CRANFIELD UNIVERSITY

XIYU SHI

SUPPORT FOR IP MOBILITY AND DIVERSITY
IN A
BROADBAND WIRELESS ACCESS NETWORK

ROYAL MILITARY COLLEGE OF SCIENCE

PhD THESIS

CRANFIELD UNIVERSITY

ROYAL MILITARY COLLEGE OF SCIENCE

DEPARTMENT OF INFORMATICS AND SIMULATION

PhD THESIS

Academic Year 2001-2002

Xiyu Shi

Support For IP Mobility and Diversity in a Broadband Wireless Access Network

Supervisor: Dr Avril Smith

July 2002

In collaboration with

The Advanced Communications Unit and The Radio Communications Research Unit
The Rutherford Appleton Laboratory

Abstract

Broadband wireless access (BWA) network working at millimetre bands possesses the advantages of quick deployment, more flexibility, wide service coverage and cost efficiency. The range of services to be provided via the system includes broadband digital television, Internet data, telephony and videoconference. Apart from broadcast digital television, all traffic is carried in Internetworking Protocol (IP) format.

Unfortunately the services of such a system are susceptible to impairment by buildings, vegetation, terrain and attenuation caused by rain, snow and sleet, etc. Accordingly the service availability and system performance can drop dramatically. In the worst case, the system will experience heavy packet loss and the services might be completely unavailable.

An extended multiprotocol label switching (MPLS) network architecture is proposed in this thesis, which allows fast mobile IP access and diversity routing for traffic under fade condition. This supports nomadic access, reduced packet loss and improved service availability in BWA network during system outage. Also developed herein is a Diversity and Shadow Flow Merging Mechanism, which, besides sending a packet on its normal path, also duplicates the packet and sends it on a separate, diverted labelled path. The shadow flow merging mechanism is responsible for merging the normal flow and shadow flow together and delivering the merged packet to its destination. It is anticipated that the packet can be successfully delivered to the destination even if one path fails completely during the system outage.

The protocol is tested on a general BWA network that is configured with Digital Video Broadcast (DVB) downlink and Multi-Frequency Time Division Multiplex Access (MF-TDMA) uplink equipments. The protocol's ability of reducing packet loss and improving service availability, during the period of link failure, is verified. It is concluded that the protocol is effective in improving the service availability of BWA network.

To

My wife Yixia and daughter Haishan

Acknowledgements

I wish to thank:

My supervisors, Avril Smith and Chris Adams, for their guidance, endurance and encouragement throughout the period of my research;

Cranfield University for funding the research;

The Advanced Communications Unit (ACU) and the Radio Communications Research Unit (RCRU) of the Rutherford Appleton Laboratory for providing the equipment for the research and the opportunity to work on the IST-EMBRACE project.

Ken Craig, Jim Taylor, Rashmi Dravid of the RCRU; John Burren, Hilda Cook, of the ACU at the Rutherford Appleton Laboratory, and Chris Cooper of the Atlas Centre of UKERNA for their assorted help;

Michael Schmidt, Otto Koudelka, Johannes Ebert, Harry Schlemmer of the Joanneum Research, Austria;

Terje Tjelta of the Telenor Research and Development, Norway.

Avril Smith, Chris Adams, John Burren, Chris Cooper, Ian Whitworth, Jim Taylor, Hilda Cook and Michael Schmidt for proof-reading this manuscript.

My family, especially my mother and father for their constant encouragement and support.

Contents

List of Tables

List of figures

Glossary

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACTS	Advanced Communication Technologies Services
ADSL	Asymmetric Digital Subscriber Loop
AGC	Automatic Gain Control
AMI	ATM Management Interface
ARP	Address Resolution Protocol
BWA	Broadband Wireless Access
CBR	Constant Bit Rate
CN	Correspondent Node
CoA	Care-of Address
COS	Class of Service
CRABS	Cellular Radio Access for Broadband Services
DiffServ	Differentiated Services
DVB	Digital Video Broadcast
DVB-S	Digital Video Broadcast-Satellite
EMBRACE	Efficient Millimetre Broadband Radio Access for Convergence and Evolution
FA	Foreign Agent
FEC	Forward Equivalent Class
HA	Home Agent
HFC	Hybrid Fibre Coax
I^2C	Inter-IC
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internetworking Protocol
IPv4	IP version 4
IST	Information Societies Technology
LAN	Local Area Network
LDP	Label Distribution Protocol
LMDS	Local Multipoint Distribution System
LSP	label Switched Path
LSR	Label Switching Router
LSSR	Loose Source Route

MAC	Media Access Control
MD	Message Digest
MH	Mobile Host
MIP	Mobile IP
MIPintMPLS	Mobile IP Integration with MPLS
MIPoverMPLS	Mobile IP over MPLS
MN	Mobile Node
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NIC	Network Interface Card
NTP	Network Time Protocol
PCR	Peak Cell Rate
PVC	Permanent Virtual Connection
QoS	Quality of Service
RARP	Reversed Address Resolution Protocol
RF	Radio Frequency
RTT	Round Trip Time
SDL	Specification Description Language
SME	Small and Medium-sized Enterprise
SNR	Signal to Noise Ratio
SPI	Synchronous Parallel Interface
TCP	Transport Control Protocol
TE	Traffic Engineering
TIP	Temporary IP
TOS	Type of Service
TS	Transport Stream
TTL	Time-to-Live
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UTC	Coordinated Universal Time
VIP	Virtual IP
VoIP	Voice over IP
WAN	Wide Area Network
xDSL	Digital Subscriber Loop

Chapter 1 Introduction

The continuous growth of interest in broadband network access stimulates the research and development of a number of broadband access techniques, including hybrid fibre coax (HFC), digital subscriber loop (xDSL) (either asymmetric or symmetric), and broadband wireless access. Compared to other techniques, broadband wireless access system has the advantage of rapid and flexible deployment, wide service coverage and economic, etc. (Norbury 2000, Craig and Tjelta 2000, Embrace 1999). In Europe the frequency band 40.5 ~ 42.5GHz and other millimetre bands are allocated for the broadband wireless access system. The range of services to be provided via this system includes broadcast digital television, interactive services, Internet data, telephony (via Voice over IP - VoIP), and video conferencing. Excluding only digital television, traffic is carried in IP format. The potential users of the broadband network will be a large number of residential users, small and medium–sized enterprises (SMEs), and a certain amount of nomadic users. Tjelta, Nordbotten and Loktu (2000), Norbury (2000) and Loktu *et al* (1999) gave a general description of requirements for the broadband radio access network, which includes service types, coverage, available capacity per user, service availability, interoperability and interworking with other networks.

The challenge to the broadband wireless access system is not supplying broadband services, but developing a system that is cost efficient (i.e. one that most people can afford) with sufficient area coverage and acceptable service availability. Service availability here means the percentage of time that the service will be (un)available as a result of atmospheric degradation (Craig 2000, p.39). Service availability requirements of different services for a general broadband wireless access system are listed in (Norbury 2000, Loktu *et al* 1999) and are as follows:

• Telephone:	99.996%
• Internet:	99.9%
• Video Conference:	99.9%
• SMEs:	>99.9%

A service availability of 99.9% equates to about 8 hours loss of service per year, and 99.99% about 1 hour per year. However, the service availability of a broadband wireless access system is more likely to be influenced by many factors such as rain, snow, sleet, terrain, vegetation, etc. Based on the data of rainfall collected by the rain radar in Norway and the UK for more than a year, Craig *et al* (1999) gave a very detailed description of the rain attenuation and rainfall rate distribution, and reported that the principle propagation cause of system outage is the presence of rain, snow, and sleet on the path between the user and the base station. They stated that rain fade causes system service outage and degradation of service availability. They also showed that the rain attenuation and the service availability at the user's receiver could be improved by radio path diversity, in which two transmitters are separated with a certain degree of angle and pointed to one receiver, while the receiver uses the combination of signals received from both transmitters to obtain an improved signal to noise ratio (SNR).

This thesis takes another approach to improving the service availability — *Route Diversity*. This is an approach in which two identical traffic flows are sent to the same destination from two wide separated base stations via different routes, while the receiver merges the two flows into one and obtains improved packet deliverability in the wake of signal fading and link failure.

It would be better to minimise the time of service outage and therefore improve the service availability from the point of view of both the system operator and users. The route diversity is believed by the author to be an effective way to achieve this objective for broadband wireless access system.

1.1 EMBRACE Background

The research work described in this thesis originated from, and constituted a part of, a large European Commission project, EMBRACE, under the contract number IST-1999-11571 of the Information Society Technologies (IST) programme. The Efficient Millimetre Broadband Radio Access for Convergence and Evolution (EMBRACE) project (Embrace 1999) developed a low-cost and efficient broadband wireless access network combining broadcast and telecommunications, allowing for broadcast and point-to-multipoint services, and taking account of the requirements of service availability and quality of service (QoS). The system operates in the 40.5 - 42.5GHz band, uses DVB-S downlink and MF-TDMA uplink, connects to the Internet in large via an Asynchronous Transfer Mode (ATM) core network and diversity multi-protocol label switching routers developed in this research. The services that can be provided through such a setup include:

Broadcast digital television: digital television programmes are carried in transport streams (TS) and broadcast to all users within radio coverage of the system.

Internet access: the system provides Internet access service for users via local Ethernet connection and IP routers at the user station. Those supported Internet data services include web browsing, file transferring, email, telnet, etc.

Multimedia services: the system also supports services such as videoconferencing, telephony and other multimedia interactive service. Data traffic is carried in IP format via the DVB-S downlink and MF-TDMA uplink.

Nomadic access: this service allows customers' access equipment to be moved to anywhere inside the interconnection network whilst keeping the original configuration unchanged.

Route diversity: the system improves service availability through diversity techniques. A user might access two or more base stations and select the one which provided the optimum signal on a dynamic basis, thus mitigating the effects of rain attenuation and the possible service degradation or interruption. Issues relating to route diversity and nomadic access in the system inspired the work presented in this thesis.

Prospective use: by offering broadband interactive multimedia services, the system will specifically support new ways of working and living, for example, tele-working, tele-education, tele-medicine, etc. Although most of these services can also be provided by wire (cable) systems, the wireless technology has substantial advantages (e.g. rapid deployment of infrastructure system and provision of services within a very short time frame), particularly in remote areas where infrastructure is less or difficult to build.

The research presented in this thesis forms the EMBRACE work package: “Cell interconnection, diversity and mobility".

This research creates a network architecture which:

- Reduces the traffic produced by standard Mobile IP tunnelling and
- Creates diversity paths, which allow duplicated IP packets with identical destination addresses to take different paths through the network.

1.2 The Framework of This Research

While there have been many research activities related to the satellite-earth site diversity, there has been very little study focused on the terrestrial line of sight systems in particular, for broadband wireless networks such as that used in EMBRACE. Craig *et al*. (1999) proved that rain attenuation at the user site could be improved by radio path diversity, and consequently, the service availability can be improved. This result was acquired from more then one year's measurements and statistics of rainfall and rain attenuation. While the main concern of that research was the improvement of the signal to noise ratio after signal combination at the receiver, it is quite different to the route diversity scheme described in this thesis.

The diversity implementation in this research is based on the diversity architecture of EMBRACE, in which a diversity user is equipped with two transceivers and antennae which point to two base stations, so that the diversity user can physically access (transmit to and receive from) two base stations. This requires the diversity user to be located in the radio frequency (RF) overlapping area of both base stations. At the network layer, the route diversity will forward the same data packet from the two base stations to the diversity user. It is anticipated that packets transferred along one out-of-service wireless link are lost, but that they are successfully transmitted along a different wireless link.

Based on the assumption that route diversity can forward the same packet onto two different paths in the wireless system, we can state that the route diversity gives a higher possibility of successful packet transfer than a system without route diversity: in other words, the packet loss rate is lower and service availability is improved.

However, this architecture creates unresolved problems such as:

1. When and how should the diversity be started at the physical layer?

2. How should the same data packet from two base stations to one user be delivered, and what should be done at the user site when such diverted data packets arrive, from the point of view of the network layer?

3. How should nomadic access be supported?

The first problem is about what kind of diversity strategy should be used. This includes considerations of several aspects of the diversity procedure, for examples, the analysis of different diversity phases, diversity state transition, diversity criteria and the tagging of diverted packets. This is the main part of the diversity protocol.

The second problem needs more explanation. In current IP implementations, nodes use destination IP address longest-matching to forward packets to the next hop. This means that without modification to the current IP forwarding mechanism, a packet can only be forwarded onto one path. Because diversity will forward a packet onto two paths, a different approach is required. A packet combining method is also required when a destination receives two identical packets. These are the initiatives behind the label diversity protocol and flow merging mechanism developed in this research.

The third problem includes analysis of the normal mobile IP implementation, and improving the performance of traffic throughput of the nomadic access in broadband wireless access network by applying label switching technique.

The work described in this thesis is a protocol which uses diversity to improve the service availability of a broadband wireless access network. A diversity routing protocol and shadow flow merging mechanism are developed and implemented. The diversity protocol uses an alternative link—a diverted path—to protect the wireless access system from data packet loss and link failure. The diverted path carries the same traffic as the normal path. Packets in the diverted path and the normal path have different diversity labels. When the diverted traffic and the normal traffic meet at the egress router, they are merged to form one flow by the shadow flow merging mechanism. There might be several different scenarios for packets arriving at the destination, e.g. the original packet and the diverted packet both arrive, or only one arrives and the other one is lost because of the link failure, or both packets are lost. The shadow flow merging mechanism needs to take all these scenarios into account. The areas of study include an investigation into diversity label structure, route diversity phases transition and algorithm, the shadow flow merging mechanism and the merging algorithm.

The work to develop a mechanism that supports nomadic service with improved performance in broadband wireless access network system is aimed at solving the third problem. The nomadic access will be supported by the integration of Mobile IP (Perkins *et al* 1996a) with multi-protocol label switching (MPLS). In this mechanism, a home diversity label switch router will label switch packets for a nomadic services user. A notifying message exchange between the mobility agents and the diversity label switch routers is needed to allow the diversity routers to track the movements of a nomadic services user and to update their label switching table. To this end, the work includes investigation of the architecture of nomadic access in a route diversity domain, the format and usage of the notifying message, and the maintenance method of label switching table at the diversity router.

The ultimate objective of this research is to apply the implemented route diversity protocol to the broadband wireless access network with the expectation of improving service availability during the period of service outage. The application is installed on a network with RF equipment, and is assessed for functionality and effectiveness, by the insertion of noise, signal attenuation and man-made breakage of the wireless link.

1.3 Thesis Organization

This thesis is divided into three sections. The first section, Chapters 2-3, contains background information. The second section, Chapters 4-6, describes the designed protocols and mechanisms of route diversity. The last section, Chapter 7-9, discusses the experimental work and the conclusions drawn. The major part of Chapter 4, and Chapters 5, 6, 7, 8 and 9 in their entirety, are the author's own work and represent the contribution to the EMBRACE project.

A description of each chapter is as follows:

Chapter 2 provides a tutorial of IP mobility support techniques and standards, taken from RFC 2002 (Perkins *et al* 1996a). Discussion is focused around mobility support in IPv4 and the major protocol components. Several earlier mobility trials and mobility support in IPv6 are also presented in this chapter.

Chapter 3 gives a description of the multiprotocol label switching protocol, as defined to date in (Rosen, Viswanathan and Callon 2001a, Rosen *et al* 2001b). This includes the explanation of the format of label stack, labelled packet forwarding and typical MPLS applications.

Chapter 4 describes the method of integration of Mobile IP with MPLS. The integration architecture, the procedure of agent discovery and registration with MPLS, the tracking of movements, label-switching table maintenance, and the forwarding of packets via label tunnel are discussed. The notifying message is introduced, and its format and function are explained. This chapter also compares the integration with Mobile IP over MPLS application.

Chapter 5 describes the route diversity protocol developed in this research. It gives the aim and model of the route diversity, and analysis of the phases involved in the diversity. The diversity protocol is discussed throughout including the considerations at each diversity phase, the setup of a route diversity label switching table and the format of the route diversity label. This chapter lays the base of this research.

Chapter 6 discusses the shadow flow merging mechanism, which is a further extension of the diversity protocol. It defines the shadow flow and flow merging, and describes the mechanism of setting each field of the diversity label for shadow flow merging. The shadow flow merging algorithm is presented in this chapter with three possible merging scenarios.

Chapter 7 describes the experimental environment used to carry out the experiments in this research. Discussion includes both the hardware and software components of the system. Hardware components listed range from network equipment to broadband wireless equipment. The software components explained cover the major part of implementation of nomadic access support with the integration of Mobile IP with MPLS, diversity routing and shadow flow merging implementation.

Chapter 8 lists and discusses the experiments undertaken that individually test the various aspects of the nomadic access, diversity routing and shadow flow merging on the established testbed. The performance improvement of the MIPintMPLS is first tested. Then the performance of diversity router is benchmarked. The capability of reducing packet loss by diversity and shadow flow merging is measured with the random packet loss model. The final part of the experiments is the implementation and application of the diversity protocol in a real broadband wireless access network system. It demonstrates how the diversity improve the service availability during the normal service outage time, proves the usefulness and benefits of the work presented in this thesis.

Chapter 9 summarises the thesis and presents the final conclusions gained from the study, and briefly explains avenues of further research.

Chapter 2 Mobile IP

Abstract

This chapter gives a detailed description of the Mobile IP protocols. The basic protocol is described, with details given of the three major component protocols: Agent Advertisement, Registration, and Tunnelling. Mobility support in IPv6 and the differences with current Mobile IP are highlighted. Three host mobility trials are then reviewed before the emerging of the current Mobile IP standard - RFC 2002.

2.1 Mobile IP Overview

The Internet uses IPv4 (RFC791, 1981) as the internetworking protocol to connect all the computers together. Each node connected to the Internet is assigned a 32-bit unique number (IP address) to identify its point of attachment to the Internet. Nodes base their packet forwarding decisions on information contained in the IP header. Specifically, routing decisions are made based upon the network-prefix portion of the IP destination address. Therefore, a node must be located on the network indicated by its IP address to receive packets destined to it; otherwise, packets destined to the node would be undeliverable.

Without Mobile IP, one of the two following mechanisms typically must be employed for a node to change its point of attachment without losing its ability to communicate in the scenario of mobile computing:

- The node must change its IP address whenever it changes its point of attachment, or
- Host-specific routes must be propagated throughout the relevant portion of the Internet routing infrastructure.

Both of these alternatives are often unacceptable. The first makes it impossible for a mobile node to maintain transport and higher-layer connections when the node changes location. The second has obvious and severe scaling problems, especially relevant considering the explosive growth in scales of notebook computers.

Mobile IP solves the above problems with a scalable mechanism to enable nodes to change their point of attachment to the Internet without changing their IP address.

2.1.1 Thinking Node Mobility as a Trip

Solomon (1998) explained Mobile IP as a trip: imaging someone is going on a business trip that lasts for a long time. Because they will be away from home for a long time, they will need to arrange their mails to be delivered at their current address - a location which might often change. How might they arrange these mails to be delivered under such conditions?

One way is that they send a change-of-address notice to everyone who might send them some correspondence. There are many problems with this solution, however:

- The change-of-address notices have to be sent every time they move to a new location;

- They have to be sure to send the notice to all correspondents, otherwise an important mail may not be redirected.

- There is no way of preventing a malicious person from sending a bogus changing-of-address notice to the correspondents in order to intercept the mail.

A better way is to leave a forwarding notice at the individual's home post office, then any mail that arrives for the home address would be forwarded to the current care-of-address by the postal system. The advantages of this solution are:

- Only one entity, the home post office, is kept informed of the current care-of-address each time the location is changed, compared with sending change-of-address notices to all the potential correspondents in the former solution;

- Some security mechanisms can be implemented so that the post office can verify that the forwarding notice is genuinely sent by an individual, and that they are authorized to send the change-of-address notice to the post office.

