# 國 立 交 通 大 學

## 電機資訊學院 資訊學程

## 碩 士 論 文

閘道式行動網路之路由最佳化

A Gateway-based Mobile IP with Route Optimization

研 究 生：江 和 俊
指導教授：簡 榮 宏 教授

中 華 民 國 九 十 四 年 六 月

# 閘道式行動網路之路由最佳化
# A Gateway-based Mobile IP with Route Optimization

研究生：江和俊　　Student：Ho-Chun Chiang
指導教授：簡榮宏　　Advisor：Rong-Hong Jan

國立交通大學
電機資訊學院 資訊學程
碩士論文

A Thesis
Submitted to Degree Program of Electrical Engineering Computer Science
College of Electrical Engineering and Computer Science
National Chiao Tung University
in Partial Fulfillment of the Requirements
for the Degree of
Master of Science
in

Computer Science

June 2005

Hsinchu, Taiwan, Republic of China

中華民國九十四年六月

# 國立交通大學

## 博碩士論文全文電子檔著作權授權書

（提供授權人裝訂於紙本論文書名頁之次頁用）

本授權書所授權之學位論文，為本人於國立交通大學 電 機 資 訊 學院 資 訊 學程， 九十三 學年度第 二 學期取得碩士學位之論文。

論文題目：閘道式行動網路之路由最佳化

指導教授：簡榮宏 教授

■ 同意 □不同意

本人茲將本著作，以非專屬、無償授權國立交通大學與台灣聯合大學系統圖書館：基於推動讀者間「資源共享、互惠合作」之理念，與回饋社會與學術研究之目的，國立交通大學及台灣聯合大學系統圖書館得不限地域、時間與次數，以紙本、光碟或數位化等各種方法收錄、重製與利用；於著作權法合理使用範圍內，讀者得進行線上檢索、閱覽、下載或列印。

| 論文全文上載網路公開之範圍及時間： | |
|---|---|
| 本校及台灣聯合大學系統區域網路 | ■ 立即公開 |
| 校外網際網路 | ■ 中華民國 95 年 7 月 25 日公開 |

**授權人：江和俊**

**親筆簽名：______________________**

**中華民國九十四年七月二十五日**

# 國立交通大學

## 博碩士紙本論文著作權授權書

(提供授權人裝訂於全文電子檔授權書之次頁用)

本授權書所授權之學位論文，為本人於國立交通大學 電 機 資 訊 學院 資 訊 學程， 九十三 學年度第 二 學期取得碩士學位之論文。

論文題目：閘道式行動網路之路由最佳化

指導教授：簡榮宏 教授

■ 同意　□不同意

本人茲將本著作，以非專屬、無償授權國立交通大學，基於推動讀者間「資源共享、互惠合作」之理念，與回饋社會與學術研究之目的，國立交通大學圖書館得以紙本收錄、重製與利用；於著作權法合理使用範圍內，讀者得進行閱覽或列印。

本論文為本人向經濟部智慧局申請專利(未申請者本條款請不予理會)的附件之一，申請文號為：________________，請將論文延至___年___月___日再公開。

**授 權 人：江 和 俊**

**親筆簽名：________________________**

**中 華 民 國 九 十 四 年 七 月 二 十 五 日**

# 國家圖書館

# 博碩士論文電子檔案上網授權書

ID:GT009167565

本授權書所授權之學位論文，為本人於國立交通大學 電 機 資 訊 學院 資 訊 學程， 九十三 學年度第 二 學期取得碩士學位之論文。

論文題目：閘道式行動網路之路由最佳化

指導教授：簡榮宏 教授

茲同意將授權人擁有著作權之上列論文全文（含摘要），非專屬、無償授權國家圖書館，不限地域、時間與次數，以微縮、光碟或其他各種數位化方式將上列論文重製，並得將數位化之上列論文及論文電子檔以上載網路方式，提供讀者基於個人非營利性質之線上檢索、閱覽、下載或列印。

※ 讀者基於非營利性質之線上檢索、閱覽、下載或列印上列論文，應依著作權法相關規定辦理。

**授權人：江和俊**

**親筆簽名：______________________**

**中華民國九十四年七月二十五日**

1. 本授權書請以黑筆撰寫，並列印二份，其中一份影印裝訂於附錄三之二(博碩士紙本論文著作權授權書)之次頁；另一份於辦理離校時繳交給系所助理，由圖書館彙總寄交國家圖書館。

# 國立交通大學

## 論文口試委員會審定書

本校 電機資訊學院專班 資訊 組 江和俊 君

所提論文:

（中文）閘道式行動網路之路由最佳化

（英文）A Gateway-based Mobile IP with Route Optimization

合於碩士資格水準、業經本委員會評審認可。

口試委員：

王國禎

指導教授：

班 主 任： 郭仁財

中華民國九十四年六月十日

# 閘道式行動網路之路由最佳化

學生：江和俊　　　　指導教授：簡榮宏 教授

國立交通大學電機資訊學院 資訊學程（研究所）碩士班

## 摘要

行動網路在漫遊過程中至今仍有許多限制，如：三角繞徑、換手延遲及封包遺失等問題。本篇論文將著重在路由最佳化的探討，並提出一個可行方案來解決行動網路中三角繞徑的問題。除了行動網路中的戶籍地代理站、外籍地代理站、行動主機及對應節點外，本方案將新增一個功能實體叫做快取代理站。快取代理站本身是一個網路閘道器，並在行動網路中擔任行動代理站的角色，用以支援行動主機及對應節點之間的路由最佳化。在此架構下，所有的對應節點並不需要修改其作業系統的核心部份也不需要額外安裝行動軟體以支援路由最佳化。藉由部署快取代理站，本方案可以避免三角繞徑問題的發生，並且可以明顯的改善行動主機及對應節點之間的傳輸效能。

關鍵字：路由最佳化、三角繞徑、行動網路

# A Gateway-based Mobile IP with Route Optimization

Student：Ho-Chun Chiang　　　　　　　Advisor：Prof. Rong-Hong Jan

Degree Program of Electrical Engineering Computer Science
National Chiao Tung University

## ABSTRACT

Mobile IP has some limitations due to triangle routing, handoff latency, and packet lost during handoff process. In this thesis, we will focus on the route optimization and propose an approach to solve the triangle routing problem in Mobile IP network. In addition to home agent, foreign agent, mobile node, and correspondent node, we add a new functional entity, called Cache Agent (CA), to our approach. The CA is a gateway and functions as a mobility agent in the correspondent network to support route optimization between mobile node and correspondent node. In this architecture, all correspondent nodes do not require installing any mobility software to support route optimization. By deploying CAs in the network, the triangle routing problem can be eliminated and the throughput between mobile node and correspondent node can be improved.

**Keyword**: Route Optimization, Triangle Routing, Mobile IP

# 誌　　　謝

首先，我要感謝指導教授－簡榮宏教授的指導與鼓勵，讓我在論文的研究及問題的解決上獲得寶貴的經驗及建議。沒有簡榮宏教授的細心指導，這篇論文是無法順利完成。同時要感謝此次的口試委員王國禎教授、曾煜棋教授及王家祥教授對本篇論文所提的指正及建議。

其次，我要感謝父母親及親友的關心；尤其是要感謝妻子惠卿在這段期間給予我最大的支持與鼓勵，讓我在家庭、事業及學業上無後顧之憂。在人生的旅途上她無怨無悔地陪伴著我，分享我每一分喜悅，陪我渡過每一次低潮，並一起與我經歷一次又一次的難關。

最後，僅將這份榮耀與喜悅，獻給我最親愛的妻子與家人及最敬愛的師長們，感謝他們長久以來的支持與關心。

# Contents

# List of Tables

# List of Figures

1896

# Abbreviations

The abbreviations used in this thesis are listed below.

| | |
|---|---|
| IP: | Internet Protocol |
| ICMP: | Internet Control Message Protocol |
| TCP: | Transmission Control Protocol |
| UDP: | User Datagram Protocol |
| ARP: | Address Resolution Protocol |
| RFC: | Request for Comments |
| MIP: | Mobile IP |
| HA: | Home Agent |
| FA: | Foreign Agent |
| CA: | Cache Agent |
| MN: | Mobile Node |
| CN: | Correspondent Node |
| MA: | Mobility Agent |
| CoA: | Care-of-Address |
| BU: | Binding Update |
| BW: | Binding Warning |
| BA: | Binding Acknowledge |

| | |
|---|---|
| GRE: | Generic Routing Encapsulation |
| IPIP: | IP Encapsulation within IP |
| HAWAII: | Handoff-Aware Wireless Access Internet Infrastructure |
| CIP: | Cellular IP |
| SIP: | Session Initiation Protocol |
| TTL: | Time To Live |
| ACK: | Acknowledgement |
| OSI: | Open System Interconnection |
| AAA: | Authentication, Authorization, and Accounting |
| NAT: | Network Address Translation |
| DHCP: | Dynamic Host Configuration Protocol |
| LAN: | Local Area Network |
| WAN: | Wide Area Network |
| SPI: | Security Parameters Index |
| gwMIP-RO: | Gateway-based Mobile IP with Route Optimization |

# Chapter 1

# Introduction

Moving while your mobile computing device is connected to Internet is becoming important to the mobile user of nowadays. Internet Protocol (IP) [1] is widely used to connect to Internet. But it is not designed for mobile networking due to IP routes packets to destination according to a fixed IP address. There are some issues must be addressed before mobile computing devices can seamless roam to another network. Those issues include fast handoff, packet loss, triangle routing, security issue, authentication issue, transmission latency, and etc.

There are several protocols that support mobility functionality, such as Cellular IP [2], HAWAII [3], Mobile IP [4], and SIP protocol [5]. Among these protocols, the Mobile IP is a good choice to provide macro mobility to support user roaming from one network to another network. Mobile IP maintains connections and provides a transparent access to mobile user's home network when the mobile user is roaming to another network. The triangle routing is a main issue in Mobile IP and route optimization solves the triangle routing in the Mobile IP network.

In this thesis, we propose an approach called Gateway-based Mobile IP to provide route optimization by adding a new entity called cache agent (CA) to the Mobile IP network. This approach not only addresses triangle routing problem, but also improves the throughput between mobile nodes and correspondent nodes. In this architecture, mobile node receives packets faster than basic Mobile IP during mobile node resides in foreign network. And there is no need of installing any mobility software into correspondent nodes; it just installs the mobility software into CAs in the Mobile IP network. To deploy this approach is easier than route optimization in the Mobile IP network.

We modify the HUT Dynamic Mobile IP software [6] to implement the necessary functionalities in the Gateway-based Mobile IP; the most functionality in this approach is almost like the functionalities in Route Optimization in Mobile IP [7]. And we compare the performance between basic Mobile IP and Gateway-based Mobile IP under different network conditions.

The remaining chapters of the thesis are organized as follows: chapter 2 gives an explanation of background and related work; chapter 3 proposes an approach of route optimization; chapter 4 contains details of implementation and evaluation; finally, conclusions and possible future work are discussed in chapter 5.

# Chapter 2

# Background and Related Work

Mobile IP is a mechanism for maintaining transparent network connectivity to mobile nodes. It enables a mobile node to be addressed by the IP address that it uses in its home network, regardless of the network to which it is currently physically attached. Therefore, ongoing network connections to a mobile host can be maintained even as the mobile node is moving from one network to the other network.

To support mobility on the Internet under the existing protocol suite, we are faced with two mutually conflicting requirements: one is a mobile node has to change its IP address whenever it changes its point of attachment, so that packets destined to the node are routed correctly; the other one is to maintain existing TCP connections, the mobile node has to keep its IP address as same IP address before. It is obvious that changing the IP address will cause the connection to be disrupted and lost.

Mobile IP is designed to solve the problem by allowing each mobile node to have two IP addresses and by transparently maintaining the binding between the two addresses. One of the IP addresses is the permanent home address that is assigned at the home network and is used to identify communication endpoints. The other one is a temporary care-of address [4] that represents the current location of the mobile node. The main goals of Mobile IP are to make mobility transparent to the higher level protocols and to make minimum changes to the existing Internet infrastructure.

The following sections describe the mobility management, the functional entities in the Mobile IP, the control messages that are used in Mobile IP, the operation of Mobile IP, and the known problems that existing in Mobile IP.

## 2.1 Mobility Management

The mobility management contains two components: location management [8] and handoff management [8]. The location management enables the network to discover the current location of the mobile node. It involves database architecture design and the transmission of signaling messages between various components of a signaling network. The handoff management enables the network to maintain a user's connection as the mobile node continues to move and change its location. In handoff management, on-going calls are modified under two conditions: signal strength deterioration [8] and user mobility [8].

From OSI network layer viewpoint, there are three types of mobility management: link layer mobility [9], network layer mobility [9], and application layer mobility [9]. Soft radio handoff [9] is an approach of the link layer mobility. Link layer mobility is limited to a single subnet, which limits its applicability to large-scale user mobility. Mobile IP, Cellular IP, and HAWAII are the approaches of the network layer mobility. SIP is an approach of the application layer mobility.

From mobility coverage viewpoint, there are two types of mobility management: one is macro mobility management [9] such as Mobile IP, and the other one is micro mobility management [9] such as Cellular IP, HAWAII, and Hierarchical MIP [10].

HAWAII is a domain-based approach for supporting mobility; it uses specialized path setup schemes which install host-based forwarding entries in specific routers to support intra-domain micro-mobility. These path setup schemes deliver excellent performance by reducing mobility related disruption to user applications [11]. Cellular IP is an Internet host mobility protocol that is optimized to provide access to a Mobile IP enabled Internet in support of fast roaming mobile nodes. SIP is designed to support real-time communication in a more efficient way. But SIP-based mobility is less suitable for TCP-based applications. It uses a combination of DHCP and AAA protocol [12] to support subnet and domain handoff.

## 2.2 Functional Entities in Mobile IP

The Mobile IP architecture introduces three functional entities: home agent, foreign agent, and mobile node [4]. In following sub-sections, we describe the behavior of these three functional entities and correspondent node [4].

### 2.2.1 Home Agent

A home agent is an IP router on a mobile node’s home network which maintains current location information for the mobile node and tunnels datagrams for delivery to the mobile node when it moves away from home network.

A home agent's main responsibility is generally to process and coordinate mobility services. The home agent receives registration requests, responds with a registration reply message, encapsulates the datagrams that addressed to its mobile node, and routes the encapsulated datagram to the mobile node’s care-of address.

### 2.2.2 Foreign Agent

A foreign agent is an IP router on a mobile node's visited network which provides routing services to the mobile node while registered with the home agent. The foreign agent decapsulates and delivers datagrams to the mobile node that were tunneled by the mobile node's home agent. For datagrams sent by a mobile node, the foreign agent may serve as a default router for registered mobile nodes.

A foreign agent's main responsibility is generally to relay a registration request and registration reply between the home agent and the mobile node and to decapsulate the encapsulated datagram for delivery to the mobile node. For transmitted datagrams, the foreign agent is generally as a default router to the mobile node.

