during and after the move if the link-layer provides connectivity to an access point of the network.

Correspondent host (CH)

A computing node that is connected to the wired network and communicates with a roaming host.

Home network

A network that a roaming host gets its IP address from. The roaming host can communicate with Internet hosts without the support of other computing nodes.

Guest network

A network that a roaming host visits. A roaming host can not communicate with other Internet hosts without roaming service.

Roaming Server (RS)

A computing node that provides roaming services to roaming hosts. Roaming servers reside in networks where roaming service is provided, including the home network and guest networks.

Home Roaming Server (HRS)

A Roaming server that resides in the home network of a Roaming Host. A home roaming server intercepts and forwards data packets on behalf of roaming hosts in the home location.

Guest Roaming Server (GRS)

A roaming server that resides in the guest network where a roaming host visits. A guest roaming server detects the existence of a roaming host in the network. It provides utilities for roaming hosts to manage their access to roaming services. It also provides packet delivery service to roaming hosts. The GRS retrieves data packets that delivered through the tunnel by HRS and delivers them the roaming host. For data packets sent by a roaming host, the GRS serves as a default gateway. A GRS also provides handoff service when a roaming host moves from one subnet to another.

Roaming host list

A list of roaming hosts that are maintained by a guest roaming server. The list contains all roaming hosts that are visiting the guest network and granted roaming service.

Away host list

A list of roaming hosts that maintained by a home roaming server. The list contains all roaming hosts that are away from the home network and registered for roaming service.

Neighbor host list

A list of roaming host that maintained by roaming servers. When a roaming host is granted handoff service, all neighboring roaming servers put the roaming host into their neighbor host lists. The neighbor host list is used for fast detection of a roaming server during handoff.

Roaming host detection

Roaming host detection concerns how a roaming server detects the existence of a roaming host.

Roaming IP service registration

Roaming IP service registration deals with service application, authentication and setup. It is the first step of roaming IP service.

Packet delivery service

Packet delivery deals with packets delivery for the RH. After a RH is attached to a guest network and granted roaming service, all packets destined to the RH are still delivered to the home location. The HRS picks up all packets and sends them to the GRS through a tunnel. The GRS retrieves the packets from the tunnel and delivers the packets to the RH directly. In the reverse direction, all packets from the RH to other hosts are picked up by the GRS and tunneled to the HRS. Then the HRS releases all packets to the network.

Handoff service

Handoff service deals with the transition of a RH from one visiting network to another. It switches the roaming service from the old subnet into the new one with minimum service disruption.

Handoff neighbor

A roaming server that is in the neighboring subnet of another roaming server. A Roaming server communicates to its handoff neighbor to provide handoff service for a roaming host that moves from its subnet to the neighbor's subnet.

Management service

Management service stores management information of roaming service. It also provides roaming servers access to the information.

3.3 Requirements of Roaming IP service

The procedures of roaming service from users' perspective are outlined in this section. One goal of Roaming IP is to provide ease of use to users. In a roaming host, protocols and tools that users are familiar with are re-used for the operations of Roaming IP. Users do not need to learn new software or new tools. After a service registration, Users will not notice differences between Roaming IP service and conventional IP service.

To gain access to roaming IP service, the minimum system requirements need to be met in the roaming host:

- A network interface card which supports the MAC protocol of the service access point. It can be wired or wireless.
- IP v4 protocol stack
- A web browser or a http capable scripts (for automatic operations)

Like other services, a user needs to get approval from the network administrator before accessing Roaming IP service. The procedure is called roaming service provisioning. The user applies for roaming service from the administrative authority of the network. After the application is approved, the administrator creates a new entry in the database of management service. User ID, password and service parameters are provisioned and given to users. It is assumed that service provision is finished for the following description.

3.3.1 Roaming service registration

Roaming service registration is the first step for Roaming IP service. After moving into a guest network, a roaming host attaches to the network via a new access point. The roaming host cannot communicate to Internet hosts. However, to set up roaming service, it's necessary for the roaming host to communicate with a registration server (i.e. a guest roaming server). In Roaming IP protocol, Roaming ARP is used to enable the communication. The following steps provide an outline of the operation of Roaming service registration:

- A roaming host moves away from its home network and attaches to a guest network.
- A web browser is launched in the roaming host. The browser reports error of home page not reachable. This is normal because the roaming service is not setup yet. The roaming host cannot connect to Internet hosts.

- The URL http://roamingip.local is typed in the web browser.
- A roaming service registration form is displayed in the web browser.
- User ID, password and service parameters are filled in the form and the form is submitted.
- If the registration is approved, a roaming service confirmation page is displayed in the web browser. If the registration fails, the reason is displayed.
- This is the end of registration.

Users can also initiate roaming IP registration in home networks. The procedure is the same as described previously. Roaming IP registration in the home network is used for setting up handoff service. After the service is set up, the mobile host can continuously communicate with other hosts when it roams out of home network to a guest network.

3.3.2 Roaming service access

After a service registration succeeds, a roaming host can communicate with other Internet hosts as if the roaming host is in its home network. The service is transparent to IP applications running in the roaming host. With full-mobile service, the roaming host has access to service without interruption when it roams between service coverage areas. For correspondent hosts (Internet hosts that talk to a roaming host), the service is also transparent. Correspondent hosts change neither the IP protocol nor their configurations. They communicate with roaming hosts in the same way regardless of the location of roaming hosts. The roaming service is also transparent to the current Internet infrastructure. There is no need to change routers or network configurations.

Roaming service is available until the service is de-registered.

3.3.3 Roaming service de-registration

If roaming service is no longer required, a roaming host de-registers the service. Roaming service can be de-registered explicitly or implicitly. When a roaming host registers for

service, the duration of the service is set. After the time expires, the service is automatically de-registered. The procedure for the explicit de-registration is outlined here:

- In a roaming host, the user launches a web browser to type in the URL http://roamingip.local
- The roaming service management form comes up in the browser.
- The user selects services de-registration and provides a User ID and password.
- The user submits the request.
- The roaming service is de-registered after the confirmation page is displayed in the web browser.

3.3.4 Handoff service

Handoff service maintains connections when a roaming host crosses boundaries of different sub networks. The operation of handoff service setup is embedded into the service registration process. To enable handoff service, the user needs to select handoff service in the registration form. The rest of operation is the same as normal service setup.

After handoff service is enabled, a roaming host maintains its communication sessions roaming across different subnets. The service is transparent to users. When the roaming host moves from guest network A to guest network B, the roaming server in network B will replace the one in network A to provide Roaming IP service to the roaming host. This handoff service requires no intervention from the user.

3.3.5 Automatic service registration

Previous sections describe manual service registration, which gives users full control of roaming services. If necessary, however these operations can be automated. Scripting languages can be used for the automation, such as Perl. [44] For example, a Perl script can be set up to run during the startup of a mobile host. The script emulates the manual

service registration. Roaming IP service becomes available after the mobile host finishes initialization.

3.4 Roaming IP protocol description

3.4.1 Roaming ARP protocol

In IP networking, packets are forwarded hop by hop until they reach the destination. Finding the correct next hop is critical for packet forwarding. For an end host, the next hop is normally the router of the local subnet. When a roaming host is in a guest network, it cannot use the same next hop (the router of its home network) to send out packets any more. A roaming server is the new next hop that will deliver packets for the roaming host. To achieve this, the next hop information needs to be updated in the roaming host. However, this update cannot be achieved by either changing configuration or the protocol stack in the mobile host because the transparency of Roaming IP needs to be maintained. Roaming ARP is a new idea to update the next hop information without introducing changes in a roaming host. With Roaming ARP, a roaming host attracts packets from roaming hosts to its network interface. Roaming ARP is also referred as roaming packet attraction. Roaming ARP is used in both roaming host detection and packet delivery service.

3.4.1.1 Conventional procedure for IP packet delivery

The conventional procedure of IP packet forwarding is described to facilitate the discussion of Roaming ARP. As shown in figure 6, RH1 is in its home subnet. The conventional IP protocol is used for its communication with other hosts. CH1 is in the same subnet as RH1. CH2 is a host connected to the Internet from a different subnet. RH1 communicates with both CH1 and CH2.

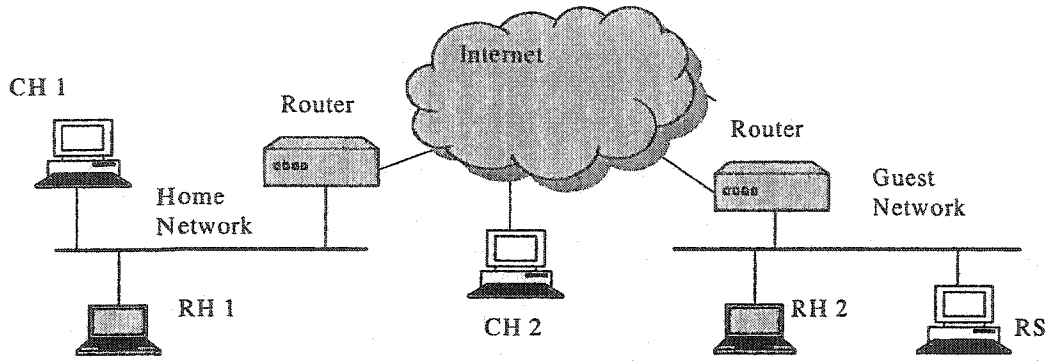


Figure 6 Roaming host detection

RH1 is assigned an IP address, a subnet mask as well as a default gateway. A default gateway is the host to which packets destined to hosts outside of the local subnet should be sent. The default gateway can be set to either the IP address of RH1 or the IP address of the router in the home network. If the default gateway is RH1, a proxy ARP[81] agent is required in the router.

In RH1, an application sends data to the IP stack with OSI layer-3 destination set to the IP address of CH1. The layer-3 address needs to be resolved to a layer-2 address. RH1 broadcasts an ARP request message, with target field set to the IP of CH1. In the home network, all hosts receive the ARP request. But only CH1 responds because its IP address matches the target field of the ARP request. Receiving the ARP reply, RH1 delivers the data packet to the layer-2 (MAC) address of CH1. The packet is successfully sent to CH1.

In the RH1, another application sends data to the IP stack with the layer-3 destination set to the IP address of CH2. The IP stack finds out that the destination IP is not in the local subnet and sends the packet to its default gateway. If the default gateway is RH1 itself, RH1 broadcasts an ARP request into the local subnet, with the target fields set to the IP address of CH2. A proxy ARP agent in the router replies to the ARP request with the MAC address of the router. If, on the other hand, the default gateway is the router, RH1 broadcasts an ARP request with the target fields set to the IP address of the router. The router replies with its own MAC address. In both cases, RH1 delivers the packet destined

to CH2 to the MAC address of the router. The router then forwards the packet to the Internet, which eventually reaches CH2.

3.4.1.2 Algorithm and message format for roaming ARP

In conventional IP packet forwarding, ARP is used to get the layer-2 (MAC) address of the next hop. ARP is the protocol that can be exploited to attract packets to roaming servers. The following defines the algorithm to attract packets from a roaming host in guest networks. In figure 6, a roaming host RH2 is in a guest network and the roaming server in the guest network is RS. RS has the IP address of RS_IP, subnet mask NET_MASK and MAC address RS_MAC.

- The roaming server listens to all ARP request messages in the subnet
- The roaming server retrieves the source IP address SRC_IP and destination IP address DST_IP from the ARP request
- If the source IP address belongs to the local subnet,

  SRC_IP AND NET_MASK == RS_IP AND NET_MASK

  the ARP request is ignored.
- Else If the destination IP address belongs to the local subnet,

  DST_IP AND NET_MASK == RS_IP AND NET_MASK

  the ARP request is ignored
- Else If the destination IP address is in the roaming host list, the ARP request is ignored.
- Else the RS generates an ARP response, the target MAC is filled with the RS_MAC (the layer 2 address of the RS).
- The roaming host delivers all IP packets to the MAC address of the roaming server until the ARP entry in the cache expires. After the ARP entry expires, the same steps repeat from the beginning.

Roaming ARP uses the same message format as the ARP[53] protocol to provide transparency. However the algorithm of roaming ARP is different from ARP. There is one roaming ARP agent running in every guest roaming server.

There are two messages defined for roaming ARP: query and reply. The message format is shown in figure 7. The format is similar for both query and reply messages except for the different Operation field, which is set to 1 for query message and 2 for reply message.

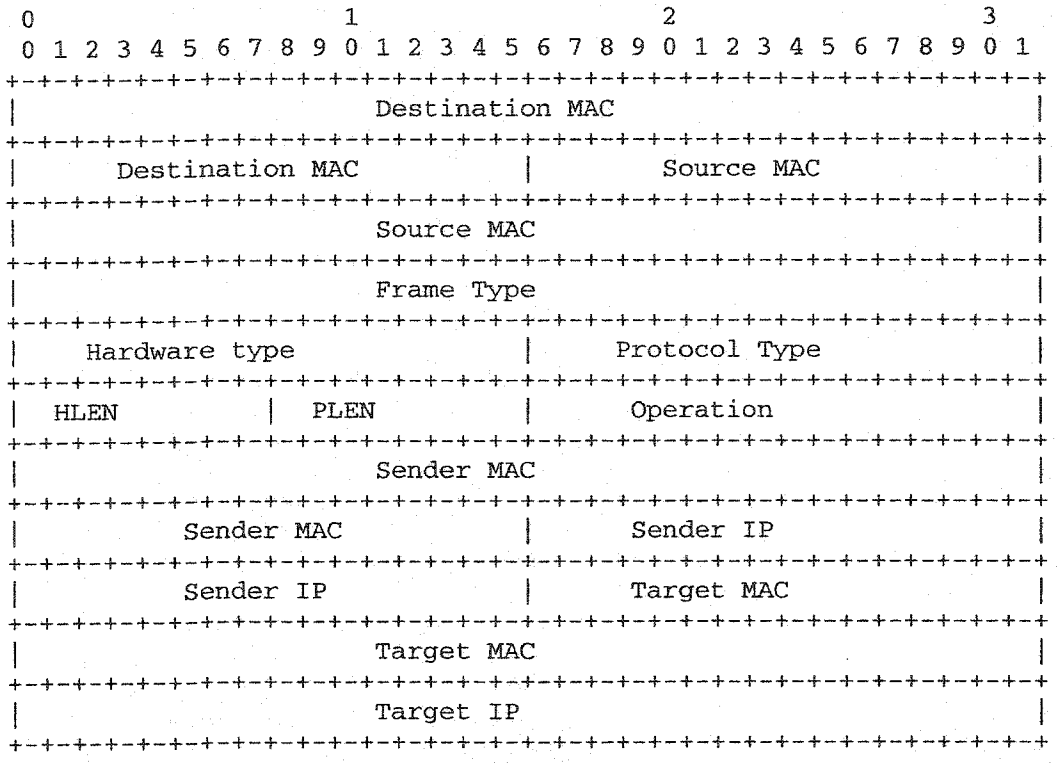


Figure 7 Roaming ARP message

3.4.1.3 Considerations of Roaming ARP

The impact of the proxy ARP agent that runs in the local router on the Roaming ARP is considered here. If the Proxy ARP function is turned on in the router, the router will respond to the ARP requests that have non-local destination IP address with its own MAC address. This function is to enable the local host to send packets to Internet without the router setting as the default gateway. This conventional response conflicts with the ARP response from the roaming server. The roaming host will be confused by the two conflicting ARP responses. This issue may be addressed by making the proxy ARP agent

more intelligent. The proxy ARP agent in the router should not respond to an ARP request with a source IP address that does not belong to the local subnet. This eliminates the conflict with the ARP response from the roaming server.

The effectiveness of the Roaming ARP algorithm with different roaming host configurations is discussed hereafter. In a roaming host, the default gateway can be set to either the roaming host itself or the router in its home network. If the default gateway is the router, the roaming host sends out an ARP request with the router's IP as the destination. The roaming server receives the ARP request and applies the defined algorithm. The result is positive and the roaming server responds to the ARP request with its own MAC address. The packets from the roaming host will now be attracted to the roaming server. If the default gateway is the roaming host itself, the destination and source IP still meet the criteria. They both are not in the local subnet. The roaming server responds to the ARP request. The result is that the roaming host will deliver all its packets to the roaming server.

From the previous discussion, it is concluded that Roaming ARP is effective for different default gateway configurations in the roaming host. In Chapter 8, the experiment result confirms this conclusion.

3.4.2 Local service name resolution protocol

In this section, a new protocol LSNRP is proposed for roaming hosts to find the roaming server. A roaming host may initiate a roaming service registration in both its home network and a guest network. In both cases, the roaming host needs to know either the domain name[11] or the IP address [73]of the registration server (i.e. the roaming server). In general, a domain name is more preferable than an IP address because it is easier to remember. When a roaming host is in its home network, it can talk to any other Internet hosts including domain name servers. Therefore a domain name can be used to identify the roaming server. However, this involves some management overhead here. For

example, the network administrator needs to publish domain names of roaming servers in all subnets and users need to remember the information.

When the roaming host is in a guest network, the challenge is greater because the roaming host does not have IP connection to Internet hosts before roaming service is set up. Without an IP connection, the roaming host cannot talk to its domain name server. So a regular domain name cannot be used to identify the roaming server. An IP address is not a satisfactory solution either since every roaming server has a unique IP address. The IP addresses of all roaming servers would need to be published and remembered and this is not manageable.

Local Service Name Resolution Protocol (LSNRP) is proposed to solve the problem. LSNRP eliminates the need for users to have any knowledge of the guest network (i.e. the domain name or IP address of the roaming server). The same local service name of roaming IP is used in all roaming subnets globally. That is to say, the user remembers and uses one name anywhere he/she visits.

Please be reminded that Roaming IP needs to provide complete transparency to the mobile host. Hence, no protocol change is allowed in the roaming host. LSNRP has to be built on existing TCP/IP protocols. The DNS protocol [11][12]is exploited in LSNRP. The DNS protocol is used to translate a domain name into an IP address. A domain name is used to identify an Internet host in a human friendly format. There is a DNS client in every host that has an IP v4 protocol stack.

To differentiate a LSNRP name from a DNS name, a new top domain name "local" is proposed for LSNRP. This domain is dedicated to name the host that provides a local service in a subnet. A local service is only available to the host in the local subnet. The same service name will be mapped into different IP addresses in different subnets. The same local service name is used globally. Users do not need to know the specific domain name or IP address of the host that provides the service any more. The local name resolution system will automatically translate the name into the IP address of the host that

provides the service. Roaming IP is the first local service defined. The name of roaming IP service is "roamingip.local".

3.4.2.1 LSNRP operations

From the client's point of view (i.e. the roaming host), the operation of LSNRP is the same as regular DNS. When a name resolution is required, the client generates a query message with the name. It sends the query message to a name server and waits for the reply. The name resolution succeeds if the client receives a reply before the timer expires. In the server side of LSNRP, the operation is different from regular DNS. Firstly the host that answers the query is different. The roaming server instead of the configured DNS server answers the query. Secondly, the method of address resolution is different. The name is mapped to the IP address of the local roaming server.

In the Internet, there are many DNS servers set up and these servers are organized into a hierarchical architecture. The servers at the lowest layer provide name service directly to clients. The IP address of a DNS server is provisioned in each Internet host. When a roaming host sends out a name query, it uses the configured IP address of the DNS server as the destination.

In Roaming IP, the DNS client can not expect a successful reply from a DNS server for the following reasons: a) the query message is sent out before the roaming service registration is done. Since the roaming host does not have IP connection to the DNS server if it is in a guest network, the query message will not reach the DNS server at all. b) If the roaming host is using LSNRP in its home network, the query message will reach the DNS server. However the DNS server does not have the knowledge to correctly map the local service name into a correct IP address because the local service name is not in the DNS system.

The LSNRP server running in the roaming server of the local subnet is tasked to answer the query. However, there is a problem that needs to be solved here. The query message is destined to the DNS server not the roaming server. The layer-3 addresses of the query

packet are set as follows: the destination is the DNS server IP address and the source is the RH IP address. In Roaming IP, a new idea is used to make the roaming server receive the query message. A roaming server monitors all DNS packets in the local subnet to identify and intercept LSNRP queries.

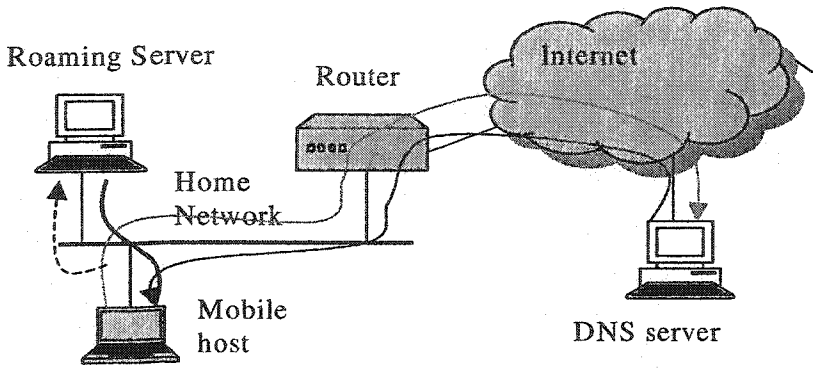


Figure 8 LSNRP in home network

3.4.2.1.1 Operations in home network

If the roaming host is in its home network (as in figure 8), the layer-2 target address of the query message is the MAC address of the router after an ARP operation. It is a uni-cast message at layer 2. The network interface of roaming server needs to be in the promiscuous mode, which is to say that it listens to all data packets in the local subnet to pick up the query message. When the roaming server captures a packet from the local subnet, the following algorithm is applied to decide whether it is a LSNRP query:

- If the packet is not an IP packet, drop it
- Else if the packet is not a UDP packet, drop it
- Else if the port number is not 53, drop it
- Else if the operation is not query, drop it
- Else if the name is not equal to "roamingip.local", drop it
- Else a LSNRP query is received.

After a LSNRP query is captured, the LSNRP server generates a reply message. In the reply message, the local service name "roamingip.local" is translated into the IP address of the roaming server. The reply message is sent to the roaming host. The time elapsed between the roaming host sending out query and receiving a LSNRP reply is T_{LSNRP}. To ensure that the roaming host accepts the reply, the message needs to appear to be from the DNS server. The following requirements must to be satisfied:

- The layer-3 source address of the reply message is set to the IP address of the DNS server even though the message is actually from the roaming server.
- The destination UDP port is set to the source port of the query message, the source port is set to 53.
- The fields inside UDP packet should follow the DNS rules.

3.4.2.1.2 Operations in guest network

If the roaming host is in a guest network (as shown in figure 9), the layer 2 destination address of the query packet is set to the MAC address the roaming server after a roaming ARP operation.

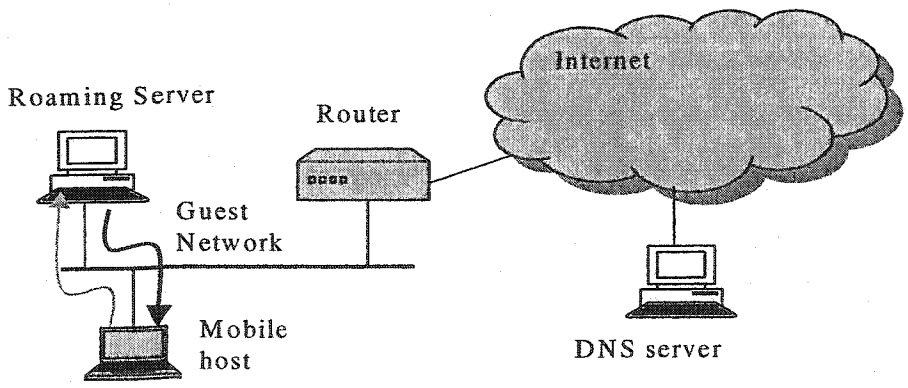


Figure 9 LSNRP in guest network

The roaming server only needs to monitor data packets delivered to its MAC address. After the roaming server captures a packet, the same algorithm is applied to identify a LSNRP query. The roaming server then generates a reply message and sends it to the roaming host.