By changing the word "mail" to "Internet Protocol data packet", "forwarding" to "tunnelling" and "post office" to "Mobile IP - enhanced router", then the preceding analogy describes how Mobile IP works almost exactly. The finer details will be introduced in the following sections.

2.1.2 Terminology

Mobile IP introduces three new functional entities (Perkins 1996a, Perkins 2002):

Mobile Node (MN)

A host or router that changes its point of attachment from one network or subnetwork to another, without changing its IP address. A mobile node can continue to communicate with other Internet nodes at any location using its (constant) IP address, assuming that link-layer connectivity to a point of attachment is available.

Home Agent (HA)

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 current location information for the mobile node.

Foreign Agent (FA)

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

A mobile node is given a home address, which is a long-term IP address on its home network. When away from its home network, a care-of address is associated with the mobile node and reflects the mobile node's current point of attachment. The mobile node uses its home address as the source address of all IP datagrams it sends, except when registering on a foreign network with a co-located care-of address[1] (CoA), the IP source address must be the care-of address.

The following terms are frequently used in connection with mobile IP:

Agent Advertisement

Foreign agents advertise their presence by using a special message, which is built by attaching a special extension to a router advertisement (Deering 1991) message.

Care-of Address

The termination point of a tunnel to a mobile node, for datagrams forwarded to the mobile node while it is away from home. There are two different kinds of care-of address: a *foreign agent care-of address,* an address of a foreign agent with which the mobile node is registered; and a *co-located care-of address*, an externally obtained local address which the mobile node has associated with one of its own network interfaces.

Correspondent Node (CN)

A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

Mobility Agent

Either a home agent or a foreign agent.

Mobility Binding

The association of a home agent address with a care-of address, along with the remaining lifetime of that association.

Tunnel

The path followed by a datagram while it is encapsulated. The model is that, while it is encapsulated, a datagram is routed to a knowledgeable decapsulating agent, which decapsulates the datagrams and then correctly delivers it to its ultimate destination.

[1] In RFC 2002 (Perkins 1996a), a co-located care-of address is defined as an external local IP address which is obtained by the mobile node in the foreign subnetwork and is associated with one of the mobile node's network interfaces. See the definition of Care-of Address in above.

2.1.3 Protocol Overview

The procedure that Mobile IP follows in routing a packet to the mobile node is the integration of three separable mechanisms:

- Discovering the care-of address;
- Registering the care-of address;
- Tunnelling to the care-of address.

The routing diagram of Mobile IP is drawn in Figure 2.1

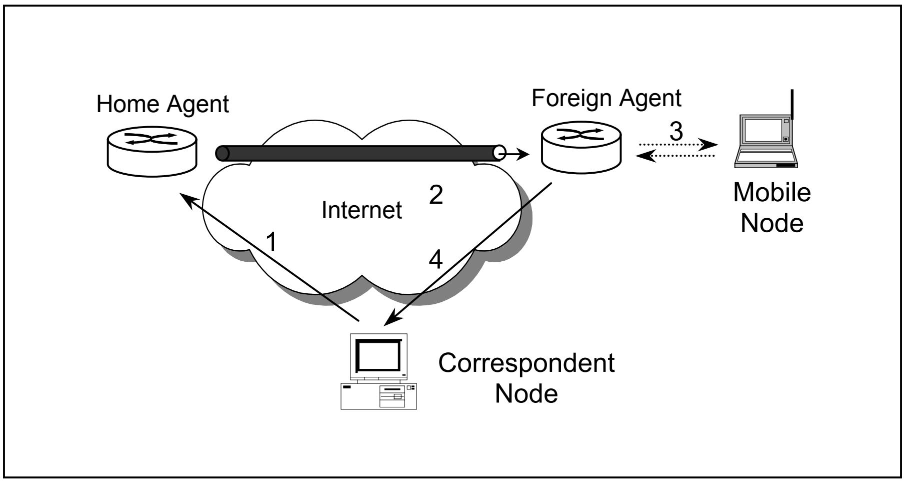


Figure 2.1 Mobile IP Datagram Flow

Figure 2.1 illustrates the routing of datagrams to and from a mobile node away from home, once the mobile node has registered with its home agent. The mobile node is presumed to be using a care-of address provided by the foreign agent:

1. A datagram to the mobile node arrives on the home network via standard IP routing.
2. The datagram is intercepted by a home agent and is tunnelled to the care-of address, shown by an arrow going through the tube.
3. The datagram is detunnelled and delivered to the mobile node.
4. For datagrams sent by the mobile node, standard IP routing delivers each to its destination. In Figure 2.1, the foreign agent is the mobile node's default router.

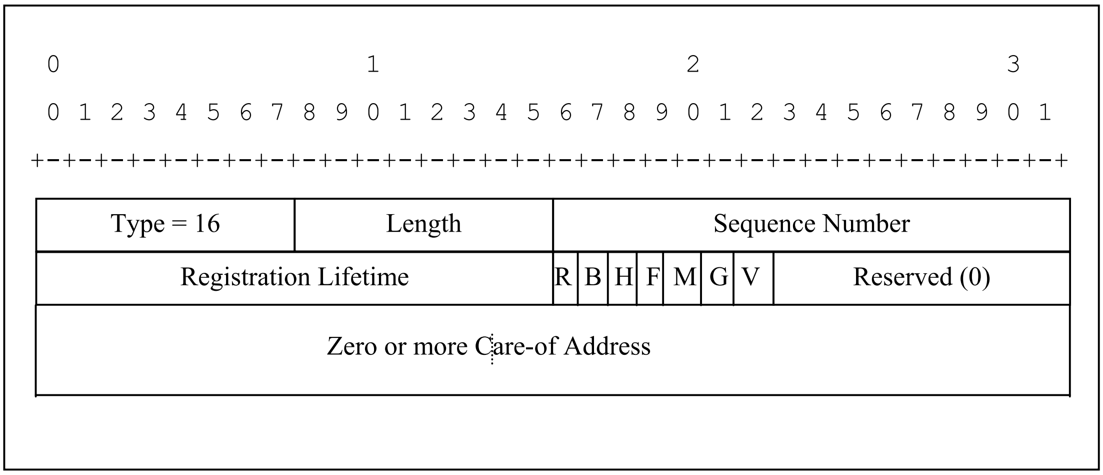
The next section will give more detail about the three cooperating parts of the protocol.

2.2 Mobile Agent Discovery

Mobile IP uses an agent discovery procedure to find the care-of address. The basic operation involves periodic broadcasts of advertisements by the mobile agents onto their directly attached sub-networks.

2.2.1 Agent Advertisement

An *agent advertisement* is an (ICMP) Router Advertisement (Deering 1991) that includes a mobility agent advertisement extension, and is shown in Figure 2.2.



```
 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 = 16   |    Length     |        Sequence Number        |
|   Registration Lifetime       |R|B|H|F|M|G|V|  Reserved (0)   |
|              Zero or more Care-of Address                     |
```

Figure 2.2 Mobility Agent Advertisement Extension Format

The type field allows mobile nodes to distinguish between the various kinds of extensions which may be applied by the mobility agent to the ICMP router advertisement; the type of mobility agent advertisement extension is 16. The length field is the length of this single extension, which only depends on how many care-of addresses are being advertised. Currently one care-of address will typically be advertised.

The flags (‘R’, ‘B’, ‘H’, ‘F’, ‘M’, ‘G’ and ‘V’) inform mobile nodes regarding special features of the advertisement, and are defined as follows:

- R Registration required. Registration with this foreign agent is required.
- B The foreign agent is busy.
- H The agent is a home agent.

- F The agent is a foreign agent.
- M Minimal encapsulation (Perkins 1996c).
- G GRE encapsulation (Hanks *et al* 1994).
- V Van Jacobson header compression (Jacobson 1990).

Note that bits 'H' and 'F' are not mutually exclusive, one mobility agent can offer services both as home agent and foreign agent.

The registration lifetime field is the longest lifetime (in seconds) that this agent is willing to accept in any registration request. The sequence number field is the count of Agent Advertisement messages sent since the agent was initialised. Special rules enable a mobile node to distinguish between foreign agent crashes, and wraparound of the sequence number field (Perkins *et al* 1996a).

2.2.2 Agent Solicitation

A mobile node is allowed to send *agent solicitation* messages in order to get mobility agent advertisements. An agent solicitation message is identical to an ICMP Router Solicitation (Deering 1991) message. Solicitations are only sent in the absence of agent advertisements and when a care-of address has not been determined through other means.

2.3 Registration

There are two kinds of registration messages, the *registration request* and the *registration reply*, both sent to User Datagram Protocol (UDP) port 434. The overall data structure of the registration messages is shown in Figure 2.3.

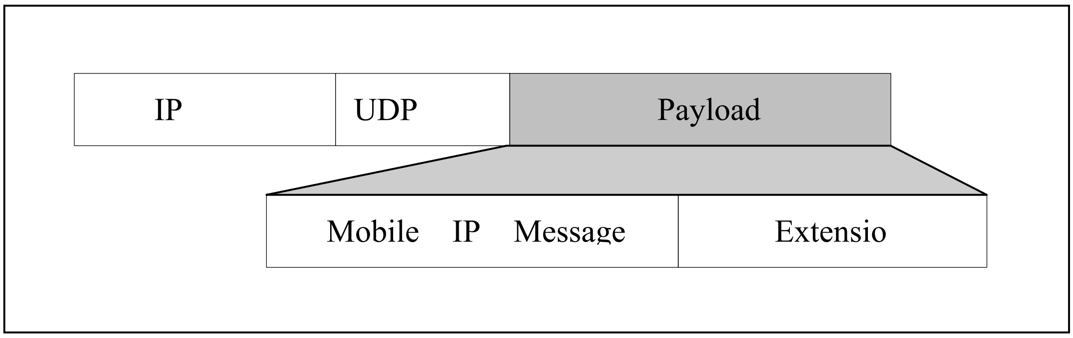


Figure 2.3 Mobile IP Registration Messages Structure

The request message allows the mobile node to inform its home agent of its current care-of address, how long it wants to use the care-of address, and any special features that may be available from the foreign agent. The foreign agent will pass the request to the home agent, and subsequently pass the reply from the home agent back to the mobile node.

2.3.1 Registration Request

After the IP and UDP headers, the registration request has the format illustrated in Figure 2.4.

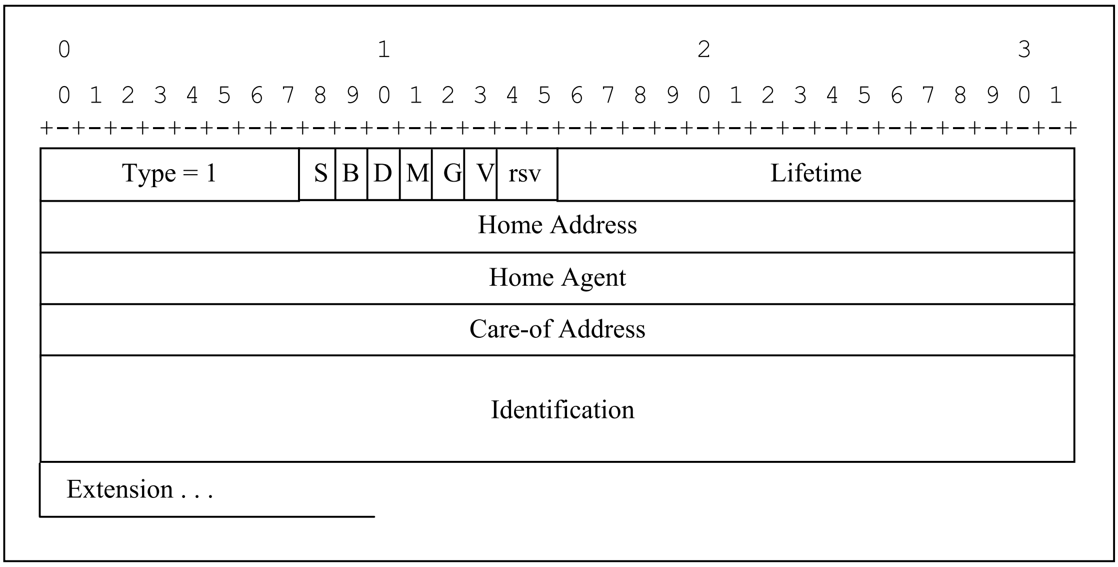


Figure 2.4 Registration Request Format

- The ‘V’ bit in the request informs the foreign agent whether *Van Jacobson compression* (Jacobson 1990) is desired.
- The ‘M’ and ‘G’ bits tell the home agent which additional encapsulation methods can be used.
- The ‘B’ bit is used to tell the home agent to encapsulate broadcast datagrams from the home network for delivery to the care-of address.
- The ‘D’ bit describes whether or not the mobile node is co-located with its care-of address, and is mainly useful for determining how to deliver broadcast and multicast datagrams to the mobile node.

The home address, home agent and the proposed care-of address are included in the request. The identification field is used for replay protection to secure the registration procedure. It is a 64-bit value that is calculated by the mobile node and checked by the home agent to identify each registration request. If the identification field is not valid the home agent sends a denying registration reply to the mobile node.

2.3.2 Registration Reply

Upon receiving a registration request, the home agent will send a reply to indicate whether the request is accepted or denied. The registration reply has the format illustrated in Figure 2.5.

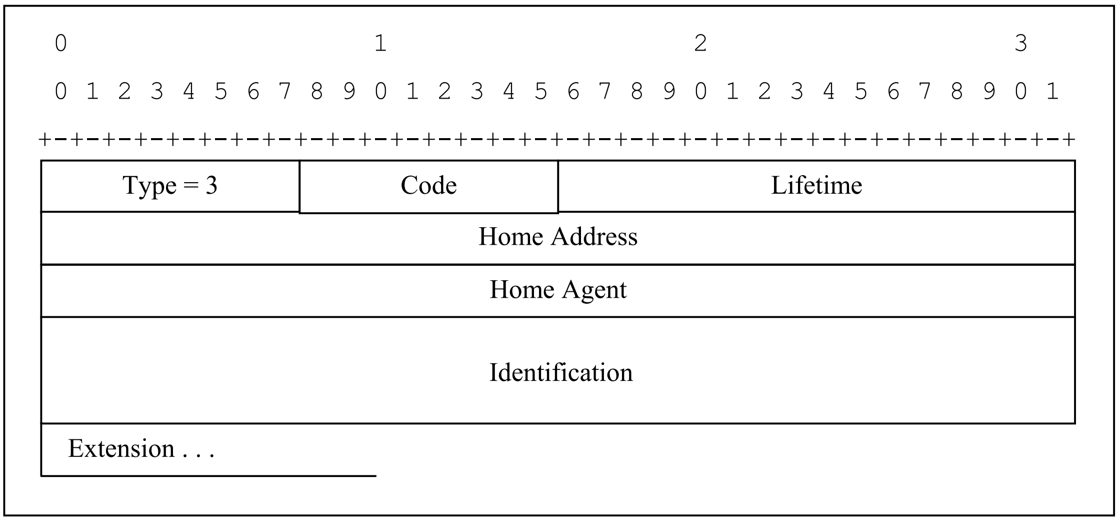


Figure 2.5 Registration Reply Format

The lifetime field tells the mobile node how long the registration will be granted by the home agent. It can be shorter than requested, but never longer. The code field describes the results of the registration request. If the registration succeeds, the code will be 0 or 1. If the registration fails, the code field offers details about what went wrong. Generally the code field will vary from 64 to 88 for a registration request denied by the foreign agent, and from 128 to 136 if denied by the home agent.

2.4 Routing and Tunnelling

After a successful registration, the home agent will begin to intercept datagrams destined for the mobile node and tunnel each one to the mobile node at its care-of address (see Figure 2.1). The tunnelling can be done by one of several encapsulation algorithms, but the default algorithm that must always be supported is simple IP-within-IP encapsulation, as described by Perkins (1996b).

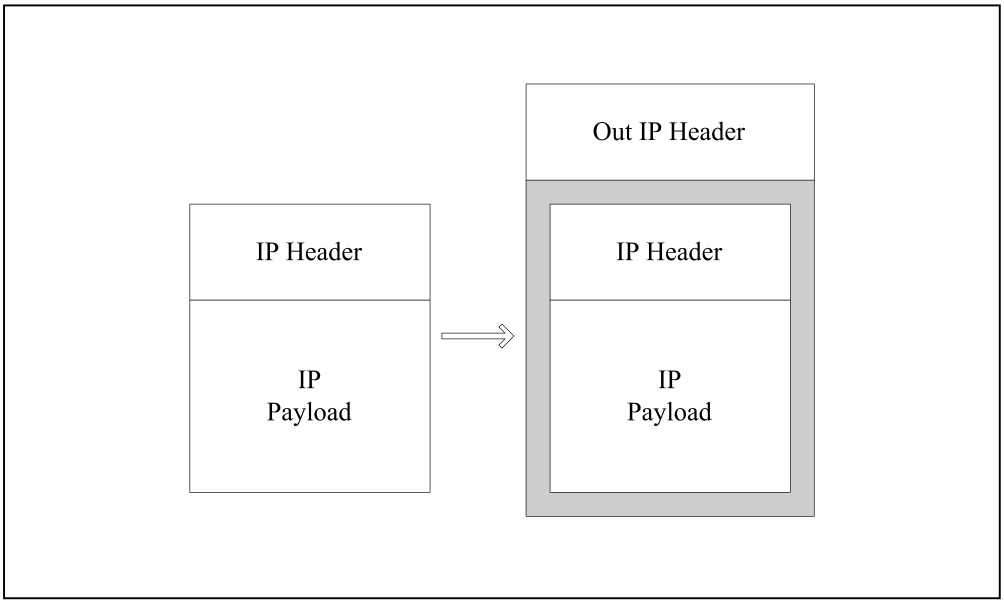


Figure 2.6   IP-within-IP encapsulation

Figure 2.6 shows how an IP datagram is encapsulated by preceding it with a new IP header (the tunnel header). The outer IP header Source Address and Destination Address identify the "endpoints" of the tunnel. The inner IP header Source Address and Destination Addresses identify the original sender and recipient of the datagram, respectively. The inner IP header is not changed by the encapsulator, except to decrement the TTL, and remains unchanged during its delivery to the tunnel exit point. No change to IP options in the inner header occurs during delivery of the encapsulated datagram through the tunnel. In the case of mobile IP, the values of the fields in the new header are selected naturally, with the care-of address used as the destination IP address in the tunnel header. The encapsulating IP header indicates the presence of the encapsulated IP datagram by using the value 4 in the outer *protocol field*[2].

Along the tunnel from home agent to foreign agent, the encapsulated packet is forwarded hop by hop according to the normal Internet routing mechanisms, until reaching the tunnel exit point – the care-of address. Then the outer header is stripped off and the original packet is delivered to the mobile node.

[2] This protocol field indicates the next level protocol used in the data portion of the Internet datagram. For example, 6 is for TCP, 17 for UDP, and 4 for IP (IP in IP encapsulation).

Packets from the mobile node, however, will take a direct route from the mobile node to the correspondent node without tunnelling through the home agent. This asymmetry is called triangle routing where a single leg of the triangle goes from the mobile node to the correspondent node, and the home agent forms the third vertex controlling the path taken by data from the correspondent node to the mobile node (Perkins 1996a).

2.5 Mobility Support in IPv6

IPv6 (Deering 1998) is the "next generation" of the Internet Protocol which will ultimately replace IPv4 as the primary network-layer protocol of the Internet. IPv6 differs in some very important ways from IPv4. The two biggest differences between IPv4 and IPv6 are the size of the IP addresses – 128 bits in IPv6 versus 32 bits in IPv4 – and the fact that many of the less frequently used fields in IPv4 have been moved out of the IPv6 header and into optional, extension headers.

Mobility Support in IPv6 (Johnson and Perkins 2000), as proposed by the Mobile IP working group, follows the design for Mobile IPv4. It retains the ideas of a home network, home agent, and the use of encapsulation to deliver packets from the home network to the mobile node's current point of attachment, while featuring the following:

- Foreign Agents are not needed in Mobile IPv6. The enormous IP address space allows very simple autoconfiguration of address. This allows a mobile node to acquire a co-located care-of address on any foreign network quickly and easily by using Stateless Address Autoconfiguration and Neighbour Discovery. As a result, the foreign agent function disappears from Mobile IPv6. This further implies that the only type of care-of address in Mobile IPv6 is the co-located care-of address.