### 2.2.3 Mobile Node

Mobile node is a host that changes its point of attachment from one network to another network. The mobile node may change its location without changing its IP address assigned in the home network’s address space; it may continue to communicate with other Internet hosts at any location by using its home IP address, assuming link-layer connectivity to a point of attachment is available.

A mobile node's main responsibility is generally to listen for agent advertisements and initiate the registration request when a change in its network connectivity is detected. When mobile node moves away from its home network; it registers its current care-of address with its home agent. When mobile node returns to its home network; it sends a registration request with the lifetime set to zero to inform its home agent to erase any previous mobility binding to it.

### 2.2.4 Correspondent Node

A correspondent node is a host that communicates with a mobile node. It can be a mobile node or a stationary node. If the node is mobile, it transmits and receives the packet via its home agent. However, if the node is stationary, it transmits and receives packets via a traditional IP router that has no mobility management capabilities.

## 2.3 Control Messages in Mobile IP

### 2.3.1 Agent Solicitation

The agent solicitation message is used to obtain a care-of-address. It cooperates with agent advertisement message to achieve location detection. An agent solicitation message is identical to an ICMP Router Solicitation [13], except its IP TTL [1] must be set to 1. A mobile node may send an agent solicitation message to a multicast address 224.0.0.11 and all mobility agents should respond to such agent solicitation message. A mobility agent may be configured to send agent advertisements message only in response to an agent solicitation message.

Agent advertisement message and agent solicitation message may not be necessary for link layers that already provide this functionality. No authentication is required for agent advertisement and agent solicitation messages. They may be authenticated using the IP Authentication Header.

Every mobile node must implement agent solicitation message. Solicitations should only be sent in the absence of agent advertisement message and when a care-of address has not been determined through a link-layer protocol or other means. The mobile node uses the same procedures, defaults, and constants for agent solicitation message as specified for ICMP Router Solicitation messages. Table 1 shows the message format of agent solicitation message.

Table 1 Agent Solicitation Message Format

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td>Type = 10</td><td>Code</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="4">Reserve (sent as 0)</td></tr>
</table>

### 2.3.2 Agent Advertisement

Agent advertisement is an extended ICMP route advertisement packet. It is used for a mobile node to decide if it attaches to a new foreign network. Agent advertisements are formed by including a MA advertisement extension in an ICMP Router Advertisement message. The Table 2 shows the message format of agent advertisement message.

Table 2 Agent Advertisement Message Format

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

<table>
<tr><td>Type = 9</td><td>Code = 0 or 16</td><td colspan="2">Checksum</td></tr>
<tr><td>Number of Address</td><td>Address Entry Size</td><td colspan="2">Lifetime</td></tr>
<tr><td colspan="4">Router Address [1]</td></tr>
<tr><td colspan="4">Preference Level [1]</td></tr>
<tr><td colspan="4">. . . . .</td></tr>
<tr><td>Type = 16</td><td>Length</td><td colspan="2">Sequence Number</td></tr>
<tr><td colspan="2">Registration Lifetime</td><td>Flags: RBHFMGrT</td><td>Reserved</td></tr>
<tr><td colspan="4">zero or more Care-of Address …</td></tr>
<tr><td colspan="4">. . . . .</td></tr>
<tr><td colspan="4">Optional Extensions …</td></tr>
</table>

| | |
|---|---|
| Type | 16 |
| Length | (6 + 4*N), where 6 accounts for the number of bytes in the Sequence Number, Registration Lifetime, flags, and reserved fields, and N is the number of care-of addresses advertised. |
| Sequence Number | The count of Agent Advertisement messages sent since the agent was initialized. |
| Registration Lifetime | The longest lifetime (measured in seconds) that this agent is willing to accept in any Registration Request. |
| Care-of Address | The advertised foreign agent care-of addresses provided by this foreign agent. An Agent Advertisement must include at least one care-of address if the 'F' bit is set. The number of care-of addresses present is determined by the Length field in the Extension. |

### 2.3.3 Registration Request

A registration request message contains the up-to-date care-of-address of a mobile node and the required lifetime by a mobile node. It is sent out from a mobile node to a home agent by a UDP packet [14]. It may or may not be forwarded by a foreign agent. Table 3 shows the message format of registration request message.

Table 3 Registration Request Message Format

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type = 1</td><td colspan="8">Flags: SBDMGrTx</td><td colspan="16">Lifetime</td></tr>
<tr><td colspan="32">Home Address</td></tr>
<tr><td colspan="32">Home Agent</td></tr>
<tr><td colspan="32">Care-of Address</td></tr>
<tr><td colspan="32">Identification</td></tr>
<tr><td colspan="32">Optional Extensions …</td></tr>
</table>

Type 1

Lifetime The number of seconds remaining before the registration is considered expired. A value of zero indicates a request for deregistration. A value of 0xffff indicates infinity.

Home Address The IP address of the mobile node.

Home Agent The IP address of the mobile node's home agent.

Care-of Address The IP address for the end of the tunnel.

Identification A 64-bit number, constructed by the mobile node, used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages.

Extensions The fixed portion of the Registration Request is followed by one or more of the Extensions. An authorization-enabling extension must be included in all Registration Requests.

### 2.3.4 Registration Reply

A registration reply message contains the notification whether a registration request is accepted or refused. The lifetime approved by the home agent is included in the message. It is sent out from a home agent to a mobile agent by a UDP packet. It may or may not be forward by a foreign agent. Table 4 shows the message format of registration reply message.