3.4.2.2 LSNRP messages

Two messages are defined in local service name resolution protocol: LSNRP query and reply. The message format of these two messages is the same as their counterparts in DNS protocol. Otherwise the DNS client in a roaming host does not understand the messages without changes to the protocol stack. In DNS, a complex message format is defined to provide flexibility[12]. LSNRP query and response are two instantiations of the generic format. UDP messages are used for LSNRP query and reply. The UDP port of the server is 53. The message format of the query and reply (excluding UDP headers) are shown in figure 10 and 11.

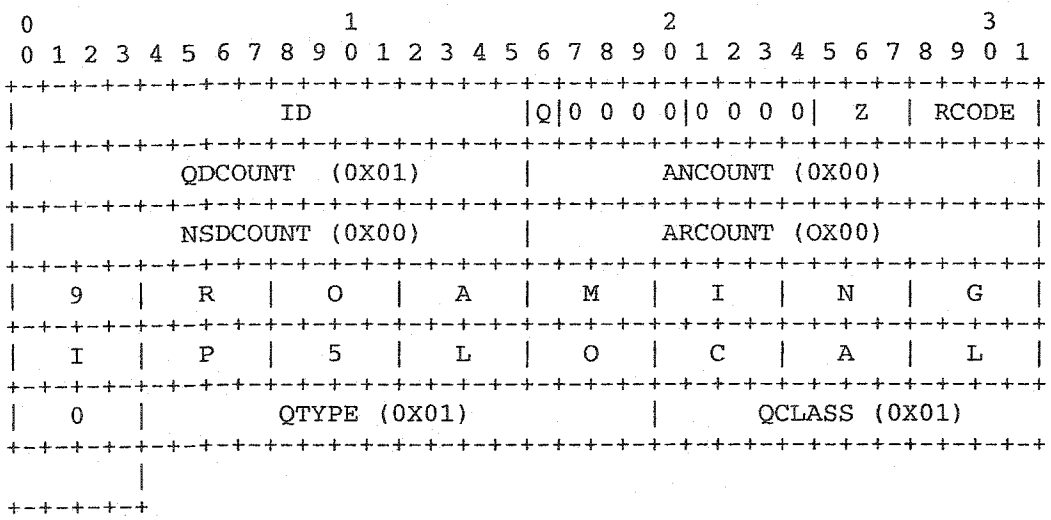
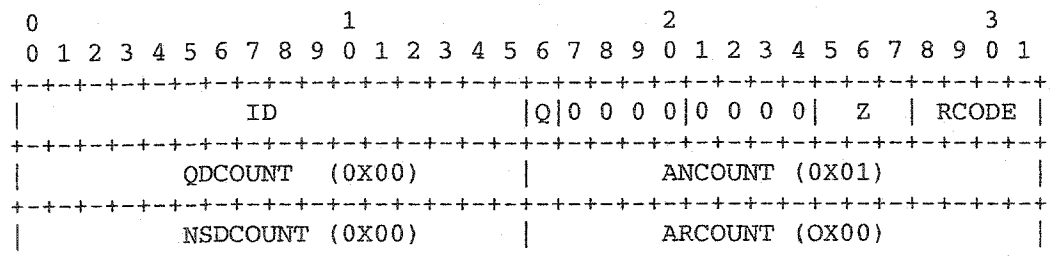


Figure 10 LSNRP query message

The first 12 octets is the message header. The ID is a 16 bit integer assigned by the program that generates the query. It is used to correlate a reply to a query. The Q bit is set to 0, which means a query message. There is one query because the question counter QDCOUNT is set to 1. Following the header is the question section. The question is "roamingip.local" in the message. For details of other fields, please refer to [12].



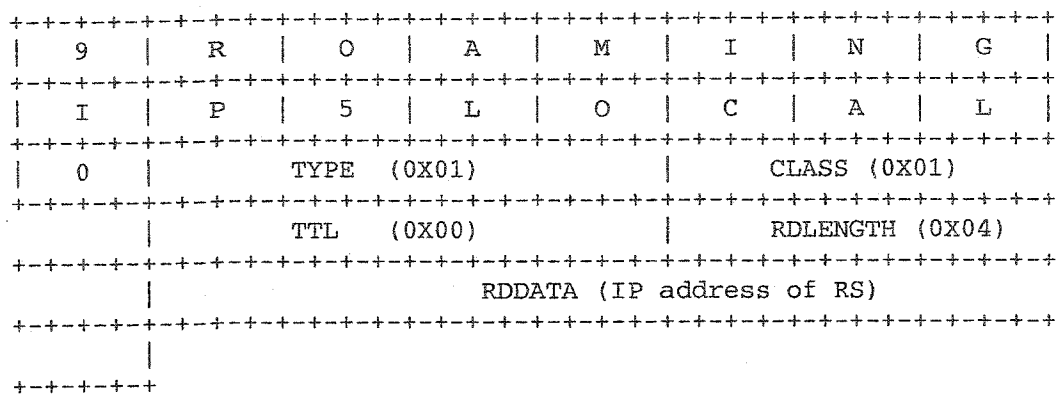


Figure 11 LSNRP reply message

In the reply message, the ID is copied from the one in the query message. The Q bit is set to 1. The return code RCODE is set to zero for a successful query. The question count is set to zero and the answer count ANCOUNT is set to 1 because this packet contains one answer. The answer section follows the header. The type of the answer is set to a host address (0X01). The class is set to the Internet (0X01). The TTL is set to 0 to indicate that the answer is only valid for this transaction. The RDDATA field contains the IP address of the roaming server.

3.4.2.3 Considerations of LSNRP

Even though the query packet is examined by the LSNRP server, it may still be delivered to the DNS server. When receiving the query, the DNS server starts a lookup for the domain name but fails to find the local service name in its database. The DNS server queries other servers at the upper layer of the DNS hierarchy until the root is reached. If no answer is found, it generates a negative reply to the sender of the query message (i.e. the roaming host). The message sequence chart of LSNRP is in figure 12:

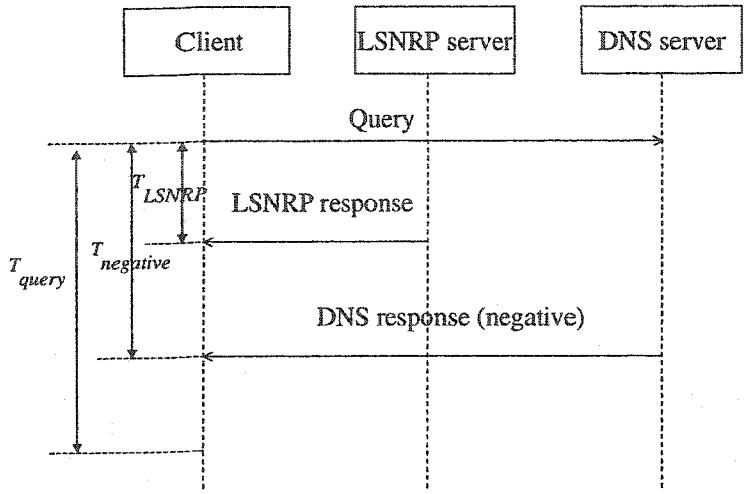


Figure 12 LSNRP message sequence

The time elapses between the roaming host sending out query message and seeing a negative reply as $T_{negative}$. After the roaming host receives the first reply, it will ignore any further message related to the query. To make a successful LSNRP query, the following must be satisfied:

$$T_{LSNRP} < T_{negative}$$

When this condition is satisfied, the LSNRP reply arrives earlier than the negative reply from the DNS server. The LSNRP reply is accepted while the DNS reply is discarded.

In the guest network, no IP communication session can be set up between the roaming host and the DNS server. So there is no need to worry about any negative reply from the DNS server.

When a DNS client sends out a query, it starts a timer T_{query}. If the timer expires before a reply is received, the client fails the query operation. Hence the second condition for a successful LSNRP query is:

$$T_{LSNRP} < T_{query}$$

The resolution of the name to an IP address is much simpler in LSNRP than in DNS. In the DNS system, a DNS server does a search in its database when receiving a name query. If no match is found, the server will escalate the query to the server in higher layer of the hierarchy. The same procedure repeats until a match is found or no match can be found at the root server. It is necessary to have such a distributed database because hundreds of millions of data entries exist. In LSNRP, a simple database is more than sufficient because the number of local services is very limited. As a matter of fact, roaming IP is the only local name defined to date. The operation of LSNRP is a lot faster than DNS. The delay of a LSNRP reply is smaller than a DNS reply. Therefore, LSNRP satisfies previously defined requirements. In chapter 8, experiment results confirm this.

3.4.3 Roaming host detection

Before providing service to a roaming host, a roaming server needs to know the existence of that roaming host. In Mobile IP, a roaming host is identified by a registration message that it sends to a foreign agent (roaming server). In roaming IP, since no new protocol is allowed in roaming hosts, a new idea is proposed for roaming host detection, which uses a message that is generated from existing protocols to identify the roaming host.

As described in section 3.3.1, the roaming host sends out data packets in a manual or automatic service registration. These packets are exploited for the roaming server to detect the roaming host. At the beginning of service registration, the roaming host tries to access the URL http://roamingip.local. "roamingip.local" is the local service name defined for Roaming IP. However, from the roaming host's perspective, it is a domain name. The roaming host sends a UDP message out to the network, which is a DNS query message to resolve the name "roamingip.local" to an IP address. The roaming server detects a roaming host by intercepting a DNS query message from the roaming host, which has "roamingip.local" in the query.

The roaming server monitors data packets in the local subnet. For each packet, the following algorithm is applied to detect a roaming host:

- If the packet is not an IP packet, drop it
- Else if the packet is not a UDP packet, drop it
- Else if the port number is not 53, drop it
- Else if the operation is not query, drop it
- Else if the name is not equal to "roamingip.local", drop it
- Else a roaming host is detected.

3.4.4 Roaming service registration process

3.4.4.1 Introduction

Roaming service registration is an important component of Roaming IP because it is the only component that directly interacts with end users. In Roaming IP, roaming registration is simple from a user's perspective. What needs to be done is to fill in a web-based application form, click the submit button and wait for the confirmation. All the complexity of roaming registration is hidden in the background. As pointed out in the section of operations of roaming service, a user ID and other parameters need to be configured by the network administration before roaming service registration is initiated.

In roaming service registration, the following is achieved:

- Validate the legitimacy of the registration request
- Obtain the service parameters for the roaming host, including the default values in the service directory and the values in the request.
- Set up home roaming server, guest roaming server and optionally roaming servers' handoff neighbors.
- Test the packet forwarding tunnels between roaming servers.

Roaming service registration is the most complicated operation of Roaming IP. The following components of the Roaming IP system are involved: roaming host, home

roaming server, guest roaming server, directory server and optionally all roaming servers' handoff neighbors.

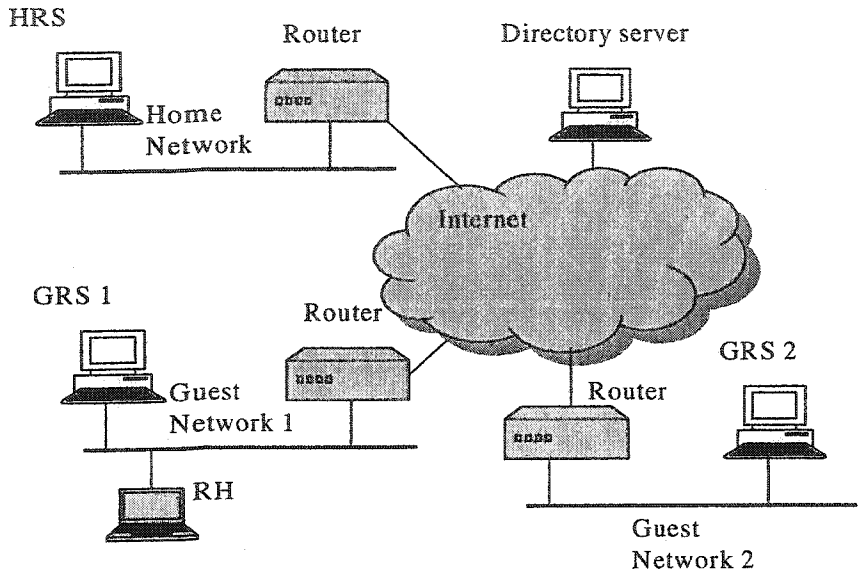


Figure 13 Roaming service registration

As shown in figure 13, the roaming host RH visits guest network 1. In guest network 1, GRS1 is the guest roaming server. In its home network, HRS is the home roaming server. RH may roam directly from guest network 1 to 2. The roaming server in guest network 2 GRS2 is a handoff neighbor of GRS1 because a handoff operation may happen between them. The user initiates the roaming registration from RH. The registration procedure is composed of the following phases:

- Phase I: Information gathering for roaming service. The roaming host and guest roaming server are involved.
- Phase II: Service validation. GRS1 and the directory server are involved.
- Phase III: Basic service setup. GRS1 and HRS are involved.
- Optionally, phase IV: Handoff service setup. GRS1, GRS2 and other handoff neighbors are involved.
- Phase V: Roaming service confirmation. The guest roaming server sends registration result back to the roaming host.

3.4.4.2 Web-based management architecture

The information like user ID and password needs to be provided for service registration. To maintain transparency to the roaming host, no new software is brought into the roaming host. Rather, a web-based management architecture is proposed for Roaming IP because a web browser is available in every computing node connected to the Internet.

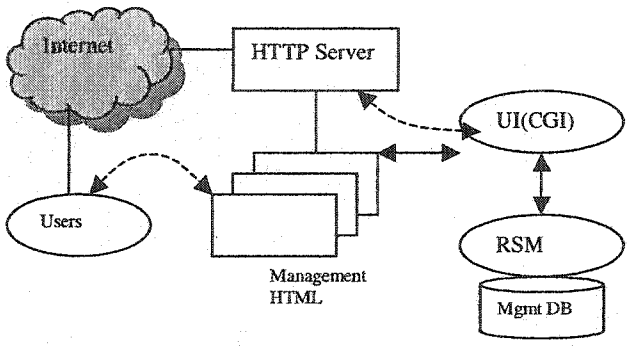


Figure 14 Web-based management architecture for roaming IP

The key components of the web-based management architecture are shown in figure 14: the HTTP server, the management HTML, the UI, the backend program RSM (Roaming Service Management) and users. The UI is a CGI[45] program. Its execution is triggered by the HTTP server when the user accesses a CGI-enabled URL. The UI has two major functions: generates management HTML (i.e. the registration form); retrieves information from the management form submitted by users and passes the information to the backend program RSM for further processing. The RSM updates the management database in the roaming server to enable roaming services. The HTTP server, management HTML, UI and backend program are all in the roaming server.

3.4.4.3 Operations of roaming service registration

3.4.4.3.1 Phase I of registration

In phase I, the roaming host finds the roaming server and obtains the service registration form. The form is filled in by the user and submitted to the roaming server. The following is defined in Roaming IP to facilitate the operations: Roaming ARP, LSNRP and the web-based management architecture. Roaming ARP is used to attract packets to the roaming server. LSNRP is used to resolve the roaming IP service name to the IP address

of the roaming server. The web-based management architecture provides a flexible user interface.

The detailed steps of phase I are:

- GRS1 attracts IP packets from RH
- RH obtains IP address of GRS1 via LSNRP
- RH sends HTTP request to obtain the registration form
- The HTTP server triggers the UI to generate a web page (in HTML) of the registration form.
- RH receives the form from the HTTP server.
- The user fills in and submits the form.
- The HTTP server receives the form and invokes the second part of the UI program.
- The UI retrieves information from the form and passes it to the backend management program.

The information in the registration form is:

- IP address of the roaming host.
- MAC address of the roaming host.
- User ID
- Password
- Service type. The user can choose full-mobile and semi-mobile services.
- Effective time of the roaming service
- Handoff service enabled/disabled

3.4.4.3.2 Phase II of registration

In phase II, the roaming server checks the legitimacy of a roaming registration request and queries the necessary information for setting up the roaming service. Both operations rely on the management information service that is discussed in chapter 5. At the end of

phase I, the UI program passes gathered information to the backend program: RSM (refer to section 3.4.4.2). The RSM program takes the following steps:

- Converts all registration information to internal format
- Creates a new entry in the roaming host list and set the state to new
- Generates a query message with the user ID and password
- Sends the query message to the directory server (refer to section 5.2) that provides management information service
- If the entry is not valid in the directory, a negative response is sent back. The RSM sends negative response to the UI and the roaming host entry is deleted.
- Else a positive response is sent back. The RSM moves the state of the roaming host entry to "authenticated"
- The RSM generates another query message with the roaming host IP as the key.
- Sends the query to the directory server.
- Retrieves the query result and puts it into the roaming service database

In the result of the second query, the home roaming server IP address is provided. The information is used to set up a communication between the guest and home roaming server for the next phase of the registration.

3.4.4.3.3 Phase III of registration

In phase III, the GRS and the HRS set up packet delivery service for the roaming host. The GRS communicates with the HRS via the RS-RS protocol for the service setup. The detailed steps of phase 3 are:

- The GRS sends a roaming host add request to the HRS
- The HRS receives the request and checks the away host counter
- If the counter is equal to or greater than the maximum, the HRS sends a negative response to the GRS with an error of "too many away hosts".
- Else the HRS increases the away host counter by one.

- The HRS creates a new entry in the away host list and set the state to new.
- The HRS does a Roaming ping (refer to section 3.4.5) to the roaming host
- If there is a response, the HRS sends negative response back to the GRS with an error of "RH at home".
- Else the HRS starts a proxy ARP service for the roaming host
- The HRS sets up an end point of the IP tunnel (refer to section 3.4.7) for the roaming host.
- The HRS sets the state of the away host entry to active
- The HRS sends a positive add response to the GRS
- The GRS starts a roaming ARP service for the roaming host
- The GRS sets up the other end point of the IP tunnel for the roaming host.
- The GRS sets the state of the roaming host entry to active

After phase III, the basic roaming service is set up. The roaming host can send and receive IP packets as if it were in its home network. However the service is maintained only in the guest subnet. Phase IV is required if the handoff service is required across different subnets.

3.4.4.3.4 Phase IV of registration

In phase IV, the GRS communicates with its handoff neighbors to prepare handoff service for the roaming host. Handoff neighbors are the roaming servers in the subnets that have a common border with the local subnet. A roaming host is able to roam directly to a handoff neighbor's subnet. The GRS signals all handoff neighbors to set up handoff service with the RS-RS protocol. The detailed steps of phase IV are:

- The GRS retrieves the list of handoff neighbors from the Roaming management service.
- The GRS sends a roaming host monitor request to each handoff neighbor

- Each handoff neighbor receives the request and checks the counter of neighbor host entries
- If the counter is equal to or greater than the maximum number, the neighbor RS sends a negative response with and error of "too many neighbor hosts"
- Else the handoff neighbor increases the counter of neighbor host entries by one
- The handoff neighbor adds the roaming host that is in the monitor request message into its neighbor host list
- The handoff neighbor sends a positive response to the GRS
- The GRS waits for responses from all handoff neighbors
- If the GRS receives all responses or the timer expires, the RSM sends a response back to the UI with a summary of the results of the handoff procedure

3.4.4.4 Phase V of registration

In phase V, the UI running in the GRS generates a confirmation web page for the registration. The page is sent back to the roaming host by the HTTP server and displayed to the user. The content of the confirmation page is based on the result from previous phases. The registration can fail at any phase. If a critical failure (e.g. the home roaming server is not available) happens, the registration jumps directly to phase V. The cause of the failure is put into the confirmation page. The information is helpful for users to understand the problem and identify a solution. If it is a non-critical failure (e.g. one handoff neighbor fails to respond), the registration will proceed. The partial failure information will be provided to the user in the confirmation page to take necessary actions. For example, the user avoids roaming into the subnet whose roaming server fails to respond.

One important consideration of phase V is to avoid the timeout of the web browser. The registration may take substantial amount of time if there is a failure in the network. The registration time is noted as $T_{registration}$. In the roaming host, a timer $T_{browser}$ is kicked off

when the user submits the registration form. The $T_{browser}$ timer is to guard the time that the web browser will wait for a response back from the HTTP server. If

$$T_{registration} > T_{browser}$$

The browser timer expires before the confirmation page is sent back. The browser deems it a failure of communicating with the HTTP server. The browser closes the session and displays an error of HTTP server not reachable. The HTTP server will not be able to send back the confirmation page even if the service registration succeeds. To address the issue, the UI program needs to generate a progress report web page periodically. The cycle of the page generation is $T_{progress}$. It must satisfy:

$$T_{progress} < T_{browser}$$

With the progress report, it is possible to keep the HTTP session alive and provide progress information to the user.

3.4.5 Roaming ping protocol

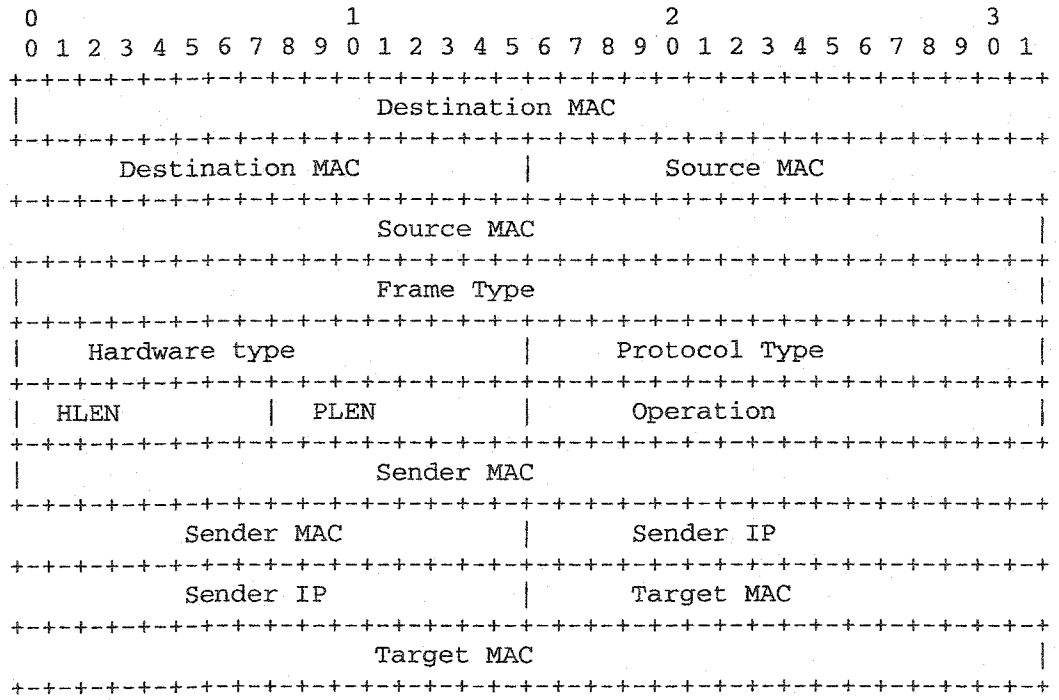
In this section, a new protocol (Roaming ping protocol) is defined for locating roaming hosts. In Mobile IP, a mobile host reports its location via a registration message. In Roaming IP, no new message can be introduced in a roaming host to identify itself because of the transparency requirement. Instead, the Roaming ping that runs in a roaming server is defined to locate a roaming host.

After a successful registration, the roaming server in a guest network has the layer 2 (MAC) address of the roaming host. All handoff neighbors also have this knowledge. In a guest network, if a roaming host is sending out data packets, a roaming server sees the packets and locates the roaming host. When the roaming host roams to a neighboring subnet, the handoff neighbor sees the packets and locates the roaming host. If the roaming is not sending any packets, it is invisible to roaming servers. The Roaming ping protocol is defined to force a roaming host send out packets to expose its location.