- Route Optimization is built as a fundamental part of Mobile IPv6, unlike Mobile IPv4 where it is an optional set of extensions that may not necessarily be supported by all nodes.

- Ingress Filtering Routers are tackled. In Mobile IPv4, when a mobile node communicates with a correspondent node, it puts its home address as the source address of the packet. Thus the “ingress filtering routers” will filter out the packet and not let the packet pass through, as the source address of the packet is different from the network from which the packet originated. This problem is solved in Mobile IPv6 by putting the care-of address as the source address and having a Home Address Destination option, allowing the use of the care-of address to be transparent over the IP layer.

- Security is simplified. One of the biggest differences between IPv6 and IPv4 is that all IPv6 nodes are expected to implement strong authentication and encryption features [IP Authentication Header, IP encapsulating security payload (ESP)] to improve Internet security. This affords a major simplification for Mobility IPv6, since all authentication procedures can be assumed to exist when needed and do not have to be specified in the Mobile IPv6 protocol.

Mobility support in IPv6 is still in the state of “work in progress” as of this writing; it is one of the most important work items on the agenda of the Mobile IP working group, and, as such, features in the mobility support in IPv6 may change in the future.

2.6 Early Attempts to Host Mobility

A number of mobile IP systems (Ioannidis and Maquire 1993, Perkins 1993, Teraoka and Tokoro 1993, Teraoka *et al* 1994, Myles, Johnson and Perkins 1995) were proposed in the early 1990s. All share a notion of mobile host (MH), and Foreign Agent, which serve as temporary points of attachment to the Internet for roaming mobile hosts. All use existing Internet routing protocols to direct packets addressed to a mobile host to a stationary computer (home agent). The fundamental differences among these systems are:

- How a home agent knows where a mobile host is;
- How ordinary hosts send directly to a mobile host’s current foreign address, avoiding the wasteful trip through the home address;
- And how the mobile hosts’ movements are treated.

2.6.1 Columbia's System

In (Ioannidis and Maquire 1993) the Columbia's system is described. Its central idea is that all mobile host (MHs) belong to a single virtual subnet, each mobile host accesses the nearest Mobile Support Router (MSR). Each mobile support router tells the IP routing system that it has an interface onto the virtual subnet, so that normal IP routers will send packets for a mobile host to the nearest mobile support router.

The system operates as follows. A mobile host registers with whatever mobile support router happens to be in its accessing range, and periodically reconfirms this registration. This particular mobile support router thus knows where the mobile host is. When a correspondent host first sends a packet to the mobile host, the packet is forwarded to the nearest mobile support router by normal IP routing. If the mobile host is registered with that mobile support router, the mobile support router can deliver the packet to the mobile host directly. If not, then the mobile support router must find the mobile host. It sends a query to all the other mobile support routers requesting the location of the mobile host, and forwards the packet to whichever mobile support router responds. It caches the mobile host's location to avoid further broadcast queries.

When the mobile host moves to a new mobile support router, it informs the previous mobile support router of its new location. The previous mobile support router will cache this information and forward any packets for the mobile host to its new location. If the previous mobile support router receives a packet forwarded by another mobile support router, it sends that mobile support router a redirect message specifying the mobile host's new location. This redirect updates that mobile support router's cached location for the mobile host.

The Columbia system's points are that it sends packets by efficient routes, even from computers that are not aware of mobile hosts, and that it has no unnecessary points of failure. It does not scale well, because mobile support routers broadcast to each other. It does have a mode of operation with improved scaling, at the cost of inefficient routing. It has no authentication, and would be vulnerable to malicious location messages.

2.6.2 Sony's VIP System

Sony's VIP system (Teraoka and Tokoro 1993, Teraoka *et al* 1994) allows both correspondent hosts and intermediate routers to cache mobile host locations. Every mobile host has a permanent Virtual IP (VIP) and a Temporary IP (TIP) address. Using the normal IP routing system, Sony's scheme arranges that a packet addressed to the virtual IP will end up at the mobile host's home agent, and that a packet addressed to the temporary IP will end up at the mobile host's current location.

A mobile host is allocated a temporary IP each time it moves to a new location; the temporary IP is an address on a radio LAN at that location. The mobile host keeps its home agent informed of its temporary IP. When the home agent receives packets addressed to the mobile host's virtual IP, it forwards them to the mobile host's temporary IP.

When the mobile host sends a packet to a correspondent host, it includes its current temporary IP in a special IP option. An enhanced correspondent host is able to remember this temporary IP, and use it instead of the virtual IP for further communication with the mobile host. Packets sent to the temporary IP use a direct route to the mobile host through the Internet, avoiding the dog-leg route through the home agent. Ordinary correspondent hosts ignore the option, and continue routing through the home agent. When the mobile host moves and acquires a new temporary IP, it is not clear how it should notify an enhanced correspondent host. Such a correspondent host might continue sending to the old temporary IP until the mobile host sends it a packet containing the new temporary IP.

The problem with the Sony system is that it relies on the routers being Sony routers. In a network that includes other than Sony routers, the special IP option carrying the temporary IP information is likely to be dropped somewhere in the net by a non- Sony compatible router or host. Furthermore, the Sony system consumes a large number of IP addresses, because every mobile host is allocated a temporary IP when it is connected to a new location and the local address server must have as large an address space reserved as the maximum number of mobile hosts connected to it.

2.6.3 IBM's System

A mobile host in IBM's system (Perkins 1993, Myles, Johnson and Perkins 1995) has a permanent IP address. Each mobile host has a home agent, and the home agent tells the IP routing system that it is the gateway for its mobile hosts. Thus when a correspondent node sends a packet to the mobile host, it ends up at the home agent, which will forward it to the mobile host. When a mobile host moves to a new location, it finds a nearby foreign agent, and sends the foreign agent's address to the mobile host's home agent. The home agent tells the mobile host's previous foreign agent to forget about the mobile host.

When a mobile host sends a packet to a correspondent host, it includes an IP Loose Source Route option (LSSR) (Braden 1989). This option records the address of the mobile host's foreign agent. The correspondent host caches the foreign agent address, and sends any further packets for the mobile host via that foreign agent. If the mobile host moves, its old foreign agent will forward packets from the correspondent host to the mobile host's home agent. Any reply from the mobile host will carry the mobile host's new location, allowing the correspondent host to update its location cache.

If all Internet hosts implemented Loose Source Route correctly, IBM's system would provide efficient routing with no changes to either correspondents or routers. In fact the Loose Source Route has not usually been properly implemented. This means that most of the packets would be sent via the home agent, so that the proposed efficient routing is, in fact, inefficient.

2.7 Conclusion

This chapter gives a detailed explanation of the current Mobile IP protocol – RFC 2002. To provide mobility service for a mobile node, the protocol involves three phases: firstly the mobile node has to find a suitable care-of address in the range of a foreign network; secondly the mobile node has to register this care-of address with its home agent successfully; lastly the home agent intercepts packets destined for the mobile node and tunnelled them to the mobile node's current location – the care-of address. This procedure only needs the mobility agents (home agent and foreign agent) and the mobile node to be aware of the movements of the mobile node, no other participants (including the correspondent nodes) need to change anything. It is well scalable and widely deployable in the Internet. As a network-layer protocol, Mobile IP is completely independent of the media over which it runs. Thus, a mobile node employing Mobile IP can move from one type of medium to another without losing connectivity.

The mobility support in IPv6 is also briefly introduced. As the IPv6 uses 128-bit addresses, it has an enormous IP address space. All the mobile nodes can get a care-of address by autoconfiguration of IP address, thus the foreign agent is removed from Mobile IPv6. Other IPv6 features make the mobility support much simpler than in IPv4.

Several earlier systems supporting host mobility are introduced in the context of the evolution of Mobile IP. Although aiming to provide host mobility, these protocols make use of different approaches. The drawbacks in these protocols include heavy router broadcast, mobile enhancement of most routers, reserving a great number of IP spaces, etc. The application of these mobile protocols is limited to certain conditions.

Chapter 3 Multiprotocol Label Switching

Abstract

In this chapter, the Multiprotocol Label Switching (MPLS) protocol is briefly explained. We begin with the conventional IP packet forwarding mechanism, and then move on to introduce the concepts of Forward Equivalent Class (FEC) and MPLS label switching principles . The most important part of MPLS - the Label, is then described in detail. The chapter summarises four typical applications of MPLS in the Internet. This chapter, combined with the Mobile IP Chapter, lays the foundation of this research.

3.1 MPLS Introduction

To understand why MPLS is deployed while the current successful IP architecture is used widely, a review of the conventional IP packet forwarding mechanism is essential.

3.1.1 Conventional IP Packet Forwarding Mechanism

In order for systems to communicate with each other, they must be able to uniquely identify each other. Network addresses enable this. A TCP/IP address identifies an interface rather than a system. Typically, a host has only a single interface and then the system and interface are effectively one and the same - in other words the interface address is synonymous with the host address. However, routers usually support multiple interfaces, and each of these interfaces may have a separate network address. Although these separate network addresses belong to the same router, IP distinguishes between the two when it delivers packets.

IP defines a packet format in RFC 791 (1981) that contains an IP *Destination Address*, where each address is unique within the entire network and contains sufficient information for the network layer to deliver the packet to the ultimate destination. To arrive at the ultimate destination, a packet is forwarded from a source system to a destination system, on a next-hop basis, passing through intermediate nodes in the path from the source to the destination.

As far as an individual node is concerned, IP packets fall into two categories: those for which the node itself is the ultimate destination and those for which any other node is the ultimate destination. A node determines if it is the ultimate destination by comparing the IP destination address field of a packet with each of its own IP addresses. If any of the addresses match, then the node is the ultimate destination of the packet. Any packets received by a node for which it is the ultimate destination are consumed, i.e., passed to the higher-layer protocol indicated by the *IP protocol field* (RFC 791, 1981) within the IP header.

When a node receives a packet for which it is not the ultimate destination, the node must determine where to forward the packet in order to move the packet closer to its ultimate destination. This selection of a next-hop to forward the packet is called “making a forwarding decision” or “routing a packet”. Each node makes a forwarding decision for every packet that is transmitted by the node independently. Every IP node, whether it is a host or a router, has an IP routing table that is used to make a forwarding decision. The “longest matching prefix” rule, stated as follows, is used to make the decision:

- If there is a host-specific route that exactly matches a packet’s IP destination address, then this route must be used to forward the packet in preference to any matching network-prefix routes in the table.

- Otherwise, if there is a network-prefix route which matches the network-prefix portion of the packet’s IP destination address, then this route must be used to forward the packet in preference to any default routes and any network-prefix routes of shorten prefix-length.

- Otherwise, if there are one or more default routes, then one of these default routes can be used to forward the packet.

This hop-by-hop destination based forwarding mechanism brings the following constraints to the service in the Internet:

- As the packet traverses the network, the packet's IP header is parsed at every node for the "largest matching prefix" to make a forwarding decision. This certainly is CPU-expensive and inefficient. It imports an extra delay at every node for every forwarded packet.

- It implies that packets with the same destination that traverse the same node in the network will follow the same path from that node. This makes it difficult for the Internet architecture to support other services, such as providing paths that are specific to particular sources, to particular services at the destination, or to a particular class of service (CoS).

While MPLS is motivated by the "IP switching" to speed up IP packet forwarding without changes to existing IP routing protocols, it can be used in many different circumstances including Traffic Engineering[3] (TE), Differentiated Services[4] (DiffServ) with Quality of Service (QoS) assurances which will be necessary for many new applications.

3.1.2 Packet Forwarding in MPLS

The concepts of *Forwarding Equivalent Clas*s (FEC) and *Label* (Rosen *et al* 2001a) are important in MPLS:

- Forwarding Equivalence Class is a group of packets which are forwarded in the same manner (e.g., over the same path, with the same forwarding treatment).

- Label is a short fixed length physically contiguous identifier that is used to identify a Forwarding Equivalence Class, usually of local significance.

In MPLS, all packets are divided into a set of forwarding equivalence classes based on:

[3] In (Awduche *et al* 2001), Traffic Engineering is defined as that aspect of Internet network engineering dealing with the issue of performance evaluation and performance optimisation of the operational IP networks. The major objectives of Internet traffic engineering are to enhance the performance of IP traffic while utilizing network resources economically and reliably.

[4] Differentiated Services is a way of providing differentiated classes of service for Internet traffic, to support various types of applications, and specific business requirements. See (Blake *et al* 1998).

- IP source address, destination address;
- IP protocol;
- TCP/UDP source/destination ports;
- TTL[5], or type of service (TOS) field;
- Other information that the packet has, e.g., the arriving interfaces.

All packets which belong to a particular forwarding equivalence class and which travel from a particular node will follow the same path. The forwarding equivalence class to which the packet is assigned then is encoded as a label. When a packet is forwarded to its next hop, the label is sent along with it; that is, the packets are "labelled" before they are forwarded.

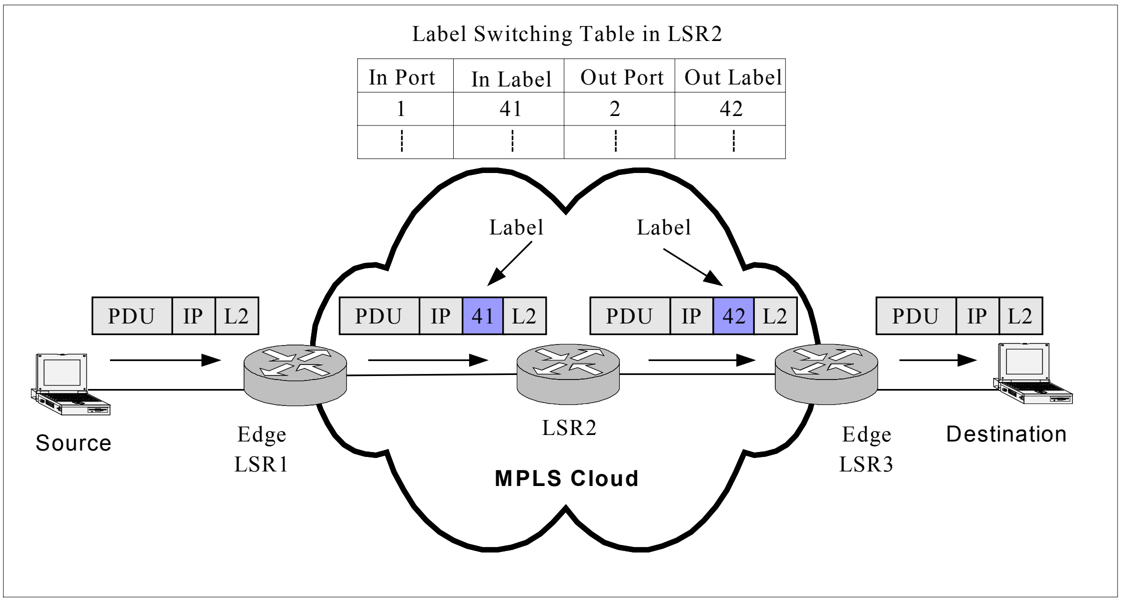
The assignment of a particular packet to a particular forwarding equivalence class is done just once, as the packet enters the network. At subsequent hops, there is no further analysis of the packet's IP header. Rather, the label is used as an index into a table that specifies the next hop and a new label. The old label is replaced with the new label, and the packet is forwarded to its next hop. The replacing of old label with a new label is referred as *Label Swapping*. Routers that forward packets based on label swapping are called *Label Switching Routers* (LSRs). The path through one or more label switching routers followed by a packet in a particular FEC is called *Label Switched Path* (LSP).

The label is removed at the egress router and the packet is re-forwarded based on the original packet.

Figure 3.1 shows an example of packet forwarding with MPLS. When the packet enters the MPLS domain, the packet header is analysed at the edge router LSR1. The packet is classified into a particular forwarding equivalence class and assigned a label (e.g., 41) according to the forwarding equivalence class to label binding table at router LSR1; then the packet is forwarded to the next hop – LSR2, along with the label. LSR2 examines the incoming packet's label and determines a new out label (e.g., 42) and the next hop. The packet is again forwarded to the next hop – edge router LSR3.

[5] Acronym of *Time to Live*, is a field in the IP header (see RFC 791) to indicate the maximum time the datagram is allowed to remain in the Internet system. Whenever the datagram passes through a router, its TTL get decremented by one. If the TTL reaches zero, then the datagram must be destroyed. The intention is to cause undeliverable datagrams to be discarded, and to bound the maximum datagram lifetime.

The label is removed at LSR3 and is forwarded to the packet's final destination by conventional packet forwarding.



Label Switching Table in LSR2

In Port	In Label	Out Port	Out Label
1	41	2	42
¦	¦	¦	¦

Figure 3.1 Diagram of MPLS (L2 here means the link layer)

The MPLS forwarding paradigm has a number of advantages over conventional packet forwarding:

1. MPLS forwarding can be done by switches which are capable of doing label look up and replacement, but are not capable of analysing the network layer headers.

2. When a packet enters the network, the ingress router can use any information it has to determine the assignment to the forwarding equivalence class. For example, packets arriving on different interfaces may be assigned to different forwarding equivalence classes. Conventional forwarding, on the other hand, can only consider information that travels with the packet in the packet header.

3. The same packet that enters the network at different routers can be labelled differently; as a result forwarding decisions that depend on ingress routers can be easily made. This allows the Internet to provide services for particular sources. This cannot be done with conventional forwarding, since the identity of a packet's ingress router does not travel with the packet.

4. With complicated considerations that determine how a packet is assigned to a forwarding equivalence class, very fine forwarding equivalence class granularity can be achieved without any impact at all on the routers that merely forward labelled packets.

5. A packet can be forced to follow a particular router which is explicitly chosen at or before the packet enters the network. In conventional forwarding, this requires the packet to carry an encoding of its route along with it. In MPLS, a label can be used to represent the route, so that the identity of explicit route need not be carried with the packet.

6. The label can be interpreted as a packet's preference or class of service, so that the router can apply different discard threshold or scheduling disciplines to different packets.

With these advantages, it is possible to implement new routing functionalities that are impossible with conventional IP forwarding. The Flow merging and QoS routing are particularly interesting for this research.

3.2 MPLS Label Format

A specific label format is not mandatory because MPLS is intended to work over any layer-two[6] protocols. Instead, label encoding is based strictly on mutual agreement between two neighbouring label-switching routers and has meaning only on the particular link between them.

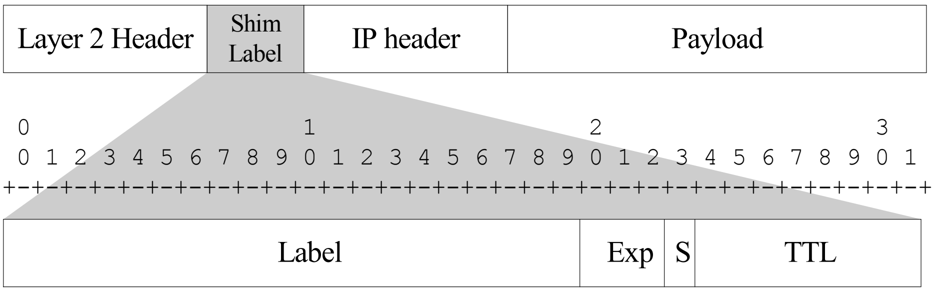
One format is that a label is inserted between the layer-2 and IP headers as a small *shim* label. A shim label, defined in (Rosen *et al* 2001b) and shown in Figure 3.2, consists of a 20-bit label value, 3-bit experimental field, 1-bit bottom of stack indication, and 8-bit time-to-live to prevent accidental looping. A packet may have been inserted several labels, i.e., a stack of labels that is represented as a sequence of label stack entries.