Table 4 Registration Reply Message Format

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
```

| | | |
|---|---|---|
| Type = 3 | Code | Lifetime |
| Home Address | | |
| Home Agent IP Address | | |
| Identification | | |
| Optional Extensions … | | |

Type 3

Code A value indicating the result of the Registration Request.

Lifetime If the Code field indicates that the registration was accepted, the Lifetime field is set to the number of seconds remaining before the registration is considered expired. A value of zero indicates that the mobile node has been deregistered. A value of 0xffff indicates infinity. If the Code field indicates that the registration was denied, the contents of the Lifetime field are unspecified and must be ignored on reception.

Home Address The IP address of the mobile node.

Home Agent The IP address of the mobile node's home agent.

Identification A 64-bit number used for matching Registration Requests with Registration Replies, and for protecting against replay attacks of registration messages.

Extensions The fixed portion of the Registration Reply is followed by one or more of the Extensions. An authorization-enabling extension must be included in all Registration Replies returned by the home agent.

## 2.4 The Operation of Mobile IP

### 2.4.1 Agent Discovery

Mobility agents advertise their presence by periodically broadcasting agent advertisement message. The agent advertisement message was designed as an extension of the ICMP router advertisement message, the message conveys following information: a list of care-of addresses and a flag indicating whether the mobility agent is a home agent or a foreign agent. According to the agent advertisement message, the mobile node has enough information to determine whether it is on the home network or a foreign network. The mobile node may also broadcast an agent solicitation message to obtain an agent advertisement message from a mobility agent immediately. No authentication is required for agent advertisement and agent solicitation messages. They may be authenticated using the IP Authentication Header. The Figure 1 shows the message flow for agent advertisement message in Mobile IP and the Figure 2 shows the message flow for agent solicitation message in Mobile IP.

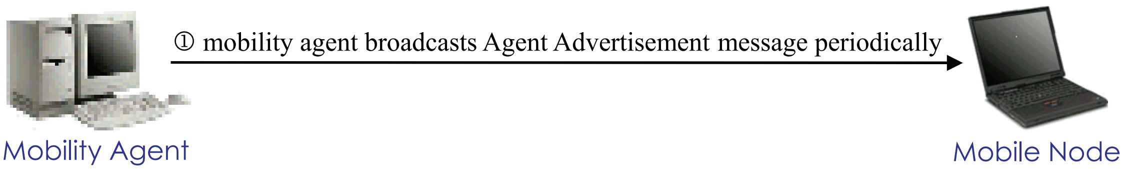

① mobility agent broadcasts Agent Advertisement message periodically
Mobility Agent
Mobile Node

Figure 1　Agent Advertisement in Mobile IP

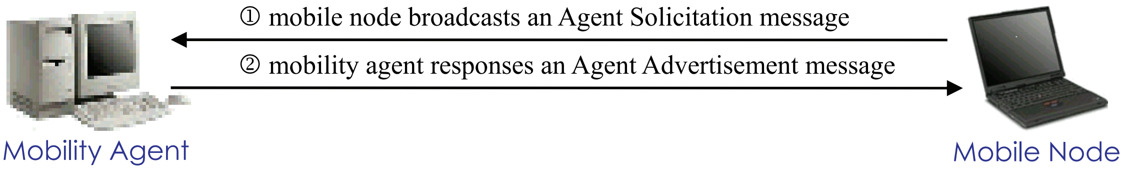

① mobile node broadcasts an Agent Solicitation message
② mobility agent responses an Agent Advertisement message
Mobility Agent
Mobile Node

Figure 2　Agent Solicitation in Mobile IP

### 2.4.2 Registration

As soon as a mobile node gets a new care-of-address, it will register its new care-of-address to its home agent by sending out the registration request message. The registration request message can be sent to the home agent directly or be forwarded by the foreign agent. If the registration request message will be forwarded by foreign agent, the foreign agent will check whether the request meets the registration requirement. If the request does not meet the registration requirement, the foreign agent will send a registration reply message with a rejection code to the mobile node and stops the forwarding. If the request meets the registration requirement, the foreign agent will forward the registration request to the home agent. When a home agent receives the request, it will send a registration reply message back to the mobile node to notify whether it accepts or rejects the request. The lifetime of this registration is included in the reply. It is the responsibility of a mobile node to re-send a registration request to its home agent when the lifetime expires. The Figure 3 shows the registration procedure in Mobile IP.

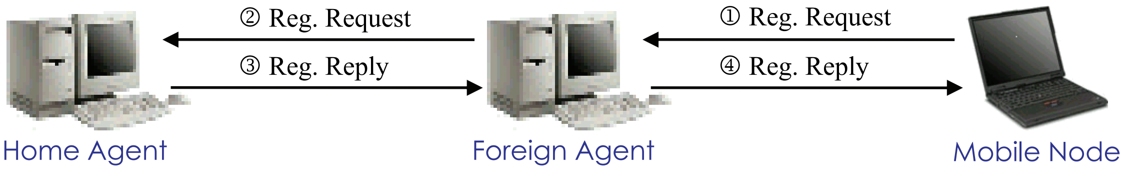


Figure 3 Registration in Mobile IP

### 2.4.3 Datagram Delivery

When a correspondent node wants to communicate with the mobile node that stays in a foreign network, it sends an IP packet addressed to the mobile node's permanent IP address. The home agent intercepts this packet and looks up the location database to find out the mobile node's care-of address. Then home agent constructs a new IP header that contains the mobile node's care-of address as the destination IP address. The original IP packet is put into the payload of this new IP packet. It then sends the packet. This process of encapsulating one IP packet into the payload of another is known as IP-within-IP encapsulation [15], or tunneling. When the encapsulated packet reaches the mobile node's current network, the foreign agent decapsulates the packet and finds out the mobile node's home address. It then looks up the visitor list to see if it has an entry for that mobile node. If there is an entry for the mobile node on the visitor list, the foreign agent relays the original IP packet to the mobile node. When the mobile node wants to send a packet to a correspondent node, it sends the packet to the foreign agent first, and then foreign agent forwards the packet to the correspondent node using normal IP routing. Figure 4 shows the message flow for datagram delivery in Mobile IP.

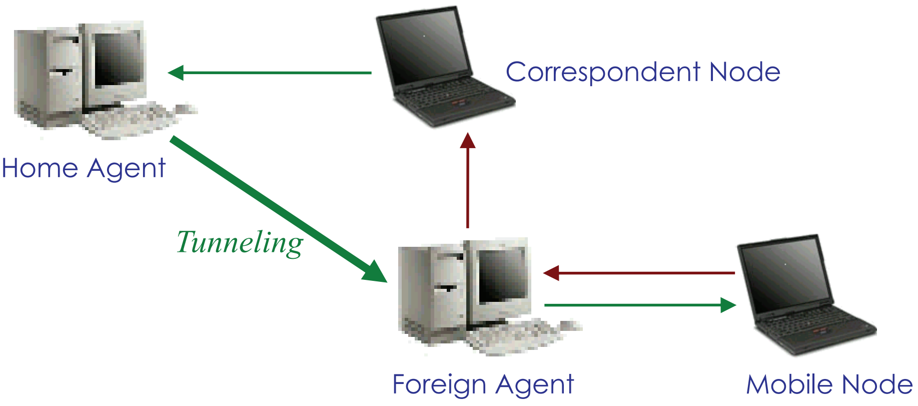


Figure 4 Datagram Delivery in Mobile IP

### 2.4.4 Deregistration

When mobile node returns to its home network, it has to deregister with its home agent by sending a registration request with the lifetime set to zero. The home agent then removes its mobility binding for the mobile node. There is no need to deregister with the foreign agent. Deregistration occurs automatically when lifetime expires. The Figure 5 shows the deregistration procedure in Mobile IP.

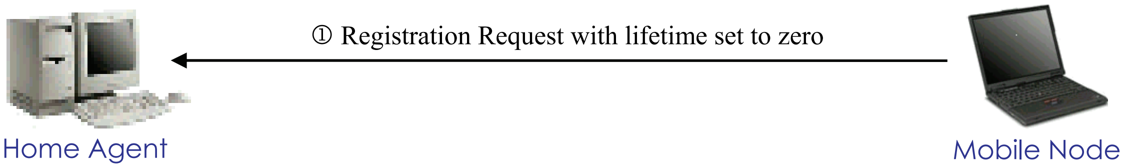


Figure 5 Deregistration in Mobile IP

1896

## 2.5 The Problems in Mobile IP

### 2.5.1 Triangle Routing

In basic Mobile IP, all packets sent to a mobile node have to travel through the home agent first and are then forwarded to the mobile node. This makes an inefficient routing from the correspondent node to the mobile node. This required routing is referred to as triangle routing [16]. A solution to the triangle routing problems would be for the correspondent node to maintain the mobile node's care-of address, and tunnel packets to care-of address directly. The home agent would inform the correspondent node of registration changes. This solution requires changes at the correspondent node and has not been widely deployed. Figure 6 shows the operation of triangle routing in Mobile IP.

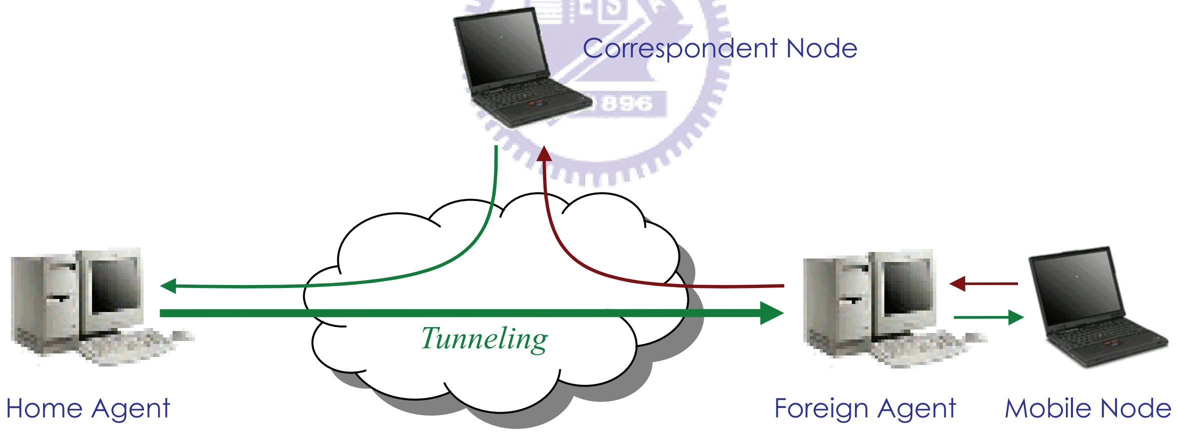


Figure 6 Triangle Routing in Mobile IP

### 2.5.2 Packet Loss

During the time interval that a mobile node leaves its previous foreign network and does not successfully register with its new care-of-address, any packet forwarded by its home agent to its old care-of-address will be lost. The packet loss will degrade the upper layer's performance seriously.

### 2.5.3 Handoff Latency

Mobile IP was not designed for fast moving hosts. The home agent handles all handoffs, although it may be far from the current network of the mobile node. The network delay adds to slow handoffs. Slow handoffs cause often packet loss, which is especially harmful to real-time applications, such as voice over IP or video streaming. TCP-based connections also suffer, since lost packets may be mistaken for congestion and results in TCP’s slow start mechanism [17].

Since the home agent handles handoffs, they cause lots of signaling traffic between the mobile node and the home agent. In high speed LANs this is not an issue, but when low speed WANs are involved and lots of mobile nodes are performing simultaneous handoffs, network congestion may result.

### 2.5.4 Ingress filtering

Many border routers discard packets coming from within the local networks if the packets do not contain a source IP address configured for one of the local networks. The border routers will transmit into the Internet only those packets that have a source IP address representing the local network. Ingress filtering [18] requires the mobile node to reverse-tunnel its transmitted packets back though the home agent.