Existing TCP/IP messages supported in the roaming host are used for the Roaming ping. The following options are considered: a layer-4 message UDP[42] or TCP, a layer-3 message like ICMP [7]or a layer-2 messages like ARP [6]. To trigger the roaming host to send out a TCP or UDP message, an application is required to listen to the port. It responds to messages delivered to the port. However, it is not expected that all roaming hosts have the same application running. Hence a layer-4 message is not a viable option. In Layer 3, ICMP is supported in every IP node, making ICMP messages a possible solution. In layer 2, ARP is mandatory for every IP node to resolve an IP address to a MAC address. In Roaming IP, ARP messages are adopted for the Roaming ping for the following reasons:

- It's guaranteed that the roaming host replies to ARP message. It is not uncommon to turn off ICMP for security reasons. For example, avoiding malicious attack.
- The overhead of ARP is smaller. ARP resides in layer 2 of the protocol stack. The logic of ARP is simple, which means less CPU consumption.
- The delay of ARP is smaller. This helps the RS to locate the roaming host faster.

There are two messages defined for Roaming ping: request and reply. They have the same format as ARP request and reply as shown in figure 15. However the way to interpret the message is different.



```
|                          Target IP                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 15 Roaming ping message

The operations of Roaming ping are:

- The roaming server sends a Roaming ping request to the roaming host. The IP address of the roaming host is filled in the field of Target IP.
- The roaming host receives the Roaming ping request message. The roaming host processes the message as an ARP request message. It generates an ARP response message. It fills the Target MAC field with its own MAC address. The message is sent to the roaming server.
- If the roaming server receives a response before the timer expires, and the response is from the roaming host itself, the Roaming ping succeeds. To verify the identity of the RH, the roaming server checks the source MAC address in the Ethernet header of the reply message. If

  Source MAC == MAC of roaming IP

  Then the ping succeeds.
- Else the Roaming ping fails.

There are some important difference between the Roaming ping and the ARP. Firstly, an ARP request uses the broadcast address in its layer-2 message header. All local hosts receive the ARP request message. While a Roaming ping request uses uni-cast layer-2 address (the MAC address of the roaming host). Only the roaming host receives the message. This prevents an unnecessary load on the rest of hosts in the subnet. Secondly, in an ARP response, the information in the ARP message fields is used. The querying node does not care about the sender of the response. But in Roaming ping, the source MAC address in the Ethernet header is used to determine that the reply is from the roaming host itself. The information in ARP message fields is ignored.

The timer for Roaming ping T_{rp} is set to the same as the timer for an ARP request T_{arp}.

$$T_{rp} = T_{arp}$$

The guest roaming server uses Roaming ping to monitor roaming hosts. If a roaming host is not alive in the guest network after some time (configurable during roaming service registration), the roaming service will be de-registered to free up resources in both the home and guest roaming servers. In roaming servers, there is a timer T_a assigned for each roaming host registered. If the timer expires, the roaming server sends out 3 final Roaming ping messages to the roaming host. If the roaming host replies to the pings, the timer is reset to zero. If the roaming host fails to reply three times, the roaming host is deemed unavailable in the network and the roaming service is de-registered. Allocated resources are then released in all roaming servers.

The Roaming ping message is also used for a roaming host search operation. If a roaming host is granted roaming service with handoff service, it is possible to roam into a new guest subnet, quietly. Without knowing the new location of the roaming host, all data packets are still delivered to the previous subnet. But the GRS there cannot find the roaming host in its subnet any more. The GRS asks all its handoff neighbors to search for the roaming host. The handoff neighbors send out Roaming pings to the roaming host in their own subnets. If a response is received, the roaming host is found. The roaming service will be transferred to the new subnet.

The home roaming server also uses Roaming ping to ensure a roaming host is not in the home network during a roaming service registration.

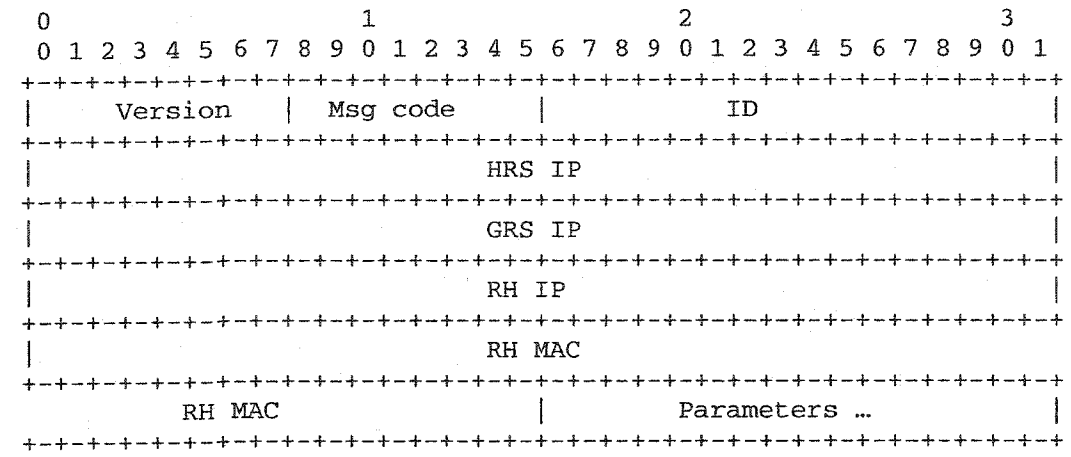
3.4.6 RS-RS protocol

To provide roaming IP service, roaming servers need to communicate with each other. The Roaming Server to Roaming Server (RS-RS) protocol is defined for transactions between roaming servers. The RS-RS protocol is built on top of TCP. TCP port 2000 is proposed for the RS-RS protocol and all roaming servers listen to that port.

In the RS-RS protocol, the following messages have been defined:

- Roaming host add request and response
- Roaming host delete request and response
- Roaming host handoff request and response
- Roaming host update request and response
- Roaming host monitor request and response
- Roaming host search request and response
- Roaming host report request and response

The message format of RS-RS protocol (excluding the TCP header) is:



Where:

Version — A 8-bit integer for the version of the protocol. It is set to 1.

Msg code — A 8-bit field specifying the type of the message. It is set by the originator.

1	RH add request
2	RH add response
3	RH delete request
4	RH delete response
5	RH handoff request
6	RH handoff response
7	RH update request
8	RH update response
9	RH monitor request
10	RH monitor response
11	RH search request
12	RH search response

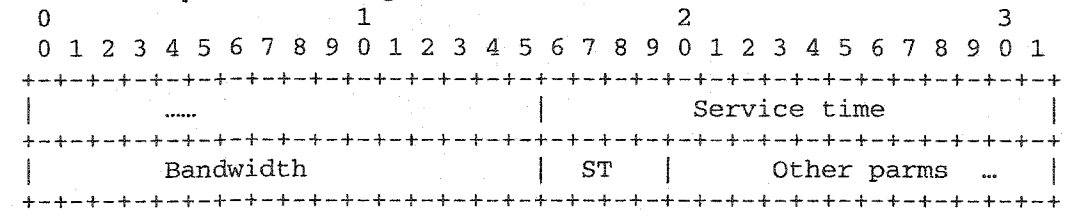
13	RH report request
14	RH report response

ID	A 16-bit identifier assigned by the application that generates the request. This identifier is copied into the corresponding response. The requester uses the identifier to match the response with the query.
HRS IP	The IP address of the home roaming server
GRS IP	The IP address of the guest roaming server
RH IP	The IP address of the roaming host
RH MAC	The MAC address of the roaming host
Parameters	These are specific parameters for different messages. The length and meaning of the parameters are dependent on the message type.

3.4.6.1 RH add request and response

These two messages are used to add a new roaming host in its home RS during service registration. When a GRS decides to grant roaming service to a roaming host, it sends a RH add request to the HRS. If the HRS agrees to accept the roaming host, it sends back a RH add response with a positive return code. Otherwise the request is rejected with a negative response. The messages are depicted in the following figures. The first 22 octets of the message are omitted because they are depicted in the previous figure.

RH add request message



Where:

Service time	A 32-bit field. It is the total service time requested for the roaming service. The unit is seconds.
Bandwidth	A 32-bit field that represents the desired bandwidth for the roaming host. The unit is bits per second.

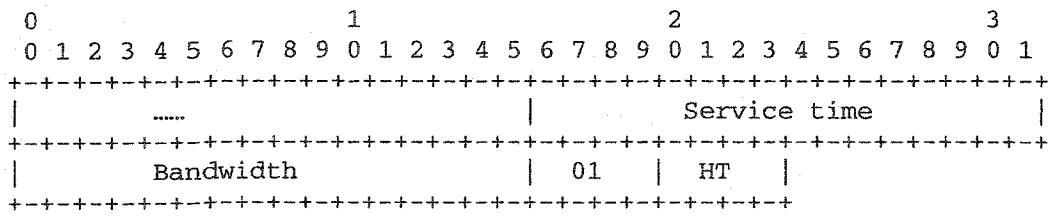
ST — A 4-bit field that represents the service type of the roaming request. The current defined values are

1 Full-mobile

2 Semi-mobile

Other parms — Parameters that are dependent on the service type.

When ST = 1, the message becomes



Where,

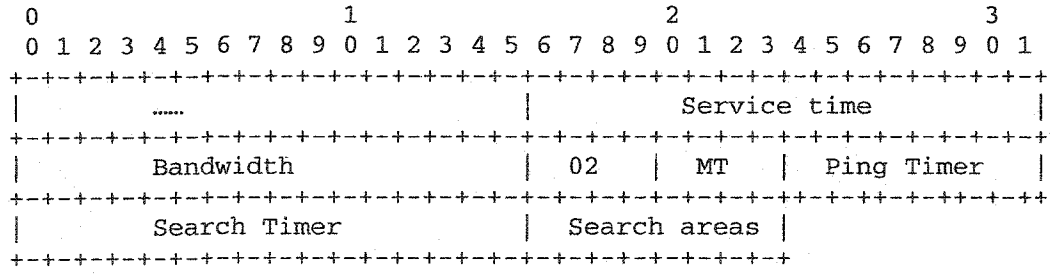
HT — A 4-bit field that represents the type of handoff.

1 No handoff

2 Handoff with fast movement detection

3 Handoff with both fast and low movement detection

When ST = 2, the message becomes



Where,

MT — A 4-bit field represents the type of migration service

1 No migration service

2 Migration without searching

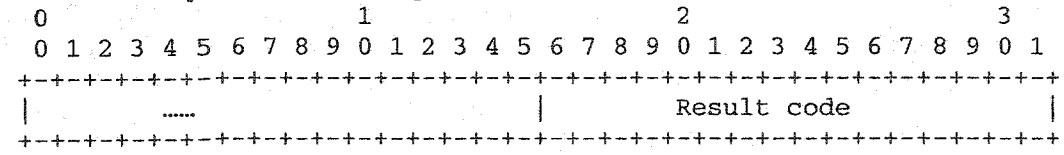
3 Migration with searching

Ping Timer — An 8-bit time interval before the roaming server sends out ARP ping to the roaming host.

Search Timer — A 16-bit time interval before the roaming host is deemed dead or out of service coverage. The roaming service will be deregistered to release network resource when the search timer expires.

Search Area — An 8-bit index to the list of areas where the roaming host may visit. The list resides in the directory server. It is set up during service configuration.

RH add response message



Where,

Result code — A 16-bit code that represents the result of the add request.

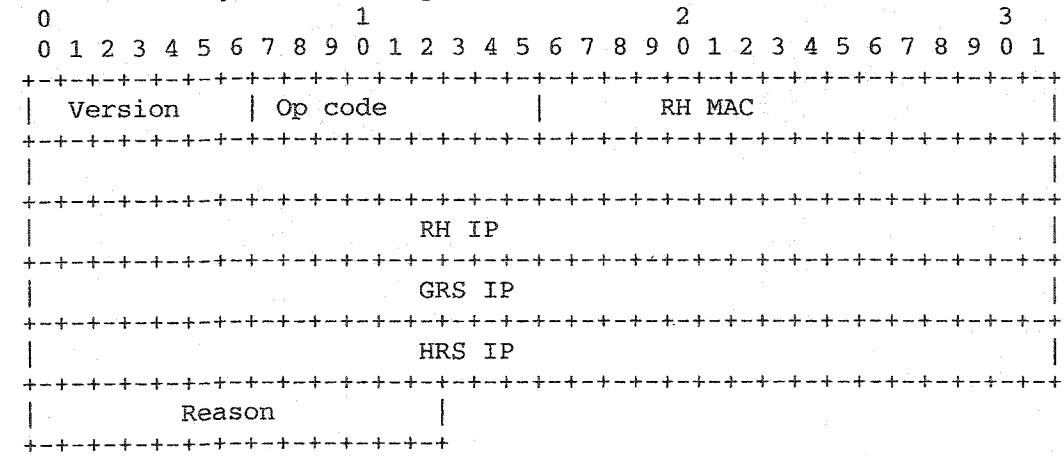
0 successful

1 failed

3.4.6.2 RH delete request and response

These two messages are used for signaling the remote end to remove a RH from the roaming host list. These messages are used for service de-registration. RH delete request can be initiated by both HRS and GRS.

RH delete request message

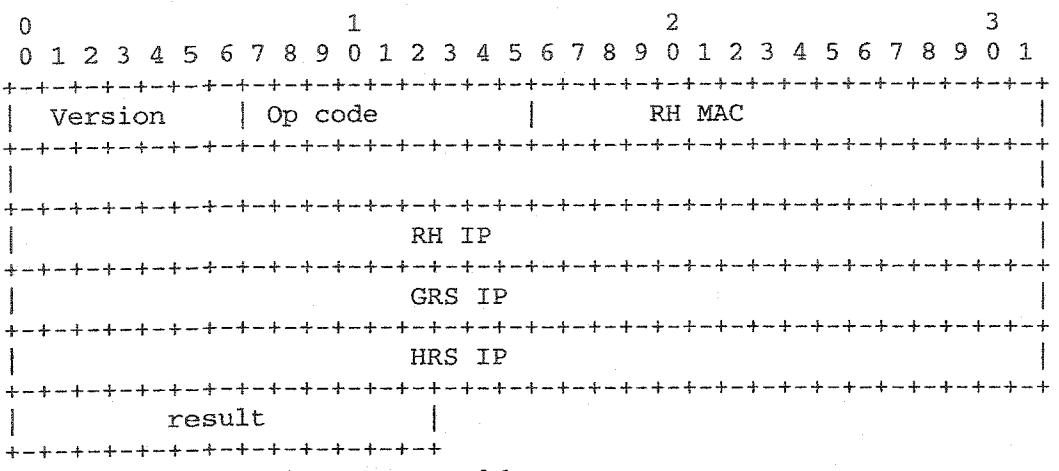


The reason code is: 0 User request

1 Timeout

2 Handoff

RH delete response message

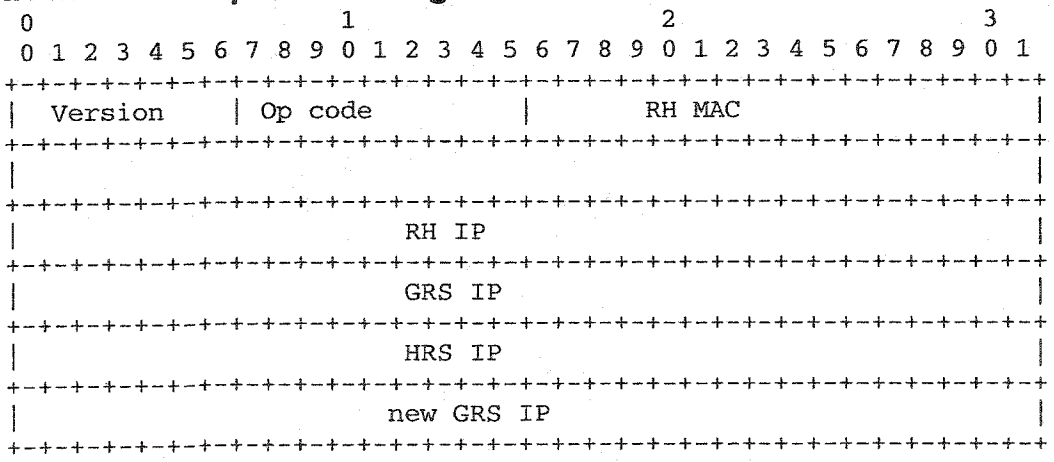


The result code is: 0 successful
1 failed

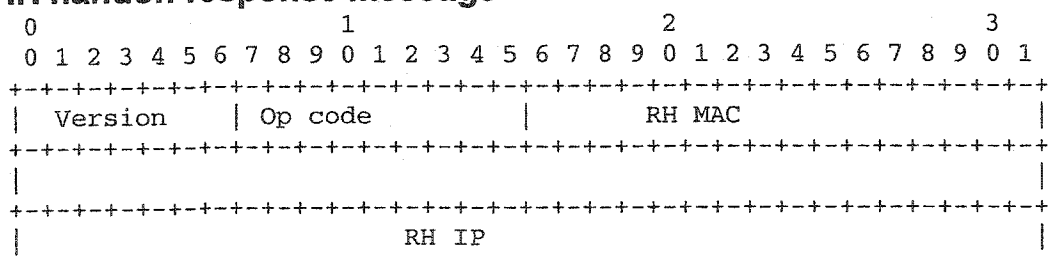
3.4.6.3 RH handoff request and response

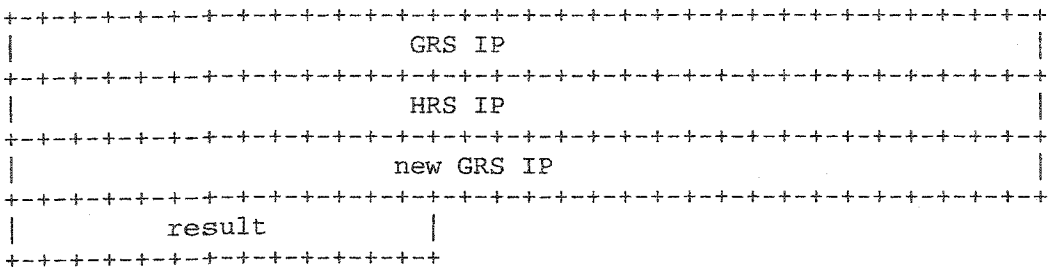
These two messages are used for signaling a handoff service. When a roaming host moves from service area 1 to service area 2, the GRS in area 2 detects the roaming host. GRS 2 uses handoff request message to signal the GRS 1 to forward data packets to the new area for the roaming host.

RH handoff request message



RH handoff response message



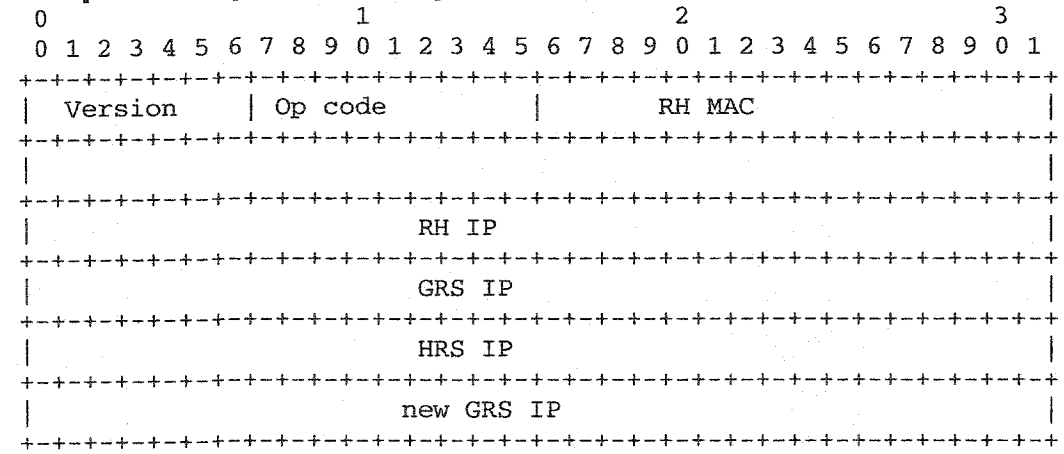


The result code is: 0 successful
1 failed

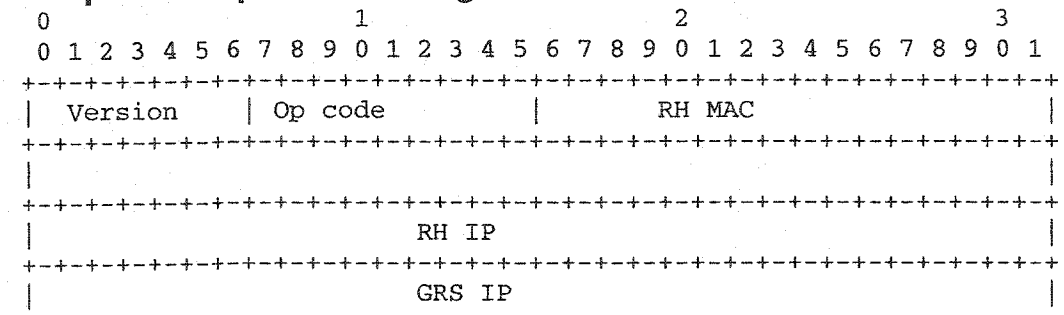
3.4.6.4 RH update request and response

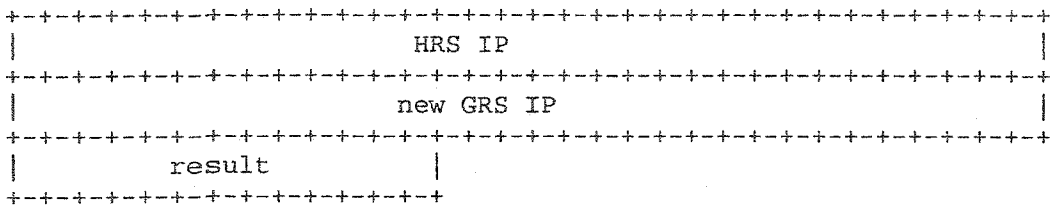
These two messages are used to signal a handoff service. When the roaming host moves from service area 1 to service area 2, the GRS in area 2 detects the roaming host. After the GRS in area 2 successfully signals the GRS in area 1 to redirect packets to area 2, it uses a RH update request message to request that the HRS transfers the service to the new area. If the operation is successful, the HRS replies with a response message with the successful result code.

RH update request message



RH update response message



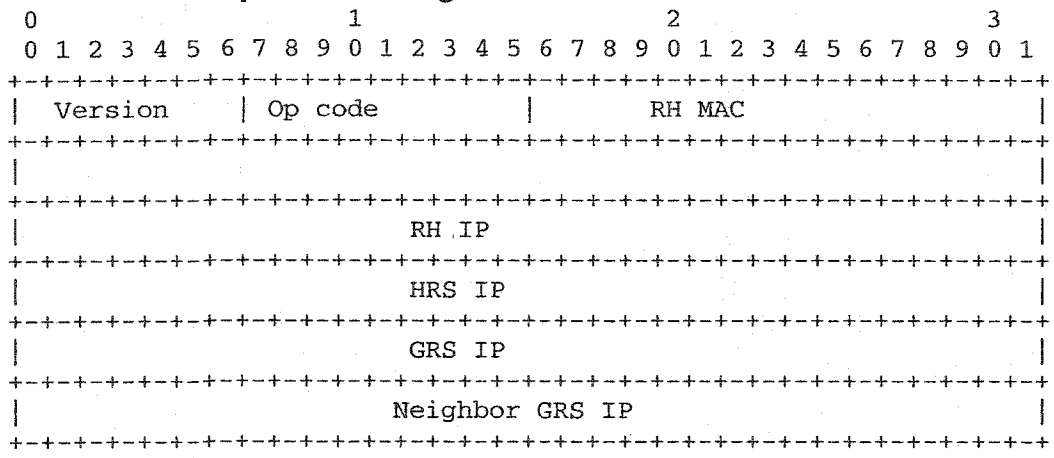


The result code is: 0 successful
1 failed

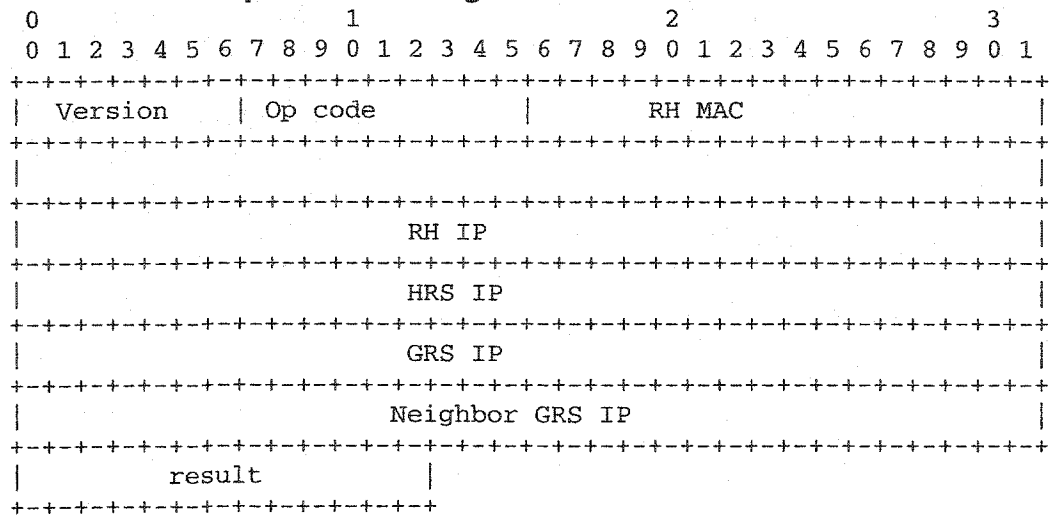
3.4.6.5 RH monitor request and response

These two messages are used to set up a handoff service for the roaming host. The GRS signals all handoff neighbors to add a roaming host into their neighbor host lists with the monitor request message and the handoff neighbors reply with the response message.

RH monitor request message



RH monitor response message



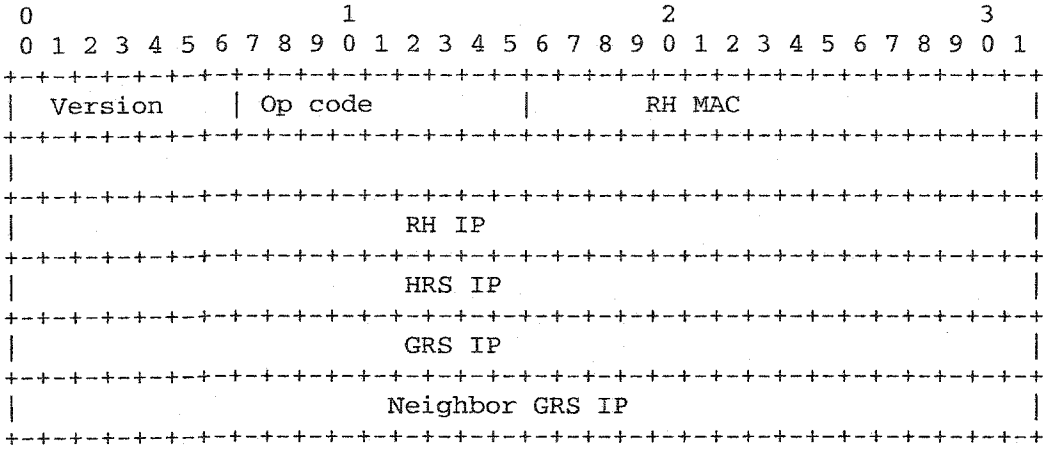
The result code is:

0	successful
1	Too many neighbor hosts

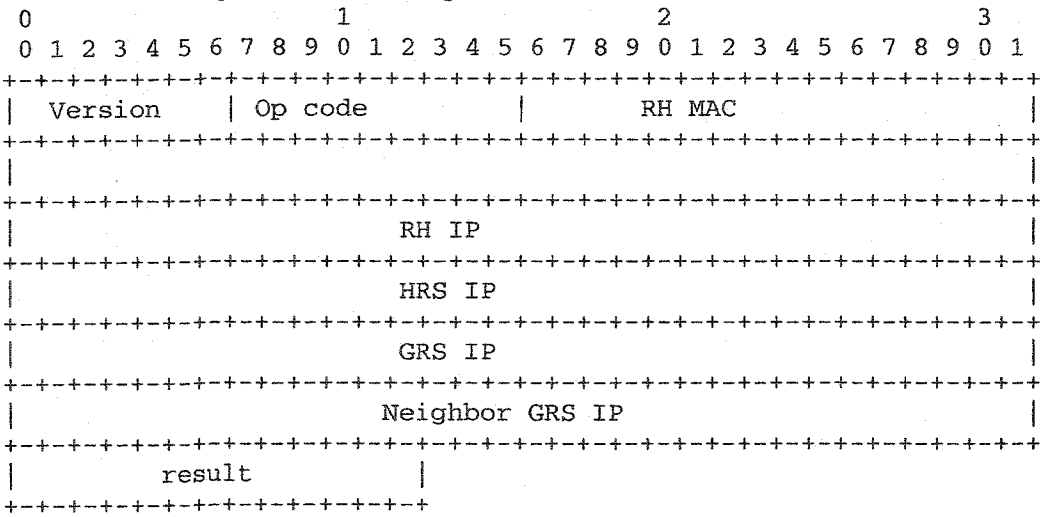
3.4.6.6 RH search request and response

These two messages are used to locate a roaming host. If a roaming host moves into a new area without sending packets, the GRS in the new area is unable to detect it and the RH is isolated from the network. To minimize the service interruption, the GRS in the original area keeps track of the RH by sending out Roaming ping messages. If a roaming host fails the Roaming ping, the GRS sends RH search request messages to signal all handoff neighbors to look for the RH. If the roaming host is found, the neighbor RS sends a positive response to the GRS. Otherwise, a negative response is sent.

RH search request message



RH search response message



The result code is: 0 Roaming host found
1 Roaming host not found

3.4.7 Roaming packet delivery

3.4.7.1 Packet delivery mechanism

As demonstrated in earlier sections, regular IP packet delivery does not work when a roaming host keeps the same IP address in a guest network (see figure 16). The packet delivery paths of both receiving and sending directions are broken. The roaming host needs support from other nodes in the network to receive and send packets from/to the Internet.

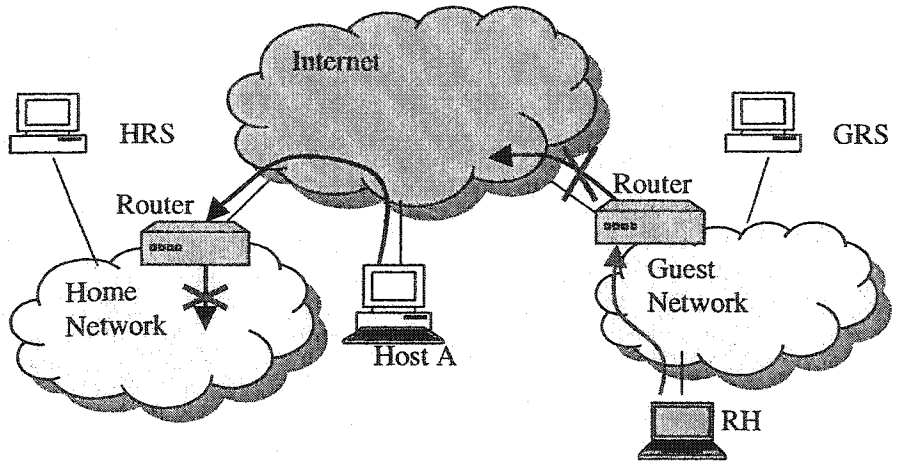


Figure 16 IP V4 packet delivery

In Roaming IP, a new mechanism is proposed to enable packet delivery. Roaming servers in the guest and home networks must support this new mechanism for packet delivery (see figure 17). In the guest network, the guest roaming server uses roaming ARP to attract all packets from roaming hosts. Due to the operation of roaming ARP, Roaming hosts send all IP packets to the MAC address of the guest roaming server. The guest roaming server tunnels the packets to the home roaming server. The home roaming server de-tunnels and sends the packets to the Internet. In the home network, the home roaming server uses proxy ARP to attract all packets destined to the roaming host. The home roaming server tunnels all the packets to the guest roaming server that is the access point for the roaming host. The guest roaming server de-tunnels the packets and sends them to

the roaming host. With this mechanism, the roaming host can both send and receive packets.

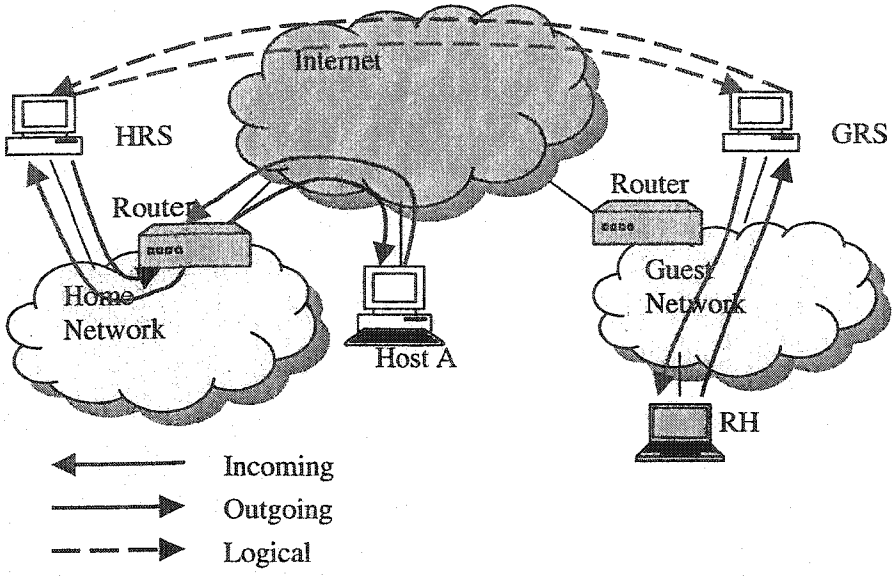


Figure 17 Packet delivery in Roaming IP

This mechanism of packet delivery for Roaming IP is fully compatible with the current IP v4 architecture while providing the necessary functionalities for Roaming IP. Though this mechanism is similar to the one used in Mobile IP, some significant differences exist. For example, the gateway that is used and the method to select the gateway for a roaming host are different. In roaming IP, the roaming server is the gateway. While in Mobile IP, both the foreign agent (roaming server) and the router in the guest network could be the gateway. In Mobile IP a new algorithm is introduced in the roaming host to select the correct gateway in a new location. While in Roaming IP, to maintain the transparency, roaming ARP is used to force the roaming host into using the roaming server as the gateway.

3.4.7.2 Protocol for packet delivery

After attracting packets, roaming servers need to tunnel the packets to their remote peers. The existing IP infrastructure is used to transport attracted packets between roaming servers. It is known that packets cannot be delivered in their original form. The original IP destination needs to be hidden from routers in the delivery path. The IP tunnels

provide such functionality. There are currently several options for tunneling: IP-IP encapsulation[24], Generic Router Encapsulation (GRE)[46][47], Minimal encapsulation[25] and MPLS[48][49].

GRE provides a generic framework to support protocol encapsulations. It provides functionalities to support different encapsulations like SNA over IP, OSI over IP or vice versa. GRE is quite complicated to implement and has a significant overhead due to its generic design.

Minimal encapsulation modifies the original IP header and inserts a minimal forwarding header. The destination IP address is changed to the ending node of the tunnel. The packet is then delivered to the ending node of the tunnel via regular IP packet forwarding. The end node restores the packet to its original form and sends it to the final destination. The overhead of minimal encapsulation is small. However it cannot be used when an original IP data packet is already fragmented since there is no room in the minimal forwarding header to store the fragmentation information.

The MPLS protocol is introduced to provide Quality of Service (QoS) to IP networks. With MPLS, all routers along the packet delivery path reserve necessary resources. The throughput and delay of the traffic is therefore guaranteed. MPLS paths can be setup between roaming servers to delivery packets for roaming hosts. The drawbacks of MPLS are its complexity and that it is not supported in many routers in the Internet.

IP-IP encapsulation provides a simple tunneling solution by encapsulating the original IP packet in the payload of the new packet. When the encapsulating node receives an IP data packet, it inserts an outer IP header before the packet's existing IP header as depicted in figure 18:

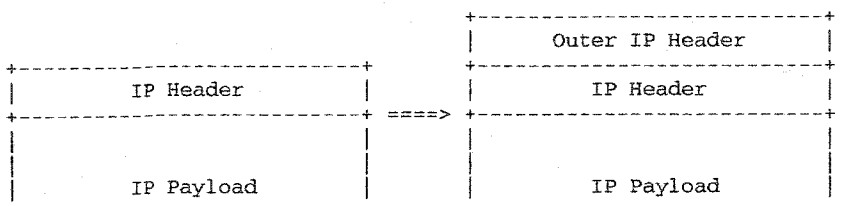


Figure 18 IP-IP encapsulation

The source address in the outer IP header is set to the starting node of the tunnel. The destination address is set to the ending node of the tunnel. The encapsulated packet is delivered to the ending node through the IP network as a normal packet. The end node of the tunnel strips the outer header after receiving the packet and delivers the packet to the final destination.

In the Roaming IP solution, IP-IP encapsulation is used for the tunnel between roaming servers. After attracting packets, guest and home roaming servers use the same algorithm to tunnel packets. Since the communication is bi-directional, roaming servers serve as both starting and ending node of tunnels. The algorithm of packet delivery is:

- A roaming server listens to IP data packets delivered to its layer 2 address (MAC address)
- If the destination IP address is the roaming server
    - If the protocol type is not IP-IP, let the normal IP stack handle the packet
    - Else strips the outer IP header and recovers the original IP packet
    - If the destination in the original IP header is in the away host list, send the packet to the final destination.
    - Else if the destination in original IP headers in the neighbor host list, tunnel the packet to the next roaming server.
    - Else drop the packet
- Else If the source IP address is in the roaming host, decrease the TTL value in the original IP header by one
    - If the TTL <= 0,
        - Drop the packet,

- An ICMP "Time exceeded" message is generated and sent to the source
- Else
  - Retrieves the HRS IP address from the roaming host entry.
  - Insert an outer IP header before the original IP header. The source IP is set to the GRS, the destination IP is set to the HRS.
  - Send the new data packet to the network.

– Else drop the packet

3.4.7.3 Considerations of packet delivery

Even though a principle objective is to provide best effort service with the current version of roaming IP, it is still helpful to keep track of the bandwidth requirements of the packet delivery service. The capabilities of packet delivery subsystem are decided by two factors: the packet handling capability of the roaming server and the capability of the tunnel between roaming servers. The Internet currently provides only best effort service. Without an end-to-end quality of service infrastructure, the bandwidth of the tunnel between roaming servers can not be guaranteed. In roaming servers, allocations of packet handling capacity are recorded for two reasons: Firstly it guarantees that the roaming server capacity is not the bottleneck, i.e. potentially a degraded service to customers may only be caused by the tunnel. Secondly it facilitates future extensions to the Roaming IP protocol. After a QoS infrastructure is available in the Internet, Roaming IP can be upgraded to provide QoS.

The unit of packet delivery capacity for a roaming server is bps, the same as for bandwidth. The network interface, CPU, memory and the architecture of the roaming server decide the capacity, which should be measured through testing. When a roaming host successfully registers for service, the home and guest roaming servers allocate a specific packet handling capacity for it. The roaming servers keep track of total capacity allocated. If there is not enough capacity left, roaming servers fail a service registration. The failure will be logged in the roaming server. The failure information is also sent back to the end user through the registration confirmation web page.

Another important factor to consider for packet delivery is the MTU (Maximum Transmit Unit) of the tunnel. In the Internet, different link layer technologies are used to connect Internet hosts together. Each link layer technology has its own MTU. For example, the MTU for Ethernet is 1500 bytes. When the size of an IP message is bigger than the MTU, it is fragmented into smaller pieces that are smaller or equal to the MTU. The fragmented packet is re-assembled in the destination. Fragmentation of IP packets introduces extra overhead to the network and decreases the efficiency of the packet delivery. In packet delivery of Roaming IP, roaming servers need to know the MTU of the tunnel. A MTU discovery solution is proposed in [50]. Roaming servers will implement such an algorithm. Roaming servers should run MTU discovery as soon as service registration succeeds. If the result from MTU discovery is MTU_{path}, then the MTU of the tunnel is