Each label stack entry is broken down into the following fields:

1. Bottom of Stack (S)

[6] Synonymous with link layer, it is the protocol layer that offers services used by the network layer.

This bit is set to one for the last entry (i.e., for the bottom of the stack) in the label stack, and zero for all other label stack entries.



Labe:	Label Value,	20 bits
Exp:	Experimental,	3 bits
S:	Bottom of Stack,	1 bit
TTL:	Time to Live,	8 bits

Figure 3.2 Format of Shim Label Stack Entry

2. Time to Live (TTL)

   This 8-bit field is used to encode a time-to-live value. An “incoming TTL” is referred as the value of the TTL field of the top label stack entry when the packet is received. An “outgoing TTL” is the result of the incoming TTL decreasing by one. Any further processing of the packet will use the outgoing TTL as the value of the TTL field of the packet’s new top label stack entry. When an IP packet is first labelled, the TTL field of the label stack entry is set to the value of the IP TTL field. When a label is popped and this label entry is at the bottom of the label stack, then the value of the IP TTL field will be replaced by the value of outgoing TTL.

   If the outgoing TTL of a labelled packet is zero, the packet’s lifetime in the network is considered to have expired; then the labelled packet should not be further forwarded and may be simply discarded.

3. Experiment Use (Exp)

   This 3-bit field is reserved for experimental use. In (Chen and H.Oh 1999), this field is referred as class of service.

4. Label Value

   This 20-bit field carries the actual value of the Label. When a labelled packet is received, the label value at the top of the label stack is examined by the label switching router to determine the next hop and the outgoing label. Before the packet is forwarded to the next hop, the label value at the top of the label stack is replaced by the outgoing label.

   There are several label values reserved (Rosen *et al* 2001b):

   a. *Label 0*: A value of 0 represents the "IP Explicit NULL Label". It is only valid at the bottom of the label stack. A packet with outgoing label 0 must be popped and forwarded then based on the IPv4 header (using conventional forwarding).

   b. *Label 1*: A value of 1 is reserved for the "Router Alert Label".

   c. *Label 2*: A value of 2 represents the "IPv6 Explicit NULL Label". Its meaning and processing is the same as that of label 0 except the forwarding is based on IPv6 header.

   d. *Label* 3: A value of 3 represents the "Implicit NULL Label". When a label switching router replaces the label at the top of the stack with a new label, but the new label is "Implicit NULL", the router will pop the stack instead of doing the replacement.

   e. Values 4 - 15 are reserved.

An important issue related to the label in MPLS is how to distribute the labels between neighbouring routers. Jamoussi (2001) and Awduche *et al* (2001b) gave two label distribution protocols (LDP) and this topic is out of the range of this research.

3.3 MPLS Applications

There are many applications for MPLS in the Internet, for example, Traffic Engineering, QoS Routing, Tunnelling and Flow Merging. These are described below.

3.3.1 Traffic Engineering

Traffic engineering allows that traffic flows are moved away from the shortest route and onto potentially less congested physical paths across the network (see Figure 3.3). This can be implemented to force a packet to follow an explicitly chosen route from the source to the destination.

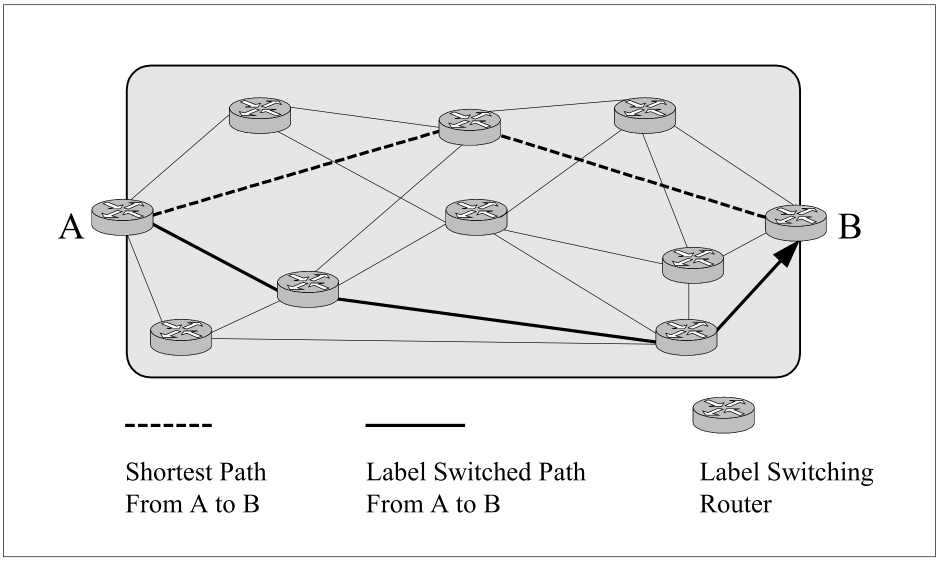


Figure 3.3 Traffic Engineering LSP .vs. Shortest Path

Traffic engineering is currently the primary application for MPLS. A successful traffic engineering solution can balance a network's aggregate traffic load on the various links, routes, and switches in the network so that none of its individual components is overutilised or underutilised. This results in a network that is more efficiently operated and provides more predictable service.

3.3.2 QoS Routing

Another application of MPLS is Quality of Service (QoS) routing. QoS routing refers to a method in which the route allocated to a particular traffic flow is chosen in response to the QoS required for that traffic flow. An MPLS network can set up multiple label switching paths between each pair of edge label switching routers. Each label switched path can be traffic engineered to provide different performance and bandwidth guarantees. An ingress router could place high-priority traffic in one label switched path, medium-priority traffic in another label switched path, best-effort traffic in a third label switched path, and less-than-best-effort traffic in a fourth label switched path. In this way, MPLS offers the network operator great flexibility in the different type of services that it can provide its users.

3.3.3 MPLS Tunnelling

When a packet enters the MPLS network, a label is inserted in the front of the packet's IP header, thus the packet is encapsulated within the MPLS network. MPLS creates a label switched path through the network for the labelled packet, then the packet switching follows this label switched path instead of routing the packet based on the destination address in the IP header. Hence MPLS effectively creates tunnels through the network.

This tunnel has a well-defined entrance, a well-defined exit, and a gate (forwarding equivalence class mapping) to control what is allowed into the tunnel. Packets entering the tunnel must pass the gating criteria. Once in the tunnel, there are no branch exits since the packet is not routed at intermediate nodes. Since only the network operator can create label switched paths, malicious users cannot create additional tunnel entrances or disrupt the network.

The overheads caused by the MPLS tunnelling depend on the depth of the label stack. In the case of a flat label stack, there is only one label stack entry and the overhead resulting from the tunnelling encapsulation is only four bytes.

3.3.4 Flow Merging

MPLS allows the mapping from IP packet to forwarding equivalence class to be performed only once at the ingress to the MPLS domain. A forwarding equivalence class is a set of packets that can be handled equivalently for the purpose of forwarding and thus is suitable for binding to a single label.

From a forwarding point of view, packets within the same subset are treated by the label switching router in the same way, even if the packets differ from each other with respect to the information in the IP header. The mapping between the information carried in the IP header of the packets and the forwarding equivalence class is many to one. That is, packets with different contents of their IP header could be mapped into the same forwarding equivalence class. For example, a set of packets whose IP destination addresses matches a particular IP address prefix can be mapped into a particular forwarding equivalence class, therefore the packets are labelled with the same label and follow the same label switched path in the MPLS domain.

Merged packets which have the same label are indistinguishable in the subsequent label switching routers, except at the egress router where the label is removed and the packets are forwarded by conventional forwarding.

3.4 Summary

This chapter provides an overview of MPLS, describing the label format and the label switching mechanism. Compared with conventional IP packet forwarding, it shows how MPLS forwards a packet with forwarding equivalence class binding and label swapping. MPLS has many advantages over the conventional IP packet forwarding, its typical applications include traffic engineering, quality of service supporting, flow merging, and traffic tunnelling. These were described.

Chapter 4 Integration of Mobile IP with MPLS

Abstract

This chapter proposes the integration of mobile IP with MPLS to get rid of the IP-in-IP encapsulation in the Mobile IP mechanism. It first introduces the necessities of this integration, then proposes a way to integrate in a single MPLS domain. The basic principle of the integration is to assign an outgoing label at the home label switching router for the mobile node; the assigned label is the same value as the label from the home agent to the foreign agent. Two MN moving scenarios are outlined for the label re-assignment. The notifying message exchanged between the mobility agents and the edge routers are introduced for the maintenances of label switching tables in the edge routers. The differences between the proposed integration scheme and Mobile IP over MPLS are listed.

4.1 Introduction

MPLS, as explained in Chapter 3, is a type of packet forwarding scheme. The packet entering the network is assigned a label according to the packet's forwarding equivalence class. A label switching router examines only the label when forwarding the packet and the IP packet header analysis is done only once when the IP packet enters the network. A labelled packet traverses the MPLS network along with an established label-switched path to the destination. A label-switched path can be seen as a tunnel starting with the ingress router and ending with the egress router. This tunnel is referred to as a *label tunnel* in this thesis.

Mobile IP is a protocol to provide mobility support over the Internet for mobile users. It is designed to serve the mobile users who wish to connect to the Internet and maintain communication as they move around. When a mobile node moves to a foreign network, the mobile node discovers its current location and registers the current location with the home agent. A tunnel between the home agent and the foreign agent is then established. IP packets destined for the mobile node will first arrive at the home agent and then be forwarded by the home agent to the mobile node's current location – the foreign agent – via this tunnel. The packet forwarding via tunnel involves two phases: IP-in-IP encapsulation and conventional IP forwarding. That is to say, a packet destined for the mobile node will have another IP header appended, and the forwarding decision of the encapsulated packet will be made at each intermediate node along with the tunnel from the home agent to the foreign agent.

For Mobile IP systems consisting of a large number of mobile users, it is crucial that the IP-in-IP encapsulation is efficient in terms of processing time at the home agent and the encapsulation overhead, and equally crucial is the time required to make a forwarding decision at each intermediate node. The amount of processing time required by the home agent depends on the number of mobile users belonging to the home network. If there are many such mobile nodes, the encapsulation processing will take a very long time. The packet overhead resulting from the extra IP header could cause the packet to be segmented and result in a longer transmitting time at the home agent. Considering that every packet forwarded by the home agent has to undergo a forwarding process, the overhead of this packet forwarding process may be too high.

The purpose of integrating Mobile IP with MPLS is to improve the packet forwarding performance and to mitigate the encapsulation overhead for mobility support in the MPLS core network. MPLS has fast label-swapping for packet forwarding and small encapsulation overhead for the label tunnelling, therefore the integration of these two protocols can compensate for the disadvantages discussed above. Another benefit is that the IP-in-IP tunnelling from the home agent to the foreign agent in Mobile IP is removed under the integration scheme.

4.2 Integration Mobile IP in MPLS domain

4.2.1 Integration Architecture Overview

The single MPLS domain integration architecture is shown in Figure 4.1. The home agent and the foreign agent are connected to the edge label switching routers LSR2 and LSR3. The functionalities of both the home agent and the foreign agent are kept unchanged as in pure Mobile IP. LSR1 is the ingress router and the correspondent node sends a packet to the mobile node. A general assumption here is that the home agent holds IP address *H.a.b.c*, the mobile node holds IP address *H.a.b.d*, and the foreign agent holds IP address *F.x.y.z*.

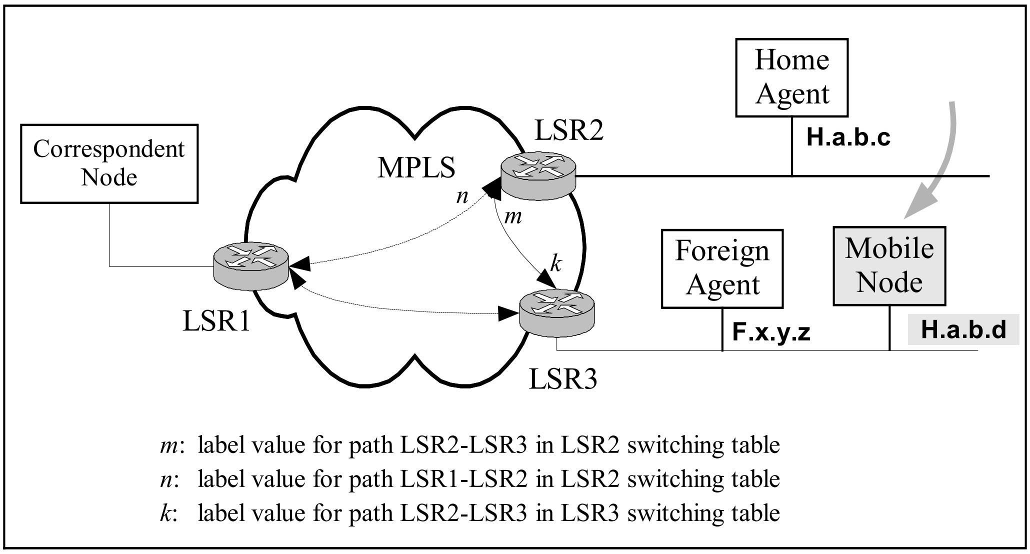

Home Agent
H.a.b.c
Correspondent Node
MPLS
LSR2
n
m
k
LSR1
LSR3
Foreign Agent
F.x.y.z
Mobile Node
H.a.b.d
m: label value for path LSR2-LSR3 in LSR2 switching table
n: label value for path LSR1-LSR2 in LSR2 switching table
k: label value for path LSR2-LSR3 in LSR3 switching table

Figure 4.1 Architecture of Integration Mobile IP in a MPLS Domain

4.2.2 Agent Discovery and Registration with MPLS

The mobile node uses the same method as in pure Mobile IP to determine its current location when it receives agent advertisements from a mobility agent. If the mobile node determines it is in a foreign network, it will get a care-of address from the foreign agent and send a registration request to the foreign agent. Note that the foreign agent functions as a normal mobility agent: it will forward the registration request to the home agent with conventional IP forwarding. When the request enters the edge router LSR3, the IP header of the registration request packet is analysed and labelled; the labelled request is then forwarded on the basis of the label-switched path between LSR3 and LSR2. When the labelled request arrives at LSR2, the label is removed from the packet and the request packet is restored to its original format. LSR2 then forwards the registration request to the home agent.

When the home agent receives the registration request message, it will complete all the procedures involved in a successful registration. Should the registration be granted, a registration reply message is sent to the foreign agent and forwarded to the mobile node by the foreign agent. The reply message also follows a label-switched path to LSR3 since it enters LSR2 and the MPLS network.

Because the exchanging of the registration request and reply is between the home agent and the foreign agent (although the mobile node triggers off the registration procedure, the request is sent to the foreign agent initially), the registration messages are forwarded along the label-switched path between the edge routers LSR2 and LSR3.

After the registration reply is sent to the mobile node from the home agent, the home agent will notify the edge router LSR2 to set up a Forwarding Equivalence Class and label binding entry for the away mobile node. LSR2 will first search its label switching table to find the row with the mobile node home address as the FEC entry, then the out label associated with the FEC of the foreign agent will be found and used as the out label for the mobile node FEC. After that, LSR2 changes the row that uses the mobile node home address as FEC in its label-switching table. It sets the out label and outgoing port entries to the value of the out label and outgoing port of the label-switched path from the home agent to the foreign agent. In this way, the edge router LSR2 in the home network can forward the packets destined for the mobile node home address to its current location in the foreign network. The modified label-switching table in edge router LSR2 is shown in Table 4.1.

FEC	In Label	Incoming Port	Out Label	Outgoing Port	Comments
F.x.y.z	Null_label	p	m	r	HA to FA
H.a.b.d	n	q	m	r	CN/HA/MN
⋮	⋮	⋮	⋮	⋮	⋮

Table 4.1 Example of Label Switching Table of Edge Router LSR2

Table 4.1 is an example of a label switching table of home edge router LSR2 after registration is accepted. In the architecture shown in Figure 4.1, the foreign agent care-of address is *F.x.y.z* and the mobile node home address is *H.a.b.d*. For the label-switched path from home agent to foreign agent, the out label is *m* and the outgoing port is *r*. The first row of Table 4.1 is about this binding of FEC to label for path from the home agent to the foreign agent. Since LSR2 is the ingress router, the in label value entry is zero (*Null_label*[7]). The second row is the label switching entry for the path from the correspondent node to the mobile node. Since LSR2 is the egress router for the packet to the mobile node's home address, the out label value is initially a *Null_label* and the outgoing port is empty; this means that the packet to the mobile node will be forwarded by the conventional IP forwarding mechanism. Because the mobile node moves to the foreign network, LSR2 will set these two entries to the value of the out label and the outgoing port of the path from the home agent to the foreign agent, i.e. out label *m* and outgoing port *r*, after LSR2 receives notification from the home agent about the registration.

When the foreign agent receives the registration reply, it relays the reply to the mobile node. The difference with pure Mobile IP is that the foreign agent notifies the foreign edge router LSR3 to set up a label switching entry in the label switching table of LSR3. LSR3 will first add an entry with the mobile node home address as the forwarding equivalence class. The value of the in label and incoming port for this FEC class are set to the same as that of the path from the home agent to the foreign agent. The value of the out label is set to *Null_label* and the outgoing port is set to empty; this means that the packet for mobile node will be forwarded from router LSR3 by conventional IP forwarding mechanism. This is shown in Table 4.2.

FEC	In Label	Incoming Port	Out Label	Outgoing Port	Comments
F.x.y.z	k	j	Null_Label	-	to FA
H.a.b.d	k	j	Null_Label	-	to MN
⋮	⋮	⋮	⋮	⋮	⋮

Table 4.2 Example of Label Switching Table of Edge Router LSR3

In Table 4.2, the first row is about the forwarding equivalence class *F.x.y.z*, which is the foreign agent in the architecture shown in Figure 4.1. For the FEC binding to the foreign agent, the in label is *k* and the incoming port is *j*, respectively. Because router LSR3 is the egress router for the label-switched path to the foreign agent, the out label

[7] Here ***Null_label*** stands for the "IP Explicit NULL Label" in MPLS. The value of Null_label is zero. See the label value explanations in §4.2.

is *Null_label* and the outgoing port is empty. For the second row of Table 4.2, its forwarding equivalence class is *H.a.b.d*, which is the mobile node home address. LSR3 will set the value of the in label and incoming port for the mobile node FEC to the same value as that of the foreign agent FEC. The out label and outgoing port number are also copied from the first row. Packets label-switched to router LSR3 and destined for the mobile node home address will be forwarded to the mobile node from LSR3 by conventional IP forwarding.

4.2.3 Datagram Delivery to Mobile Node via Label Tunnel

There are two possibilities for the locations of mobile node: mobile node is either in the home network or has moved to a foreign network. In both cases, datagrams from the correspondent node to the mobile node are firstly destined to the mobile node home network along a label-switched path. In the architecture in Figure 4.1, the label-switched path is from the edge router LSR1 to the edge router LSR2.

If the mobile node is in the home network, the label-switching table of LSR2 will have a row in which the forwarding equivalence class is the mobile node's home address. Router LSR2 is the egress router for the labelled packet destined for the mobile node, therefore the value of the out label will be *Null_label* and the outgoing port is empty. The in label and incoming port is unchanged as in Table 4.1. Thus the labelled packet will be delivered to the IP layer in LSR2 and then forwarded to the mobile node by conventional IP forwarding.

If the mobile node is in the foreign network, packets from the correspondent node to the mobile node still arrive firstly at the edge router of the home network along a label-switched path. After a successful registration with the home agent, the label switching table in router LSR2 modifies the row with the mobile node home address as the forwarding equivalence class as shown in Table 4.1: the value of the out label and outgoing port are the values of the label-switched path from the home agent to the foreign agent. The packet is then delivered from the home edge router to foreign edge router along the label-switched path from home agent to foreign agent. The foreign edge router LSR3 receives the packet and looks up its label-switching table (see Table 4.2). Since it is the egress of the label-switched path from home agent to foreign agent and the out label is *Null_label* and outgoing port is empty, the foreign edge router removes the label and sends the packets to the IP layer. Finally, the foreign edge router forwards the packet to the mobile node based on the conventional IP forwarding. At this point, it is not necessary that the packet is firstly forwarded to the foreign agent and then forwarded to the mobile node by the foreign agent, because the foreign edge router has been notified of the existence of the mobile node after a successful registration and has already set up a host-specific IP forwarding route to the mobile node. The mobile node receives the packet sent by the correspondent node.