### 2.5.5 Security issues

Firewalls cause difficulty for Mobile IP because they block all classes of incoming packets that do not meet specified criteria. It presents difficulties for mobile nodes wishing to communicate with other nodes within their home networks. Such communications, originating from the mobile node, carry the mobile node's home address, and would thus be blocked by the firewall.

# Chapter 3

# A Gateway-based Approach for Mobile IP Route Optimization

In this chapter, we propose an approach to demonstrate route optimization is function wok in Gateway-based Mobile IP. The Gateway-based Mobile IP introduces the utilization of the binding cache [7] in CA to eliminate the triangle routing problem. In this architecture, we only need to install new mobility software in CA instead of correspondent nodes to achieve route optimization in Mobile IP network. As we can expect that it is very convenient to deploy this design into the real world.

## 3.1 Design of Route Optimization Requirements

In Mobile IP without Route Optimization, there is need to monitor traffic and forward packets to mobile nodes by home agent. The idea behind the Gateway-based Mobile IP with Route Optimization is that CA caches the location information of mobile nodes into binding cache. A home agent has to monitor the traffic to check whether a CA has a mobile node's current location information. If not, the home agent will utilize the UDP datagram and ICMP message [19], like *traceroute* utility in Linux, to obtain the IP address of CA. At first time, when home agent intercepts a packet from a correspondent node for a mobile node, it tunnels the packet to the mobile node as usual, but also sends a binding update message [7] to the CA telling it of the mobile node's current care-of address. CA uses information from binding update message to create or update a binding entry for the mobile node. After the cache is updated, any packet destined to the mobile node will be tunneled by the CA and sent directly to the mobile node's care-of address without any assistance from the home agent.

### 3.1.1 Cache Agent Considerations

This approach utilizes the CA that install mobility software to instead of correspondent node in Mobile IP network to support route optimization function. Like home agent and foreign agent, the CA listens on the UDP port 434 for any route optimization messages. It encapsulates the IP messages to be sent to the mobile node in another IP header whose destination address is the care-of address. And then the traditional IP routers will be able to route those packets to the care-of address.

The CA may communicate to several mobile nodes at the same time. There are two timers will be used in this approach. The first timer is used to limit the amount of time to wait for the binding update message to come back. And the second timer is the life time of the binding cache entry [20].

### 3.1.2 Home Agent Considerations

The home agent should send a binding update message to the CA in following two situations: the first situation is when home agent receives a binding warning message [7] and the second situation is when home agent receives an IP datagram to be forwarded to the mobile node.

Before home agent sends a binding update message to the CA, it needs to know the IP address of CA. Like *traceroute* utility in Linux, the home agent utilizes the UDP datagram and ICMP message to obtain the IP address of CA. The *traceroute* utility traces the route of an IP packet by sending a UDP probe packet with small TTL. From the output of *traceroute*, home agent can observe the intermediate routers that the UDP packet travels through. Finally home agent gets the IP address of CA.

### 3.1.3 Foreign Agent Considerations

The foreign agent is responsible to create an entry in binding cache at receipt of the binding update message. When mobile node moves from old foreign network to new foreign network, it sends out a registration request message with previous foreign agent notification extension [7] to new foreign agent telling it of the IP address of mobile node’s previous foreign agent. After receiving the request, the new foreign agent sends a binding update message to previous foreign agent and previous foreign agent responses a binding acknowledgment message back to new foreign agent. The new foreign agent will keep sending binding update messages to the previous foreign agent until the new foreign agent receives a binding acknowledgment message [7]. The previous foreign agent should then delete the mobile node's visitor list entry and, if a new care-of address is included in the binding update message, create an entry for the mobile node with its new care-of address. The previous foreign agent may send out a binding warning message to home agent when it receives a packet that destined to mobile node. And then home agent sends a binding update to CA to inform it to modify the mobile node’s binding entry.

When foreign agent receives a packet tunneled from a CA, it will create a tunneling entry for the CA. When foreign agent receives a binding update message with information that mobile node already moving to other network, it will delete the mobile node’s binding entry and delete a tunneling entry for the CAs that associated to the mobile node.

### 3.1.4 Mobile Node Considerations

When mobile node detects it stays in a new foreign network, it may send out a registration request message with previous foreign agent notification extension to new foreign agent. This request implies that mobile node informs new foreign agent to send a binding update message to mobile node's previous foreign agent, to notify it that the mobile node has moved [7]. By attaching previous foreign agent notification extension to registration request message, the mobile node can smooth handoff from old foreign network to new foreign network. The extension includes only those values needed to construct the binding update message that are not already contained in the registration request message.

### 3.1.5 Binding Cache

Binding cache is used to store the care-of address of one or more mobile nodes. In the absence of any binding cache entry, datagrams destined for a mobile node will be routed to the mobile node's home network, and then tunneled to the mobile node's current care-of address by the mobile node's home agent. If the sender has a binding cache entry for the destination mobile node, it may tunnel the datagram directly to the care-of address indicated in the cached mobility binding.

Any node may maintain a binding cache to optimize its own communication with mobile nodes. A node may create or update a binding cache entry for a mobile node only when it has received and authenticated the mobile node's mobility binding. As before, each binding in the binding cache also has an associated lifetime, specified in the binding update message in which the node obtained the binding. After the expiration of this time period, the binding is deleted from the cache.

## 3.2 The Operation of Gateway-based Mobile IP

The operation of Gateway-based Mobile IP is very similar to the operation of Mobile IP with route optimization. When mobile node senses it stays in a visited network, it may send out a registration request message to foreign agent as the registration procedure in basic Mobile IP. The CA does not have mobile node's binding entry in the meanwhile and all the IP packets that destined to mobile node are tunneled by home agent as the tunneling operation in basic Mobile IP. Home agent will monitor the traffic to check whether the packet is destined to mobile node's care-of address or not. If yes, the home agent will utilize the ICMP message and UDP datagram to obtain the IP address of CA, and then sending out a binding update message to CA. The CA will create or update the mobile node's binding entry when it receives a binding update message. After that, all the IP packets that destined to mobile node will be tunneled from CA to foreign agent directly without any assistance from home agent. Figure 7 shows the operation of Gateway-based Mobile IP.

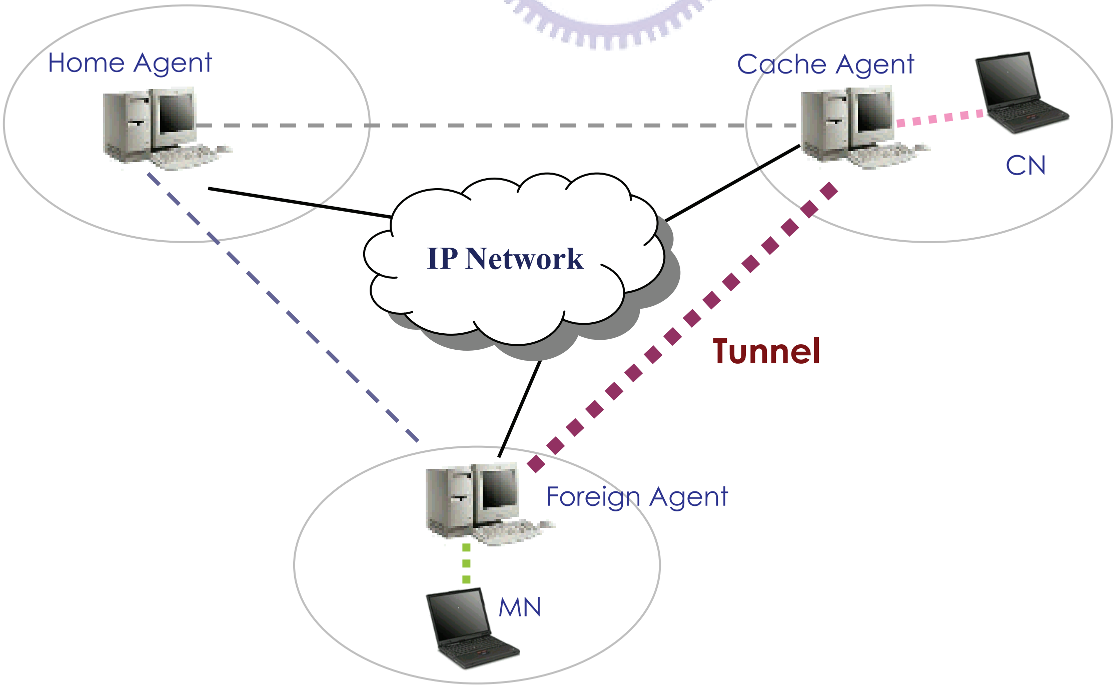


Figure 7 The Operation of Gateway-based Mobile IP

## 3.3 Control Messages in Gateway-based Mobile IP

Gateway-based Mobile IP defines a set of control messages, sent with UDP datagram using well-known port number 434. The following sections describe the message format and the definition of each field for these control messages.