$$MTU_{tunnel} = MTU_{path} - 20$$

Because the outer header introduced by IP-IP is 20 bytes long.

For the roaming host, the most important performance data of the packet delivery service is the delay and the throughput. A packet delivery delay is expected due to extra hops introduced in the end to end route. The throughput of packet delivery service is decided by the capabilities of the roaming servers and the tunnel. In section 7.3, both the delay and throughput are measured for the Roaming IP implementation. The packet delivery service of the tested system provides a satisfactory performance.

3.4.7.4 Fault handling in packet delivery

It's very important to handle fault scenarios for packet delivery because proper notifications help user to identify root causes of faults. In traditional IP networking, ICMP[7] is used for this purpose. When a failure is detected along the path, an ICMP message is generated by the entity that detects the failure and sent it back to the node that originated the data packets. The originating node takes appropriate action based on the feedback embedded in the ICMP message. A similar mechanism is needed for the Roaming IP solution.

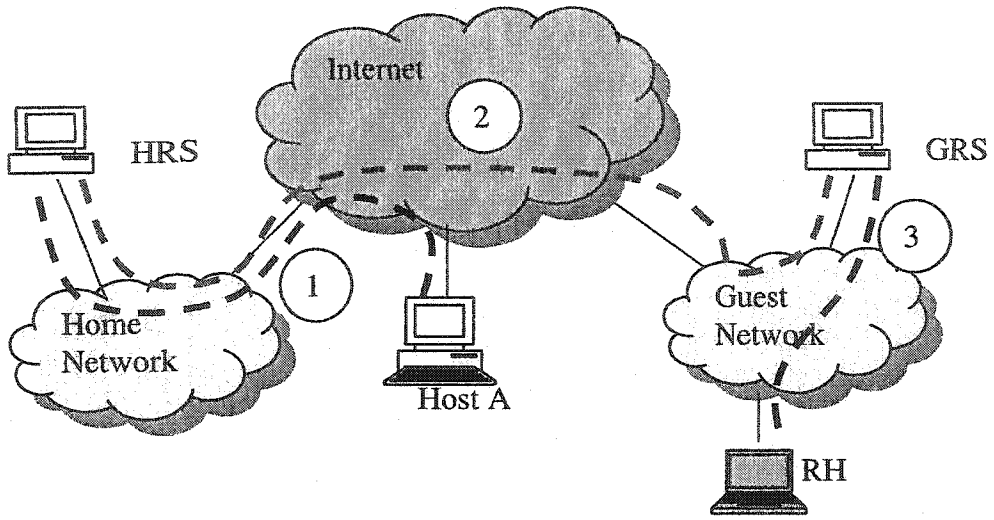


Figure 19 Packet delivery paths in Roaming IP

In figure 19, an end-to-end path from a correspondent host A to a roaming host is shown. The path is composed of three sections: A to HRS, HRS to GRS and GRS to the RH. For the first section, data packets are delivered in their original format. Regular IP packet forwarding and traditional ICMP-based failure handling is applied.

For the second section, between HRS and GRS, data packets are delivered in an IP-IP tunnel. In this section, special considerations should be given to failure handling. When a failure occurs in the IP-IP tunnel, an ICMP message is generated. But this ICMP message is destined to the RS instead of the originator (the RH or host A). The RS should interpret the ICMP message and relay information back to the originators.

To simplify the description, one direction of the packet delivery is discussed here, from host A to the RH. The fault handling of the reverse direction is the same. When a delivery failure happens in the tunnel, different types of ICMP messages are generated for different failure scenarios. Only a subset of the ICMP messages needs to be relayed back to the originator. The subset is discussed here:

- Destination Unreachable (type 3)

  This message is further divided into different types:

- Network unreachable/host unreachable/protocol unreachable (code 0-2)

  All these messages mean data packets cannot be delivered to the GRS through the tunnel. So the original destination (i.e. the RH) is not reachable. The HRS needs to generate a Host unreachable (type 3, code 1) ICMP message and send to host A.
- Datagram too big (code 4)

  This means the non-fragmentation bit is set in the IP header but the media along the path can't handle the size of the PDU. The HRS should generate a datagram too big ICMP message (type3, code 4) and send to host A

- Source Quench (Type)

  This message indicates the tunnel is congested. The originator needs to slow down sending. The GRS should generate a Source Quench message to the original source host A.
- Time exceeded (Type 11)

  This message means a routing problem inside the tunnel. The destination GRS is not reachable. So the original destination RH is not reachable either. The GRS should generate a destination unreachable message to the original source host A.

For other ICMP messages, the HRS should handle them locally according to the ICMP protocol. No information needs to be relayed back to the originator.

In the ICMP message generated in the tunnel, 28 bytes of the tunneled IP message are included as specified by the ICMP protocol. The outer IP header occupies the first 20 bytes leaving only 8 bytes for the original IP header. The source and destination addresses are located at the thirteenth to twentieth bytes of the original IP header. This means that the source and destination of the original IP packet are not included in the ICMP message. Without the knowledge of the IP address of the originator, no ICMP message can be relayed to the originator. In "IP Encapsulation within IP"[24], a solution is proposed to maintain a soft state for each tunnel, which is changed according to the ICMP message received. Based on the soft state, the encapsulater (starting node of the tunnel) generates appropriate ICMP message when subsequent IP packets arrive. There

are two disadvantages of this approach: it is expensive to maintain soft states; the congestion of the tunnel cannot be handled properly because ICMP Source Quench cannot be correctly represented by the soft-state.

In the Roaming IP proposal, a new scheme is proposed to address the ICMP message relaying for the roaming server. In the roaming server, there is information to determine what node an ICMP message should be relayed to. The roaming server maintains a list of users of each tunnel. The list is updated in the service registration/de-registration process. When an ICMP message is received from the tunnel, the information is relayed to all roaming hosts that use the tunnel. Even though only one roaming host's packet triggers the generation of the ICMP message, the information embedded in the ICMP message is applicable to all hosts that use the tunnel. Therefore it is appropriate to relay the ICMP message to all hosts that use that tunnel. With this scheme, the tunnel failure information can be correctly relayed to the source without maintaining a soft state of the tunnel.

In the third section of the path of packet delivery, the GRS retrieves data packets from the IP-IP tunnel. Then it uses the traditional IP packet forwarding to deliver packets to the RH. If the RH does not accept the packet, the GRS should do the following:

- If Handoff service is not enabled for the RH,
    - the GRS drops all packets
    - The GRS generates an ICMP message "Destination un-reachable"
    - Sends the ICMP message to the originator (i.e. host A) through IP-IP tunnel.
- Else
    - The GRS starts to buffers all data packets locally
    - The GRS starts RH search operation
    - If local buffer is full before the RH is found, the GRS generates an ICMP message "Destination un-reachable" and sends it back to the originator (i.e. host A) through the IP-IP tunnel. Also all buffered packets are discarded.

Chapter 4 Handoff service

4.1 Introduction

With the Roaming IP solution, a roaming host can move into different service areas (subnets). Correct packet forwarding is required after the roaming host moves into a new service area. For full-mobile services, it is required to maintain the communication session when and after a mobile host roams across the boundary of service areas. In the roaming IP proposal, handoff service is defined to provide continuous roaming service during and after a transition from a subnet to another. As mentioned in the beginning of chapter 3, Roaming IP deals with layer 3 (network layer) handoff.

The handoff service of roaming IP enables a roaming host (with semi-mobile service) to roam among different service areas without re-registration while having network connection everywhere. The handoff service enables a roaming host (with full-mobile service) to continuously to communicate with other hosts while roaming between RS access points. When a roaming host moves into a new service area, the roaming server in the new area provides the service. All packets destined to a roaming host are redirected to the new roaming server and then delivered to the destination. The goal of handoff service is to minimize interruption to this networking service. There are two key steps in the procedure of a handoff: movement detection of the roaming host and switch of roaming service from the original server to the new one.

4.2 Roaming host movement detection

Movement detection is the first step of a successful handoff. Different options of movement detection are explored for Roaming IP. The movement detection of Mobile IP is examined first, followed by the proposals for Roaming IP.

4.2.1 Movement detection in Mobile IP

In IETF-MIP, the architecture relies on the mobile host to report its location. The mobile host is responsible for detecting its movement. In a wireless network, when a mobile host roams across the boundary of service areas, a link layer handoff is triggered first. The base station in the new service area provides a point-to-point link to the mobile host. But the mobile host cannot decide whether the link layer handoff should trigger a network layer handoff because link layer handoff does not necessarily mean the mobile host enters a new subnet (service area). Layer-2 handoff also happens when the roaming host moves between different base stations in the same subnet (area). MIP has to rely on other methods to detect movement.

In MIP, a mobile host decides its location by applying a movement detection algorithm against the periodic Agent Advertisement Messages that it receives. Two algorithms are proposed in [23] Lazy Cell Switching (LCS) and Pattern Matching (PM). The third Eager Cell Switching (ECS) is proposed in [55]. The movement detection delays of three algorithms are T_{lcs} , T_{pm} and T_{ecs} respectively. In "Performance Analysis of Mobile IP handoff"[31], the author provides the mean of those delays. The interval of agent advertisement message is X.

$$T_{lcs} = 2.5X$$
$$T_{pm} = 2.5X$$
$$T_{ecs} = 0.5X$$

In MIP, X is recommended to 1 second. The theoretic delays for LCS, PM and ECS are 2.5, 2.5 and 0.5 second respectively. The detection delay has adverse impact to the handoff performance.

There are a few proposals to improve the movement detection. In "Performance Analysis of TCP/UDP during mobile IP handoff"[77], the authors propose that the mobile host sends agent solicitation message after every link layer handoff. The delay to wait for regular agent advertisement message is eliminated. The authors show the improvement by simulation result. The limitation of the proposal is the overhead introduced.

Bandwidth is required for both solicitation and advertisement message even when an intra-subnet layer-two handoff happens. The mobile IP stack needs to be informed about every layer-two handoff. The foreign agent may be overloaded by the solicitation messages. In "An Efficient TCP Mechanism for Mobile IP Handoffs'[35], the authors propose an early movement detection in the TCP layer by evaluating the arrival of packets. When a movement is deemed to happen, the mobile host sends an agent solicitation message. It eliminates the waiting time for a regular agent advertisement message. This proposal requires changes in the TCP layer, which is not preferable.

4.2.2 Movement detection of Roaming IP

As illustrated, the mobile host is responsible for detecting the movement in MIP. Due to the condition that a RH cannot be modified, Roaming IP employs a different approach. In Roaming IP, Roaming servers are responsible for movement detection. Roaming servers are fixed in the network and have the knowledge of their location. When receiving a packet from the roaming host, the roaming server can conclude that the roaming host is in its subnet. Hence the location of the roaming host is identified. With this approach, the transparency of Roaming IP to the mobile host is maintained. No new software is required in the mobile host to do movement detection. In Roaming IP, handoff service is provided for both semi-mobile and full-mobile services. The movement detections of semi and full-mobile hosts are different because of the different characteristic of the movement. They are discussed separately in the following sections.

4.2.2.1 Movement detection of full-mobile host

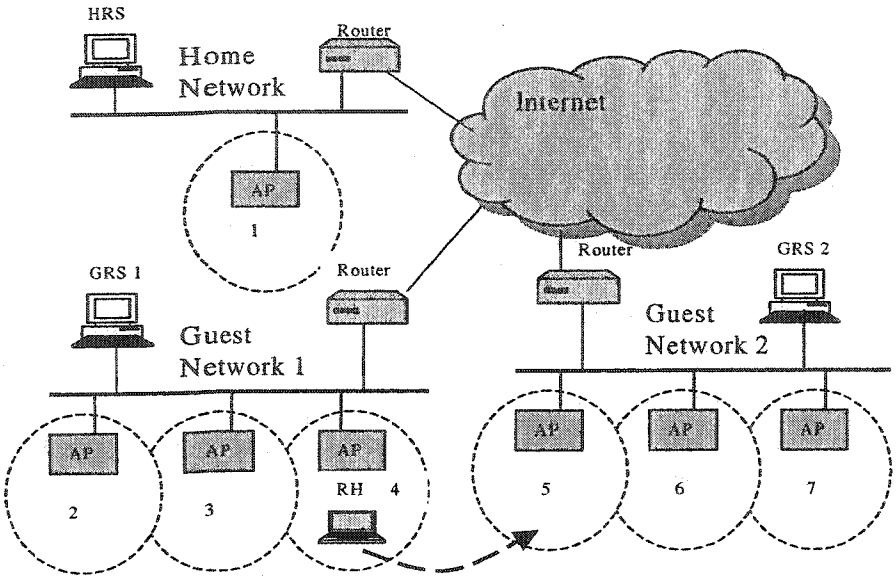


Figure 20 The Movement of a full-mobile host

A roaming host with full-mobile service can maintain communication session while roaming anywhere of the service coverage area. When the roaming host migrates into a new subnet, it needs to connect to the network via a new access point. A layer-2 handoff occurs, which switches the network connection to the new access point. The detail of layer-2 handoff is outside the scope of this thesis. After a layer-2 handoff, the roaming host connects to the network via the new access point. As shown in figure 20, AP5 is the base station that provides the link layer connection for the roaming host in the new subnet. After AP5 detects the roaming host, it reports to the roaming server GRS2 in the subnet. The layer-2 address (MAC) of the roaming host is included in the report. The roaming server uses the reported information to detect the movement of a roaming host. The roaming server uses the following algorithm:

- Retrieve the MAC address of the reported host
- If the MAC address is in the neighbor list, a roaming host is detected. Start a handoff for the roaming host.
- Else the reported host is not a roaming host that requires handoff, do nothing

When the roaming host moves within the same subnet, it can also trigger layer 2 handoffs. For example, the roaming host moves from the coverage of AP5 to AP6. Such layer-2 handoffs will not trigger a layer-3 handoff. They should not be reported to the roaming server. To eliminate unnecessary report messages, only base stations that are located at the border of different subnets send layer-2 notifications to the roaming server. Because base stations are part of the fixed infrastructure, the location information is static, which can be pre-configured by the operator. The algorithm for the base station is:

- Monitor new hosts
- If a host joins, note its layer-2 (MAC) addresses
- If the base station is at the border of a subnet, generate a layer-2 handoff notification and sends it to the roaming server
- Else do nothing

After identifying potential candidates through layer-2 handoff, some more information is necessary to decide an inter-subnet movement of the roaming host. The neighbor list is sufficient to make a conclusive decision. Every roaming server that provides handoff service has a neighbor list. The hosts in the monitor list of a roaming server are able to migrate from a neighboring subnet to the roaming server's subnet. The roaming server builds the neighbor list during roaming service registration. In phase IV of roaming registration, the guest roaming server informs all its handoff neighbors to put the roaming host into their neighbor list.

4.2.2.2 Movement detection of semi-mobile host

A semi-mobile host does not have any network activity during the move. It closes its communication sessions before it moves. It may not go through a layer-2 handoff when it crosses the boundary of different service areas. After reaching the new location and regaining physical connection to the network, it may keep silent for a while. If the network can detect the existence of the roaming host even if it does not have layer-3 network activity (i.e. sending or receiving IP packets), similar movement detection described in previous section may be used. For example, in an IEEE802.11 wireless

LAN, the base station detects the existence of a roaming host after a layer 2 handoff. If the network does not see the roaming host when it is silent, new schemes must be proposed. For example, the roaming server cannot detect a roaming host that is plugged into the Ethernet switch in the new subnet. Three types of movement detection are proposed for semi-mobile hosts: active reporting, passive monitoring and active searching.

Active reporting is very similar to the movement detection of full-mobile hosts. It is used when the network access point has the capability to detect the roaming host and report it to the roaming server. The roaming server searches the MAC address of the reported host in its neighbor list. If the MAC address is found, the host is a handoff host that makes an inter-subnet movement.

Passive monitoring relies on the roaming servers. It does not have dependency on the capability of the network access points. It is as fast as active reporting if the roaming host starts to send packets right after moving into new subnet. With passive monitoring, all roaming servers passively listen to packets in the subnet. The roaming server compares the source MAC address against the neighbor list. If a match is found, a handoff host is detected.

If both active reporting and passive monitoring are not valid, the active searching is used. There are two types of active searching. The difference is how the searching is triggered. The first type of active searching is started by the roaming host monitor function. After roaming service is set up, the guest roaming server keeps track of the roaming host with Roaming ping message. If a roaming host fails to response to Roaming ping three times, it's deemed out of the service area. A searching will be started by the roaming server. The second type of search is started by the packet delivery function. If the packet delivery function fails to deliver packets to the roaming host, it starts a search. The roaming server initiates a roaming host search operation by sending out search requests to handoff neighbors. All handoff neighbors (roaming servers) send out Roaming ping to the roaming host in their own service area. If the roaming host is in one of the area, it replies

to the Roaming ping. The roaming host is detected by the roaming server that receives the reply.

4.3 Service switchover

The second phase of a handoff is service switchover. After a roaming host moves into a new subnet (service area), packet delivery is still required for both directions (incoming and outgoing). When it roams into the new subnet, the roaming host experiences a link layer handoff and its layer-2 connection to the network is provided by the access point in the new subnet. Following that, the layer-3 service packet delivery is switched to the new roaming server. One objective of Roaming IP is to provide a fast and smooth switchover that has minimum service disruption.

4.3.1 Switchover for outgoing traffic

The solution to continue the packet delivery service in outgoing direction is examined first. After moving into the new subnet, if the ARP cache is flushed by the layer-2 handoff, the roaming host sends out an ARP request to find the MAC address of the next hop. The roaming server replies to the ARP request with its own MAC address. All outgoing packets are delivered to the roaming server. If the ARP cache stays, the roaming host uses the MAC address of the old next hop (i.e. the roaming server in the previous subnet) to deliver outgoing packets. The roaming server in the new subnet is able to receive all packets because it listens to the layer-2 addresses of its handoff neighbors. After receiving the packets, the roaming server tunnels all packets to the home roaming server of the roaming host. The home roaming server de-tunnels the packets and sends them to the final destination. That is to say, the roaming host can send out packets to other hosts right after it moves into the new service area. The operation of service switchover of outgoing packets is:

- The roaming server listens to the MAC addresses of its handoff neighbors
- The roaming server turns on the roaming ARP function for the roaming host
- The roaming server tunnels all received packets to the home roaming server of the detected roaming host.

An analysis of the impact of the switchover operation to traffic is provided here. Firstly, the operation does not introduce packet duplication. The link layer guarantees the roaming host to send packets to only one network access point, only one roaming server receives the packets. Secondly, the delay of the operation T_d is minimized. If the ARP cache is not flushed, T_d is zero. The roaming host regains ability to send out packets immediately after the layer-2 handoff. If the ARP cache is flushed, T_d is equal to the time of an address resolution operation T_{ARP}. Lastly, the operation does not cause packet loss.

4.3.2 Switchover for incoming traffic

It is more complicated to continue the packet delivery service in the incoming direction. After the roaming host moves into the new service area, the rest of the network is not aware of the location change. All incoming packets are still delivered to the original guest roaming server. After a roaming host is detected in the new area, the roaming server there initiates the service switchover. Two options of the switchover are considered here:

- Hard switchover. The guest roaming server in the new service area signals to the home roaming server directly to request packet redirection to the new area. The home roaming server set up packet forwarding destined to the new guest roaming server. Then the home roaming server signals the roaming server in the old service area to remove the roaming host. All data packets received during the transition are discarded.
- Soft switchover. The guest roaming server in the old service area buffers data packets when the roaming host is not receiving them. The guest roaming server in the new service area signals the guest roaming server in the old area to re-direct traffic to the new location. Then it signals the home roaming server to set up packet forwarding to the new area.

In Roaming IP, soft switchover is selected because it alleviates the packet loss. In "Optimized Smooth Handoffs in Mobile IP" [40] and Handoff enhancement in Mobile-IP environment"[36], the authors provide proofs that buffering in the roaming server alleviates packet loss. A major side effect of buffering packet is packet duplication. Packet duplication may trigger congestion control in TCP, which degrades the

performance of packet delivery.[51] A duplicate elimination mechanism is proposed in [40], in which the roaming host buffers the identification and source address fields in the IP headers of the packets received. During the handoff, the buffered information is sent to the previous roaming server that will drop those packets received by the roaming host already. Unfortunately such a mechanism cannot be applied in Roaming IP because no new protocol is allowed in the roaming host due to the requirement of complete transparency. The issue is addressed with the proposed novel switchover procedure.

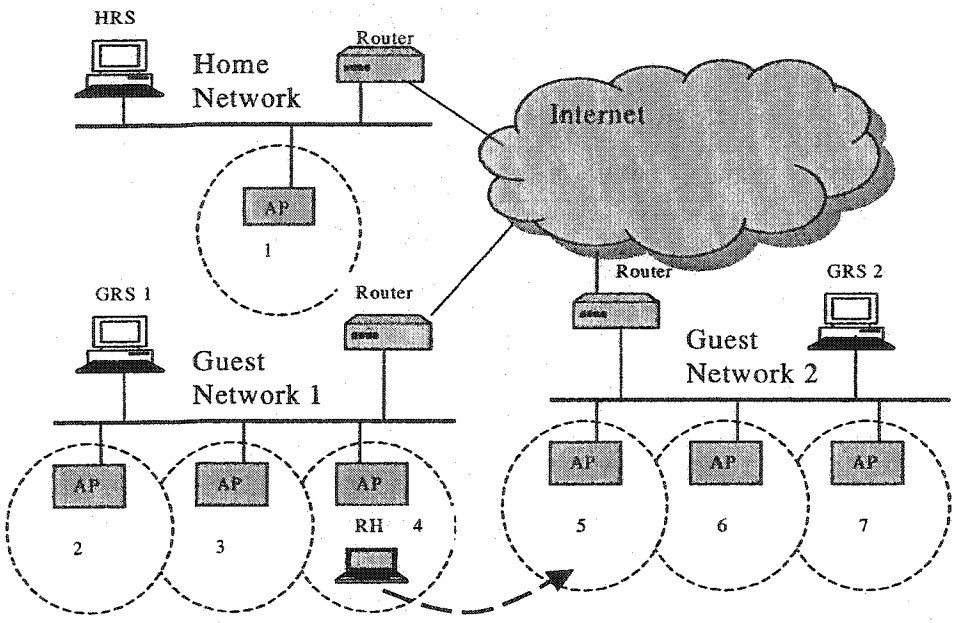


Figure 21 Service switchover

Figure 21 is used to describe the service switchover of Roaming IP. A roaming host RH successfully registers a full-mobile service in guest network 1 (subnet 1). The roaming servers in home network, guest network 1 and 2 are HRS, GRS1 and GRS2 respectively. The RH roams into guest network 2 (subnet 2), which triggers a layer-2 handoff, a movement detection and a service switchover of outgoing direction. Because the service switchover for incoming direction is not finished yet, all incoming packets are still tunneled to GRS1. GRS1 stores all packets in its buffers because RH is not reachable. GRS2 detects the roaming host and starts the service switchover of incoming traffic. The procedure of the service switchover is:

- GRS2 starts to de-tunnel packets for RH

- GRS2 sends a handoff request to GRS1 and sends an update request to HRS.
- GRS1 starts to forward packets to GRS2 including those in the buffer. All packets are forwarded in their arrival sequence.
- HRS sets GRS2 as the guest roaming server for the roaming host. It stops tunneling packets of the roaming host to GRS1 and buffers all packets. After waiting time $T_{hrs\_sw\_hold}$, it starts to tunnel the packets to GRS2. By now, the correct path of packet forwarding has been set up. $T_{hrs\_sw\_hold}$ is an engineering parameter to eliminate disorder of packets.
- HRS signals GRS1 to remove RH from its roaming host list
- In the meanwhile, GRS2 signals handoff neighbors to add RH to their neighbor list
- GRS2 adds RH into its roaming host list and removes it from the neighbor list

The message sequence chart of the procedure is shown in figure 22.

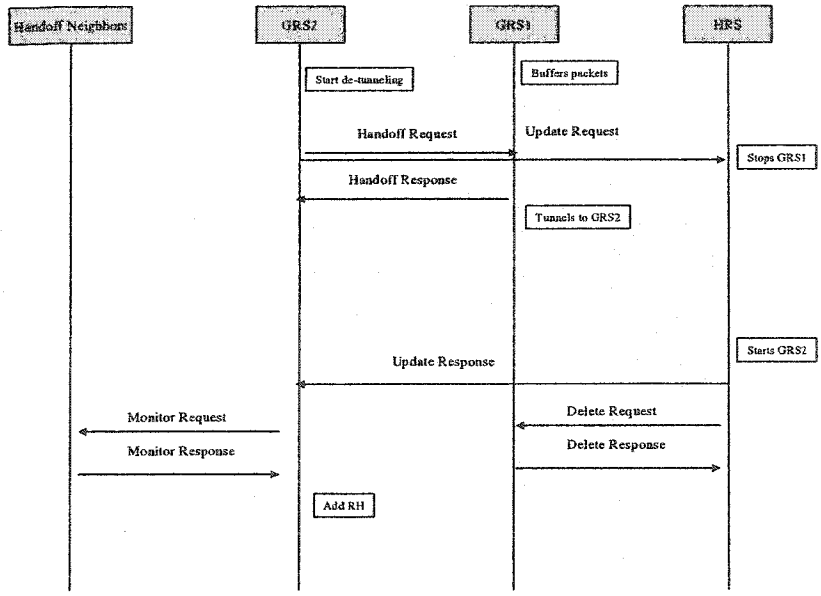


Figure 22 Message sequence of service switchover

4.3.3 Analysis of switchover

The impact of switchover procedure to the incoming traffic needs to be analyzed to identify the vulnerable period T_{vul} [36] in which data packets are lost. Let's take a look at the timing diagram of a switchover in figure 23. CH is the correspondent host that sends packets to the roaming host (RH). GRS2 detects RH after it moves into the new subnet. GRS2 signals GRS1 to tunnel packets to the new subnet. The delay between the detection of RH and GRS1's starting to tunnel to GRS2 is D_1. During D_1, GRS1 is unable to deliver packets to RH. Packets destined to RH are buffered in GRS1 like message C in figure 23. After D_1, GRS1 re-tunnels the packets to GRS2. GRS2 then sends the packets to RH. The first phase of switchover finishes. In the second phase, GRS2 signals HRS to select GRS2 as the guest roaming server of RH. HRS tunnels the packets to GRS2 instead of GRS1. In the whole procedure of switchover, there is no packet lost. The proposed scheme does not have a vulnerable period.

$T_{vul} = 0$

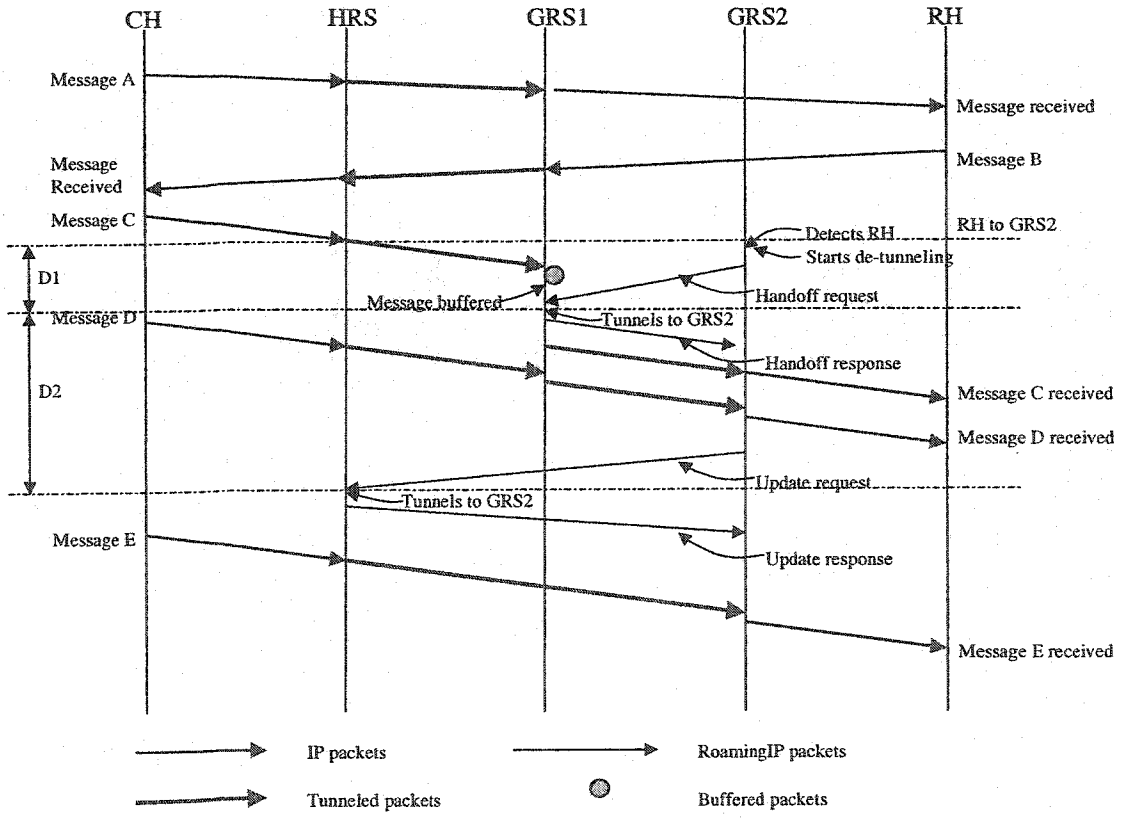


Figure 23 Sequence of service switchover

The introduction of a new phase in our scheme addresses the issue of packet duplication from buffering. The new roaming server signals the old one to re-tunnel packets to the new location before it signals the home roaming server. During the transition, packets are buffered in the old roaming server. This scheme guarantees that the home roaming server does not re-send the buffered packets to the new roaming server. Only one copy of the packets is delivered via the old roaming server. The introduction of the extra phase brings other benefits. Firstly the requirement of the size of the buffers in the roaming server is well contained. Assuming the arrival rate of packet is A, the number of packets needs to be buffered due to the switchover is:

$$S_b = \mathrm{A} * D_1$$

D_1 is the signaling delay between GRS1 and GRS2. Because GRS1 and GRS2 are neighbors, the signaling delay is at the range of milliseconds. Hence S_b is insignificant. Secondly, the period introduced by the switchover that no packet is delivered is only D_1. A small D_1 helps to ensure the total delay smaller that retransmission timer (T_{RTT}) in TCP. If T_{RTT} expires before buffered packets are delivered to and acknowledged by the RH, the buffered packets will be discarded by the TCP. A re-transmission is inevitable.[78] This seriously impacts the performance.

The proposed scheme guarantees the sequence of packets. If packets arrive at the destination in the wrong sequence, they will be retransmitted by the TCP layer. This causes a service disruption. In the first phase of proposed scheme, all packets follow the same path CH-HRS-GRS1-GRS2-RH. The original sequence is maintained by conventional IP packet delivery. In the second phase, packets travel through a new path CH-HRS-GRS2-RH after the HRS sets GRS2 as the guest roaming server for RH. The HRS waits a period $T_{hrs\_sw\_hold}$ before it starts to tunnel packets through the new path. All packets traveling through the old path are guaranteed to arrive at RH earlier than those with the new path. $T_{hrs\_sw\_hold}$ is an engineering parameter. The value of $T_{hrs\_sw\_delay}$ should be slightly bigger than the delivery delay between GRS1 and GRS2. Given the

fact that they are neighbors, the delay is at the range of milliseconds. The introduction of $T_{hrs\_sw\_hold}$ does not affect the overall performance.

4.4 Performance Analysis of Roaming IP handoff

The roaming host with a full-mobile service maintains its communication sessions during a handoff. For a full-mobile roaming host, service disruption is likely to happen during a handoff because the packet delivery service needs to be moved from one roaming server to another. Packets are not delivered before a handoff succeeds. The service disruption time is equal to the handoff time for connectionless UDP. But the service disruption to connection-oriented TCP is more severe. A handoff delay may trigger the congestion control mechanism of TCP.[56][57] TCP perceives the packet lost due to handoff delay as an indication of congestion that requires a TCP exponential back off and slow-start. After the handoff is finished, TCP will not immediately resume the communication. The service disruption to TCP is bigger than the handoff delay. According to the experiments results in "Performance of TCP and UDP during Mobile IP Handoffs in Single-Agent Sub networks"[38], LCS and PM cause UDP interruption for about 6s and TCP for 10s; while ECS cause UDP interruption for 3s and TCP for 6s. In a different experiment, [78]the authors show similar results. The service disruption time is around 6s for TCP.

For a semi-mobile host, handoff delay is not an issue because it does not communicate during the move. There is no requirement to start communication in the new subnet immediately. Our analysis is for the full-mobile hosts.

In Roaming IP, the handoff delay consists of the time of roaming host detection and service switchover:

$$T_{handoff} = T_{detection} + T_{switchover} \qquad (1)$$

where $T_{detectioin}$ is the delay of detecting the roaming host and $T_{switchover}$ is the delay of packet delivery switched to the new roaming server.

4.4.1 Detection delay

The movement detection of Roaming IP for full-mobile hosts has two steps: the layer-2 handoff and the reporting to the roaming server. The total detection delay is

$$T_{detection} = T_{reporting} + T_{layer2\_handoff} \quad (2)$$

The time for a layer-2 handoff $T_{layer2\_handoff}$ is at the range of milliseconds. In [80], it takes less than 10 ms to finish a layer-2 handoff.

$$T_{layer2\_handoff} < 10 \text{ ms} \quad (3)$$

The reporting time $T_{reporting}$ is equal to the delivery delay from the base station to the roaming server. Because the base station and the roaming server are in the same subnet and connected through a wired LAN, it can be assumed

$$T_{reporting} < 2 \text{ ms} \quad (4)$$

4.4.2 Switchover delay

During the service switchover, the packet delivery pauses temporarily in the original GRS and the HRS. In the original GRS, the contribution of the pause to the switchover delay starts when the roaming host is detected and ends when the original GRS begins to tunnel packets to the new GRS. The duration of this pause is equal to the signaling delay from the new roaming server to the old one plus the tunneling delay from the old roaming server to the new one, i.e. the round trip delivery delay $T_{rs\_round\_trip}$ between the GRSs. The GRSs are neighbors and connected through a wired network. In a typical configuration, the GRSs are 2 hops away from each other, it is assumed

$$T_{rs\_round\_trip} < 5 \text{ ms} \quad (5)$$

The pause in the HRS is to hold off the tunneling to the new GRS. The duration is $T_{hrs\_sw\_hold}$. $T_{hrs\_sw\_hold}$ is an engineering parameter and required to be slightly bigger than the one-way delivery delay $0.5T_{rs\_round\_trip}$ between the old and new roaming server. $T_{hrs\_sw\_hold}$ needs to satisfy (6)

$$0.5T_{rs\_round\_trip} < T_{hrs\_sw\_hold} \quad (6)$$

Based on (5) and (6), $T_{hrs\_sw\_hold}$ is set to 3 ms in Roaming IP

$$T_{hrs\_sw\_hold} = 3 \text{ ms} \tag{7}$$

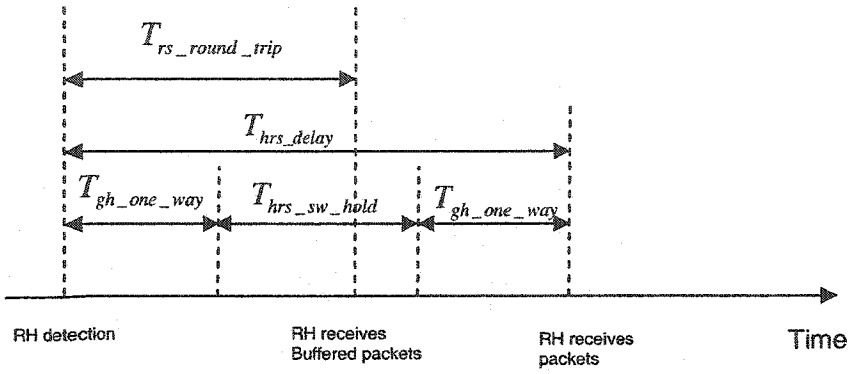


Figure 24 Switchover delay

As in figure 24, the total switchover delay is the bigger of T_{hrs_delay} and $T_{rs\_round\_trip}$.

$$T_{hrs\_delay} = T_{hrs\_sw\_hold} + 2\,T_{gh\_one\_way} = T_{hrs\_sw\_hold} + T_{gh\_round\_trip} \tag{8}$$

$T_{gh\_round\_trip}$ is the round trip delay between the new GRS and the HRS. Because the HRS is further away from the GRS, normally

$$T_{gh\_round\_trip} \geq T_{rs\_round\_trip} \tag{9}$$

From (6), (8) and (9),

$$T_{hrs\_delay} > 1.5\,T_{rs\_round\_trip} \tag{10}$$

So the total switchover delay is

$$T_{switchover} = T_{hrs\_sw\_hold} + T_{gh\_round\_trip} \tag{11}$$

4.4.3 Handoff delay

From (1), (2) and (10), the total handoff delay of roaming IP is:

$$T_{handoff} = T_{layer2\_handoff} + T_{reporting} + T_{hrs\_sw\_hold} + T_{gh\_round\_trip} \tag{11}$$

From (3), (4) and (7),

$$T_{handoff} < 10 + 2 + 3 + T_{gh\_round\_trip} = 15 + T_{gh\_round\_trip} \tag{12}$$

4.4.4 Service disruption time

The service disruption time to UDP is the same as total handoff time because UDP recovers to send packets right after the handoff is done. To make service disruption time to TCP the same as the total handoff time, the following condition must be met: [5]

$$T_{handoff} < T_{RTT} \tag{12}$$

Where T_{RTT} is the retransmission timer of TCP.

The calculation of the retransmission timer T_{RTT} is based on the roundtrip delay $T_{TCP\_round\_trip}$ of the TCP connection.

$$T_{RTT} = \mathrm{k}\, T_{TCP\_round\_trip} \tag{13}$$

Where k is a constant. In the Internet today, k is normally set to 3. [82]

As in figure 21, the original path of the TCP connection is CH-HRS-GRS1-RH and the round trip delay is:

$$T_{TCP\_round\_trip} = T_1 + T_2 + T_3 \tag{14}$$

Where T_1, T_2 and T_3 are the round trip delay between CH and HRS, HRS and GRS1, GRS1 and RH respectively.

The requirement of avoiding a TCP retransmission in Roaming IP is:

$$T_{handoff} < 3\, T_{TCP\_round\_trip} \tag{15}$$

For (12), (14) and (15), the following must be satisfied to avoid the TCP retransmission:

$$T_{gh\_round\_trip} < 3\,(T_1 + T_2 + T_3 - 5) \tag{16}$$

It is known that the round trip delay between Internet hosts varies significantly, however, it is normally in the range of tens of ms. Hence the sum of T_1 and T_2 is significantly greater than 5 ms. $T_{gh\_round\_trip}$ is approximately the same as T_3 .because the two GRSs are neighbors. So (16) is normally satisfied, which means that there is no TCP retransmission and the service disruption time is equal to the handoff time.

In section 7.4, the performance of handoff service is evaluated. In the testing system, there is no TCP retransmission and the service disruption time is minimized to the handoff delay.

.

Chapter 5 Roaming service management

To provide an end-to-end solution, it is necessary to address the management of roaming IP service. A directory is proposed to store the information and provide fast and reliable access.

5.1 Architecture of roaming service management

Before the roaming host initiates service registration for roaming IP, the management Information associated with the roaming host/user should exist in the system. The network administrator controls the roaming IP management information. When a user applies for roaming IP service and receives the approval, the network administrator creates a new data entry for the user in the management database. Roaming servers use the information to manage roaming IP service. During roaming service registration, the roaming server needs to confirm the authentication information. The roaming server also needs to obtain the service related parameters. The key information associated with a roaming host is:

- User ID and password to control the access to roaming IP service
- Service level profile for each user. This describes the service available to each user.
- Home network and home roaming server for each roaming host. This information is used for roaming service registration
- Predefined service parameter for each roaming host

There is one entry for each roaming host in the network. The size of the management data is in proportion to the number of roaming hosts. There can be millions of entries in the global Internet. Every roaming server need to have access to the data because every roaming host is possible to be in its service area. There are huge numbers of subnets and we need to have at least one roaming server per subnet. The number of users of the management information is huge. It is not practical to store all the information locally in each roaming server due to both the size of the database and number of roaming servers. We need to store the information in a common database system. The common database

provides single interface for the administrators to manage the information. The common database is a distributed system because of the size of the information. A distributed system is also necessary to provide multiple access points to large amount of users for acceptable performance. The architecture of roaming service management is shown in the figure 25.

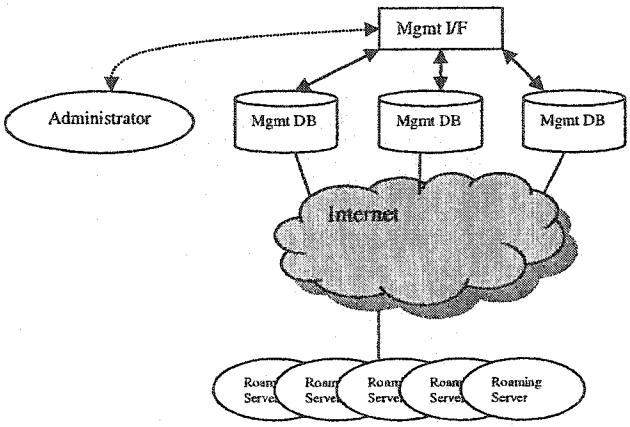


Figure 25 Architecture of roaming service management

All management information is stored in the distributed database. Each server is responsible for a subset of the data. The data can be divided with different criteria. One logical way of division is based on the administrative areas. Every server stores the information of all roaming hosts in its area. Administrators manage all servers via a consolidated interface. All roaming servers have connections to directory servers via the Internet. A default database server is assigned for each roaming server. A data access request will be referred to other servers if the default server does not have the answer locally.

5.2 Directory service

The characteristic of management information of Roaming IP is:

- Only limited applications need to make modification to the information.
- The information does not change often.
- Many applications need read access to the information.

Directory service can satisfy all the requirements. It also fit well into the architecture described in the previous section.

A directory is a special database[61][62][63][64]that contains mostly descriptive, attribute-based information. The information is generally read more often than it is written. An update of a directory is typically an all-or-nothing operation. There is no need for transaction or rollback schemes. A directory is normally designed to provide a quick response to large amount of lookup or search operations. There are three components in a directory service: directory server, management system and directory applications.[79] A directory server is used to store all directory information and provide lookup service. The management system is used to manage the directory itself. Directory applications are user of the directory information. LDAP (Light Weight Directory Access Protocol) is the standard for directory service by IETF.[61][63].

In a LDAP directory, information is stored as entries that have a collection of attributes. Each attribute has a unique name, called distinguished name (DN). Each attribute also has a type and one or more values. There are basic types defined in the standard, like "cn" for common name, "mail" for email address, etc. There also can be user-defined types. The values depend on what type of attribute it is. For example, a mail attribute can have value "frank@uottawa.ca". The LDAP directory is based on client-server model. One or more LDAP servers contain the data making up the directory. A LDAP client connects to a LDAP server and queries for information. The server responds with an answer or a pointer to the next server that may have the answer.

LDAP is the protocol selected to provide directory service for Roaming IP. LDAP is suitable for the needs to provide highly available, distributed systems. LDAP also provides quick lookup service for a large number of directory applications.

5.2.1 Management system for the directory

There are three types of directory management system: command line utilities, application based management system and web-based management system. [64] The advantages of Web-based management system are: 1) Web browser is Cross-platform and available on almost every computer on the Internet; 2) User friendly interface can be provided; 3) Thin client. All the complexity is on the central server, which is easier to manage. To make roaming IP more portable and easy to use, the web-based LDAP management system proposed in "Design and Implementation of Secure Web-based LDAP Management System"[79] is adopted for Roaming IP.

The architecture of proposed web based LDAP management system is illustrated in figure 26. Directory administrator manages directory data or directory server through web pages generated by the HTTP server. The HTTP server retrieves all data presented in the web page and passes them to the DM through CGI interface. DM (directory Management Module) manages directory entries in the LDAP server and the server itself. The responsibilities of DM are listed as follows:

- LDAP server maintenance
- Directory entry maintenance
- Directory schema maintenance
- LDAP server monitoring
- Maintain management information database

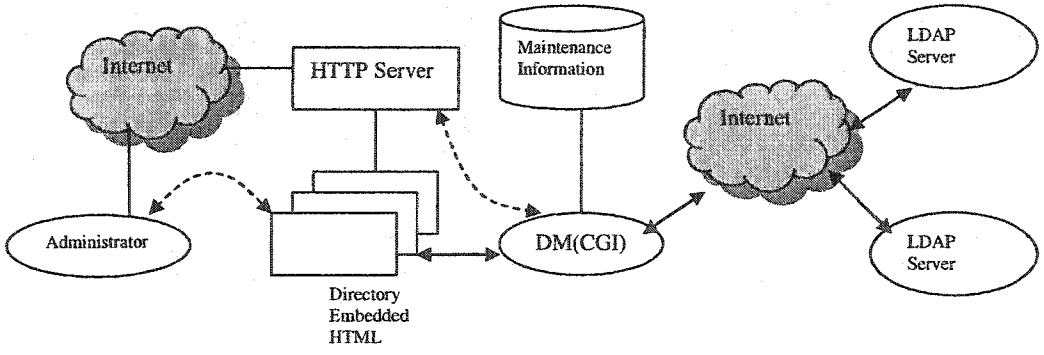


Figure 26 Management of directory service

5.2.2 Interface for applications

In LDAP, operations are defined for information access. The operations of adding, deleting and changing entries are used for the directory management. However, the search operation is mostly used. It is used to get information for LDAP clients (e.g. roaming servers). The LDAP APIs are defined in RFC 1823. [65]

The steps to use LDAP APIs to access a directory are:

- Open a connection to an LDAP server
- Authenticate to the LDAP server
- Perform some LDAP operations and obtain results
- Close the connection

A brief description of APIs that are used in Roaming IP is given here. For a complete specification of each API, please refer to RFC 1823 [65].

5.2.2.1 Opening a connection