The datagram delivering procedure is depicted by Figure 4.2.

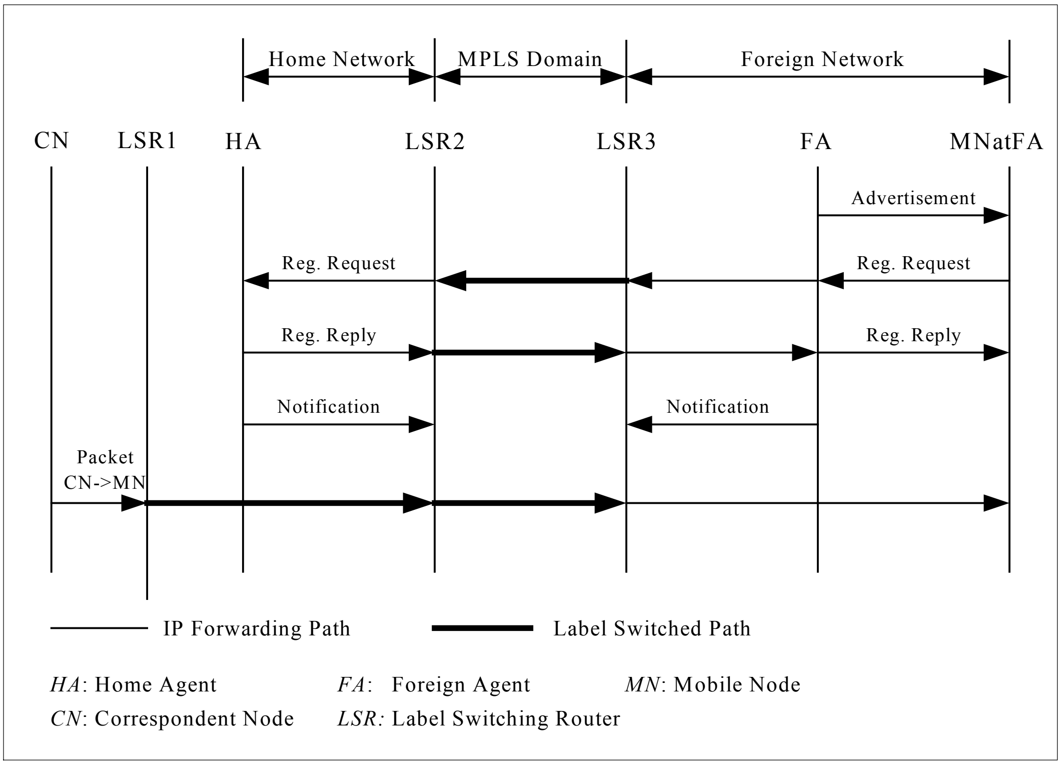


Figure 4.2 Datagram Delivering Procedure via Label Tunnel

4.2.4 Mobile Node Stay in Foreign Network

During its stay in the foreign network, the mobile node needs to regularly register its current location – the foreign agent care-of address – with the home agent before its current registered lifetime is due to expire, just as in pure Mobile IP. Each accepted registration forces the home agent and the foreign agent to notify the related edge routers to maintain their label switching tables and refresh the related entries. In this way, the label-switched path for mobile node from the home network to foreign networks will keep activated within the registered lifetime.

If the registered lifetime has expired and no new registration is accepted, the home agent and the foreign agent should not serve the mobile node anymore. This results in the home agent sending a notifying message to the home edge router to disable the label-switched path that uses the mobile node home address as forwarding equivalence class. To disable the label-switched path, the simplest way is to clear all entries for the mobile node row in the label-switching table of the home edge router. In the architecture shown in Figure 4.1, for example, if the registered lifetime of the mobile node has expired, the second row in Table 4.1 will be cleared. The same clearing procedure occurs also in the foreign network: the foreign agent sends a notifying message to the foreign edge router to indicate the expiry of lifetime, the foreign edge router then clears the row with the mobile node home address as the forwarding equivalence class from its label-switching table. In Table 4.2 the second row is cleared.

The whole registration procedure described in Section 4.2.2 will be started again if the mobile nodes are booted from power-off states in the foreign network. In this case, the label-switching tables in the edge router LSR2 and LSR3 will show the same as in Table 4.1 and Table 4.2 for the network architecture shown in Figure 4.1.

4.2.5 Mobile Node Moves to Another Foreign Network

The network diagram for a mobile node moving from one foreign network to another is shown in Figure 4.3. Assume Foreign Agent 2 is the new foreign agent and its IP address is *F'.u.v.w*.

Once the mobile node enters the new foreign network, it will follow the registration procedure described in section 4.2.2 to register with the home agent. For the scenario in Figure 4.3, if the registration is successful and the home label switching router LSR2 receives a notifying message from the home agent, LSR2 will modify its label switching table to forward the packet destined for the mobile node home address to the new foreign network. The modified label-switching table in LSR2 is shown in the Table 4.3.

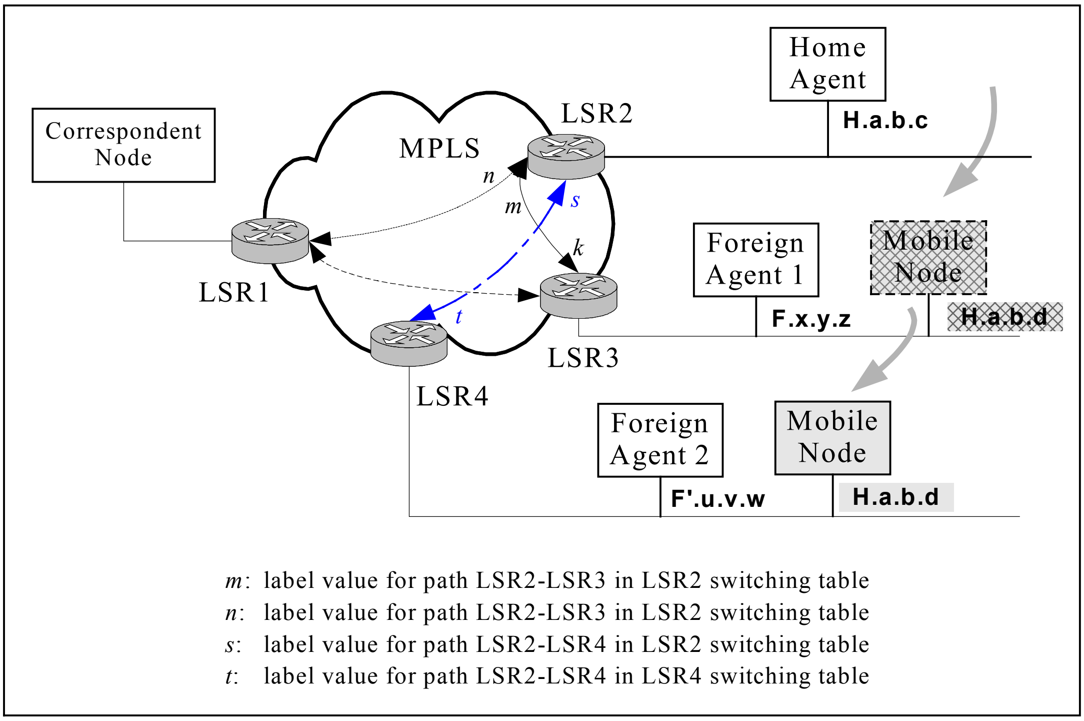

Home Agent
Correspondent Node
MPLS
LSR2
H.a.b.c
n
m
s
k
LSR1
Foreign Agent 1
Mobile Node
F.x.y.z
H.a.b.d
t
LSR3
LSR4
Foreign Agent 2
Mobile Node
F'.u.v.w
H.a.b.d
m: label value for path LSR2-LSR3 in LSR2 switching table
n: label value for path LSR2-LSR3 in LSR2 switching table
s: label value for path LSR2-LSR4 in LSR2 switching table
t: label value for path LSR2-LSR4 in LSR4 switching table

Figure 4.3 Diagram of Mobile Node Moving from One Foreign Network to Another within a Single MPLS Domain

FEC	In Label	Incoming Port	Out Label	Outgoing Port	Comments
F.x.y.z	Null_label	p	m	r	HA to FA1
H.a.b.d	n	q	**m→s**	**r→g**	CN/HA/MN
F'.u.v.w	Null_label	p	s	g	HA to FA2
⋮	⋮	⋮	⋮	⋮	⋮

Table 4.3 Example of Label Switching Table of Edge Router LSR2 After Mobile Node Moving to a New Foreign Network

The third row in Table 4.3 is for the label-switched path from LSR2 to the new foreign agent. The new foreign agent IP address *F'.u.v.w* is the forwarding equivalence class. LSR2 is the ingress router for this path, therefore the in label is *Null_label*. The second row is for the label-switched path from LSR2 to the current location of the mobile node. After the mobile node moves to the new foreign agent, the out label and outgoing port of the second row are modified to the same value as that of the third row. The packet from the correspondent node to the mobile node is label-switched to LSR2 along path LSR1-LSR2; LSR2 receives the packet with in label *n* from incoming port *q*. LSR2 looks up its label-switching table and outputs the packet with label *s* to outgoing port *g*.

After label-swapping along path from LSR2 to LSR4, the packet finally arrives at LSR4 with label *t*. LSR4 now decides to remove the label and deliver the packet to the mobile node with conventional IP forwarding.

The registered lifetime in the previous foreign agent (Foreign Agent 1 shown in Figure 4.3) expires after no succeeding registrations for sometime. The previous foreign agent then sends a notifying message to its edge router LSR3; the edge router will modify its label-switching table to disable the row with the mobile node home address as forwarding equivalence class. In Figure 4.3, this causes the edge router LSR3 and Foreign Agent 1 to stop providing service for the away mobile node.

4.2.6 Mobile Node Moves Back Home

In this section, the packet delivering procedure after the mobile node returns to its home network is discussed.

When the mobile node returns to the home network, it sends a de-registration request with the requested zero lifetime to the home agent. The de-registration procedure in the home agent is the same as described in the Mobile IP protocol. If the de-registration request is accepted, the home agent will send a notifying message to the edge label switch router at the home network. The edge router then needs to modify its label-switching table for the row with the mobile node home address as the forwarding equivalence class. Because the mobile node is at home and the edge router is the egress for packets to the mobile node, the out label for the mobile node entry is set to *Null_label* and the outgoing port is set to the port to which the home network is connected. If the de-registration is rejected by the home agent, the home agent will send a notifying message to the edge label switching router; this will force the router to delete the entry with mobile node home address as forwarding equivalence class from the label switching table for the reason of securing the network. In the scenario of Figure 4.1, the modified label-switching table in edge router LSR2 after a accepted de-registration has entries shown in Table 4.4.

FEC	In Label	Incoming Port	Out Label	Outgoing Port	Comments
F.x.y.z	Null_label	p	m	r	HA to FA
H.a.b.d	n	q	Null_label	p	CN/HA/MN
⋮	⋮	⋮	⋮	⋮	⋮

Table 4.4 Examples of Label Switching Table of LSR2 After Mobile Node Moving Back Home

In Table 4.4, the second row is for the mobile node forwarding from edge router LSR2 to the mobile node. Packets from the correspondent node are received at incoming port *q* with in label *n* by edge router LSR2. With label *n* as an index, LSR2 looks up its label-switching table and determines the out label and outgoing port. In this case the out label is *Null_label*, which means the packets need to strip off the label and be delivered to the destination by conventional packet forwarding.

After the mobile node has left the foreign network, no registration request is received by the foreign agent. The registered lifetime in the foreign agent is expired after the period of a lifetime. The edge router in the foreign network will delete the forwarding equivalence class for the mobile node from its label-switching table. Afterwards, the processing in the foreign agent and the foreign edge router is the same as described in Section 4.2.5.

4.3 Notifying Message

In the proposed integration scheme, mobility agents are only responsible for the mobile node’s registration process. The IP-in-IP encapsulation, the packet interception by the home agent and the IP packet tunnelling are all removed from the integration scheme. Instead we use a label tunnel from the home edge router to the foreign edge router for delivering packets to the mobile node. The edge routers respond to the registration process by receiving a notification from the mobility agents. If the mobility agent accepts a registration request, it notifies the edge router to set up a label-switched path for the mobile node to its current location; if the registration request is denied, the mobility agent notifies the edge router to tear down the established label-switched path for the mobile node. The format of the notifying message is shown in Figure 4.4.

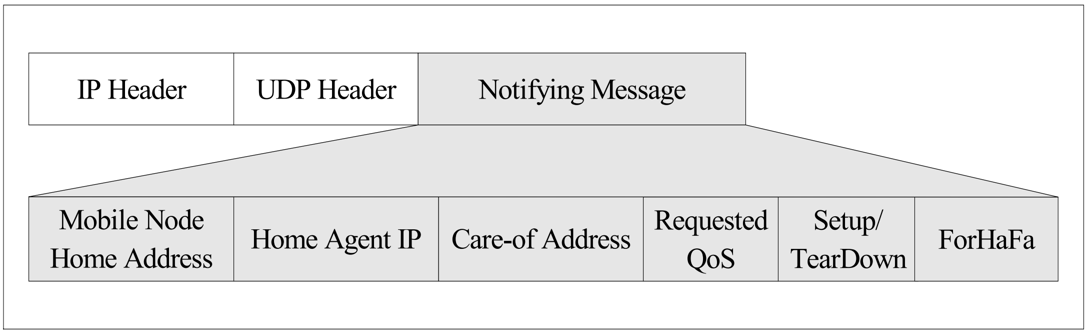


Figure 4.4 Format of Notifying Message

The Mobile Node Home Address, the Home Agent IP and the Care-of Address fields are self-explanatory. They have the same meaning as in the Mobile IP protocol. When the mobile node registers with the home agent from the foreign agent, the care-of address is the IP address of the foreign agent; when it returns home and de-registers with the home agent, the care-of address is the IP address of the home agent. To support multiple mobile nodes which might be in different foreign networks, the mobile nodes home addresses and the care-of addresses are needed to send to the edge routers.

The *Requested QoS* field is used to indicate the class of services for this mobile node. The supported QoS will be discussed in Chapter 7.

The *ForHaFa* is used to indicate the type of mobility services the mobility agent is serving as. A mobility agent can act as the home agent for some mobile nodes and also as the foreign agent for other mobile nodes in the proposed integration scheme.

The *Setup/TearDown* field is used to indicate the type of label switching table maintenance in the edge router. The edge router adheres to the following principles to maintain its label-switching table:

- If the home agent accepts a registration request, the home agent will send a notifying message with Setup/Teardown field set to true (setup) to the home edge router. The home edge router then will set up a label-switched path from the home edge router to the edge router in the foreign network. The label-switched path will use the mobile node home address as the forwarding equivalence class.

- If the label-switched path to be set up already exists in the label-switching table, the edge router will keep the path activated until further notification is received.

- When the foreign agent relays the accepted registration reply to the mobile node, it also sends a notification to the edge router in the foreign network, this will make the edge router in the foreign network maintain its label-switching table. As a result a label-switched path for the mobile node is also set up in the foreign edge router. The path will use the mobile node home address as the forwarding equivalence class and *Null_label* as the out label.

- If a registration request is rejected by either the home agent or the foreign agent, a notification is also sent to the edge router with Setup/Teardown field set to false (teardown). In this case, the edge routers who receive this notification will have to delete the established label-switched path for the mobile node. If no such path exists, the notification is simply ignored.

4.4 Integration and Mobile IP over MPLS

Mobile IP can be used in the MPLS networks with another configuration - Mobile IP over MPLS (MIPoverMPLS). By Mobile IP over MPLS, we mean that all the three entities (the mobile node, the home agent and the foreign agent) and their functions are the same as in pure Mobile IP without any changes; the MPLS network is merely used as a core network. The main features of the Mobile IP protocol, including IP-in-IP encapsulating in the home agent, packet intercept by the home agent and tunnelling from the home agent to the mobile node, are unchanged. In addition, when an IP-in-IP encapsulated packet passes through the MPLS network, it is again labelled by the label-switching router. This imports another layer of encapsulation. When the network in Figure 4.1, for example, is used as the architecture for Mobile IP over MPLS, the packet delivering procedure for both Integration and Mobile IP over MPLS can be drawn as in Figure 4.5 for the purpose of comparison.

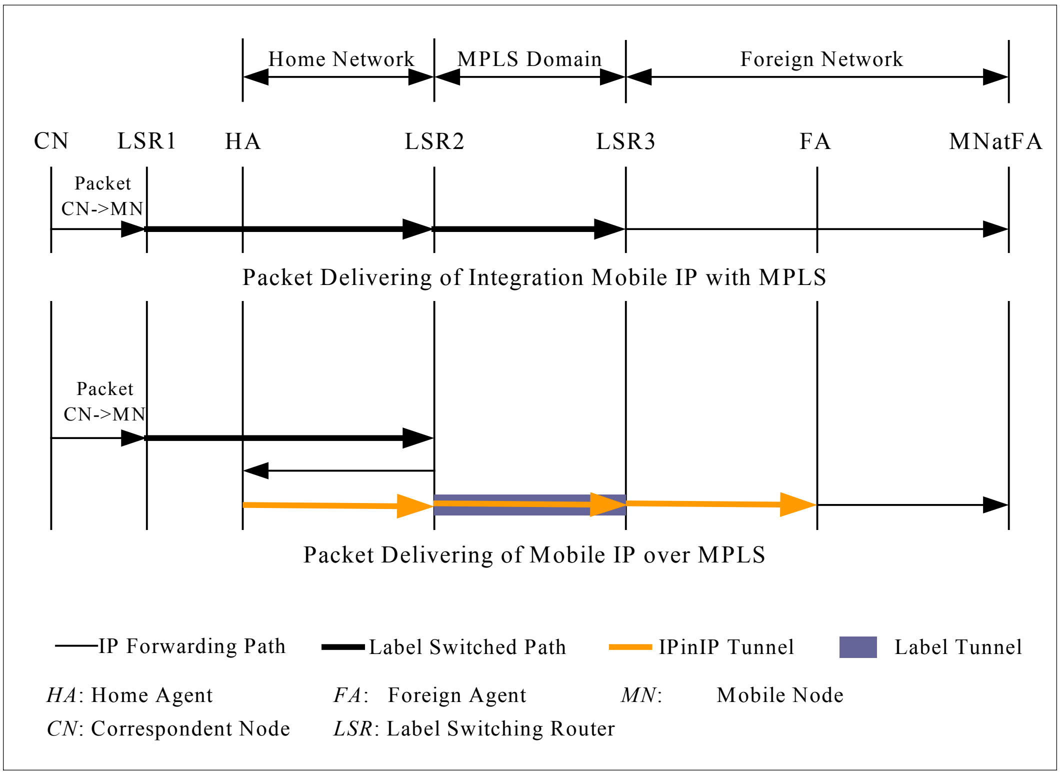


Figure 4.5 Comparison of Packet Delivering Procedure for Mobile IP over MPLS

From Figure 4.5, the major differences between the integration scheme and the Mobile IP over MPLS can be summarised as:

- The packet from the correspondent node to the mobile node does not arrive at the home agent in the integration scheme, however the packet has to be first delivered to the home agent for further tunnelling to the mobile node in the Mobile IP over MPLS scheme.

- The home agent intercepts the packet for the mobile node and encapsulates the packet with IP-in-IP in the Mobile IP over MPLS. In the integration scheme, there is no need for the home agent to do so.