### 3.3.1 Binding Warning

A binding warning message is used to transmit advice that a binding update is needed by one or more foreign agents or cache agents that have either no binding cache entry or an out-of-date binding cache entry for some mobile nodes. When a foreign agent that receives a packet that destined to a mobile node that already moving to other foreign network, it must send out a binding warning message to home agent to request it to send a binding update message to CA. If the foreign agent does not have any information about the mobile node's home agent, the foreign agent should send a binding warning message to the CA. Table 5 shows the message format of binding warning message.

Table 5 Binding Warning Message Format

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type = 16</td><td colspan="24">Reserved (sent as 0)</td></tr>
<tr><td colspan="32">Mobile Node Home Address</td></tr>
<tr><td colspan="32">Target Node Address …</td></tr>
</table>

Type 16

Mobile Node Home Address The home address of the mobile node to which the Binding Warning message refers.

Target Node Address Zero or more addresses of nodes. Each address should be the target of a Binding Update message sent by the home agent. If no addresses are present, the recipient of the message is the intended target for the message.

### 3.3.2 Binding Request

A binding request message [7] is used by a CA to request a mobile node's current binding information from the mobile node's home agent or a mobile node. When the home agent receives a binding request message, it looks up its location database and determines the correct binding information to be sent to the CA. If the binding update is allowed to expire, the CA and the home agent send a binding request to the mobile node to get the mobile node’s current binding information. The mobile node responds to the binding request with its new binding update. After receiving the new care-of address, the CA and the home agent send a binding acknowledgement to the mobile node. Before satisfying the request, the home agent is required to check whether or not the mobile node has allowed the information to be disseminated. The Table 6 shows the message format of binding request message.

Table 6 Binding Request Message Format

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type = 17</td><td colspan="24">Reserved (sent as 0)</td></tr>
<tr><td colspan="32">Mobile Node Home Address</td></tr>
<tr><td colspan="32">Identification</td></tr>
</table>

Type 17

Mobile Node Home Address The home address of the mobile node to which the Binding Request refers.

Identification A 64-bit sequence number, assigned by the node sending the Binding Request message, used to assist in matching requests with replies, and in protecting against replay attacks.

### 3.3.3 Binding Update

The binding update message is used for notification of a mobile node's current mobility binding. A binding update should also be sent by a mobile node, or by the foreign agent with which the mobile node is registering, when notifying the mobile node's previous foreign agent that the mobile node has moved. A binding acknowledge message should be returned if a node that receiving a binding update message in which the 'A' bit is set. The binding update message should be sent in the following situations:

- in response to a Binding Request message
- in response to a Binding Warning message
- in response to the reception of a Binding Warning extension to a Registration Request
- in response to the reception of a packet destined for a mobile node

Table 7 Binding Update Message Format

| 0 | | | | | | | | | | 1 | | | | | | | | | | 2 | | | | | | | | | | 3 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | 1 |
| Type = 18 | | | | | | | | A I M G | | | | Reserved | | | | Lifetime | | | | | | | | | | | | | | | |
| Mobile Node Home Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Care-of Address | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Identification | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Extension … | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Type 18

Lifetime The number of seconds remaining before the binding cache entry must be considered expired.

Mobile Node Home Address The home address of the mobile node to which the Binding Update message refers.

Care-of Address The current care-of address of the mobile node.

Identification It is used to assist in matching requests with replies.

### 3.3.4 Binding Acknowledge

A binding acknowledge message is used to acknowledge receipt of a binding update message. It should be sent by a node that receiving a binding update message in which the acknowledge bit is set. The following values are the allowable values for the Status:

- 128 reason unspecified
- 129 administratively prohibited
- 130 insufficient resources
- 131 sending node failed authentication
- 133 identification mismatch
- 134 poorly formed Binding Update

The Table 8 shows the message format of binding acknowledge message.

Table 8 Binding Acknowledge Message Format

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type = 19</td><td colspan="16">Reserved</td><td colspan="8">Status</td></tr>
<tr><td colspan="32">Mobile Node Home Address</td></tr>
<tr><td colspan="32">Identification</td></tr>
</table>

Type 19

Status If the Status is nonzero, this acknowledgment is negative. For instance, if the Binding Update was not accepted, but the incoming datagram has the Acknowledge flag set, then the status code should be set appropriately in the Binding Acknowledge message.

Mobile Node Home Address Copied from the Binding Update message being acknowledged.

Identification Copied from the Binding Update message being acknowledged, if present there.

### 3.3.5 Previous Foreign Agent Notification Extension

The previous foreign agent notification extension may be included in a registration request message sent to a mobility agent. It instructs the mobility agent to send a binding update message to the mobile node's previous foreign agent on behalf of the mobile node, to notify it that the mobile node has moved. The previous foreign agent should then delete the mobile node's visitor list entry and, if a new care-of address is included in the binding update message, create a binding cache entry for the mobile node with its new care-of address. The Table 9 shows the message format of previous foreign agent notification extension.

Table 9 Previous Foreign Agent Notification Extension Format

<table>
<tr><td>0</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>3</td><td></td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td></tr>
<tr><td colspan="8">Type = 96</td><td colspan="8">Length</td><td colspan="16">Cache Lifetime</td></tr>
<tr><td colspan="32">Previous Foreign Agent Address</td></tr>
<tr><td colspan="32">New Care-of Address</td></tr>
<tr><td colspan="32">SPI</td></tr>
<tr><td colspan="32">Authenticator …</td></tr>
</table>

Type 96

Cache Lifetime The number of seconds remaining before the binding cache entry created by the previous foreign agent must be considered expired.

Previous Foreign Agent Address The IP address of the mobile node's previous foreign agent to which the new foreign agent should send a Binding Update message on behalf of the mobile node.

New Care-of Address The address for the new mobility agent to send in the Binding Update message to the previous foreign agent.

SPI Security Parameters Index (4 bytes).

Authenticator The authenticator value to be used in the Route Optimization Authentication extension in the Binding Update message.

## 3.4 Message Flow of Gateway-based Mobile IP

This section describes the messages flows that are used in our approach. Figure 8 illustrates the message flow for binding request; Figure 9 illustrates the message flow for mobile node moves to foreign network; Figure 10 illustrates the message flow for mobile node moves to new foreign network; Figure 11 illustrates the message flow for mobile node returns to home network.