```
LDAP *ldap_open ( char *hostname, int portno);
```

Ldap_open() is defined to open a connection to the LDAP server. There are two parameters for the function call: hostname and portno. The hostname is a list of names or IP addresses of the LDAP server. The portno is the TCP port number of the LDAP server. Ldap_open() returns a "connection handle", a pointer to an LDAP structure that will be used by the subsequent calls to the connection.

5.2.2.2 Authenticating to the directory

```
Int ldap_bind( LDAP *ld, char *dn, char *cred, int method );
```

Ldap_bind() is used to authenticate to the directory. There are four parameters for the function call. The ld is the connection handle; The dn is the name of the entry to bind; The cred is the credentials; And the method is the authentication method to use. A successful bind call is necessary before attempting other operations over the connection.

5.2.2.3 Closing the connection

```
Int ldap_unbind ( LDAP *ld)
```

Ldap_unbind() is used to unbind from the directory and close the connection. The ld parameter is the connection handle.

5.2.2.4 Searching

```
Int ldap_search (
      LDAP        *ld,
      Char        *base,
      Int         scope,
      Char        *filter,
      Char        *attrs[];
      Int         attrsonly
)
```

ldap_search() is used to search the LDAP directory and return a requested set of attributes. The base parameter is the dn of the entry at which to start the search; The scope parameter indicates the scope of search; The attrs is an array of string indicating what attributes to return.

5.2.2.5 Reading an entry

The search API is used to read an entry. In the search operation, the base is set to the DN of the entry to load. Scope is set to LDAP_SCOPE_BASE. Filter is set to "(objectclass=*)". Attrs contains the list of attributes to return.

5.2.2.6 Adding an entry

```
Int ldap_add (LDAP *ld, char *dn, LDAPMod *attrs[] );
```

Ldap_add() is used to add entries to the LDAP directory. Ld is the connection handle; dn is the name of the entry to add; attrs is the entry's attributes.

5.2.2.7 Deleting an entry

```
Int ldap_delete ( LDAP *ld, char *dn );
```

Ldap_delete is used to delete entries from the directory. Ld is the connection handle and dn is the name of the entry to delete.

5.3 Directory structure for Roaming IP

The high level directory for roaming IP is defined in figure 27.

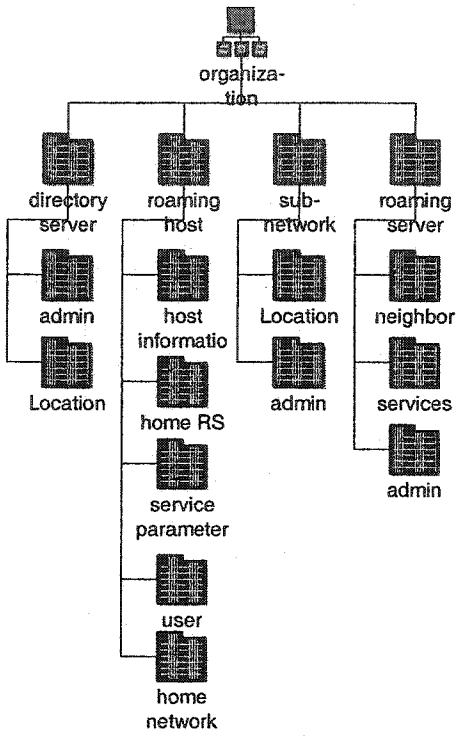


Figure 27 Directory structure

Chapter 6 Implementation of Roaming IP

In this chapter, an implementation of roaming IP is presented. The prototype system is developed in a PC running Linux as the operating system. The implementation is tested on Red Hat Linux 7.0. To make the implementation suitable for future research, thoughts are given to the expandability and portability. Modular design is used for the whole project. Standard C language, portable system calls and third party libraries are used to provide portability across different platforms.

6.1 Architecture

The architecture of the roaming server is illustrated in figure 28. It is composed of three parts: data plane, management plane and front end. The data plane is responsible for intercepting packets, forwarding packets and responding to packets. The control plane is responsible for managing the dynamic information of roaming service and static information of roaming server itself. The front end enables users to manage roaming service. It provides multiple user interfaces to control the system. The detailed description of each component is as follows:

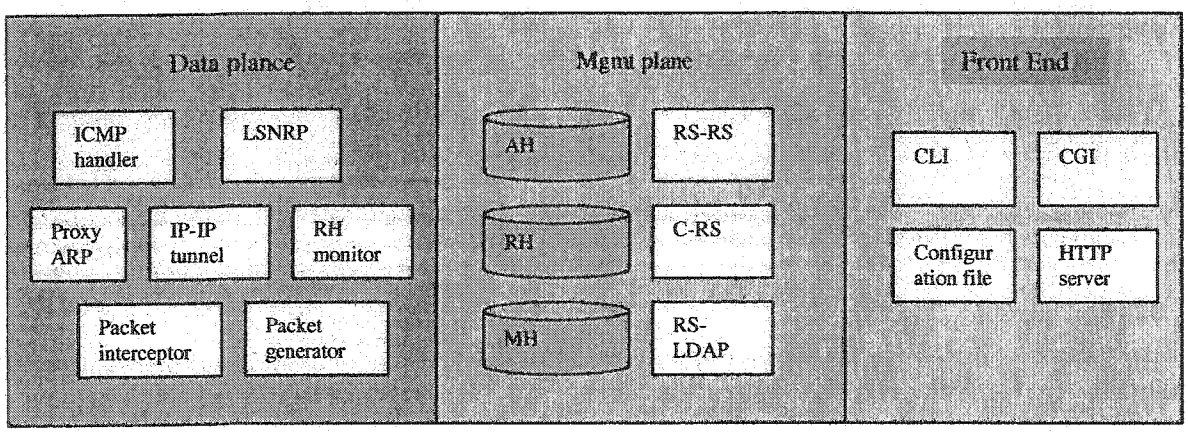


Figure 28 Roaming server architecture

Packet interceptor: the packet interceptor listens to all data packets on the network interface. Following the rule defined in Roaming IP, the packet interceptor either passes the packet to other component for further processing or discards the packet right away.

Packet generator: The packet generator is a set of utilities provided for other application to generate, manipulate Ethernet/IP data packet and send the packet out to the network.

IP-IP tunnel: IP-IP tunnel is responsible for encapsulation and forwarding IP packets for roaming hosts. It is also responsible for de-capsulation of IP packets and delivery to the destination.

RH monitor: It is responsible for keeping track of roaming host in the service area. It is also responsible for handoff host searches upon request from the management plane. RH monitor periodically send out ARP ping request to roaming hosts. If a roaming host fails to response to the request. The RH monitor reports it to the management plane for further action.

Proxy ARP: Proxy ARP is used to attract data packets from roaming hosts and other network nodes that communicate with roaming hosts. In the home network, Proxy ARP replies to ARP request of a roaming host with its own layer 2 address (MAC address). In the guest network, Proxy ARP replies to ARP request from a roaming host with its own layer 2 address. After a successful proxy ARP reply, data packets are delivered to the roaming server.

ICMP handler: ICMP handler monitors ICMP messages generated inside the IP-IP tunnel. Following the rules defined in Roaming IP, the ICMP handler analyzes the cause of the failure. It then generates and sends an ICMP message to the originator of the original IP packet. This provides debug information for the originator.

LSNRP: LSNRP resolves the local service name of the roaming server into IP address. At the beginning of service registration, a user types in the generic local service name of

roaming IP. The name needs to be mapped into the IP address of the roaming server. LSNRP generates and send back a DNS reply message for the DNS request from the roaming host.

There are three important databases in the management plane: Away Host (AH) list, Roaming Host (RH) list and Neighbor Host (NH) list. These three databases control the behavior of the data plane. The AH list is used in home roaming servers. It contains all mobile hosts that leaves the home network and registers for roaming service in a guest network. The home roaming server attracts data packets destined to all away hosts and sends them to guest roaming servers through IP-IP tunnels. The RH list is used in guest roaming servers. It contains all mobile hosts that are granted roaming service by the roaming server. The NH list contains all mobile hosts that may move into the area of the roaming server from its handoff neighbors.

RS-RS: This component manages the communications between roaming servers, including roaming service maintenance, handoff and roaming host search. This component implements the RS-RS protocol. It updates the databases to control the data plane.

C-RS: This component manages the communication between a roaming server and clients of user interface. This component waits for request from client and takes appropriate action. It provides an interface for the front end to control the roaming server.

RS-LDAP: This component provides an interface to the LDAP directory server for the roaming server. The following information is necessary for roaming service: authentication of users, home roaming server and service parameters of roaming hosts.

Front end: Three different user interfaces are provided with the front end. The Command Line Interface (CLI) provides an ASCII based utility to manage roaming service. It's for developers and experienced users. The HTTP server together with CGI problem provides a web-based user interface. The configuration file component is used to configure the

roaming server, provide non-volatile storage for the configuration data and provision large amount of data.

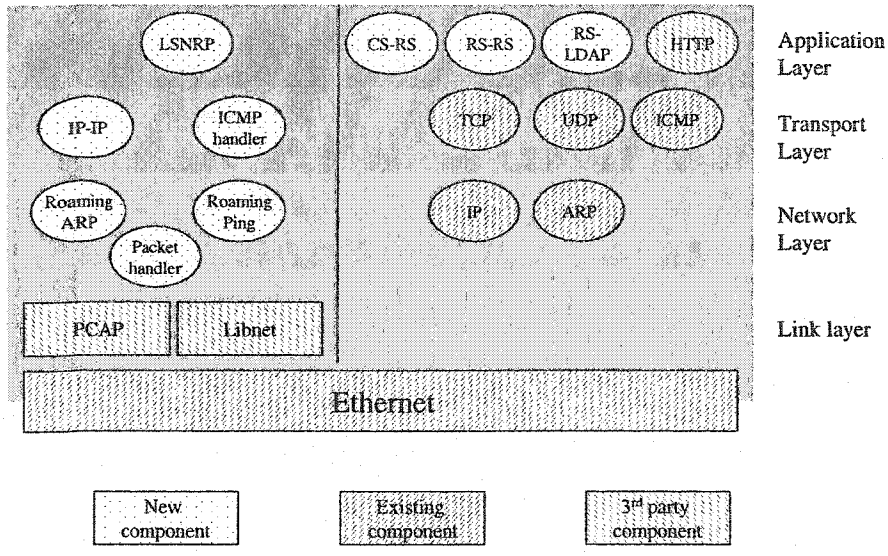


Figure 29 Protocol stacks of roaming server

Figure 29 shows how components fit into the protocol stack and their relationship with the TCP/IP components. The components of data plane are built on top of some powerful 3rd party network libraries. While the rest of components sit above the regular IP stacks. Every incoming packet is accessible to the 3rd party stack and the IP stacks. The 3rd party stack and IP stack process the packet independently.

6.2 Data plane

The data plane provides packet manipulation and delivery service. At the beginning of the development, the data plane was developed in the Linux kernel for optimal performance. But it is inconvenient to build an application into the kernel: more difficult to debug, much longer time to make a change, etc. Moreover, the portability of the implementation is not maintained by putting the solution into the kernel. It is decided to implement this solution in the user space. The purpose of the implementation is for research and the performance is given lower priority.

To implement the data plane, access to the network programming interfaces are required. The key requirements are listed as follows:

- Ability to monitor all layer 2 (MAC) data packets. We need to see all packets including broadcast packets (e.g. ARP request) and uni-cast packets regardless of the destination MAC address.
- Access to the Ethernet and IP header of all packets that intercepted
- Ability to manipulate the headers and data fields of packets.
- Ability to send data packets to layer 2, bypassing the IP routing and ARP.

Networking APIs are normally provided by the operating system. Applications access the communication protocol stack through the APIs. The best-known example of network API is the Berkeley socket interface. Linux provides the socket interface. But the socket interface does not provide some of the functionalities that required for roaming IP. It is decided to use third party network libraries for this implementation. PCAP [66] is used to capture all data packets. Libnet [67] is chosen for manipulating data packets. These two libraries provide not only the necessary functionalities but also the portability. They are supported by multiple platforms including Linux, other Unix and Windows.

6.2.1 Packet interception

The packet handler listens to all packets in the LAN that the roaming server provides service. During the initialization, the packet handler opens a network interface via PCAP APIs. Then it waits on the interface for data packets. When a packet arrives, the packet handler dispatches it to the destination like Roaming Ping and Roaming ARP. The pseudo code for packet handler is:

```
/* Set up the PCAP interface to intercept packets from the
Ethernet interface */
pd = pcap_open_live(my_config.if_name, 2000, 1, 100, ebuf);

      if (pcap_compile(pd, &fcode, "\0", 1,
my_config.if_netmask.s_addr) < 0) {
            syslog(LOG_ERR, "%s: %s", program_name,
pcap_geterr(pd));
            return(1);
      }
```

```
      if (pcap_setfilter(pd, &fcode) < 0) {
            syslog(LOG_ERR, "%s: %s", program_name,
pcap_geterr(pd));
            return(1);

      }


/* Spawn a child task to handle packets in the background */
pid = fork();

            if (pid > 0) return; /* This will return back to the
main*/
            if (pid < 0) {
                        syslog(LOG_ERR, "%s: fork failed: %s",
program_name, strerror(errno));
                  return;     }


/* Wait for packets. When a packet arrives, pass it to the packet
handler "process_packet" */
if (pcap_loop(pd, -1, process_packet, 0) < 0) {
            syslog(LOG_ERR, "%s: pcap_loop: %s", program_name,
pcap_geterr(pd));
            return(1);
      }

void process_packet (u_char *user, const struct
pcap_pkthdr *h, const u_char *bp)

{
      switch (ntohs(ether_hdr->ether_type))
      {   case (ETHERTYPE_IP):
                  process_ip(bp);
                  break;


      /* Pass the ARP request to the Roaming ARP handler */

          case (ETHERTYPE_ARP):
                  process_arp(bp);
                  break;
      }
}

void process_ip(const u_char* bp)
{

      /* Pass the DNS request to the LSNRP handler */
      if ((ip_hdr->ip_p == IPPROTO_UDP) && recv_port == 0x035))
            process_dns(bp);

      /* Pass the IPIP tunnel message to the IPIP handler */
      if (ip_hdr->ip_p == IPPROTO_IPIP) process_IPIP
}
```

6.2.2 Packet manipulation and generation

After receiving a packet from the roaming host, a roaming server needs to respond based on the packet type. The response involves packet manipulation and generation that use Libnet and raw socket APIs. During the initialization, a Libnet socket and a raw socket are opened.

```
/* The Libnet socket is used for general packet generation
ip_socket = libnet_open_raw_sock(IPPROTO_RAW);

/* The raw socket is used for sending IP-IP tunnel packets
*/


ip_socket_ip = socket(AF_INET, SOCK_RAW, IPPROTO_IP);
```

6.2.2.1 ARP reply

The pseudo code for generating ARP reply is as followed:

```
/* Construct and transmit an ARP reply */
      int send_arpreply(struct in_addr *target_ipaddr,
                        unsigned char *her_hwaddr, struct in_addr
                        *her_ipaddr)
      {
            char ebuf[PCAP_ERRBUF_SIZE];
            u_char buf[ARP_H+ETH_H];
            int count;
            char eth_str[20];

            memset(buf, 0, ARP_H + ETH_H);
            libnet_build_ethernet(her_hwaddr, my_config.if_hwaddr,
             ETHERTYPE_ARP, NULL, 0, buf);

       /* ARP header */
            libnet_build_arp(ARPHRD_ETHER, ETHERTYPE_IP,
                  ETHERADDRLEN, IPADDRLEN,
                  ARPOP_REPLY,
                  my_config.if_hwaddr,
                  (u_char *)&(target_ipaddr->s_addr),
                  her_hwaddr, (u_char *)&(her_ipaddr->s_addr),
                  NULL, 0, buf + ETH_H);

       /* Send out the packet */
            count = libnet_write_link_layer(ln, (const u_char *)
                        my_config.if_name, buf, ARP_H + ETH_H);
            printf("Send_arpreply: send out bytes: %d\n", count);

            return count;
      }
```

6.2.2.2 DNS reply

The pseudo code for DNS reply generation is

```
/* generate the DNS IP packet */
libnet_build_dns (ntohs(dns_hdr->id),
                  htons(0x8085),
                  1,
                  1,
                  1,
                  0,
                  dns_data,
                  dns_data_1,
                  packet_buffer+LIBNET_IP_H + LIBNET_UDP_H);

libnet_build_udp (recv_port, //udp_hdr->uh_dport,
                  send_port, //udp_hdr->uh_sport,
                  packet_buffer+LIBNET_IP_H + LIBNET_UDP_H,
                  LIBNET_DNS_H + dns_data_1,
                  packet_buffer+LIBNET_IP_H);

libnet_build_ip (LIBNET_UDP_H + LIBNET_DNS_H + dns_data_1,
                 ip_hdr->ip_tos,
                 ip_hdr->ip_id,
                 ip_hdr->ip_off,
                 255,
                 ip_hdr->ip_p,
                 ip_hdr->ip_dst.s_addr,
                 ip_hdr->ip_src.s_addr,
                 packet_buffer + LIBNET_IP_H,
                 LIBNET_UDP_H + LIBNET_DNS_H     + dns_data_1,
                 packet_buffer);
libnet_do_checksum (packet_buffer, IPPROTO_UDP, LIBNET_UDP_H +
                 LIBNET_DNS_H  + dns_data_1);

/* send out the packet */
libnet_write_ip(ip_socket, packet_buffer, LIBNET_IP_H +
                 LIBNET_UDP_H + LIBNET_DNS_H + dns_data_1);
```

6.2.2.3 IP packet tunneling

The pseudo code of IP over IP tunneling is:

```
Int send_packet_to_tunnel(const u_char* payload,
                          /* pointer to IP packet */
                            struct in_addr* ip_dest)
                          /* pointer to destination IP address*/
{

      in_ip_hdr = (struct libnet_ip_hdr*) payload;
      packet_len = LIBNET_IP_H + ntohs( in_ip_hdr->ip_len);

      memset(&sin, 0, sizeof(struct sockaddr_in));
      sin.sin_family  = AF_INET;
      sin.sin_addr.s_addr = ip_dest->s_addr;
```

```
        c = sendto(ip_socket_raw, payload,
              ntohs(in_ip_hdr->ip_len), 0, (struct sockaddr *)&sin,
              sizeof(struct sockaddr)); // send the payload out.
}
```

6.3 Management plane

In the management plane, three different components: RS-RS, RS-Client and RS-LDAP are implemented. All three components run on top of the TCP protocol. As regular network applications, there are not special requirement to the networking API. The socket API provided by Linux is used to access TCP services. The RS-LDAP component is responsible for getting roaming IP management information form the directory server. The protocol between the directory server and a client (e.g. the roaming server) is LDAP. To communicate with the LDAP server, the APIs and libraries provided by OpenLDAP[72] are used.

6.3.1 Roaming databases

In the management plane, there are three important databases: Roaming host list, away host list and neighbor host list. The roaming service and behavior of the data plane are controlled by the information in these three databases. The databases need to provide very fast search capability. All three databases are implemented in C data structures. Hash tables are created for fast searching.

6.3.1.1 Roaming host entry

The C structure definition of a roam host entry is presented here.

```
/*This is for Guest RS to admin roam hosts*/
struct roam_host_entry
{
      struct roam_host_entry  *next;
      struct in_addr          ip_rh;
      struct in_addr          ip_hrs;
      struct in_addr          ip_grs;
      char                    hwaddr_rh[6];
      int               state;
};
```

6.3.1.2 Away host entry

The C structure definition of an away host entry is presented here.

```
struct away_host_entry
{
        struct away_host_entry  *next;
        struct in_addr          ip_ah;
        struct in_addr          ip_hrs;
        struct in_addr          ip_grs;
        int                     state;
};
```

6.3.1.3 Neighbor host entry

The C structure definition of a neighbor host entry is presented here.

```
struct neighbor_host_entry
{
        struct neighbor_host_entry    *next;
        struct in_addr          ip_nh;
        struct in_addr          ip_hrs; //IP of home RS
        struct in_addr          ip_grs; //IP of the current guest
RS
        struct in_addr          ip_drs; //IP of the destined guest
RS
        int                     state;
};
```

6.3.2 RS-RS and RS-Client

The RS-RS component implements the roaming server to roaming server protocol. A roaming server listens to TCP port 2000 for incoming request. When a message is received, it is handled based on the operation code. The RS-Client component implements the management client to roaming server protocol. A roaming server listens to TCP port 2001 for messages from a management client. Because RS-RS and RS-Client handle similar operations like add, delete roaming hosts, the message formats are similar. One message format is defined for both RS-RS and RS-Client components.

The message format is defined in the following C structure.

```
struct rs_con_msg

{
        unsigned char           version;
        enum rs_con_op_code     op_code;
        char                hwaddr_host[6];
        union {
              struct in_addr    ip_rh;
```

```
            struct in_addr      ip_ah;
        } roamip;
        struct in_addr          ip_grs;
        struct in_addr          ip_hrs;
        struct in_addr          ip_drs;
        enum rs_con_res_code    res_code;

};


enum rs_con_op_code {

        SS_ADD_AH_REQUEST = 0,
        SS_ADD_AH_REPLY = 1,

        SS_DEL_AH_REQUEST = 2,
        SS_DEL_AH_REPLY,
        SS_AUDIT_REQUEST,
        SS_AUDIT_REPLY,
        SS_HANDOFF_REQUEST,
        SS_HANDOFF_REPLY,
        SS_UPDATE_REQUEST,
        SS_UPDATE_REPLY,

        CS_ADD_RH_REQUEST = 101,
        CS_ADD_RH_UPDATE = 102,   /* This is the message to confirm
                                     entry added locally, still
                                     waiting for remote confirmation
                                  */
        CS_ADD_RH_REPLY,
        CS_DEL_RH_REQUEST,
        CS_DEL_RH_REPLY,