- In addition to the label tunnel between edge routers from the home network to the foreign network, the Mobile IP over MPLS scheme requires another IP tunnel to exist between the home agent and the foreign agent. This means that the packet destined for the mobile node is encapsulated twice when it is forwarded from the home agent to the foreign agent: once when the IP-in-IP encapsulation occurs at the home agent, and again when the label encapsulation occurs at the edge label-switching router. In the integration scheme, only one label encapsulation occurs at the edge router.

- At the foreign network, the packet is directly forwarded to the mobile node from the edge router when the integration scheme is used; in the Mobile IP over MPLS scheme the packet will have to be forwarded to the foreign agent along with the IP encapsulation header and then be sent to the mobile node from the foreign agent.

Because the integration scheme does not require packet interception, IP-in-IP encapsulation and IP tunnelling from home agent to the foreign agent, these functions are simply removed from the integration scheme. As a result of these simplifications, the integration scheme is more efficient then the pure Mobile IP and Mobile IP over MPLS in terms of the network throughput, processing delay and encapsulation overheads.

4.5 Summary

In this chapter, a scheme to integrate Mobile IP with MPLS is proposed. The integration scheme uses label encapsulation instead of IP encapsulation for packet forwarding to the mobile node. The scheme requires no packet interception, IP-in-IP encapsulation and IP tunnelling at the home agent. All the phases related to deliver packets to the mobile node are studied. A new message, Notification, is introduced into the integration scheme. The major function of the notifying message is to ensure the edge label-switching router maintains its label-switching table for the mobile node’s moving between home network and foreign networks. A comparison between the proposed integration scheme and the scheme named as Mobile IP over MPLS is also given in this chapter.

Migrating the Mobile IP to the platform of MPLS, however, is not the only objective of the proposed integration scheme. Support of the quality of service and route diversion for mobile nodes and improvement of the network availability in some extremely application circumstances is far more important. These issues will be studied in the following chapters.

Chapter 5 Route Diversity

Abstract

In this chapter, route diversity is proposed to improve the accessibility of an interconnected broadband wireless IP network in the rain fade situation. The scheme sets up a duplicated traffic stream to a second base station when the route diversity is activated. The duplicated traffic stream is called "shadow flow". It has been shown that the use of a route diversion scheme can provide better performance in terms of network accessibility, reliability and packet loss ratio. In this chapter, the route diversity application circumstances and network model are defined, and the details of the route diversity scheme are given. A simple Quality of Service (QoS) solution in the route diversion scheme is also proposed in this chapter.

5.1 Purpose of Route Diversity

Route diversity is proposed to counteract the heavy rain fading effect on the broadband wireless network by providing the user site with another RF path to an alternative base station. Consider a broadband wireless network using 40 GHz range frequency, (for example, the one used in Embrace (1999)), it offers the possibility of potential bandwidth for network providers. The services include digital television broadcast and Internet. Unfortunately rain at this frequency can cause heavy signal fades, possibly resulting in bit errors and packet loss, even after coding; in the worst case the link between the user site and the base station could be totally lost, hence the required services are absolutely unavailable. So, in the real world, we need a scheme that can provide better service availability in those deep fading circumstances. Route diversity is such a scheme based on the assumption that an alternative route provided for the user site can improve the service availability and the service quality of the broadband wireless network.

The use of alternative paths in former ACTS project CRABS has been shown to produce a significant decrease in outage time in some configurations. As an example of the benefits of diversity in wet weather situations, a non-diversity service offering

99.9% availability (corresponding to typically a 15 dB fade depth) could obtain the same availability with 4 dB less margin, or alternatively increase availability to 99.97% for the same fade margin, with two-way diversity on a path length of 4 Km. This is derived from the one year measurement data carried out in the UK and is reported by Craig *et al* (1999). This reported diversity result is only concerned with the rain signal attenuations.

Diversity is not as easy as simply having an alternative base station and tuning the antenna to the alternative direction. Actually the system should consider how the data streams are delivered from and to the new base station after the router is also changed with the diversion. This will be studied in the following sections.

5.2 Model of Route Diversity

The diagram of route diversity is shown in Figure 5.1. Base stations are connected together with the ATM backbone network. The traffic from the base station to the user site is transmitted within a DVB stream, while the up link from the user site to the base station is a multi-frequency time division multiplex access channel. User site 1 is located in an overlapped area where it can transmit to and receive from both base stations. User site 1 is the so-called diverted client. User site 2 can only access to/from base station 2.

To the concern of the user site, it either sends packets to other users through the base station or receives packets from other users through the base station. Even traffic from/to another user site within the same local cell has to pass through the base station. At the base stations and the user sites there are MPLS label switching routers which decide where the packet is going to deliver to and subsequently assign a suitable label to the packet.

Usually user site 1 communicates with the base station 1. The route diversity procedure can be described as a four phases mechanism:

- *Detection and Decision Phase*. The link between the base station and the user site is degrading as a consequence of the signal fading, mainly caused by rain. The fading is detected at the user site 1, and it determines whether or not to activate the route diversity according to the measured fading level. If the fading reaches a preset threshold, user site 1 will make a diversity decision.

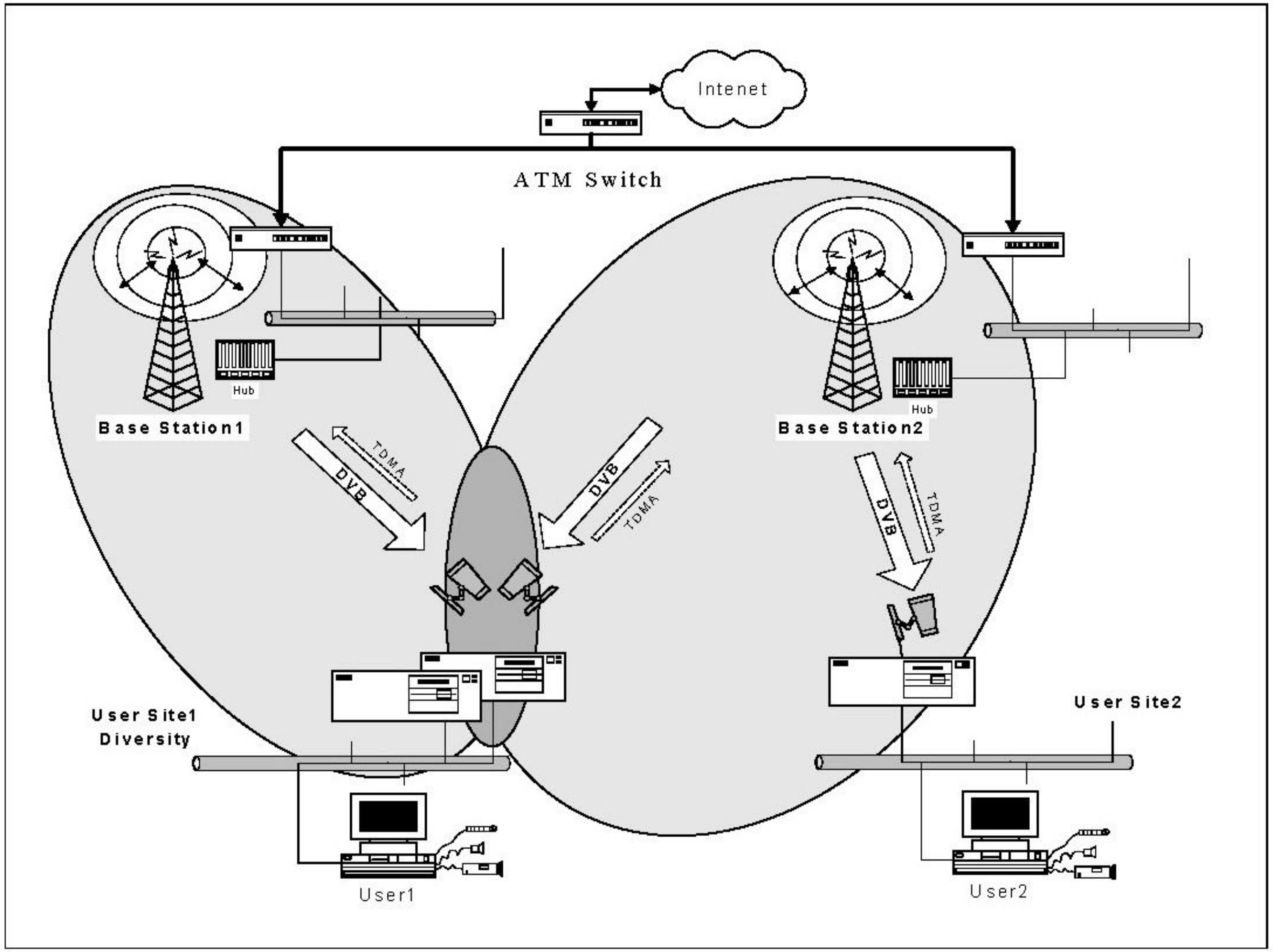


Figure 5.1 Diagram of Router Diversity

Further link degradation might cause packet loss or even an unavailable link between the user site 1 and the base station 1.

- *Diversion Phase*. After making the diversity decision, user site 1 enters the diversion phase. It establishes a diversion path to the base station 2. It also changes its label-switching table so that the packet can be label-switched to both base stations. Packets destined for users other than the users connected to the user site 1 are duplicated, labelled and switched to base station 1 and base station 2. The duplicated packet flow that follows the diversion path is called *shadow flow*.

- *Optional Coexistence Phase*. The shadow flow and the original flow will co-exist in the system for the period of diversion. User site 1 can also determine whether to keep the original flow and the shadow flow co-existing or just use the shadow flow and shutdown the faded original flow.

- *Restoration Phase*. When the fade and link degradation start to decrease, the original link between the user site 1 and the base station 1 is restored to normal. If the original link has been restored to normal (for example, the signal fading stands above a preset level) for a predetermined time, the fade detector could determine that the original link has been restored to normal, and then the user site 1 is signalled to terminate the route diversity. The diverted path is therefore torn-down and the shadow flow is shutdown with the diversion path. This restoration phase is the last phase of the route diversity procedure.

As stated in the diversion phase, the original packets will be label-switched to the base station 1, while the duplicated packets will be label-switched to the base station 2. At the user site 1, the original packets are differentiated from the duplicated packets by assigning different labels to packets. The label switching routers within the network will ensure the packets are delivered to the destination edge label-switching router. With the labelled packets moving closer to the destination, the original packets and the duplicated packets are getting more indistinguishable. Finally, the egress router of the destination user receives the packet. Here the destination router may receive two identical packets from two different paths, or, because the original packets are delivered through a faded path, they may be lost and as a consequence, the destination router might only receive one packet from the diverted route. The destination router must only deliver one copy of the packet; so in the case of receiving duplicates, it must discard one. The method of merging multiple packets into a single packet is termed *flow merging* and forms the basis of chapter 6.

5.3 Route Diversity Protocol

To fulfil the route diversity requirements in Section 5.2, a dedicated protocol for route diversity is proposed. The route diversity protocol is described in the following sections in accordance with the event sequence of the route diversity. The description of the protocol is focused on the considerations of the diversion phase.

5.3.1 Detection and Decision Phase Considerations

There should be a fade detector in the diversity-enabled user site. The fade detector can be a standalone box, a user application that runs on the user site router, or a combination of both. It monitors the link quality between the user site 1 and the base station 1 (see Figure 5.1), and predicts the degrading tendency of the link quality. If the link quality degrades to a predefined level, the detector signals the label switching router at the user site to start the route diversity and the label switching router transits to the diversion phase.

Depending on the type of fade detector, several parameters or their combinations could be used to monitor the link quality. If the fade detector is a DVB-S receiver, for example, the signal to noise ratio (SNR), lock status and bit errors can be the candidates of link quality monitoring parameters. The threshold of diversity should be determined by application requirement, environment and experimental measurement.

5.3.2 Diversion Phase Considerations

MPLS is used to implement the route diversity. The basic principle is that:

1. The IP header of each outgoing packet at the diversity-enabled user site is parsed and mapped to a forwarding equivalence class according to the packet destination IP address, destination IP address mask and the required quality of service.

2. There are two label binding entries for the above forwarding equivalence class in the label-switching table of the user site label switching router. These entries have the same forwarding equivalence class, but they will have different outgoing labels and outgoing ports. One entry is used to switch the packet to the original base station from the user site; the other entry is used to switch the duplicated packet to the alternative base station along the diverted path.

3. There might be multiple diverted paths that could switch one packet to multiple alternative base stations from one diversity-enabled user site. In the case of multiple diverted paths existence, there must be multiple label binding entries in the label-switching table of the user site label switching router, respectively. These label-binding entries have to have the same forwarding equivalence classes, but will have different outgoing labels and outgoing ports which correspond to different diverted paths.

4. For the purpose of flow merging in the destination label switching router, special information about the packet origin is carried also in the label header. The specific information is an extension to the standard label and will be explained later, in section 5.3.2.3.

The principles listed above are mainly related to how the route diversity forwarding equivalence class is mapped to, how the label-switching table is modified for the diversion and what the route diversity label consists of.

5.3.2.1 Route Diversity Forwarding Equivalence Class

The mapping from a packet IP header to the forwarding equivalence class in route diversity is a combination of three elements: the packet destination IP address, the destination IP address mask and the required quality of service treatment. This means that the route diversity forwarding equivalence class is derived from the following triple element combination:

$$FEC \equiv \{DestIP, DestMask, QoS\};$$

where *DestIP* is the packet destination IP address, *DestMask* is the destination IP address mask with the value range [0..32], and *QoS* is the required quality of service for this packet.

If the diverted path is to be used by a set of destination users which share the same IP address prefix, the *DestMask* can be used to mask the lower portion of the IP address and leave the unmasked higher portion to map to the forwarding equivalence class. The *DestMask* is not necessarily identical to the destination subnet segment's netmask, its use is wholly specific to network operators. It is an integer to indicate how many prefix bits of the destination IP address are used to the map of the forwarding equivalence class. If the *DestMask* is 32, the whole destination IP address is used to the map of the forwarding equivalence class; this is a one-to-one mapping. If the *DestMask* takes any other value than 32, the mapping of forwarding equivalence class is multiple (IP)-to-one (FEC).

The required quality of service treatment to the packet is also considered in the mapping of forwarding equivalence class, so that the system can give some traffic the diversion privilege for the specified QoS request, while others may not be allowed the diversion. Section 5.4 introduces a simple QoS scheme for the test of the route diversity.

5.3.2.2 Route Diversity Label Switching Table

Each time the route diversity is invoked, the label switching router in the diversity-enabled user site needs to modify its label-switching table to forward a duplicated packet to the diverted path. This results in two label switching entries for the same forwarding equivalence class in the label switching table; one entry is used to forward the original packet to its usual base station, the other entry is used for the diverted path to forward a duplicated packet to an alternative base station. For the system model in Figure 5.1, the modified label-switching table in user site 1 is shown in Table 5.1.

FEC	In	Incoming	Out	Outgoing	Comments
(DestIP, DestMask, QoS)	Label	Port	Label	Port	
(w.x.y.z, n, q)	Null_label	p	m1	g1	Original Path
(w.x.y.z, n, q)	Null_label	p	m2	g2	Diverted Path
⋮	⋮	⋮	⋮	⋮	⋮

Table 5.1 Example of Label-Switching Table in a Diversity-Enabled User Site After Activating the Route Diversity

Following is the list of notations in the above table:

w.x.y.z: an host IP address which is not directly connected to the user site 1 in Figure 5.1 and packets destined for it need to be diverted to base station 2.

n: the unmasked number of bits of the destination IP address.

q: the required quality of service treatment for the packet destined for w.x.y.z.

p: the incoming port from where the packet is coming to the label switching router in the user site 1.

m1: the out label for the original path from the user site 1 to the base station 1.

g1: the outgoing port from where the packet is send to the original user site 1.

m2: the out label for the diverted path from the user site 1 to the base station 2.

g2: the outgoing port of the label switching router in the user site 1. From the outgoing port *g2* the duplicated packet is diverted to the alternative base station 2.

In Table 5.1, the first row is for the original label-switched path from the user site 1 to the base station 1. For packets destined for the host IP address *w.x.y.z* where the QoS requirement is *q*, the incoming label is *Null_label* because it is sourced from the subnet segment of the user site 1. The label switching router in the user site 1 analyses the packet's IP header and maps to the forwarding equivalence class *(w.x.y.z, n, q)* in the first row, looks up the label-switching table, chooses the label *m1* as the out label for this packet and sends the labelled packet to the base station 1 along the original path via outgoing port *g1*.

The shaded row in Table 5.1 is inserted into the label-switching table after the route diversity is activated. This row corresponds to the diverted path from the user site 1 to the alternative base station 2. It is different from the first row in the out-label and outgoing port; it directs the label switching router to send a labelled packet with out-label *m2* from the user site 1 to the base station 2 via outgoing port *g2*. When a packet with destination *w.x.y.z* and QoS *q* arrives at the label switching router in the user site 1, the label switching router gets the forwarding equivalence class mapping *(w.x.y.z, n, q)*. There are two entries for the forwarding equivalence class *(w.x.y.z, n, q)* in the label-switching table; this results in that the packet is firstly labelled with out-label *m1*, then a duplicated packet is generated and labelled with out-label *m2,* by the label switching router in the user site 1. The packet with out-label *m1* will be sent to the base station 1 via outgoing port *g1* along the original path, while the packet with out label *m2* will be sent t to the base station 2 via outgoing port *g2* along the diverted path.

It is possible that there are more than two entries for the same forwarding equivalence class in the label-switching table to allow a multiple diversion scheme, as long as they have different pair of out labels and outgoing ports.

As the label-switching tables of the label switching routers in the base stations, there is no need to change anything for the route diversity.

5.3.2.3 Route Diversity Label Information

The proposed route diversity protocol uses of an extended label format shown in Figure 5.2. The format is based on the label header described in Section 3.2. The *Label* field is the value of the label, the *TTL* field still means Time-to-Live for this labelled packet in the MPLS network. In addition, there is a new diversity specific field in the extended label header in Figure 5.1.

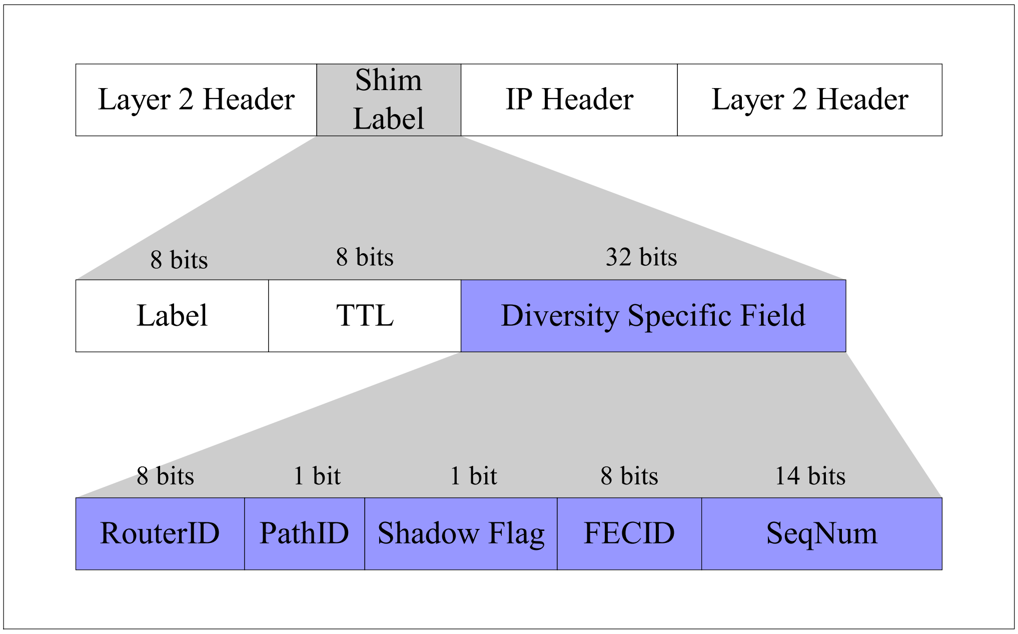


Figure 5.1 Format of the Route Diversity Label

The subfields in the diversity specific field are defined as follows:

RouterID

The ingress router's identification from where the packet enters the network and is labelled. Each ingress router within the MPLS domain is given an unique *RouterID*. When the packet is forwarded to the destination by label switching mechanism, the ingress router identification is also transferred as a part of the route diversity label with the packet and arrives at the egress router. From this field, the egress router knows from where the labelled packet originated. The router identification field is only examined at the egress router, and not by any intermediate nodes.