### 3.4.1 Binding Request Message

If a binding entry in binding cache that binding for one mobile node's care-of address is about to expire. The CA will send a binding request message to the home agent. After receiving this request, the home agent response a binding update message to the CA. Then CA refresh the lifetime of the binding. The Figure 8 shows the message flow of binding request message.

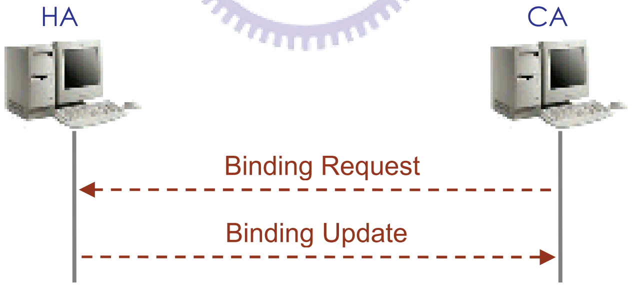


Figure 8 Message Flow for Binding Request

Step 1. CA sends a Binding Request message to HA.

Step 2. HA response a Binding Update message to CA.

### 3.4.2 MN Moves to foreign network

When mobile node moves its location from home network to foreign network, it will do the standard registration procedure via foreign agent to home agent first. At that time, the CA does not sense the location changing of mobile node; it will forward the packets to home agent as before. Home agent encapsulates the packet and forwards it to foreign agent as specified in Mobile IP. At the same time, home agent will inform CA that mobile node already changing its location by sending a binding update message. CA will add the binding entry into the binding cache and forwards packets to foreign agent directly later on. The Figure 9 shows the message flow of mobile node moves to foreign network.

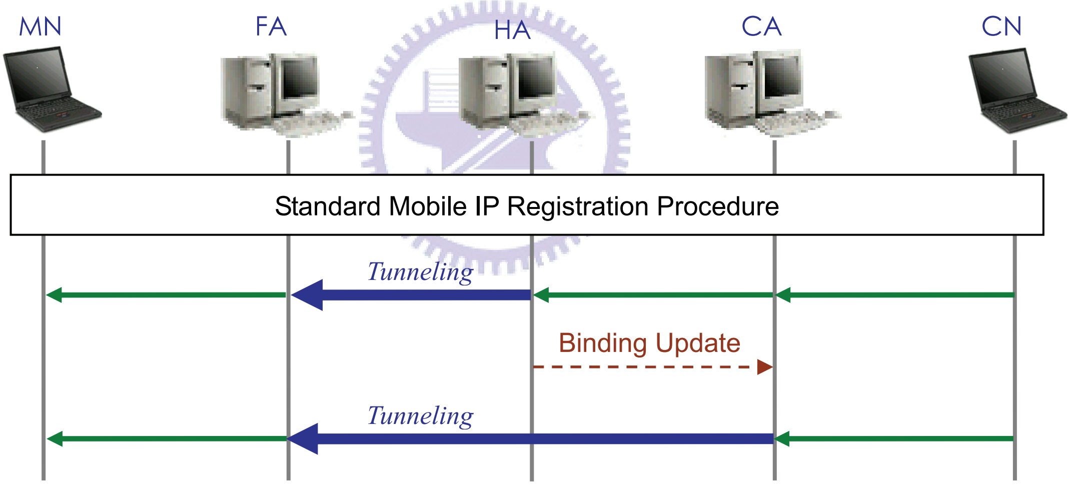


Figure 9 Message Flow for MN moves to foreign network

Step 1. Perform standard Mobile IP registration procedure.

Step 2. CA forwards the packets to HA as usual.

Step 3. HA tunnels the packets to FA and sends a Binding Update message to CA at the same time.

Step 4. CA tunnels the packets to FA directly.

### 3.4.3 MN Moves to new foreign network

When mobile node moves its location from first foreign network to second foreign network, it sends a registration request message to new foreign agent. Then the new foreign agent sends the binding request message to old foreign agent. The old foreign agent responses a binding ACK message to old foreign agent, and forward the registration request message to home agent. Home agent responses a registration reply message to mobile node through new foreign agent. The Figure 10 shows the message flow of mobile node moves to new foreign network.

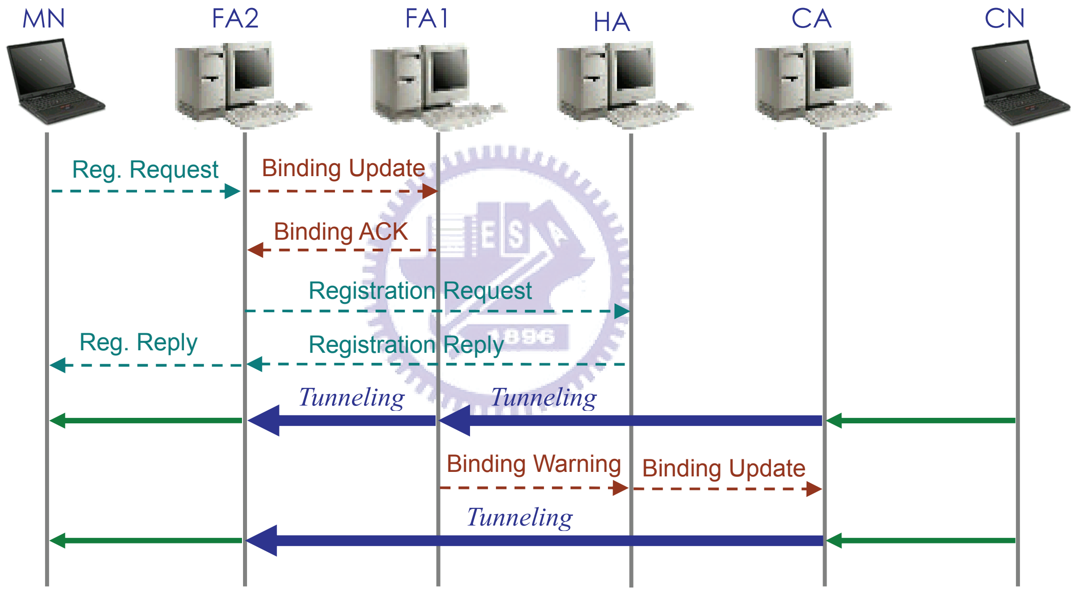


Figure 10 Message Flow for MN moves to new foreign network

Step 1. MN sends a Registration Request message to FA2.

Step 2. FA2 sends a Binding Update message to FA1. FA1 response a Binding ACK to FA2.

Step 3. FA2 forwards the Registration Request message to HA.

Step 4. HA responses a Registration Reply message to MN through FA2.

Step 5. FA1 sends a Binding Warning message to HA when it receives a packet from CA. Then HA sends a Binding Update message to CA.

Step 6. CA forwards packets to FA2 directly after CA add a MN's binding entry.

### 3.4.4 MN returns to home network

When mobile node returns to its home network, it sends a registration request message with lifetime set to 0 to home agent. After receiving the request, the home agent will delete the mobile node's binding entry and responses a registration reply message to mobile node. Then home agent sends a binding update message to foreign agent and CA respectively. After that, the CA forwards all packets that destined to mobile node to home agent as traditional IP routing. The Figure 11 shows the message flow of mobile node returns to home network.

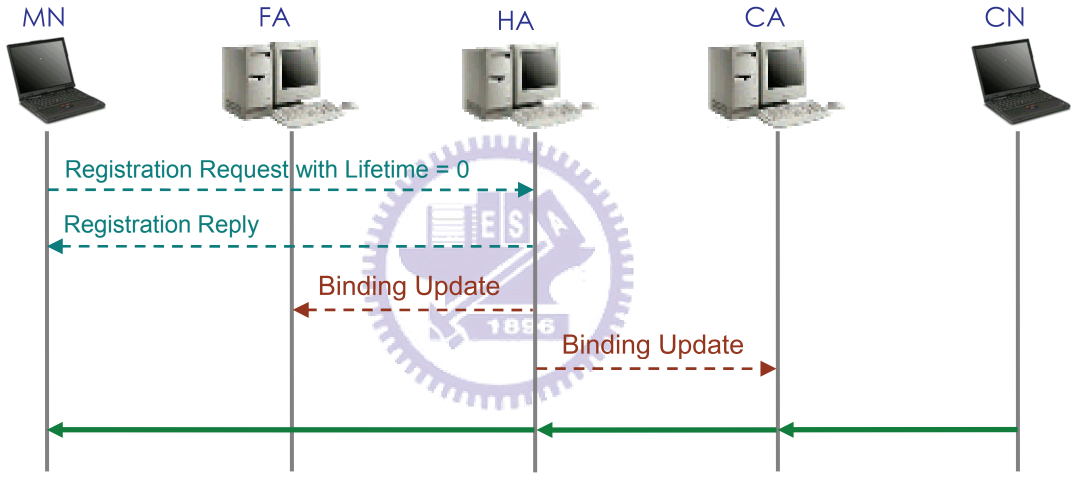


Figure 11 Message Flow for MN returns to home network

Step 1. MN returns to its home network and sends a Registration Request message with lifetime set to 0 to HA.

Step 2. HA delete the mobile node's binding entry and responses a Registration Reply message to MN.

Step 3. HA sends a Binding Update message to FA and CA respectively.

Step 4. CA forwards packets to HA.

# Chapter 4

# Implementation and Evaluation

## 4.1 Implementation

The implementation of Gateway-based Mobile IP with route optimization called gwMIP-RO that running on Linux platform. This implementation is based on the HUT Dynamic Mobile IP software and contains two parts: first part is the enhancements of Home Agent, Foreign Agent, and Mobile Node; and second part is creating a new functional entity called Cache Agent. In this implementation, we have implemented most required capabilities on CA. Therefore, gwMIP-RO can support route optimization in all Mobile IP network. The following sections described the kernel requirements, how to compile the package, how to install the package, and how to run the package.

### 4.1.1 Kernel Requirements

The supported kernel versions in this implementation are Linux 2.2.x and 2.4.x kernel versions. The following kernel options are needed to make a compatible kernel:

- Loadable module support (if `ipip` tunneling is used as a module)
- Networking options:
  - Packet socket (`CONFIG_PACKET`)
  - Kernel/User netlink socket (`CONFIG_NETLINK`)
  - Routing messages (`CONFIG_RTNETLINK`)
  - IP: Socket Filtering (`CONFIG_FILTER`)
  - IP: tunneling (`CONFIG_NET_IPIP`)

- Following options are needed for Foreign Agents:
    - IP: advanced router (`CONFIG_IP_ADVANCED_ROUTER`)
    - IP: policy routing (`CONFIG_IP_MULTIPLE_TABLES`)

### 4.1.2 Compiling the package

We use the compiler GCC 2.7.2.3 or gcc version egcs-2.91.66 (egcs-1.1.2 release) to compile the package. The procedures are shown as below:

1. unpack the package into some directory and '`cd`' into the directory (`tar xvzf dynamics-0.8.1.tar.gz ; cd dynamics-0.8.1`)
2. run '`./configure`' which checks that the program can be compiled on your system and finds out paths to needed files
3. run '`make`' to compile the program

### 4.1.3 Installing the package

By running '`make install`' to install the package into your system. The package is divided into separate entities: Home Agent, Foreign Agent, Cache Agent and Mobile Node. Each one is run on a dedicated machine and only one configuration file need to be configured.

### 4.1.4 Running the package

First, make sure you have sufficient privileges to do all the required operations. The program is used as normal daemon program that fork into background and the calling process returns immediately. The daemons can also be started on foreground to help debugging with command line arguments '`--fg --debug`'.

The program is started by running the installed program dynhad, dynfad, dyncad or dynmnd. The path to the configuration file must be given with '`--config`' command line argument, if it is not in the default installation directory.

## 4.2 Evaluation

### 4.2.1 Evaluation Purpose

This evaluation provides you a performance comparison between the basic Mobile IP and Gateway-based Mobile IP under different network conditions. This evaluation defines five network conditions: one millisecond of round-trip time, three milliseconds of round-trip time, five milliseconds of round-trip time, eight milliseconds of round-trip time, and ten milliseconds of round-trip time. There are two criteria to measure the performance in this evaluation. The first criterion is ‘throughput’ test and the second criterion is ‘response time’ test. The throughput is the amount of data transferred by a network in a time unit. Generally, it is expressed as Mbps. The response time is the time that needed for one transaction. The formal definitions of both criteria are shown below.

**Throughput**

The total number of bytes sent and received by the EndPoint1 in the group is divided by the elapsed time of the longest-running pair in the group.

**Response Time**

The response time is the inverse of the transaction rate; it is the time, in seconds, needed for one transaction. The transaction rate is the number of script transactions that are executed per second.

Bytes_Sent = the number of bytes sent by Endpoint 1 of a pair

Bytes_Received = the number of bytes received by the endpoint of a pair

Throughput_Units = the current throughput units value, in bytes per second.

Throughput = (Bytes_Sent + Bytes_Received_By_ep1) / Throughput_Units / Measured_Time

Response Time = Measured_Time / Transaction_Count

### 4.2.2 Test Configurations

There are totally eight test equipments are used in this evaluation. In this section, we list the detailed specification of these test equipments and their test configurations.

**Test Equipments**

| | |
|---|---|
| Home Agent: | Acer TraveMate 345T / CPU: P3-450 MHz / RAM: 128MB |