        CS_SW_RH_REQUEST = 201,
        CS_SW_RH_REPLY

};
```

6.4 Front end

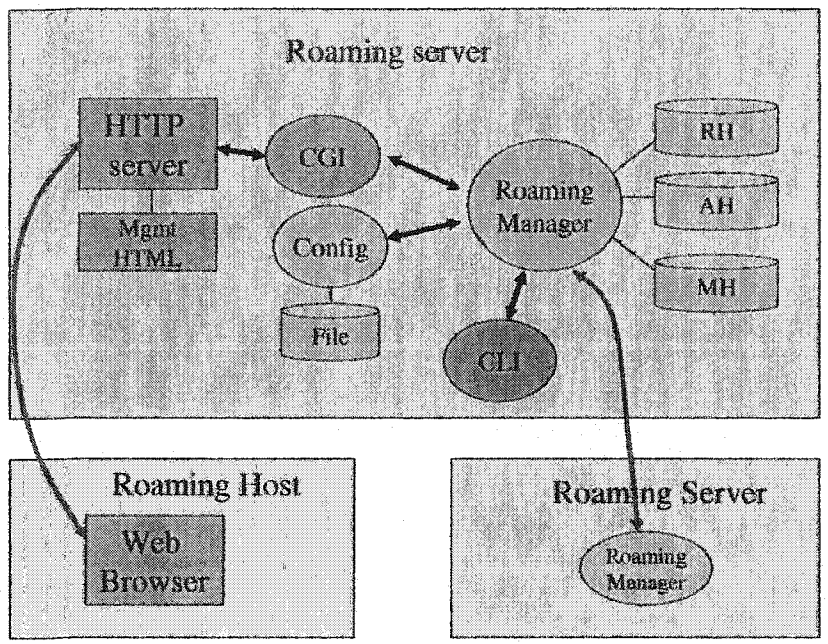


Figure 30 Front end of roaming server

The components of the front end are depicted in figure 30. The front end provides man-machine interfaces for users and network administrators. The interfaces are used to manage both roaming server and roaming services. The web based interface is developed for end users to register/de-register roaming services. It provides complete transparency to the roaming host. The CGI program converts the information gathered from the web page to internal data structure. It passes the data to the management plane via a Client-RS protocol. The configuration information of the roaming server is managed through the configuration file. The administrator of the roaming server provisions the roaming server by editing the text configuration file. Roaming service information can be also input from the configuration file. The function is useful for setting up test environment for research. The configuration file component also provides a non-volatile storage for management information. With the CLI, the user can change, access and delete the information of both roaming server and roaming services.

In the implementation, an Apache [68]HTTP server is used for the web-based interface. The Apache server is an open source development that is widely accepted in the Internet. A third party APIs[69] is used to do CGI programming. It provides the features to easily retrieve the information embedded in the web forms.

Chapter 7 Experiments and results

In Roaming IP proposal, a suite of new protocols are introduced: Roaming ARP, Local Service Name Resolution Protocol, Roaming Ping protocol, packet delivery service and handoff service. All of the protocols are implemented in Linux platform with C language. Experiments are carried out to evaluate the correctness and effectiveness of the protocols as well as measure the performance of Roaming. In this chapter, experiments are presented for Roaming ARP, Local Service Name Resolution Protocol, Roaming packet delivery and handoff service. The focus of experiments of roaming ARP and LSNRP is to demonstrate the effectiveness of the protocol in real world implementations. In Roaming ARP test, mobile hosts with different operating systems (Windows 98, 2000, XP and Linux) are tested. In LSNRP test, both home network and guest network scenarios are covered.

The key performance attributes of packet delivery are the throughput and delay. In the experiments, the throughput and delay of the Roaming IP packet delivery service are measured and compared with the regular IP service.

In Chapter 4, the handoff procedure of Roaming IP is described in detail. A thorough analysis provided the proof that Roaming IP handoff does not introduce packet lost during the transition between service areas. Hence the handoff does not trigger the TCP retransmission timeout that causes significant service disruptions. In the experiment presented here, a mobile host communicates with the correspondent host over TCP/IP protocols before, during and after a handoff. The TCP traffic is captured by a third node. The sequence number of each TCP packet is analyzed to determine if a packet lost/re-transmission occurs. When the same sequence number is used for transmission more than once, it confirms a packet lost.

7.1 Roaming ARP

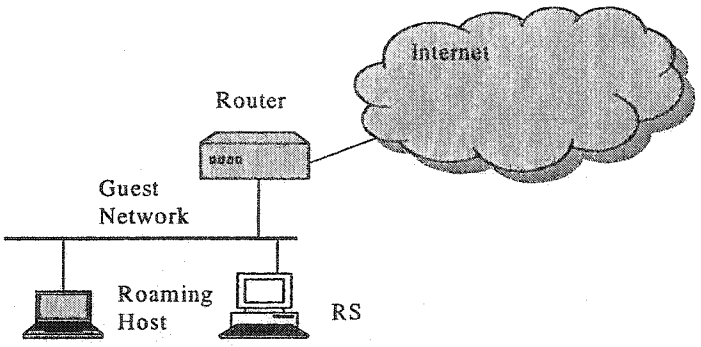


Figure 31 Test of Roaming ARP

The first set of experiments is to test the effectiveness of Roaming ARP protocol. The test bed consists of a roaming host and a roaming server as shown in figure 31. All hosts in the local network are connected with 10 Base-T Ethernet. The roaming server RS is a PC with a Pentium II 300 MHz CPU. The roaming server runs on Linux operating system with a Roaming ARP implementation. The roaming host RH is a regular PC. Tcpdump[66] is used to capture all data packets in the LAN. If RH delivers all its IP packets to the MAC address of RS, the experiment is successful.

The IP configurations of RH and RS are shown in table 1.

	IP address	Subnet Mask	Default Gateway
RS	192.168.1.10	255.255.255.0	192.168.2.1
RH (Scenario 1)	192.168.2.101	255.255.255.0	192.168.2.1
RH (Scenario 2)	192.168.2.101	255.255.255.0	192.168.2.101

Table 1. Configurations for Roaming ARP test

In scenario 1, the roaming host has its default gateway set to the router of its subnet. In scenario 2, the default gateway is set to the IP address of the roaming host. Both are valid configurations in the Internet. Roaming hosts with four different OSs are used in the test, including Linux, Windows 2000, Windows NT and Windows XP.

The test is run 20 times for each operating system and each scenario. The numbers of success are captured in table 2.

	Linux	Windows 2000	Windows 98	Windows XP
Scenario 1	20	20	20	20
Scenario 2	20	20	20	20

Table 2. Results for Roaming ARP test

From the result, it is confirmed that roaming ARP is an effective protocol to attract packets from the roaming host to the roaming server.

7.2 LSNRP protocol

The second set of experiments is to test the effectiveness of LSNRP. The test bed consists of a roaming host, a roaming server and two DNS servers as shown in figure 32. All hosts in the local network are connected with 10 Base-T Ethernet. The roaming server is a PC with a Pentium II 300 MHz CPU. The roaming server runs the Linux operating system with a LSNRP implementation. The roaming host is a regular PC. Different operating systems are used in the roaming host to check if LSNRP is effective for IP stacks in different OS. DNS server 1 several hops away from the roaming host, which represents the typical setup in the Internet. While DNS server 2 is in the same LAN as the roaming host. That is the worst case for LSNRP because the response from DNS server 2 is the fastest. In the test, Tcpdump is used to capture all data packets in the LAN.

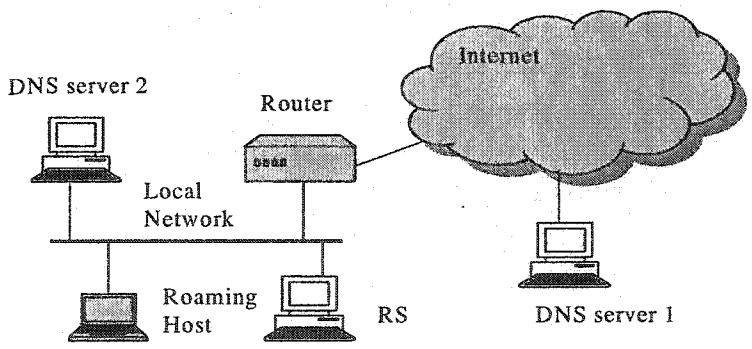


Figure 32 Test of LSNRP

Captured packets and display on the roaming host are used to determine whether a LSNRP operation succeeds. In the roaming host, the URL of local service name of roaming IP http://roamingip.local is typed in a web browser. If the web page of roaming IP service management is displayed in the browser, the LSNRP name resolution

succeeds. It is also observed if the roaming host drops the negative DNS reply from the DNS server. The delay of reply messages are calculated from the log of packets. Tests are run with different combinations of DNS servers and operating systems in the roaming host. Each test is repeated five times and the means are recorded. The results are presented in table 3.

DNS server	OS	LSNRP success (Times)	LSNRP Reply Delay (ms)	DNS Reply Delay (ms)
1	Linux	5	0.190	35.898
1	Windows 2000	5	0.235	36.659
1	Windows 98	5	0.196	37.992
1	Windows XP	5	0.243	38.233
2	Linux	5	0.232	23.45
2	Windows 2000	5	0.197	25.92
2	Windows 98	5	0.212	22.53
2	Windows XP	5	0.215	22.48

Table 3. Results of LSNRP test

In all tests, the roaming service registration form is successfully returned on the roaming host. It is observed that the roaming server replies to all DNS request of "roamingip.local" in less than 0.3 ms. The reply from LSNRP server is one order of magnitude faster than the negative reply from the DNS servers. It is also observed that an ICMP message of "port not reachable" is sent from the PC to the DNS server after the negative DNS reply because the DNS client in the PC closes the UDP port after receiving the reply from the roaming server. Hence the negative DNS reply is discarded. It is concluded that LSNRP is effective.

7.3 Performance of packet delivery service

The test bed for packet delivery service is shown in figure 33. Two PCs running Linux are Roaming Servers (GRS and HRS). An implementation of Roaming IP runs in the

roaming servers. GRS and HRS are in LAN 1 and 2 respectively. The roaming host RH is connected to LAN 1. The correspondent host CH is in LAN 2. LAN 1 and 2 are connected via a router. The IP addresses of all nodes are listed in the following table.

Node	IP address	Subnet mask
CH	192.168.2.101	255.255.255.0
GRS	192.168.1.10	255.255.255.0
HRS	192.168.2.10	255.255.255.0
CH	192.168.2.30	255.255.255.0

Table 4. IP addresses for packet delivery test

In the test, the performance of roaming IP packet delivery is evaluated by the measurement of throughput and delay. As shown in figure 33, the traffic of two different paths: RH-router-CH (dashed line) and RH-GRS-router-HRS-CH (solid line) are measured.

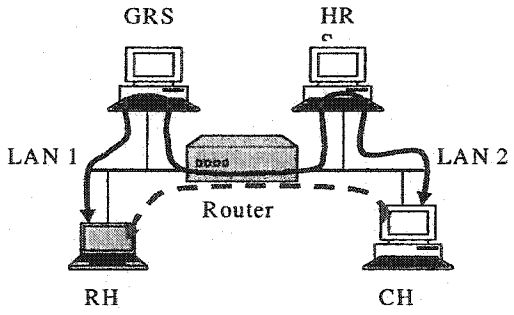


Figure 33 Performance of packet delivery

To make the traffic follows the second path, the roaming IP service is setup for the RH. In the test setup, the service registration is bypassed because the purpose of the test is to evaluate the packet delivery. RH is put into the configuration file of HRS and GRS. In RH, the default gateway is set to GRS. RH sends all packets destined to CH to the MAC address of its default gateway GRS. The packets are tunneled to HRS and eventually delivered to CH.

7.3.1 Delay of packet delivery service

The ping tool is used to measure the delay of packet delivery. Different sizes of messages are sent between CH and RH. In each test, 100 packets are sent between CH and RH. The average delays are presented in table 5. For each column, the IP packet size, the delay of the direct connection, the delay of roaming service and the delta are listed from top to bottom. The curves of the delays and the delta against the packet size are depicted in figure 34.

	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7
IP packet size (bytes)	84	428	828	1228	1428	1628	2028
Direct delay (ms)	0.787	1.781	2.867	3.957	4.525	4.938	5.766
Roam delay (ms)	1.917	3.517	3.321	4.646	6.09	6.572	7.024
Delta (ms)	1.13	1.736	0.454	0.689	1.565	1.634	1.258

Table 5. Delay of packet delivery

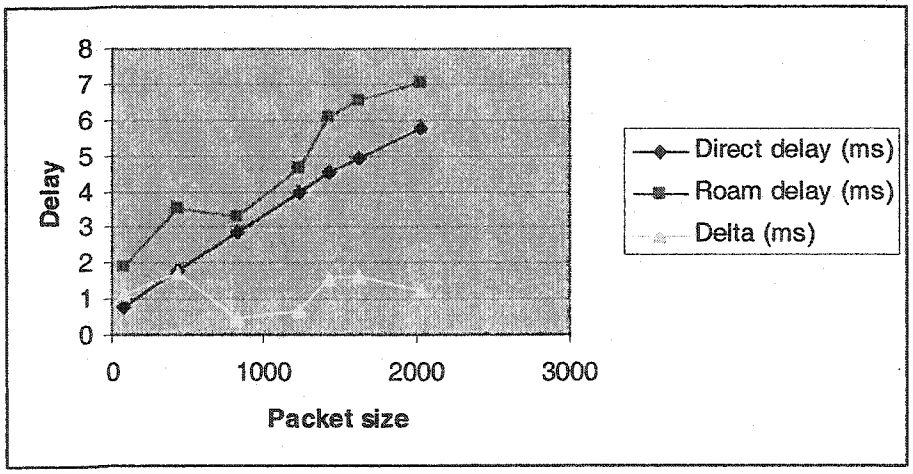


Figure 34 Delay of roaming service

In average, the roaming service introduces a delay of less than 2 ms which is insignificant to the IP packet delivery, given the fact that the round trip delays between 2 Internet hosts are normally in the range of tens to hundreds of ms. The delay of the packet delivery service is composed of the packet processing time and the packet delivery time between

two roaming servers. In the Internet, the delay of roaming service would be greater because more intermediate routers exist between roaming servers, which makes the delivery delay greater.

7.3.2 Throughput of packet delivery

TTCP (Test TCP)[70][71] is used to measure the throughput between CH and RH. In TTCP, the user can select the size of the IP buffer and the number of the buffers to send. During the test, the number of buffers to send is 10,000 and the buffer size of TTCP varies from 100 to 2000 bytes. All performance results are listed in table 6. For each column of the table, the buffer size, the throughput of the direction connection, the throughput of the roaming service and the delta are listed from top to bottom. At the end of the table, the averages are provided.

Buffer (Bytes)	100	200	300	400	500	600	700	800
Direct (KB/s)	1085.9	1087.5	1085.27	1091.3	1081.7	1083.9	1084.4	1084.5
Roam (KB/s)	1038	1027.5	1037.27	1015.9	1056.8	1066.1	1090.3	997.75
Delta (KB/s)	47.81	60.03	48	75.36	24.96	17.83	-5.9	86.71

Buffer (Bytes)	900	1000	1100	1200	1300	1400	1500	1600
Direct (KB/s)	1085	1084.6	1082.77	1083.1	1083.1	1081.9	1082.1	1084.1
Roam (KB/s)	1025.9	1041.5	1060.48	1081.1	1077.7	1088.1	1070.4	1070.1
Delta (KB/s)	59.15	43.08	22.29	2.01	5.39	-6.18	11.68	13.92

Buffer (Bytes)	1700	1800	1900	2000	**Average**
Direct (KB/s)	1083.8	1082.5	1083.17	1082.5	**1084.15**
Roam (KB/s)	1061.3	1072.2	1068.01	1077.7	**1056.2**
Delta (KB/s)	22.48	10.29	15.16	4.81	**27.944**

Table 6. TCP throughput

The throughput data is also plotted against the buffer size as in figure 35. In average, the throughput of roaming service is slightly lower than the direct connection and the variation of roaming service throughput is greater with different buffer size.

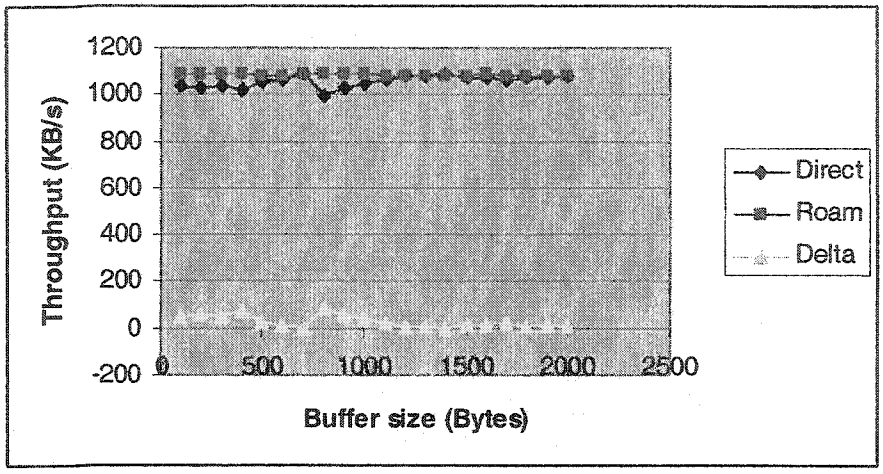


Figure 35 Chart of TCP throughput

7.4 Performance of handoff

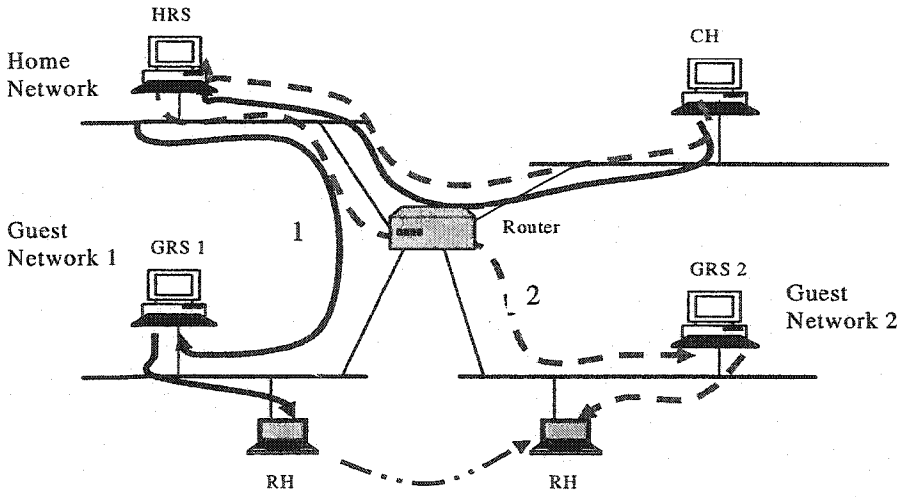


Figure 36 Handoff performance

In this experiment, the service disruption caused by a handoff is evaluated. The test bed is set up as in figure 36. There are three subnets connected by a router: Home Network, Guest Network 1 and Guest Network 2. The roaming host RH registers for roaming IP service in Guest Network 1. A correspondent host CH starts a communication session with RH. Maintaining the communication session, RH roams from Guest Network 1 to 2. GRS1, GRS2 and HRS do a handoff for RH. The traffic follows path 1 (the solid line) initially. After a handoff, the traffic traverses path 2 (the dashed line). In the test, TTCP is

used to generate traffic and Tcpdump is used for capturing the traffic. The test result is presented in figure 37 and table 7.

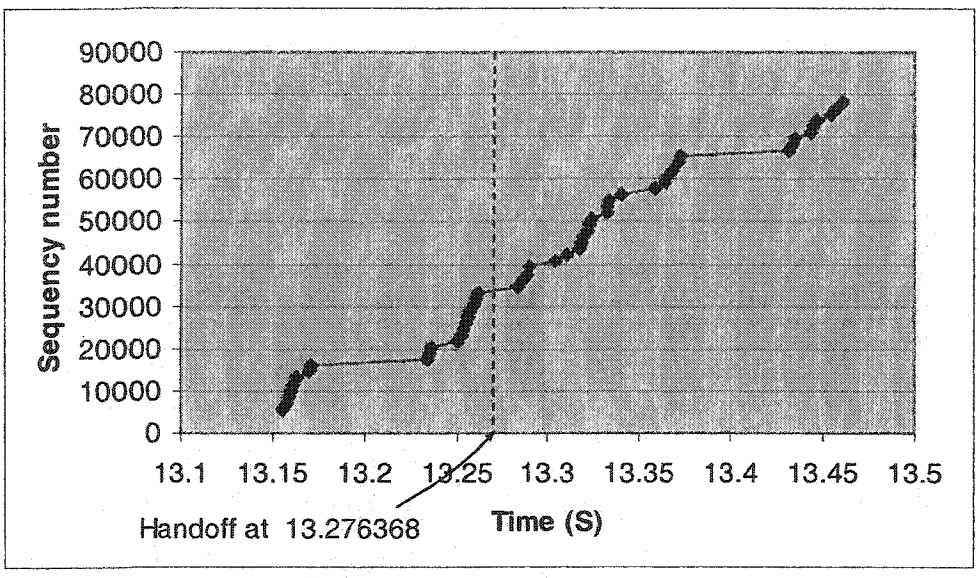


Figure 37 Handoff chart

In Figure 37, the Y axis is the sequence number of IP packets that are delivered to the roaming host and the X axis is the time that elapses since the beginning of the test. A handoff happened at time of 13.276368 second. The curve does not stay flat after the handoff, which indicates that there is not packet lost or retransmission of packets.

	1	2	3	4	5	6	7	8
Time (s)	13.25745	13.25875	13.26012	13.26142	13.28357	13.28498	13.28895	13.29014
Sequence number	28960	30408	31856	33304	34752	36200	37648	39096
Delta		1448	1448	1448	1448	1448	1448	1448

Table 7. Packet sequence number of handoff

In table 7, the sequence number and time of delivery are listed for packets around the handoff period. The handoff happened between packet 4 and 5. The sequence number increases 1448 from packet 4 to 5, the same as the rest of packets. This indicates that there is no packet lost during the handoff. Furthermore, the delay that caused by the handoff is smaller than the TCP retransmission timeout. This confirms the analysis in chapter 4.

Chapter 8 Summary and Conclusions

In this thesis, the requirements of mobile networking are discussed. Based on an analysis of packet delivery in IPv4, it is concluded that traditional IPv4 can not provide mobile networking service. The fundamental requirement of IP roaming to the network layer is to provide reachability of a mobile host in the network. Surveys of existing proposals of mobile IP networking service are presented with advantages and limitations of each proposal. Among the existing proposals, Mobile IP is the preferable solution for mobile networking. However, none of the existing proposal provides transparent service for mobile networking. A new solution Roaming IP is proposed in this thesis to satisfy the transparency requirement. Roaming IP has the following advantages compared to Mobile IP.

- Roaming IP provides complete transparency to roaming hosts
- Roaming IP keeps the complexity in fixed nodes instead of the mobile hosts.
- Roaming IP is applicable for both semi-mobile and full-mobile hosts
- Roaming IP provides fast and smooth handoff

A few novel ideas are adopted to define Roaming IP solution. They are:

- Roaming ARP for packet attraction
- Roaming ping for locating roaming hosts
- LSNRP
- Roaming host movement detection
- RS-RS protocol
- Two-phase service switchover
- Using directory service for Roaming IP management

The effectiveness of Roaming IP protocols is analyzed in the thesis and it is concluded that Roaming IP is an effective solution to provide mobile networking service with IPv4.

Furthermore, analysis is carried out for the handoff performance and it is concluded that Roaming IP provides a fast and smooth handoff service.

This thesis also presents an architecture and implementation of Roaming IP. With the implementation, the effectiveness of the protocols is validated. Performance of packet delivery and handoff is evaluated and is deemed to satisfy requirements of mobile networking. In conclusion, Roaming IP is a viable solution to provide transparent mobile networking service.

The areas of future research are:

- To provide QoS in packet delivery. The proposal in this thesis provides only best effort service
- To provide support of multicast
- To provide a redundancy solution
- To provide a solution for route optimization. Like Mobile IP, the packet forwarding in Roaming IP follows a sub-optimal route. Route optimizations are required to improve the efficiency of packet forwarding

References

[1] http://www.isc.org/

[2] IDC http://www.idc.com

[3] W. Richard Stevens, "TCP/IP Illustrated, Volume 1, the protocol", Addison Wesley, 1994

[4] Postel, J., Editor, "Internet Protocol", STD 5, RFC 791, September 1981.

[5] Postel, J., "DoD standard Transmission Control Protocol", RFC 761, Jan-01-1980.

[6] Postel, J., "Multi-LAN Address Resolution", RFC 925, October 1984.

[7] Postel, J., "Internet Control Message Protocol", RFC 0792, Sep-01-1981.

[8] W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[9] Hedrick, C., "Routing Information Protocol", STD 34, RFC 1058, Rutgers University, June 1988.

[10] Moy, J., "OSPF Version 2", RFC 1247, July 1991.

[11] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[12] Mockapetris, P., "Domain Names - Implementation and Specification", STD 13, RFC 1035, November 1987.

[13] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, Bucknell University, March 1997

[14] Vixie (Ed.), P., Thomson, S., Rekhter, Y. and J. Bound, "Dynamic Updates in the Domain Name System", RFC 2136, April 1997.

[15] B. Wellington. "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

[16] Alex C. Snoeren , Hari Balakrishnan, "An end-to-end approach to host mobility", Proceedings of the sixth annual international conference on Mobile computing and networking, 2000 , Boston, Massachusetts, United States, Pages: 155 – 166

[17] Perkins, C.E. "Simplified routing for mobile computers using TCP/IP", Wireless LAN Implementation, 1992. Proceedings., IEEE Conference on , 1992, Page(s): 7 -13

[18] F. Teraoka, M.Tokoro. "VIP: Host Migration Transparency in IP Networks: The VIP approach", Computer Communication Review, Vol.23, No.1, Jan 1993

[19] Fumio Teraoka , Yasuhiko Yokore , Mario Tokoro, "A Network Architecture Providing Host Migration Transparency", ACM SIGCOMM Computer Communication Review , Proceedings of the conference on Communications architecture & protocols August 1991, Volume 21, Issue 4

[20] Fumio Teraoka , Keisuke Uehara , Hideki Sunahara , Jun Murai, "VIP: A protocol Providing Host mobility", Communications of the ACM August 1994 Volume 37 Issue 8

[21] Perkins, C.E.; Bhagwat, P., "A mobile networking system based on Internet protocol", IEEE Personal Communications , Volume: 1 Issue: 1 , 1st Qtr. 1994, Page(s): 32 -41

[22] Bhagwat, P.; Perkins, C.; Tripathi, S., "Network layer mobility: an architecture and survey", IEEE Personal Communications , Volume: 3 Issue: 3 , June 1996, Page(s): 54 -64

[23] Perkins, C., Editor, "IP Mobility Support", RFC 2002, October 1996.

[24] C. Perkins. "IP Encapsulation within IP". RFC 2003, October 1996.

[25] C. Perkins. "Minimal Encapsulation within IP". RFC 2004, October 1996.

[26] Perkins, C.E.; Jagannadh, T., "DHCP for mobile networking with TCP/IP", Computers and Communications, 1995. Proceedings., IEEE Symposium on , 1995 Page(s): 255 –261

[27] JinHo Ahn; ChongSun Hwang, "Efficient fault-tolerant protocol for mobility agents in mobile IP", Parallel and Distributed Processing Symposium., Proceedings 15th International , 2001, Page(s): 1273 –1280

[28] Chikarmane, V.; Bunt, R.; Williamson, C., "Mobile IP-based multicast as a service for mobile hosts", Services in Distributed and Networked Environments, 1995., Second International Workshop on , 1995, Page(s): 11 –18

[29] Lin, C.R.; Kai-Min Wang, "Mobile multicast support in IP networks", INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, Volume: 3, 2000, Page(s): 1664 - 1672 vol.3

[30] Gossain, H.; Agrawal, D.P., "A differential service based approach to deliver multicast messages over mobile IP", Vehicular Technology Conference, 2001. VTC 2001 spring. IEEE VTS 53rd, 2001, Page(s): 2182 -2186 vol.3

[31] Fikouras, N.A.; El Malki, K.; Cvetkovic, S.R.; Kraner, M., "Performance analysis of Mobile IP handoffs", Microwave Conference, 1999 Asia Pacific, 1999, Page(s): 770 -773 vol.3

[32] Ihara, T.; Ohnishi, H.; Takagi, Y., "Mobile IP route optimization method for a carrier-scale IP network", Engineering of Complex Computer Systems, 2000. ICECCS 2000. Proceedings. Sixth IEEE International Conference on, 2000, Page(s): 120 –121

[33] Qiang Gao; Acampora, A., "A virtual home agent based route optimization for mobile IP", Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE, Volume: 2, 2000, Page(s): 592 -596 vol.2

[34] Jyh-Cheng Chen; Agrawal, P., "Fast link layer and intra-domain handoffs for mobile Internet", Computer Software and Applications Conference, 2000. COMPSAC 2000. The 24th Annual International, 2000, Page(s): 325 –330

[35] Jae-Woo Kwon; Hee-Dong Park; You-Ze Cho, "An efficient TCP mechanism for Mobile IP handoffs", Electrical and Electronic Technology, 2001. TENCON. Proceedings of IEEE Region 10 International Conference on, Volume: 1, 2001, Page(s): 278 -281 vol.1

[36] Woo, W.; Leung, V.C.M., "Handoff enhancement in mobile-IP environment", Universal Personal Communications, 1996. Record. 1996 5th IEEE International Conference on, Volume: 2, 1996
Page(s): 760 -764 vol.2

[37] Ye Min-hua; Wang Zhe-wei; Zhang Hui-min; Liu Yu, "Performance analysis of TCP/UDP during Mobile IP handoffs", Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences on, Volume: 2, 2001, Page(s): 724 -729 vol.2

[38] Fikouras, N.A.; El Malki, K.; Cvetkovic, S.R.; Smythe, C., "Performance of TCP and UDP during mobile IP handoffs in single-agent subnetworks", Wireless Communications and Networking Conference, 1999. WCNC. 1999 IEEE, 1999, Page(s): 1258 -1262 vol.3

[39] Stephane, A.; Mihailovic, A.; Aghvami, A.H., "Mechanisms and hierarchical topology for fast handover in wireless IP networks", IEEE Communications Magazine, Volume: 38 Issue: 11, Nov. 2000, Page(s): 112 –115

[40] Perkins, C.E.; Kuang-Yeh Wang, "Optimized smooth handoffs in Mobile IP", Computers and Communications, 1999. Proceedings. IEEE International Symposium on, 1999, Page(s): 340 –346

[41] Jon Chiung-shien Wu, "Intelligent handoff for Mobile Wireless Internet", Mobile Networks and Applications 6, 67-79, 2001

[42] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[43] Baatz, S.; Frank, M.; Gopffarth, R.; Kassatkine, D.; Martini, P.; Schetelig, M.; Vilavaara, A , "Handoff support for mobility with IP over Bluetooth.", Local Computer Networks, 2000. LCN 2000. Proceedings. 25th Annual IEEE Conference on , 2000, Page(s): 143 -154

[44] http://www.perl.org/

[45] http://www.cgi.org

[46] Hanks, S., Li, T., Farinacci, D. and P. Traina, "Generic Routing Encapsulation", RFC 1701, October 1994.

[47] Hanks, S., Li, T., Farinacci, D. and P. Traina, "Generic Routing Encapsulation over IPv4 networks", RFC 1702, October 1994.

[48] Rosen, E., Callon, R. and A. Vishwanathan, "Multi-Protocol Label Switching Architecture", RFC 3031, January 2001.

[49] Andersson, L., Doolan, P., Feldman, N., Fredette, A. and R. Thomas, "Label Distribution Protocol", RFC 3036, January 2001.

[50] J.C. Mogul, S.E. Deering., "Path MTU discovery", RFC 1191. Nov-01-1990.

[51] W.Stevens. TCP Slow Start, Congestion Avoidance, Fast Retransmission, and Fast Recovery Algorithms. Network Working Group, RFC 2001, Jan 1997

[52] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.

[53] Plummer, D., "An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Addresses for Transmission on Ethernet Hardware", STD 37, RFC 826, November 1982.

[54] Bhagwat, P.; Perkins, C.; Tripathi, S. "Network layer mobility: an architecture and survey ", IEEE Personal Communications, Volume: 3 Issue: 3, June 1996, Page(s): 54 –64

[55] Perkins C., "Mobile IP, Design Principles and Practices" Addison Wesley, 1998

[56] "TCP Congestion Control," RFC2581, April 1999.

[57] "TCP Slow start, congestion avoidance, fast recovery algorithms", RFC 2001, Jan 1997

[58] R. Droms. "Dynamic Host Configuration Protocol". RFC 1541, October 1993.

[59] J. Moy. "OSPF Version 2". RFC 1583, March 1994.

[60] P. Mockapetris, RFC 882, DOMAIN NAMES - CONCEPTS and FACILITIES, , November 1983

[61] The SLAPD and SLURPD Administrator's guide

[62] Lightweight Directory Access Protocol (V2) RFC 1777

[63] Lightweight Directory Access Protocol (V3) RFC 2251

[64] Heninz Johner, Larry Brown, Franz-Stefan Hinner, Wofgan Reis, Johan Westman, "Understanding LDAP", http://www.redbooks.ibm.com.

[65] T. Howes, M. Smith., "The LDAP Application Program Interface", RFC 1823, August 1995.

[66] http://www.tcpdump.org

[67] http://www.packetfactory.net

[68] http://www.apache.org

[69] http://www.boutell.com/cgic/

[70] http://ftp.arl.mil/~mike/ttcp.html

[71] http://www.pcausa.com/Utilities/pcattcp.htm

[72] http://www.openldap.org

[73] Reynolds, J., and J. Postel, "Assigned Numbers", STD 2, RFC 1700, USC/Information Sciences Institute, October 1994.

[74] Dell'Abate, M.; De Marco, M.; Trecordi, V. "Performance evaluation of Mobile IP protocols in a wireless environment ", Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on , Volume: 3 , 1998, Page(s): 1810 -1816 vol.3

[75] Ramón Cáceres , Venkata N. Padmanabhan, "Fast and scalable wireless handoffs in supports of mobile Internet audio", Mobile Networks and Applications December 1998, Volume 3 Issue 4

[76] Cheng Lin Tan , Kin Mun Lye , "A Fast Handoff Scheme for Wireless Networks" Stephen Pink, Proceedings of the second ACM international workshop on Wireless mobile multimedia August 1999

[77] Ye Min-hua; Wang Zhe-wei; Zhang Hui-min; Liu Yu "Performance Analysis of TCP/UDP during mobile IP handoff" Info-tech and Info-net, 2001. Proceedings. ICII 2001 - Beijing. 2001 International Conferences on , Volume: 2 , 2001, Page(s): 724 -729 vol.2

[78] Anne Fladenmuller , Ranil De Silva, "The effect of mobile IP handoffs on the performance of TCP", Mobile Networks and Applications, May 1999, Volume 4 Issue 2

[79] Yang, C.S.; Liu, C.Y.; Chen, J.H.; Sung, C.Y. "Design and implementation of secure Web-based LDAP management system", Information Networking, 2001. Proceedings. 15th International Conference on , 2001, Page(s): 259 -264

[80] http://www.columbia.edu/itc/ee/e6951/2002spring/ClassPresentation/Group7_fast handoff.pdf

[81] Braden, R., and J. Postel, "Requirements for Internet Gateways", RFC 1009, USC/Information Sciences Institute, June 1987.

[82] Wright, G. and W. Stevens, "TCP/IP Illustrated, Volume 2: The Implementation", Addison-Wesley, 1995