PathID

A bit flag to show that this labelled packet is sent to the normal path or the diverted path. The ingress router determines which path the labelled packet will be sent to. If the packet is sent to the normal path, the *PathID* is reset to 0; otherwise the packet is sent to the diverted path and the *PathID* is set to 1. From the *PathID* bit, the egress router knows whether the received packet is from a normal route or a diversion route.

Shadow Flag

A bit flag to show that this labelled packet has an accompanied shadow packet which is merely a duplication of the original packet. When the route diversity is activated, the packet is sent to both the normal path and the diverted path. The *Shadow Flag* of the route diversion label is set to 1 for the labelled packet sent on both paths. If the egress router receives a packet with *Shadow Flag* set to 1, the egress router knows that there is another copy for the received packet from a different route.

FECID

The packet's forwarding equivalence class identification when the packet is parsed at the ingress router for labelling. When an IP packet is received at the ingress router in the user site, it is mapped to a forwarding equivalence class in accordance with the fields in the IP header. The identification of the forwarding equivalence class is embedded into the route diversity label and carried to the egress router along with the labelled packet. By this method, a packet in the normal flow and its accompanied packet in the diverted path have the same *FECID*. The egress router uses the *FECID* to merge flows which belong to the same forwarding equivalence class.

SeqNum

The sequence number of a packet in a forwarding equivalence class of flow. The ingress router maintains a sequence number counter, *SeqNum*, for each forwarding equivalence class. It starts from 0 after the ingress router is booted up from cold, and the maximal sequence number is 16383 ($2^{14} - 1$). Each time a packet is mapped to a specific forwarding equivalence class and forwarded to the next hop, the *SeqNum* counter corresponding to this forwarding equivalence class is increased by one. For a duplicated packet that is sent out along the diverted path, its sequence number is the same as that of the packet in the normal path. The counter rolls over after it reaches the maximum and starts from 1024 (hence the egress router knows that the ingress router is just booted up if the received sequence number is less than 1024).

Through examining the packet's sequence number for the specified forwarding equivalence class and the ingress router identification, the egress router knows whether a flow from an ingress router has experienced packet loss and uses the flow merging to possibly minimise the packet loss ratio.

With the combination of route diversity label fields described above, the egress router can translate the received packet in terms of the following:

- where the labelled packet comes from,
- which path the labelled packet follows,
- whether there is a duplicated packet for this labelled packet,
- what the packet's original forwarding equivalence class is, and
- whether the traffic flow with the specified forwarding equivalence class from that router has experienced any packet loss.

All of the fields in the route diversity label are considered thoroughly when the normal flow and the shadow flow are merged at the egress label switching router.

5.3.3 Coexistence Phase Consideration

The normal flow and the shadow flow will coexist in the network if the ingress label switching router in the diversity-enabled user site decides to do so in the diversion duration. The original flow takes the path from the user site to its normal base station (the user site 1 and the base station 1 in Figure 5.1, respectively), whilst the duplicated flow takes the route from the user site to an alternative base station - the diverted base station (the user site 1 and the base station 2 in Figure 5.1, respectively). Eventually, both flows should arrive at the egress label switching router of the destined network segment. Assuming both flows arrive without packet loss, the egress router must merge the flows and deliver the packet to its destination. This could reduce the possibility of packet loss sharply in the case of one or both paths being severely affected by rain fading.

As an option the ingress label switching router in the diversity-enabled user site might only use the diverted path for the delivery of packets, and it might teardown the path to the normal base station. In this case, there will be only one copy of the packet which follows the diverted path and arrives at the egress label switching router in the destination network. The ingress router should set the route diversity label fields correctly: the *PathID* is set to 1 to indicate it is delivered through a diverted path, and the *Shadow Flag* should be set to 0 to indicate that there are not any duplicated packets to be delivered from other routes.

5.3.4 Restoration Phase Consideration

In the restoration phase, the diverted path is torn down and there is no duplicated packet sent out via the diverted path. The traffic for a specified forwarding equivalence class, which is also delivered through a diverted path in the diversion phase, requests only to be delivered along the normal path. The *PathID* and the *Shadow Flag* fields of the packet's route diversity label are both set to 0 to indicate that this is a normal labelled packet that flows along the normal path. To teardown the diverted path, the ingress router needs to remove the label switching entry, which is set up for labelling and delivering a duplicated packet to the diverted path, from its label switching table. No changes are required for the label-switching tables of the intermediate routers and the egress router.

5.4 QoS Issues in Route Diversity

By using MPLS in the route diversity scheme, the QoS routing could be implemented relatively easily. In this thesis, the traffic is seen as three classes shown in Table 5.2.

The class of *Standard* stands for the traffic which is delivered by Best Efforts, for example, Email exchange, FTP file transferring and HTTP web browsing. There are no guarantees to this class of traffic on delivery, bandwidth and delay or delay jitter. The class of *High* stands for the traffic which needs to be treated with a certain kind of priority, for example, applications such as IP Telephony and Video Conferencing. These traffic require guaranteed bandwidth, lower delay and packet loss ratio. The last class, *Shadow*, can be used by any type of applications if the users request such a QoS service to achieve a higher packet deliverability.

QoS	Code	Properties
Standard	0x00	Best Efforts, No guarantee on delivery, bandwidth or delay
High	0x01	High Priority, Reserved bandwidth and network resources, low drop rate and delay
Shadow	0x08	Make a duplicated stream with path diversity. This can be combined with *High* QoS and used by any type of traffic

Table 5.2 Example of QoS Requirements in Route Diversity

The route diversity scheme provides a convenient routing mechanism for the above QoS requirements. This is shown in Table 5.3.

FEC		ming	Out	Outgoing	Comments
(DestIP, DestMask, QoS)	Label	Port	Label	Port	
(w.x.y.z, n, 0x00)	Null_label	p	m1	g1	For class *Standard*
(w.x.y.z, n, 0x01)	Null_label	p	m2	g2	For class *High* Priority
(w.x.y.z, n, 0x08)	Null_label	p	m3	g3	For class *Shadow*
(w.x.y.z, n, 0x08)	Null_label	p	m4	g4	For class *Shadow*
⋮	⋮	⋮	⋮	⋮	⋮

Table 5.3 Example of Label Switching Table for QoS in Route Diversity Scheme
(All the notations retain their meanings as in Table 5.1)

Assume that the first row provides a route for best effort traffic, the second row stands for a route in which the bandwidth is guaranteed, while the third and fourth rows are shadow routes for the traffic with the *Shadow* QoS request. Thus packets destined for the same node or network segment will be correctly mapped to a suitable route, consistent with their QoS request, if the QoS requests of the packets are properly encoded according to Table 5.2.

5.5 Summary

Route diversity is a scheme to provide a duplicated traffic flow to an alternative base station for any flow which could be experiencing access problems to a usual base station, in situations of localised rain fading in the broadband wireless IP network. The duplicated traffic flow is termed "*shadow flow*" and the usual base station is the base station that the user site normally accesses. The route diversity scheme is based on MPLS to generate a shadow flow: for the entry which needs a diverted path in the label-switching table in the user site, a second label switching entry is inserted into the label-switching table; the forwarding equivalence classes of these two entries are the same, but the out-labels and outgoing ports of these two entries are different. These will result in the packet being delivered to two different paths, the original path and the diverted path.

The route diversity procedure involves four phases: the detection and decision phase, the diversion phase, the optional coexistence phase and the restoration phase. These phases are explained in this chapter and the focus is on the diversion phase and the related protocol information. The route diversity label is a modified MPLS label. Several fields in the route diversity label are set for the purpose of flow merging which will be described in the next chapter.

This chapter also gives a simple solution for QoS routing in the broadband wireless IP network. Packets can be forwarded to different routes according to the packets' QoS requirements. For certain types of packet, route diversity can even be used to provide a higher priority and reliable packet delivery.

Chapter 6 Shadow Flow Merging

Abstract

This chapter is focused on the merging of original flows and their shadow flows. A shadow flow is generated when an ingress router in the diversity domain duplicates a received packet and forwards the duplicated packet to a diverted path by MPLS label switching. Consequently two identical packets normally arrive at the egress router, one from the original path and the other from the diverted path. The flow merging mechanism is responsible for merging the shadow flow with the original flow to form again a single flow. The characteristics of shadow flow are discussed, and the disciplines to set the fields of the diversity label for the merging of flows are given in the first part of this chapter. The flow merging algorithm is discussed in the second part of this chapter, along with several merging scenarios. The flow mechanism uses a special sequence number arrangement and this is also explained fully in this chapter.

6.1 The Characteristics of the Shadow Flow

In the route diversity scheme, whenever the diversion-enabled ingress router receives packets, it not only forwards the packets to the original path but also duplicates the received packets and forwards the duplicated packets to a diverted path that leads to an alternative base station. The diverted packet has a label value which is different to the label value of the original packet that flows along the original path, even though it originates from the same ingress router original and terminates at the same egress router as that of the original packet. We call the diverted flow a *shadow flow*, as it shadows the original flow. When the diverted flow and the original flow meet at the egress router of the diversity MPLS domain, a single flow is regenerated by combining the two original flows—this we call *flow merging*.

A formal definition of the two terms is given below:

Shadow flow:

A flow which carries the same packets from the same ingress router to the same egress router as that of the original flow, but has different label value and takes a different label-switched path to the original flow in the diversity MPLS domain.

Flow Merging:

Flow merging combines multiple flows from different label-switched paths into one flow at the egress label-switching router. An example of multiple flows is an original flow and its shadow flow, which travel different routes before arriving at the same egress point.

For flow merging at the egress router, two packets can be thought as shadows of each other and merged into one flow only when their *ShadowID*s are both set to one and their *PathID*s are complementary.

In this thesis the term shadow flow refers to a diverted flow of the original flow, and the packets in the shadow flow are referred to as shadow packets. The shadow packets are assigned different labels from the original packets, and are then forwarded to the shadow path and form the shadow flow. The labels of the shadow packets are in the format of route diversity labels described in Section 5.3.2.3. To assign the original packets and the shadow packets with different labels that allow the flows to be merged at the egress router, the following rules must be applied:

1. The value of the label is assigned as indicated in the label-switching table of the ingress router in the user site when the packet IP header is parsed by the ingress router. The value of the TTL field is copied from the IP header and decremented by one.

2. For the original packet, the diversity label fields must be set as follows:

    - *RouterID* is set to the identification of the ingress router from where the packet enters the diversity domain and requests the diversity service. Routers in the diversity MPLS domain are identified by their *RouterID*s. The *RouterID* is unique within the diversity MPLS domain.
    - *PathID* is reset to 0 (zero), because the packet is forwarded to the original path.

  - *ShadowID* is set to 1 (one) to indicate that there is a shadow packet for this diversity labelled packet. If no shadow packet exists, the *ShadowID* flag should be set to 0 (zero).
  - *FECID* is set to the identification of forwarding equivalence class of the packet at the ingress router. The *FECID* is locally meaningful at the ingress router.
  - *SeqNum* is set to the value of the counter that keeps the sequence number of packets forwarded in the above forwarding equivalence class.

3. For the shadow packet, the diversity label fields must be set as follows:
    - *RouterID* is set to the same value as in the original packet described in above.
    - *PathID* is set to 1 (one), because the packet is forwarded to the shadow path.
    - *ShadowID* is set to 1 (one) to indicate that this is a shadow packet. Alternatively it is interpreted to mean that there is an accompanied packet for this diversity labelled packet.
    - *FECID* is set to the same value as in the label of the original packet described in above. The meaning is that the shadow packet and the original packet belong to the same forwarding equivalence class.
    - *SeqNum* is set to the same value as in the label of original packet described in above.

4. For the reason of QoS routing, packets can be diverted to a privileged path without the existence of a shadow flow. In this case, the label of the diverted packet is as described in the original packet except that:
    - *PathID* is set to 1 (one) to indicate that this packet is sent to an alternative path other than its original path.
    - *ShadowID* is set to 0 (zero) to indicate that there is no shadow packet for this diverted packet.

The shadow flow and its original flow have different characteristics in terms of the fields of the route diversity label. According to the different combinations of original flow and shadow flow, there could be four types of flow in the diversity MPLS domain, namely:

- the original flow without shadow,
- the original flow with shadow,
- the shadow flow,
- the diverted flow with no shadow.

The fields of the route diversity label for each of these flows are different from each other in accordance with the labelling disciplines described above. The characteristics comparison for the four types of flow can be easily obtained according to the various fields in their route diversity labels. Assume the following notations are used for the different fields of the route diversity label when a packet is label-switched in one of the four types of flow:

l: the label value of the route diversity labels for the original flow without shadow and original flow with shadow;

l': the label value of the route diversity labels for the shadow flow;

l'': the label value of the route diversity label for the diverted flow;

ttl: the value of ttl field of the route diversity labels for the original flows, while *ttl'* and *ttl''* are used to indicate these TTLs might not be the same;

r: the identification of the ingress router from where the packet enters into the diversity MPLS domain;

fec: the packet's forwarding equivalence class identification;

seq: the packet sequence number in the above forwarding equivalence class.

Then the fields of the route diversity labels for the four types of flow can be compared as shown in Table 6.1.

	Original Flow (no shadow)	Original Flow (with shadow)	Shadow Flow	Diverted Flow
Label	*l*	*l*	*l'*	*l''*
TTL	*ttl*	*ttl*	*ttl'*	*ttl''*
RouterID	*r*	*r*	*r*	*r*
PathID	0	0	1	1
ShadowID	0	1	1	0
FECID	*fec*	*fec*	*fec*	*fec*
SeqNum	*seq*	*seq*	*seq*	*seq*

Table 6.1 Comparison of the fields of route diversity labels for different flows

For the four types of flow, Table 6.1 shows that their *TTL*s, *RouterID*s, *FECID*s and *SeqNum*s are identical, no matter whether the packet is label-switched on the original path without a shadow packet, label-switched to the original path with a shadow packet, or only diverted to a privilege path by the label-switching mechanism. This is simply because the mappings from the packet IP header to the forwarding equivalence class are the same one, i.e. *fec*. The differences among these different flows are mainly in the fields of *Label* value, *PathID* and *ShadowID*.

For the original flow without shadow (see column two in Table 6.1), its label value equates to that of the original flow with shadow which is shown in the third column in the above table; this means that the packet is label switched to the same original path in both situations. Therefore the *PathID*s of the two columns are both set to 0 (zero). Notice the difference of the *ShadowID*s in the two columns: for original flow without shadow the *ShadowID* is 0, but for the original flow with shadow the *ShadowID* is 1 to indicate explicitly that there is a shadowed packet to couple with this labelled packet.

In Table 6.1 column four shows the settings of the various fields in the label of the shadow packets. Comparing the original flow with the shadow, there are two differences between the labels. The first is the label value of the two flows, one being *l* and the other *l'*. The packet with label value *l* travels along the original path, and the packet with label value *l'* along the shadow path. The second difference is in the *PathID*s: the shadow packet's *PathID* is set to 1 while the original packet's *PathID* is reset to 0. At the egress router, the flow merging mechanism examines the received packets' *PathID*s to determine whether packets come from the original flow or the shadow flow. Also note that the *ShadowID* fields for the original flow and the shadow flow are both set to one, because they are shadows of each other.

Compared with the original flow with no shadow (column two) in Table 6.1, the diverted flow (column five) has a different label value and *PathID*, but the *ShadowID*s are the same. With label value *l''*, the diverted packet is sent to the diverted path; and the *ShadowID* field of the diverted packet label is set to zero, which means no shadow packet is sent out to accompany the diverted packet. The egress router will not do flow merging for packets arriving with the *PathID* field set to 1 (one) and the *ShadowID* field reset to 0 (zero).

Compared with the shadow flow (column four) in Table 6.1, the diverted packet is different from the shadow packet in the fields of label value and *ShadowID*. With different label values *l'* and *l''*, the shadow packet and diverted packet could travel along different label-switched paths from the ingress router to the egress router in the diversity MPLS domain; with different *ShadowID*s, the egress router can distinguish diverted packets from shadow packets although their *PathID* are all set to one (one is a flag to indicate the packets come from an alternative path other then the original path).

In brief, two flows are said to be shadows of each other if they have equal *RouterID*s, *FECID*s and *SeqNum*s, complementary *PathID*s and their *ShadowID*s are set to 1 (one). A diverted flow is identified by its *PathID* being set to one and its *ShadowID* being set to zero.

6.2 Flow Merging

6.2.1 Shadow Flow Merging

Originating from the same ingress label-switching router and flowing along different label-switched paths, an original flow and a shadow flow meet at the egress router of the diversity MPLS domain. To deliver the packets carried in these shadowed flows to their destination, the two flows need to be merged into a single flow. This merging is completed by the flow merging mechanism. In the conditions of the original path and the shadow path possessing different route latencies and packet loss probabilities, the flow merging mechanism should be tolerant of these fluctuations.

The following heuristics are applied to the flow merging:

- The flows are first queued according to the packets' *RouterID*s, *FECID*s and *PathID*s;

- A check is carried out to ensure that the flows to be merged are shadows of each other;

- The current sequence numbers of the two queued flows are calculated to check the identity of the shadowed flows;

- If the packet with sequence number *N-1* is the last successfully merged packet, and a packet with sequence number *N* is available at both queued flows, the merging process takes a packet from one flow and discards the identically numbered packet from the second flow;

- If a packet with sequence number *N* is not available from one flow (sequence number *N+1* or other larger sequence number is available but not *N*), then the merging process takes the packet with sequence number *N* from the other flow if it is available. If packet N is not available on either flow, the merging process waits for a short time; the waiting time is estimated from measuring the time offset between the two flows on a regular basis if the overall delay is greatly varying. If packet N arrives on a flow after its identical packet N has been taken from the other flow, it is discarded by the flow merging mechanism.

- If the packet with sequence number *N* is still absent from both flows after the waiting period, the packet is thought of as missing and the merging process goes back to the top of the loop looking for packet with sequence number *N+1*.

The three cases below with accompanying Figures 6.1, 6.2 and 6.3, are used to explain the algorithm in detail, and to illustrate how the mechanism deals with exception cases which may occur in packet arrivals.

Case 1: Packet N available on both flows

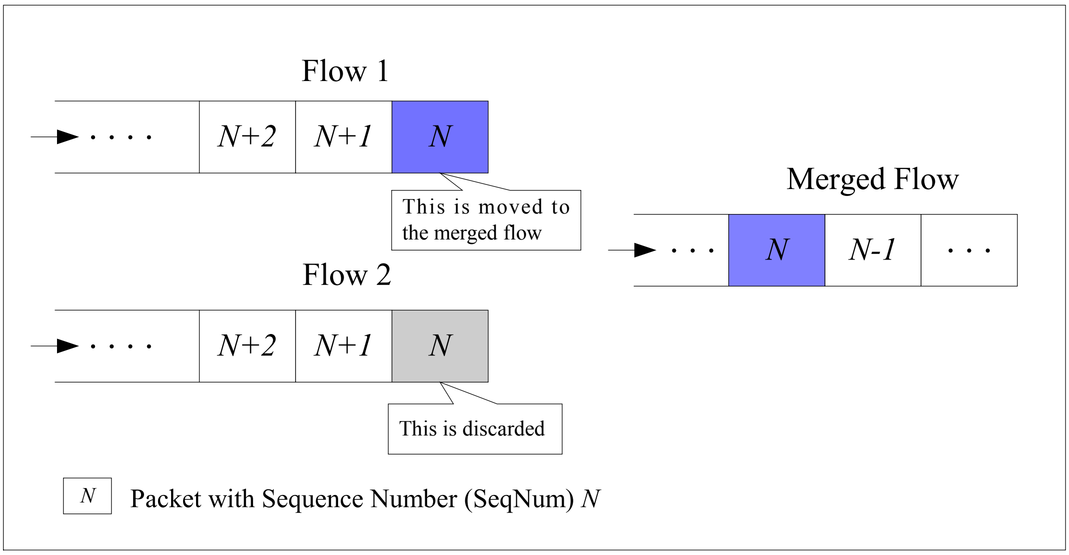


Figure 6.1 Flow Merging Queues When Packet N Is Available in Both Flows

In this case, Flow 1 and Flow 2 are shadow flows and queued at the egress router waiting for the flow merging mechanism to be activated. The flows came from the same ingress router with an equal forwarding equivalence class.