| Foreign Agent: | Dell LATITUDE D600 / CPU: P4-1400 MHz / RAM 512MB |
| Cache Agent: | IBM ThinkPad X24 / CPU: P3-800 MHz / RAM: 128MB |
| IP Router: | ASUS P4P800-VM PC / CPU: P4-3.0 GHz / RAM: 1GB |
| Mobile Node: | IBM ThinkPad R30 / CPU: P3-900 MHz / RAM 256MB |
| Correspondent Node1: | Toshiba Satellite 31CDT / CPU: P3-900 MHz / RAM: 384MB |
| Correspondent Node2: | Toshiba Satellite 31CDT / CPU: P3-900 MHz / RAM: 384MB |
| Correspondent Node3: | Toshiba Satellite 31CDT / CPU: P3-900 MHz / RAM: 384MB |

**Test Configurations**

| | |
|---|---|
| Home Agent: | Kernel Linux 2.4.7<br>HUT Dynamic MIP dynhad version 0.8.1<br>eth0: 200.1.10.1 mask: 255.255.255.0 gateway: 200.1.10.254<br>eth1: 200.1.20.1 mask: 255.255.255.0 gateway: 200.1.20.254 |
| Foreign Agent: | Kernel Linux 2.4.7<br>HUT Dynamic MIP dynfad version 0.8.1<br>eth0: 200.2.10.1 mask: 255.255.255.0 gateway: 200.1.10.254<br>eth1: 200.2.20.1 mask: 255.255.255.0 gateway: 200.1.20.254 |
| Cache Agent: | Kernel Linux 2.4.7<br>gwMIP-RO version 0.1<br>eth0: 200.3.10.1 mask: 255.255.255.0 gateway: 200.3.10.254<br>eth1: 200.3.20.1 mask: 255.255.255.0 gateway: 200.3.20.254 |
| IP Router: | Kernel Linux 2.4.7<br>NIST Net version 2.0.12b |

eth0: 200.1.10.254 mask: 255.255.255.0
eth1: 200.2.10.254 mask: 255.255.255.0
eth2: 200.3.10.254 mask: 255.255.255.0
route add -net 200.1.20.0 mask 255.255.255.0 gw 200.1.10.1
route add -net 200.2.20.0 mask 255.255.255.0 gw 200.2.10.1
route add -net 200.3.20.0 mask 255.255.255.0 gw 200.3.10.1

Mobile Node: Kernel Linux 2.4.7
HUT Dynamic MIP dynmnd version 0.8.1
NetIQ Performance Endpoint version 5.0
eth0: 200.1.20.2 mask: 255.255.255.0 gateway: 200.1.20.1

Correspondent Node: Kernel Linux 2.4.7
NetIQ Chariot console version 5.0
NetIQ Performance Endpoint version 5.0
eth0: 200.1.20.2 netmask: 255.255.255.0 gateway: 200.1.20.1

Network Emulator: NIST-Net Network Emulator version 2.0.12b

Benchmark Tool: Benchmark Server: NetIQ Chariot Console version 5.0
Benchmark Client: NetIQ Performance Endpoint version 5.0
Benchmark Script: High_Performance_Throughput.scr

### 4.2.3 Evaluation Scenarios

In this evaluation, we use NetIQ Chariot console for throughput test and response time test. In Chariot console, we create a new pair that includes two endpoints: one is CN with IP address 200.3.20.2 and the other one is MN with IP address 200.1.20.2. The Chariot script *High_Performance_Throughput* is executed with the CN running as endpoint1 (data transmitter) and the MN running as endpoint2 (data receiver). The Chariot script *High_Performance_Throughput* is then executed again with the MN running as endpoint1 (data transmitter) and the CN running as endpoint2 (data receiver). Repeat above procedures until five networks conditions are evaluated. In this evaluation, we use NIST-Net to emulate five network conditions. NIST-Net is a network emulator that is capable to emulate a wide variety of network conditions.

### 4.2.4 Network Topology

There are eight computing devices are used in this evaluation. One desktop for HA, one desktop for FA, one desktop for CA, one desktop for IP Router equipped, one notebook for MN, and three notebooks for CNs. The NIST-NET network emulator will be installed in IP Router. The Chariot Console will be installed in CN1 and the Performance Endpoint will be installed in CN1, CN2, CN3 and MN. Figure 12 shows the Gateway-based Mobile IP test bed.

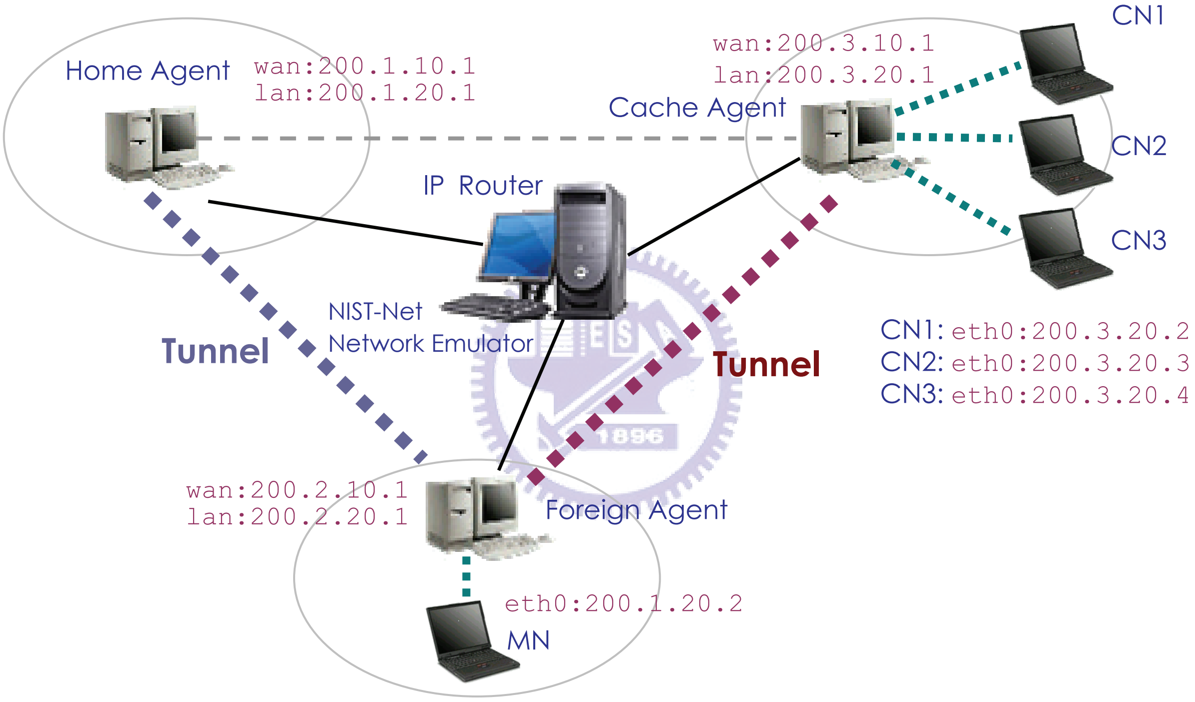


Figure 12 Gateway-based Mobile IP Test bed

### 4.2.5 Evaluation Results

Following data will show the evaluation results of throughput test from CN to MN, throughput test from MN to CN, response time test from CN to MN, response time test from MN to CN, throughput test from multiple CNs to MN. From Figure 18 to Figure 29, we can see the more detailed evaluation results of 1 ms of round-trip time and 5ms of round-trip time two network conditions.

### 1. Throughput Test: CN to MN

Table 10 shows the throughput performance from CN to MN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

Table 10 Throughput Performance of CN to MN

| RTT (ms) \ Tunneling Mode | RTT = 1 ms | RTT = 3 ms | RTT = 5 ms | RTT = 8 ms | RTT = 10 ms |
|---|---|---|---|---|---|
| Routing Optimization | 90.550 Mbps | 90.485 Mbps | 90.657 Mbps | 90.536 Mbps | 90.580 Mbps |
| Triangle Tunneling | 90.134 Mbps | 77.048 Mbps | 62.005 Mbps | 45.932 Mbps | 39.289 Mbps |
| Reverse Tunneling | 87.216 Mbps | 72.865 Mbps | 57.652 Mbps | 43.367 Mbps | 37.104 Mbps |

Figure 13 shows the throughput performance comparison from CN to MN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

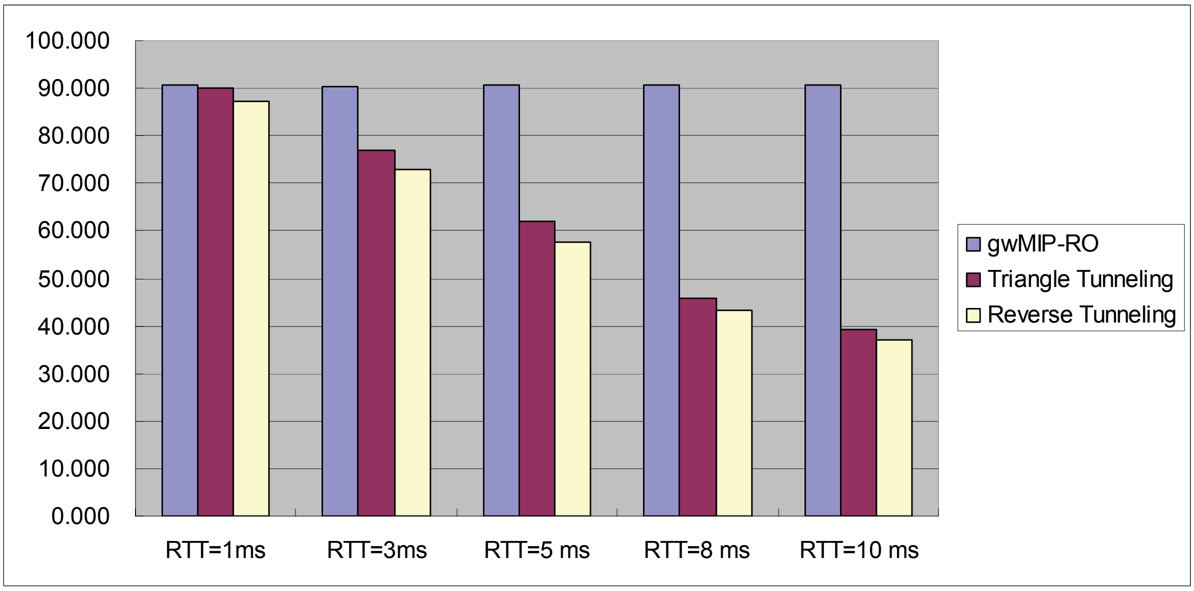


Figure 13 Throughput Performance Comparison of CN to MN

### 2. Throughput Test: MN to CN

Table 11 shows the throughput performance from MN to CN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

Table 11 Throughput Performance of MN to CN

| RTT (ms) \ Tunneling Mode | RTT = 1 ms | RTT = 3 ms | RTT = 5 ms | RTT = 8 ms | RTT = 10 ms |
|---|---|---|---|---|---|
| Routing Optimization | 90.682 Mbps | 90.462 Mbps | 90.787 Mbps | 90.513 Mbps | 90.529 Mbps |
| Triangle Tunneling | 90.619 Mbps | 88.775 Mbps | 87.678 Mbps | 86.438 Mbps | 85.517 Mbps |
| Reverse Tunneling | 87.635 Mbps | 73.660 Mbps | 57.677 Mbps | 43.234 Mbps | 37.090 Mbps |

Figure 14 shows the throughput performance comparison from MN to CN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

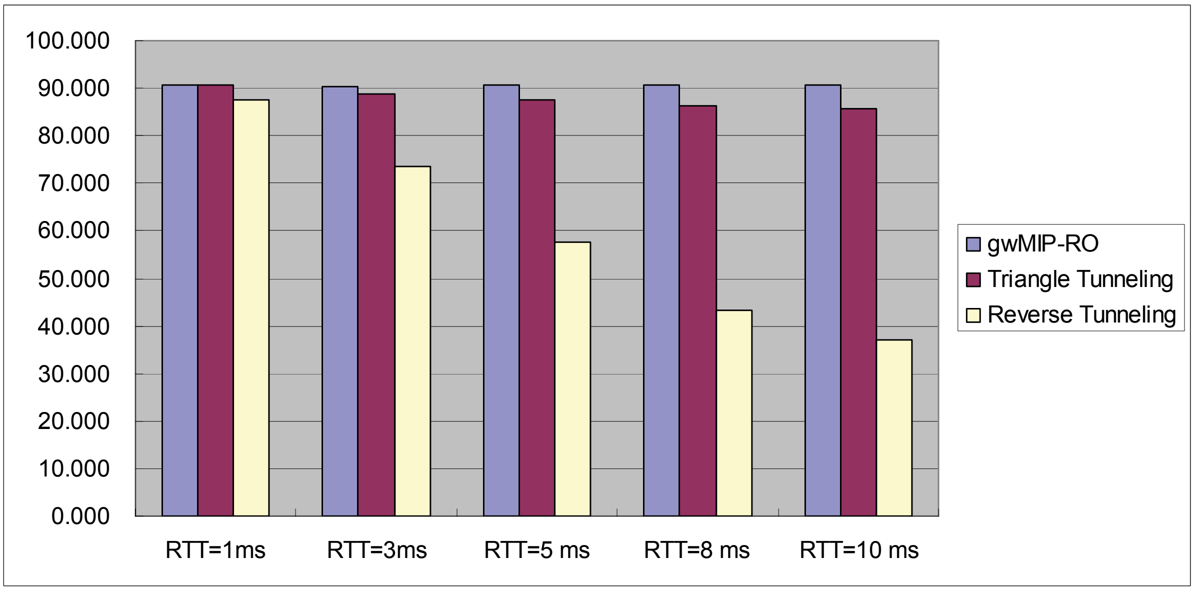


Figure 14 Throughput Performance Comparison of MN to CN

### 3. Response Time Test: CN to MN

Table 12 shows the response time from CN to MN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

Table 12 Response Time of CN to MN

| RTT (ms) \ Tunneling Mode | RTT = 1 ms | RTT = 3 ms | RTT = 5 ms | RTT = 8 ms | RTT = 10 ms |
|---|---|---|---|---|---|
| Routing Optimization | 0.883 sec | 0.882 sec | 0.879 sec | 0.884 sec | 0.883 sec |
| Triangle Tunneling | 0.887 sec | 1.038 sec | 1.289 sec | 1.741 sec | 2.035 sec |
| Reverse Tunneling | 0.917 sec | 1.097 sec | 1.387 sec | 1.844 sec | 2.155 sec |

Figure 15 shows the response time comparison from CN to MN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

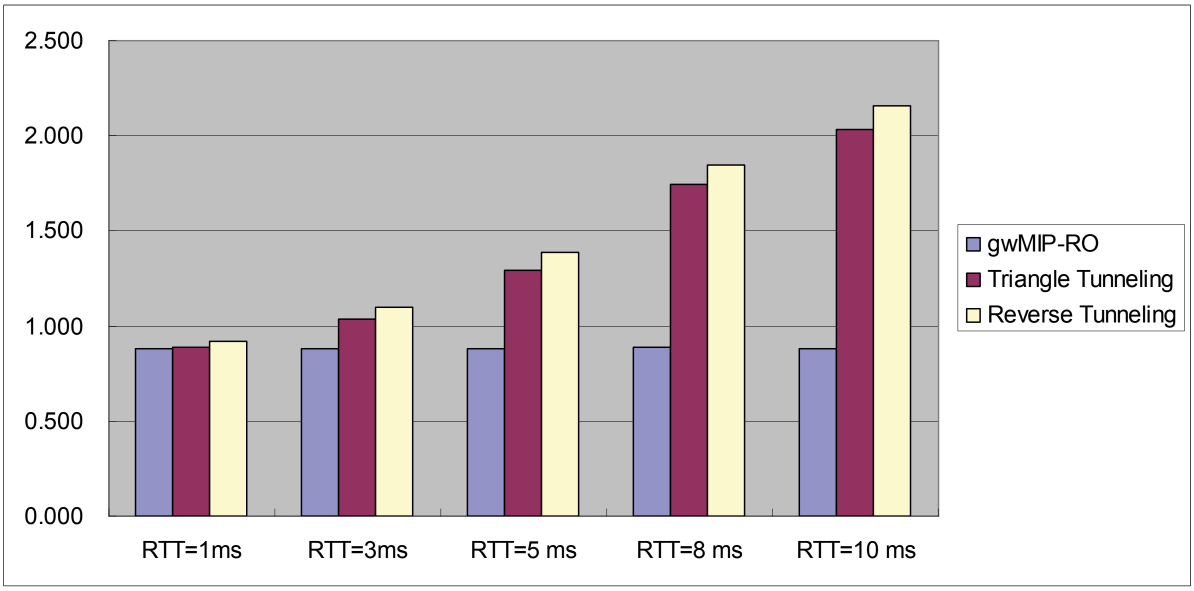


Figure 15 Response Time Comparison of CN to MN

### 4. Response Time Test: MN to CN

Table 13 shows the response time from MN to CN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

Table 13  Response Time of MN to CN

| RTT (ms) \ Tunneling Mode | RTT = 1 ms | RTT = 3 ms | RTT = 5 ms | RTT = 8 ms | RTT = 10 ms |
|---|---|---|---|---|---|
| Routing Optimization | 0.882 sec | 0.880 sec | 0.875 sec | 0.879 sec | 0.880 sec |
| Triangle Tunneling | 0.883 sec | 0.900 sec | 0.912 sec | 0.925 sec | 0.935 sec |
| Reverse Tunneling | 0.952 sec | 1.085 sec | 1.386 sec | 1.850 sec | 2.156 sec |

Figure 16 shows the response time comparison from MN to CN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms and three tunneling modes: rough optimization in Gateway-based Mobile IP, triangle tunneling in basic Mobile IP, and reserve tunneling in basic Mobile IP.

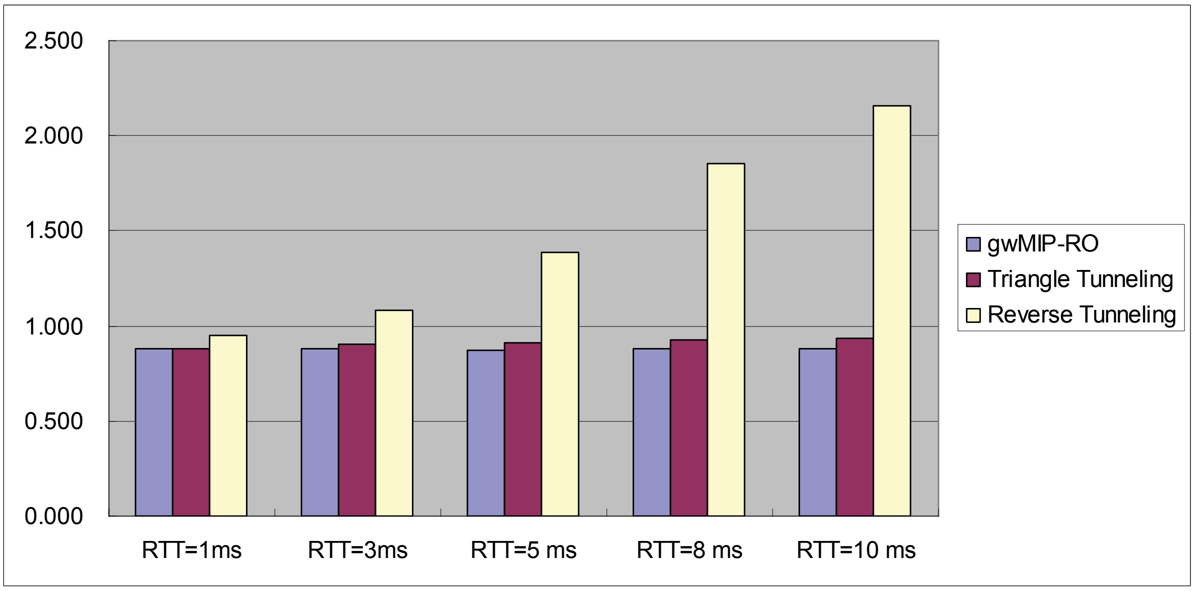


Figure 16  Response Time Comparison of MN to CN

### 5. Throughput Test: Multiple CNs to MN

Table 14 shows the throughput performance from multiple CNs to MN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms. The number of CN will be one CN, two CNs, and three CNs. Figure 30 shows a snapshot of two CNs transmit packets to MN under 5ms of RTT. Figure 31 shows a snapshot of three CNs transmit packets to MN under 5ms of RTT.

Table 14 Throughput Performance of Multiple CNs to MN

| RTT (ms) \ Number of CN | RTT = 1 ms | RTT = 3 ms | RTT = 5 ms | RTT = 8 ms | RTT = 10 ms |
|---|---|---|---|---|---|
| One CN | 90.550 Mbps | 90.485 Mbps | 90.657 Mbps | 90.536 Mbps | 90.580 Mbps |
| Two CNs | 90.688 Mbps | 90.268 Mbps | 90.788 Mbps | 90.441 Mbps | 90.486 Mbps |
| Three CNs | 90.565 Mbps | 90.482 Mbps | 90.476 Mbps | 90.436 Mbps | 90.503 Mbps |

Figure 17 shows the throughput performance comparison from multiple CNs to MN transmission direction under five network conditions: RTT = 1ms, RTT = 3ms, RTT = 5ms, RTT = 8ms, and RTT = 10ms. The number of CN will be one CN, two CNs, and three CNs.

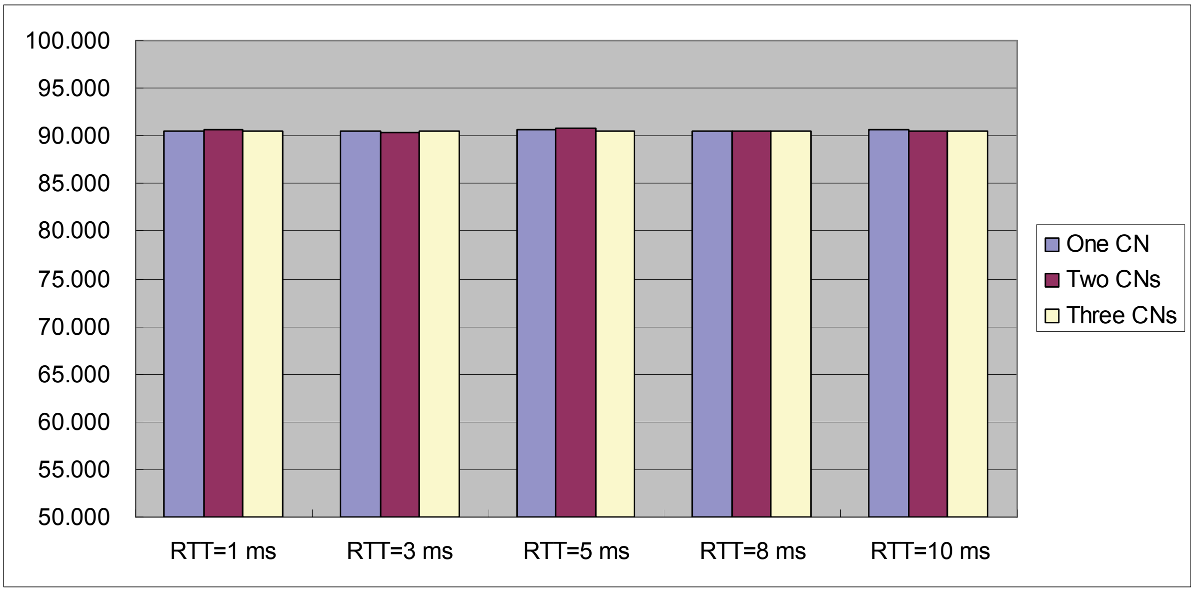


Figure 17 Throughput Performance Comparison of Multiple CNs to MN

## 1. CN to MN with 1ms of RTT

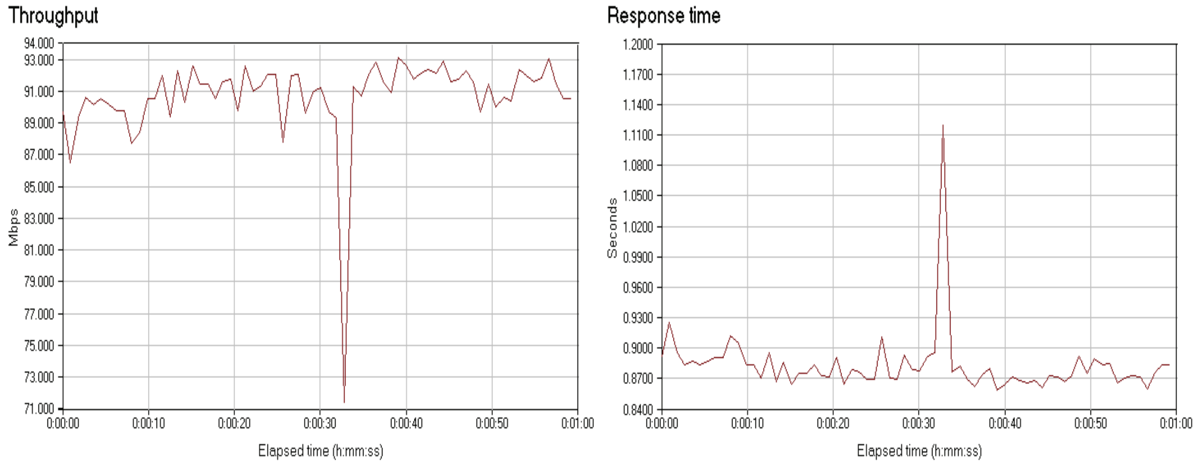


Figure 18 CN to MN with 1ms of RTT in Route Optimization

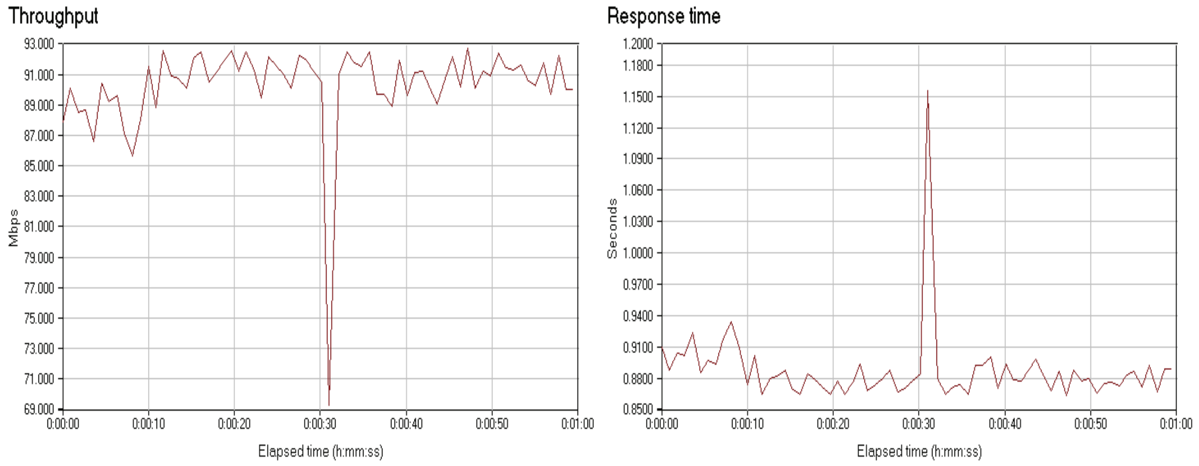


Figure 19 CN to MN with 1ms of RTT in Triangle Tunneling

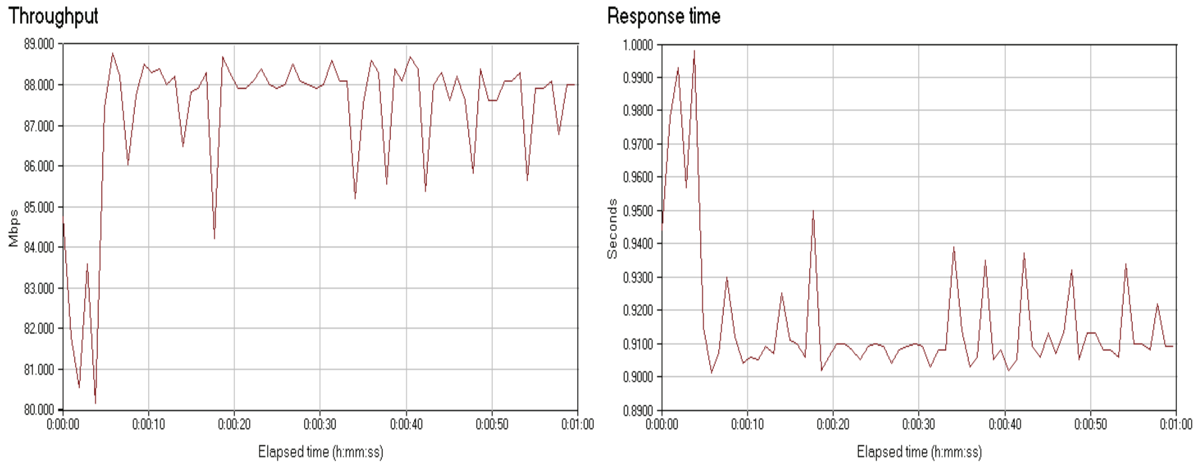


Figure 20 CN to MN with 1ms of RTT in Reverse Tunneling

## 2. MN to CN with 1ms of RTT

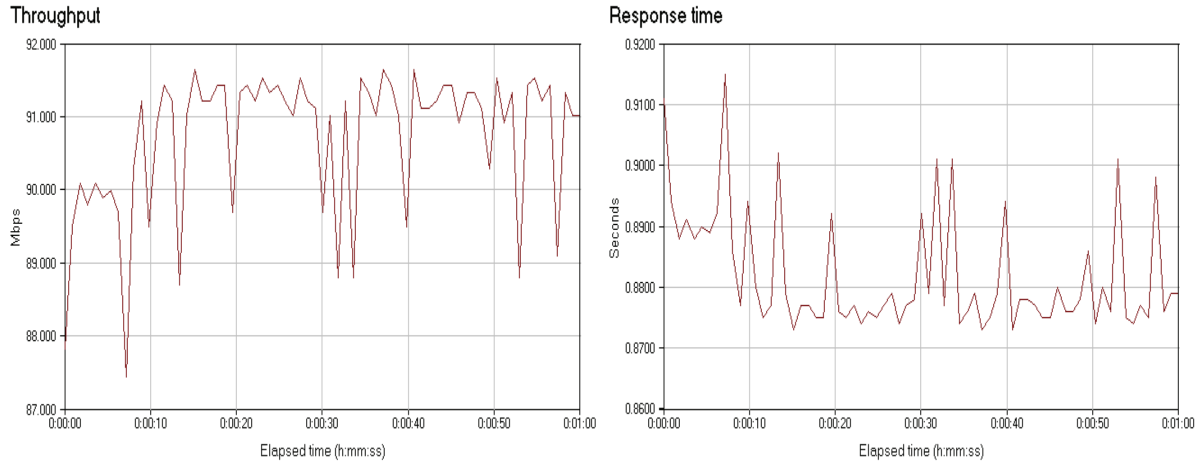


Figure 21 NM to CN with 1ms of RTT in Route Optimization

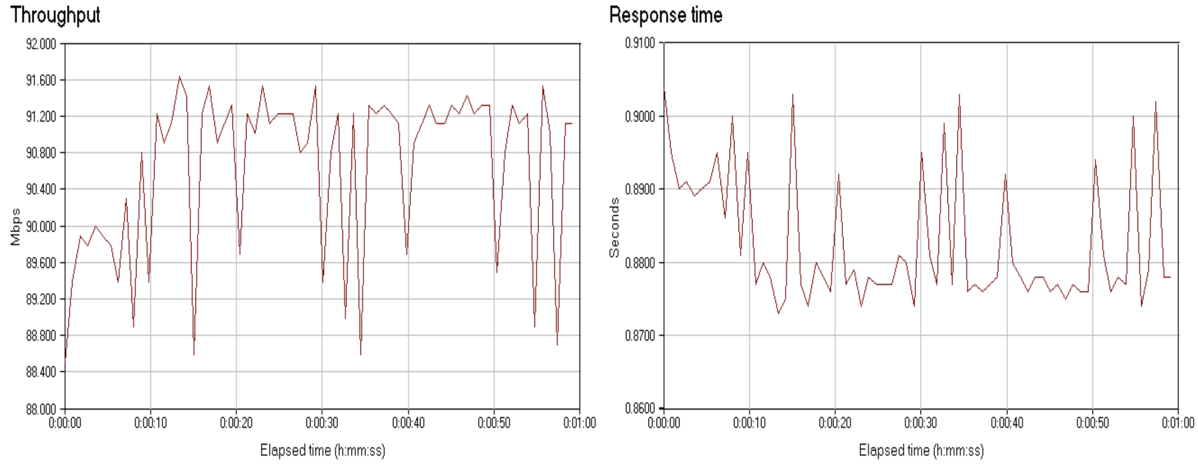


Figure 22 NM to CN with 1ms of RTT in Triangle Tunneling

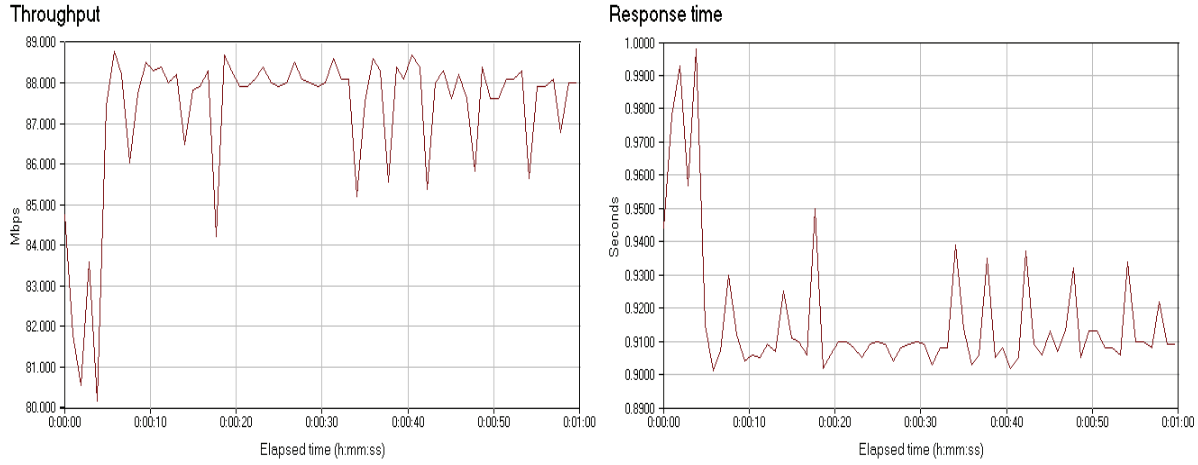


Figure 23 NM to CN with 1ms of RTT in Reverse Tunneling

## 3. CN to MN with 5ms of RTT

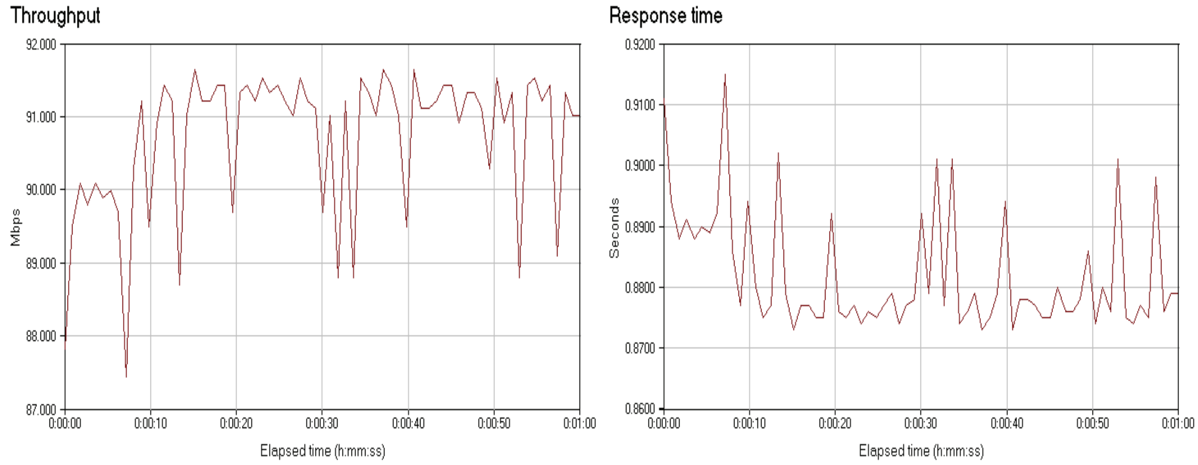


Figure 24 CN to MN with 5ms of RTT in Route Optimization

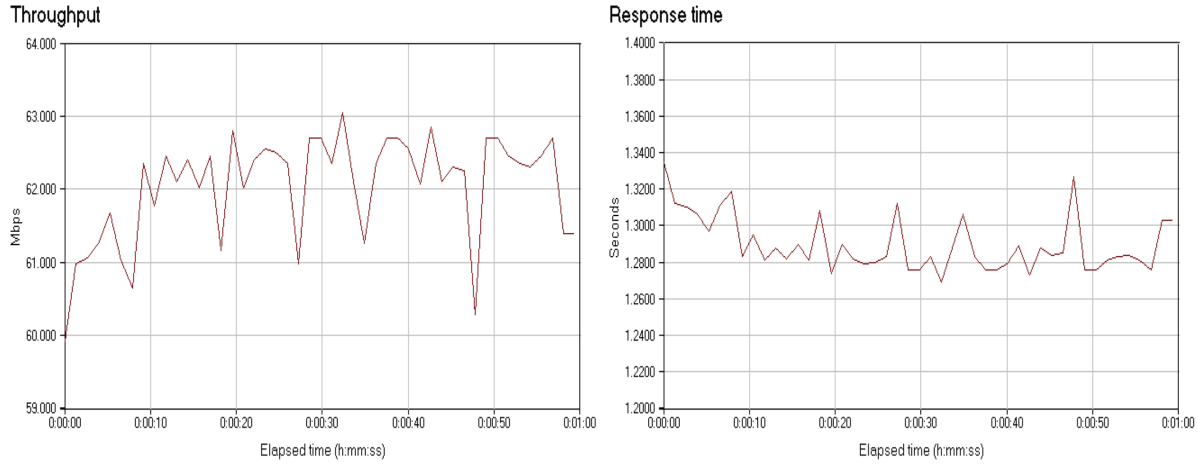


Figure 25 CN to MN with 5ms of RTT in Triangle Tunneling

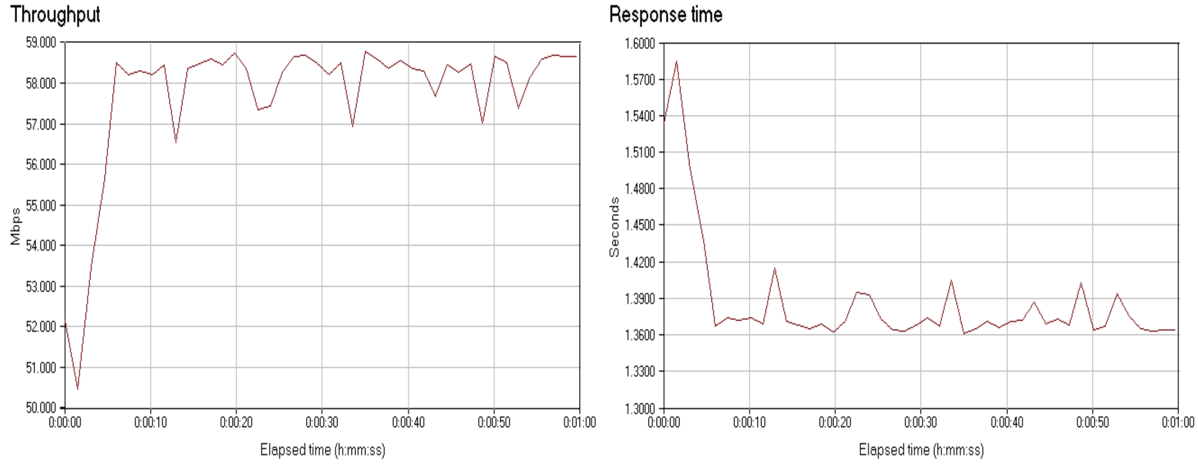


Figure 26 CN to MN with 5ms of RTT in Reverse Tunneling

## 4. MN to CN with 5ms of RTT

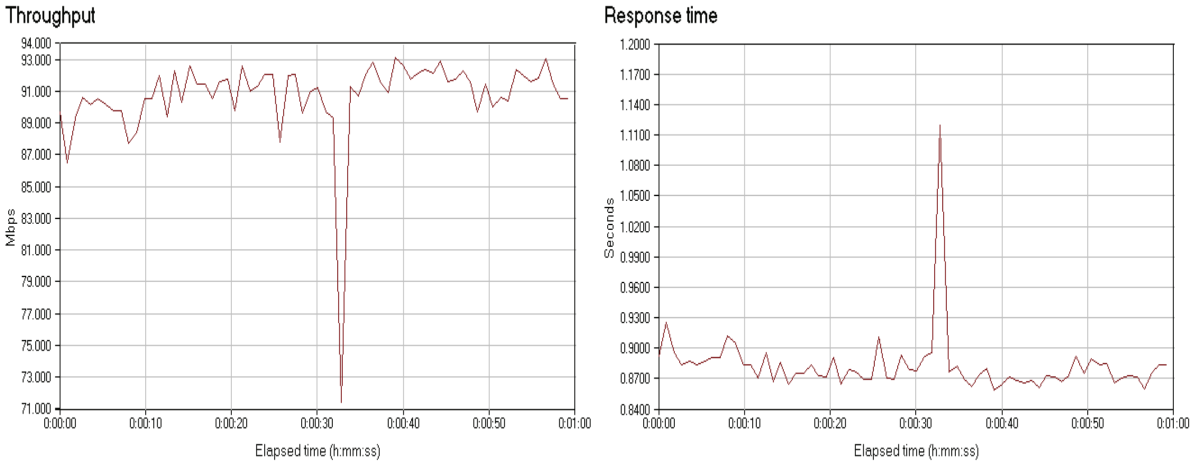


Figure 27 NM to CN with 5ms of RTT in Route Optimization

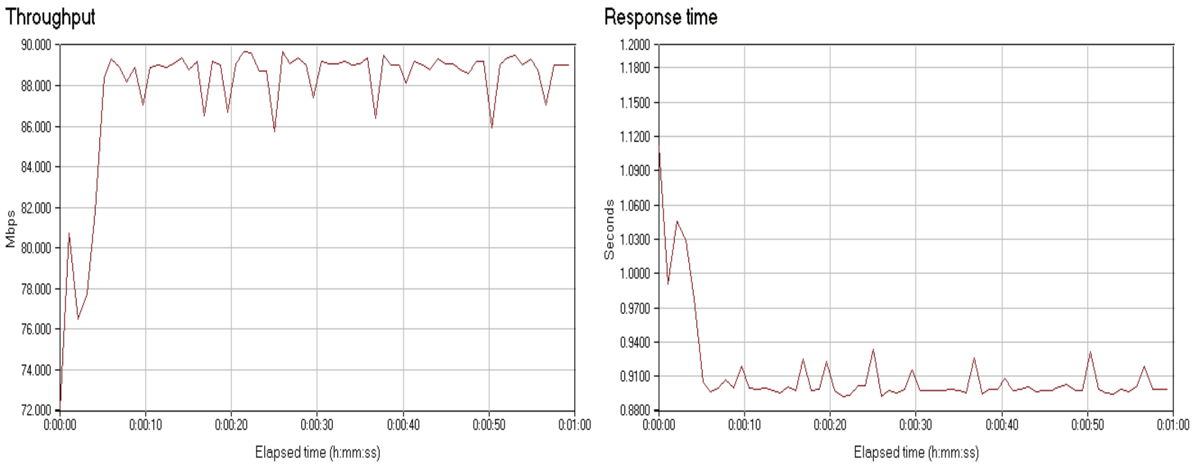


Figure 28 NM to CN with 5ms of RTT in Triangle Tunneling

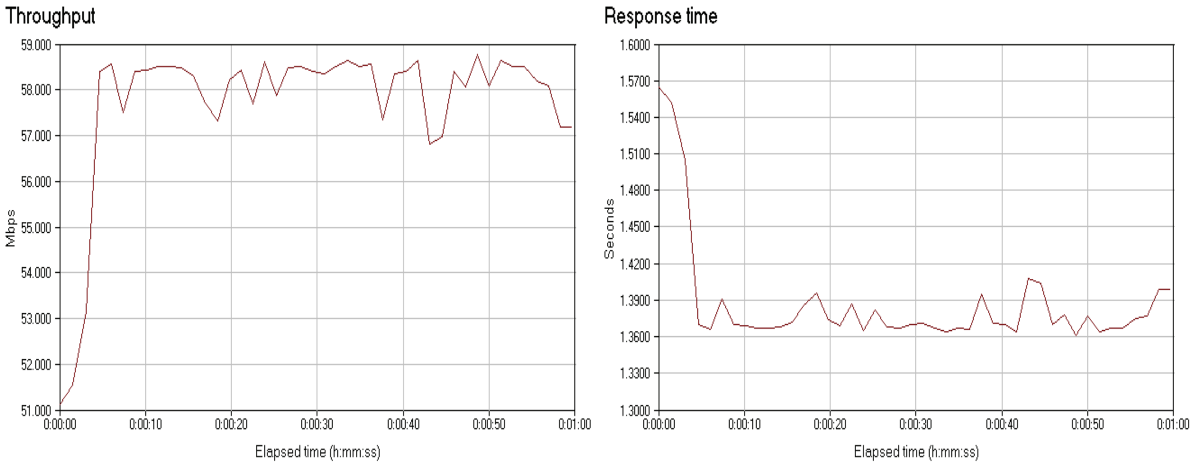
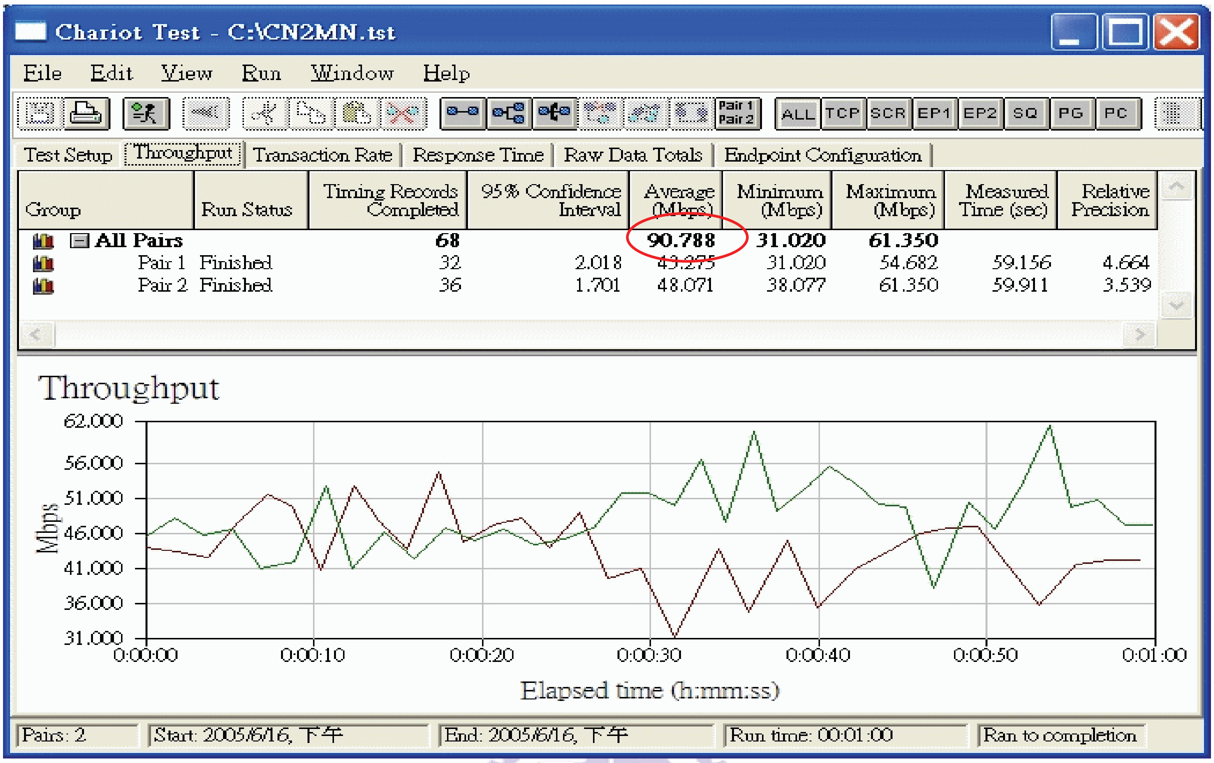


Figure 29 NM to CN with 5ms of RTT in Reverse Tunneling

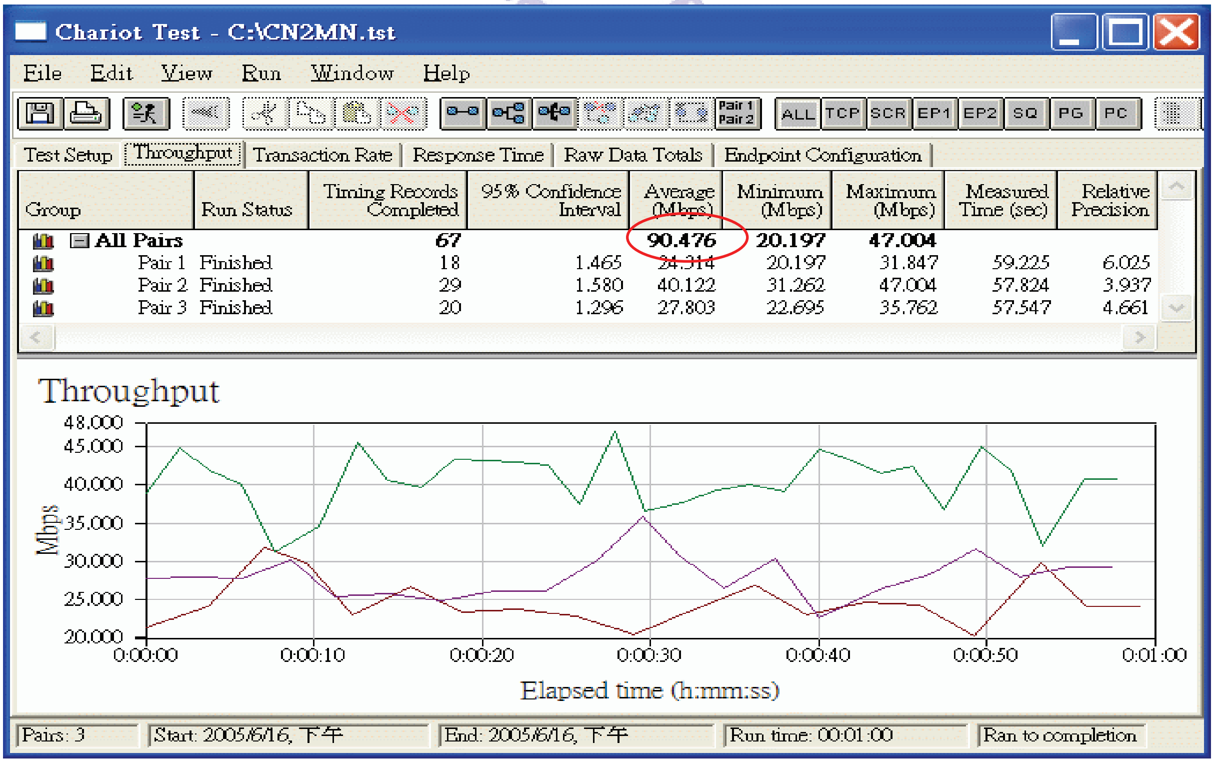
## 5. Multiple CNs to MN with 5ms of RTT


Chariot Test - C:\CN2MN.tst
File Edit View Run Window Help
Pair 1 Pair 2
ALL TCP SCR EP1 EP2 SQ PG PC
Test Setup Throughput Transaction Rate Response Time Raw Data Totals Endpoint Configuration
Throughput
62.000
56.000
51.000
46.000
41.000
36.000
31.000
Mbps
0:00:00
0:00:10
0:00:20
0:00:30
0:00:40
0:00:50
0:01:00
Elapsed time (h:mm:ss)

| Group | Run Status | Timing Records Completed | 95% Confidence Interval | Average (Mbps) | Minimum (Mbps) | Maximum (Mbps) | Measured Time (sec) | Relative Precision |
|---|---|---|---|---|---|---|---|---|
| **All Pairs** | | **68** | | **90.788** | **31.020** | **61.350** | | |
| Pair 1 | Finished | 32 | 2.018 | 43.275 | 31.020 | 54.682 | 59.156 | 4.664 |
| Pair 2 | Finished | 36 | 1.701 | 48.071 | 38.077 | 61.350 | 59.911 | 3.539 |

Pairs: 2 | Start: 2005/6/16, 下午 | End: 2005/6/16, 下午 | Run time: 00:01:00 | Ran to completion

Figure 30 Two CNs to MN with 5ms of RTT in Route Optimization


Chariot Test - C:\CN2MN.tst
File Edit View Run Window Help
Pair 1 Pair 2
ALL TCP SCR EP1 EP2 SQ PG PC
Test Setup Throughput Transaction Rate Response Time Raw Data Totals Endpoint Configuration
Throughput
48.000
45.000
40.000
35.000
30.000
25.000
20.000
Mbps
0:00:00
0:00:10
0:00:20
0:00:30
0:00:40
0:00:50
0:01:00
Elapsed time (h:mm:ss)

| Group | Run Status | Timing Records Completed | 95% Confidence Interval | Average (Mbps) | Minimum (Mbps) | Maximum (Mbps) | Measured Time (sec) | Relative Precision |
|---|---|---|---|---|---|---|---|---|
| **All Pairs** | | **67** | | **90.476** | **20.197** | **47.004** | | |
| Pair 1 | Finished | 18 | 1.465 | 24.314 | 20.197 | 31.847 | 59.225 | 6.025 |
| Pair 2 | Finished | 29 | 1.580 | 40.122 | 31.262 | 47.004 | 57.824 | 3.937 |
| Pair 3 | Finished | 20 | 1.296 | 27.803 | 22.695 | 35.762 | 57.547 | 4.661 |

Pairs: 3 | Start: 2005/6/16, 下午 | End: 2005/6/16, 下午 | Run time: 00:01:00 | Ran to completion

Figure 31 Three CNs to MN with 5ms of RTT in Route Optimization

### 4.2.6 Evaluation Summary

Various tests have been conducted on our evaluation. In evaluation results above, we can see that when round-trip time is becoming bigger, the throughput performance of Mobile IP will be obviously degraded. But the throughput performance of Gateway-based Mobile IP is almost keeping the same under different network conditions. So we got a conclusion that route optimization in Gateway-based Mobile IP has better throughput performance than triangle tunneling in basic Mobile IP and reverse tunneling in basic Mobile IP under different network conditions.

We also design a test case that multiple correspondent nodes transmit packets to mobile node simultaneously to see whether the throughput performance will be affected or not. In Table 14 we can see that there is no obviously impact on throughput performance when the number of correspondent node in this test is increasing to two correspondent nodes or even to three correspondent nodes.

# Chapter 5

# Conclusions

In this thesis, we give an approach to solve triangle routing that existing in basic Mobile IP. Our approach introduces a cache agent that maintains a binding cache to provide transparent connections between correspondent nodes and mobile nodes.

From evaluation results, we can see that Gateway-based Mobile IP has better throughput than both triangle tunneling and reverses tunneling in basic Mobile IP. The value of RTT between mobile node and correspondent node is becoming bigger; the improvement of throughput is obviously becoming better. The throughput does not degrade, even when cache agent serves multiple correspondent nodes simultaneously. Our approach not only addresses the triangle routing problem, but also improves the throughput between mobile nodes and correspondent nodes.

The key technique of this approach is to maintain the binding cache in cache agent instead of all mobility-aware correspondent nodes in Mobile IP network. This means that the correspondent nodes do not require installing any mobility software to support route optimization. It is clear that deploying Gateway-based Mobile IP is easier than deploying basic Mobile IP into the real world.

In this thesis, we only consider triangle routing problem in our approach. There are some important issues, such as Authentication, Authorization, and Accounting (AAA), security issue, handoff issue, location privacy and NAT Mobile IP, in basic Mobile IP deserve to investigate further.

# References

[1] J. Postel, "Internet Protocol", *RFC 791*, September 1981.

[2] A. T. Campbell et al., "An Overview of Cellular IP", *IEEE Wireless Communications and Networking Conference (WCNC)*, September 1999, pp. 606-611.

[3] R. Ramjee et al., "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks", *IEEE/ACM Transactions on Networking*, vol. 10, June 2002, pp. 396-410.

[4] C. Perkins, "IPv4 Mobility Support", *RFC 3344*, August 2002.

[5] J. Rosenberg et al., "SIP: Session Initiation Protocol", *RFC 3261*, June 2002.

[6] D. Forsberg et al., "Dynamics - HUT Mobile IP Technical Document", *technical-document.txt*, http://dynamics.sourceforge.net, October 1999.

[7] C. Perkins and D. Johnson, "Route Optimization in Mobile IP", *draft-ietf-mobileip-optim-11.txt*, Internet Draft, IETF, September 2001.

[8] I. F. Akyildiz et al., "Mobility Management in Next Generation Wireless Systems", *In Proceedings of the IEEE*, vol. 87, August 1999, pp. 1347-1384.

[9] A. T. Campbell et al., "Comparison of IP Micromobility Protocols", *IEEE Wireless Communications*, Feb. 2002, pp. 72-82.

[10] E. Gustafsson et al., "Mobile IPv4 Regional Registration", *draft-ietf-mobileip-reg-tunnel-09.txt*, Internet Draft, IETF, June 2004.

[11] I. F. Akyildiz et al., “A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems”, *IEEE Wireless Communications*, August 2004, pp. 16-28.

[12] P. Bhagwat et al., “Network Layer Mobility: An Architecture and Survey”, *IEEE Personal Communications*, June 1996, pp. 54-64.

[13] D. Deering, “ICMP Router Discovery Messages”, *RFC 1256*, September 1991.

[14] J. Postel, “User Datagram Protocol”, *RFC 768*, August 1980.

[15] C. Perkins, “IP Encapsulation within IP”, *RFC 2003*, May 1996.

[16] T. S. Huang, “Mobile IP with Router Optimization for Windows”, *Master Thesis*, National Chiao Tung University, June 1998.

[17] H. W. Lin, “A Gateway Approach for Mobility Integration of GPRS and Wireless LANs”, *Master Thesis*, National Thsing Hua University, June 2003.

[18] C. H. Wu et al., “Bi-directional Route Optimization in Mobile IP over Wireless LAN”, *IEEE Semiannual Vehicular Technology Conference*, September 2002.

[19] J. Postel, “Internet Control Message Protocol”, *RFC 792*, September 1981.

[20] I. W. Wu et al., “A Seamless Handoff Approach of Mobile IP Protocol for Mobile Wireless Data Networks”, *IEEE Transactions on Consumer Electronics*, vol. 48, May 2002, pp. 335-344.