After merging the packet with sequence number *N-1*, the mechanism looks for a packet with sequence number *N*. The mechanism first checks the packet sequence number from the Flow 1 and finds packet *N* is available, so it takes packet *N* from this flow and moves it to the merged flow. When checking Flow 2, the mechanism finds that packet *N* is also available; however, as it isn't required it is discarded.

Case 2: Packet N available on only one Flow

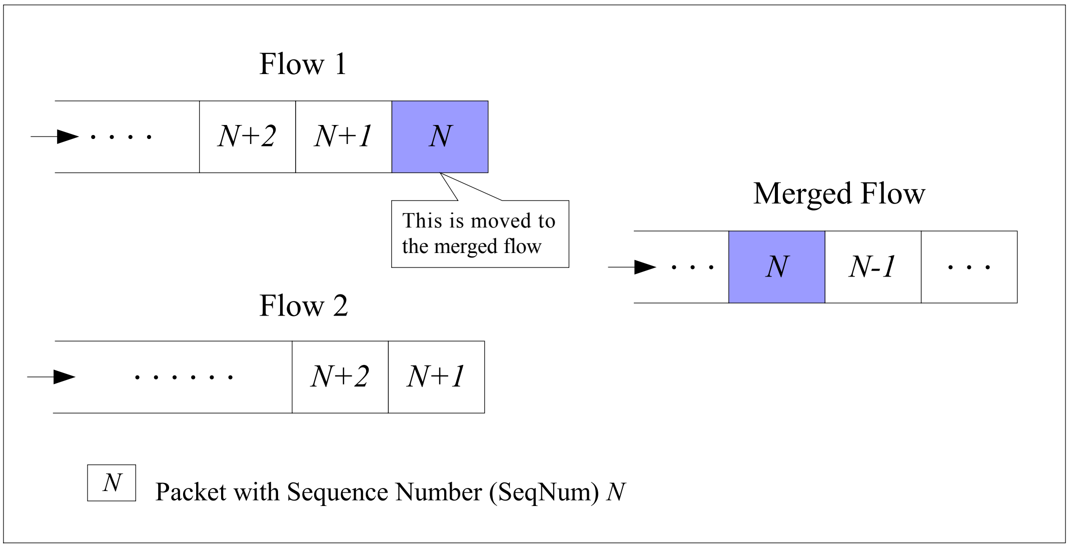


Figure 6.2 Flow Merging Queues When Packet N Is Only Available in One Flow

Figure 6.2 shows the case when the packet with sequence number *N* is only available in one flow. This might happen if the packet is dropped in one path during the forwarding from the ingress router to the egress router or if the packet is subjected to a long delay at some intermediate nodes of the path.

In this case, the mechanism looks first for packet *N* in Flow 1 and finds that it is available. The mechanism takes the packet and moves it to the merged flow. It then moves on to check if Packet N is available in Flow 2. The packet available here is N + 1, so in this case the mechanism simply moves on to process the merging of packet N + 1. Packet N+1 is then taken to the merged flow from Flow 2.

In the case where packet N has been delayed and eventually it arrives on Flow 2, the mechanism simply discards it.

Case 3: Packet N not available on either flow

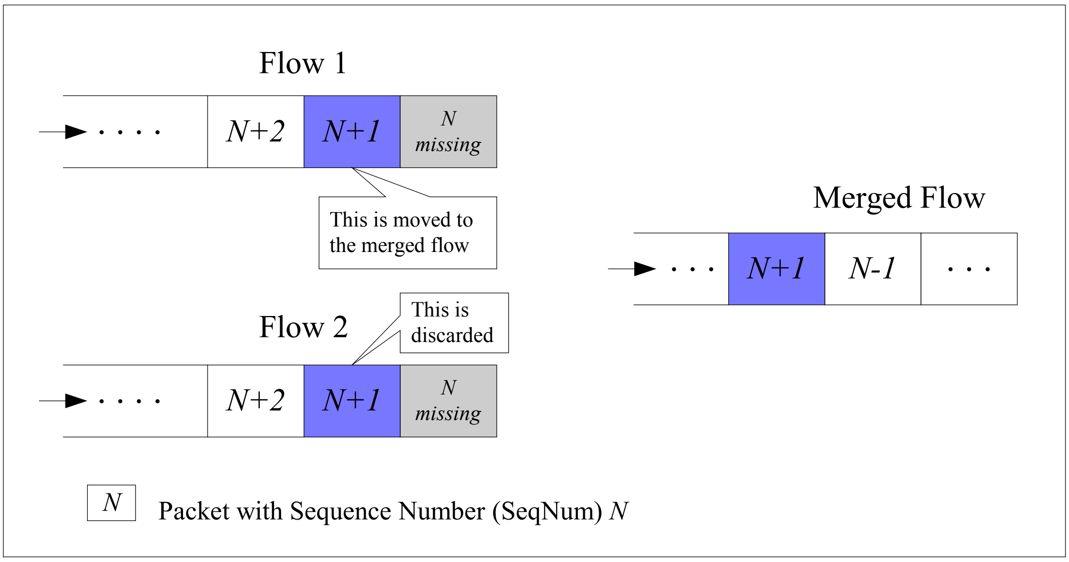


Figure 6.3 Flow Merging Queues when Packet N is not available in either flow

Figure 6.3 shows an example in which the packets to be merged are not available in either flow. After the packet with sequence number *N-1* has been merged, the mechanism looks for packets with sequence number *N*. It first checks the sequence number of packet queued in flow 1 and finds the next available packet's sequence number is *N+1*; the mechanism then checks the available packet's sequence number of flow 2. At this point there are three possibilities for the packet in flow 2:

1. The first possibility is that packet *N+1* (or other packet with sequence number greater than *N+1*) is the next available packet in flow 2. At this point, the mechanism knows that packet *N* is missing, and therefore moves packet *N+1* to the merged flow.

2. The second possibility is that there is not any packet available in flow 2 and the merging process must begin a timeout. During the timeout,

   - If any packets with sequence number less than *N* arrive during the timeout, the packets are discarded [8].

[8] One exception is that the ingress router is rebooted/restarted during this waiting time. In this case the sequence number will be restarted from 0 (zero) and less than N. See §6.2.2 for more details.

- If packet *N* arrives during the timeout, the mechanism performs as described in Case 2.
- If packet *N+1* (or other packet with sequence number greater than *N+1*) arrives during the timeout, the merging process will also move to the merging of packet *N+1*.
- If the timeout period has expired and packet *N* has still not arrived on Flow 2, the packet is regarded as missing and the merging process will move to the merging of next packet with sequence number *N+1*.

3. The third possibility is that the packet's sequence number in flow 2 is less than *N*, while *N* is the sequence number the merging process is looking for. Any packets with sequence number less than *N* will be discarded from flow 2, until the sequence number *N* or greater than *N* arrives.

It was found that this mechanism gives an advantage in that the merged flow has lower packet loss ratio and packet delay. This is because the merged flow is always filled with the first available packet from either the original flow or the shadow flow.

6.2.2 Special Sequence Number Processing

The flow merging scheme described in the previous section shows that the packet sequence number - the *SeqNum* field in the diversity label, is the most important criterion to the merging of the original flow with its shadow flow. In the structure of diversity label defined in §6.3.2.3, the *SeqNum* is a 14 bit field which ranges from 0 to 16383 (i.e., $2^{14}-1$). The rules defining the management of *SeqNum* are as follows:

- Start from 0 (zero) when the egress router is booted up or restarted;
- Increase by 1 (one) when a packet is sent out according to a specified forwarding equivalence class;
- After reaching the maximal value, the next increase makes it roll over and start again from 1024.

This is useful for the merging process at the egress router to identify whether an ingress router is just rebooted/restarted or the sequence number is merely rolled over during the merging. Supposing the sequence number of the last merged packet is *N-1*, the merging process is looking for the next packet with sequence number *N*, and for some reason the ingress router is rebooted/restarted and hence the sequence number is started from zero. Therefore the sequence number of the received packet at egress router will be less than *N*. Obviously the merging process should not discard the packet with sequence number less than *N*, instead this packet should be merged as usual.

The opposite case is that the received sequence number is equal to or greater than 1024 while the merging process is looking for sequence number *N*, the egress router can determine that the packets with sequence number between N and the maximal sequence number are lost during the forwarding from ingress router to egress router.

The following algorithm shows how these two rules are applied.

```
IF Last merged sequence number == $N-1$
    IF Next received sequence number starts from 0
            Ingress router is just booted up;
            No packet loss;
    END IF

    IF Next received sequence number starts from 1024
            Packet with sequence number $i$ is lost, $i = N, N+1, \dots, 2^{14}-1$;
    END IF
END IF
```

This application of the starting sequence number makes it possible for the egress router to distinguish the rebooting/restarting of the ingress router from packet loss, and sequence number rollover.

6.3 Summary

Flow merging is used to merge two or more flows into a single flow at the egress router. The flows to be merged should be shadow flows of each other. By shadow flows, we mean that the flows are the same in fields such as the originating nodes, the egress routers, the forwarding equivalence classes and the label-switched packet sequence number. The shadow flows take different routes from the original flows to arrive at the egress router and to be merged into one flow for the delivery to the destination.

In the definition of route diversity, an alternative path from the user site to the destination is a shadow path of the original path, and an alternative flow is a shadow flow of the original flow. The original flow and the shadow flow are labelled differently; however for the purpose of merging the original flow with its shadow flow, the labels have to be correctly set in accordance with the path which the packet will travel from the ingress router to the egress router. The first part of this chapter gives the disciplines of setting the fields of a diversity label. With different combinations of *PathID* and *ShadowID* in the diversity labels, there could be four flows in the diversity MPLS domain, namely the original flow without shadow, the original flow with shadow, the shadow flow and the diverted flow. This chapter also discussed the features of these flows by comparing one flow with the others.

It is essential to the success of the scheme to have a successful, rigorous flow merging mechanism, and the second part of this chapter focused on the description of the flow merging algorithm. The merging algorithm is based on the calculation of the packet sequence number of the original flow and the shadow flow. Three different merging scenarios are discussed in detail to explain the merging algorithm. The sequence number field of the diversity label is arranged as starting from 0, increasing by one for each forwarded packet and rolling over and starting from 1024 when it reaches the maximal sequence number, so that the egress router can distinguish a rebooted/restarted ingress router from discontinuous packet sequence number which also means packet losing. An additional advantage of the scheme is that the merged flow has lower packet loss ratio and packet delay compared with the original flow or the shadow flow.

Chapter 7 Experimental Testbed

Abstract

The aim of the study is to provide a scheme of nomadic and diversity access services for wireless broadband IP network with MPLS. Therefore two real networks of computers are built to demonstrate the proposed scheme's ability and to benchmark the system. One network is a preliminary testbed for the purpose of studying of the proposed schemes, in which no RF equipment is involved; the other network is set up for a general wireless broadband system, in which the required RF equipment is involved. The experimental testbed is described in two parts in this chapter. The hardware setup is explained in the first part, which includes the aforesaid two configurations of computer networks. The software components developed for the testbed are described in the second part. Since the study mainly focuses on the implementation of the proposed scheme, several software components that form part of the route diversity system are included.

7.1 Hardware Setup

In the previous chapters, a scheme to provide nomadic and route diversity services for broadband wireless network (for instance, a Local Multipoint Distribution System – LMDS) with MPLS is proposed. To demonstrate the proposed scheme's capability and to evaluate the system, two real computer networks have been built. The preliminary network was built for the implementation and measurement of the proposed scheme of nomadic access and route diversity with MPLS, the aim is mainly to prove the abilities of the proposed scheme. However, with more and more RF equipments becoming available, and with the requirements for further study of the scheme in the EMBRACE project, the migration of the proposed scheme from the preliminary testbed to a more general broadband wireless system was inevitable. Consequently a generalized testing system with the support of the required RF equipments was set up in the Joanneum Research at Graz in Austria.

7.1.1 Preliminary System Setup

The preliminary system is set up for the implementation and measurement of the proposed nomadic and route diversity services with MPLS in a wired network environment. Figure 7.1 illustrates this hardware configuration. The network consists of one ATM switch, three diversity-enabled MPLS routers and five user machines. The user machines are located in three separated local sites that belong to different IP domains. Of the three user sites, two are configured with user machines as mobility agents to support the nomadic access in the system. The network is in a star topology with routers physically connected to the ATM switch, but logically the routers are mesh connected with each other. Within a local user site, the local network is in a bus topology with cheaper Ethernet connections to the router and many users. ATM and Ethernet are chosen to represent the currently available network solutions.

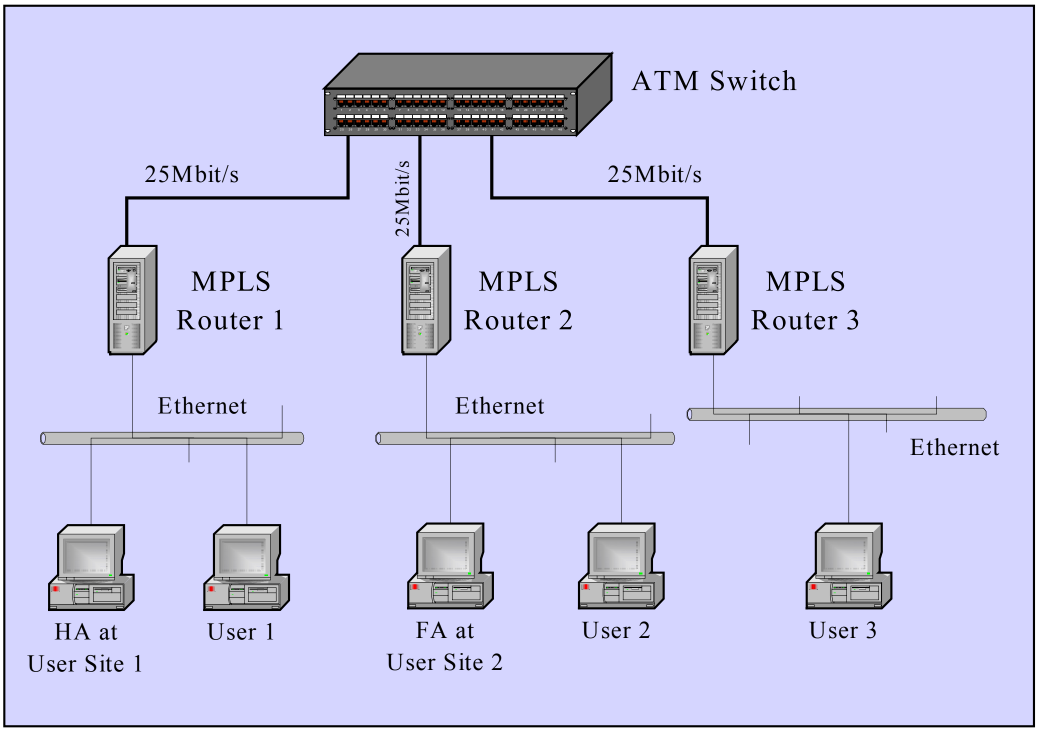


Figure 7.1 Preliminary Network Configuration

The same PCs are used for the user machines and routers in the preliminary network configuration. Table 7.1 lists the specifications of each PC. All processing including route diversity label switching, shadow flow merging and integrating nomadic support with MPLS is done in software running on the application layer of Linux system. Apart from NICs, no specific hardware is used.

Configuration	User Machine	Router
Operating System	Red Hat Linux 6.2 with Kernel 2.3.99/2.4.0	Red Hat Linux 6.2 with Kernel 2.3.99/2.4.0
RAM	128 MB	128 MB
Ethernet NIC	10 Mbps	10 Mbps
ATM NIC		ForeLE25, 25 Mbps

Table 7.1 User and Router PCs Technical Specification

7.1.2 ATM Switch

The ATM Switch, a ForeRunner ASX-200 (Fore Systems, Inc. 1997b) switch with two NM-6/25UTPEC 25 Mbps (TP25) modules, performs the network connection amongst the separated user sites. The use of TP25 modules is a compromise between performance and expenditure at user site. Permanent Virtual Connections (PVCs) are set on the ATM switch using its ATM Management Interface (AMI) (Fore Systems, Inc. 1997b) . Separate PVCs are used for transporting ATM Adaptation Layer 5 (AAL5) blocks on Available Bit Rate (ABR) and Constant Bit Rate (CBR) contracts. The bandwidths of constant bit rate channels are restricted by using the Usage Parameter Control (UPC) to specify their respective Peak Cell Rate (PCR). The usage parameter control contracts further specify that non-compliant packets be discarded to prevent current conditions affecting results. The ABR channels are not assigned to UPC contracts to allow as much traffic to pass as the available bandwidth could accommodate. In the preliminary network configuration, all label-switched paths between the diversity MPLS routers are set up based on PVCs with CBR or ABR contracts, according to the paths' requirements.

7.1.3 Diversity-Enabled Label Switching Router

The diversity-enabled MPLS router is a PC specified in Table 7.1. It connects to user sites with Ethernet cards and to the ATM core network with a Fore LE25 ATM card. It receives all link layer Ethernet frames by opening the Ethernet devices in "raw" mode, and sets the devices in promiscuous mode so that all frames on the local Ethernet can be captured and filtered. With the ATM device, different PVCs are established between the router and the ATM switch statically to represent different diversity label-switched paths. The diversity-enabled label-switching routers conform to the rules proposed for the route diversity and shadow flow merging. According to the diversity routing disciplines set in the router, packets are sent to different diversity label-switched paths via the ATM device and the shadow flow merging is also completed at the diversity-enabled label switching router.

7.1.4 Mobility Agent

The mobility agents include one home agent and one foreign agent in the preliminary network configuration shown in Figure 7.1. Both the home agent and the foreign agent are PCs specified in Table 7.1. A mobility agent connects to the user site and the diversity MPLS router with Ethernet card directly. In cooperation with the diversity MPLS router, the mobility agent looks after the movements of nomadic nodes and provides a label-tunnel for nomadic nodes between the home diversity MPLS router and the foreign diversity MPLS router. Differing from the standard Mobile IP protocol, a mobility agent in the preliminary network configuration is not responsible for forwarding packets destined for the nomadic node to its current foreign network; instead it uses a notification message to instruct the home diversity MPLS router to establish a label-tunnel to the foreign diversity MPLS router, so that packets destined for the nomadic node are label-switched to the foreign network via the established label-tunnel by the diversity MPLS router in the home network. The mobility agent and the diversity MPLS router in Figure 7.1 support the schemes of integrating Mobile IP with MPLS proposed in Chapter 4.

7.1.5 General System Setup

A trial route diversity system set up for a general broadband wireless network is shown in Figure 7.2. The system is very similar to the preliminary configuration shown in Figure 7.1, except for the wireless link and the corresponding equipments. The system consists of an ATM switch, diversity-enabled MPLS routers, user machines, Cobra[9] system and Lissy[10] system (Joanneum Research *et al* 2001) for wireless connections. The core network is an ATM network including the ATM switch, R3, R4 and R5 in a physical star topology. User sites are located in the range of RF coverage of their respective base stations, while user site 1 is located in the overlapped area of base station 1 and base station 2 for the route diversity experiment. The RF links L_{1u}, L_{1u}', L_{1d} and L_{1d}' illustrate the capability of user site 1 being able to access to base station 1 and base station 2.

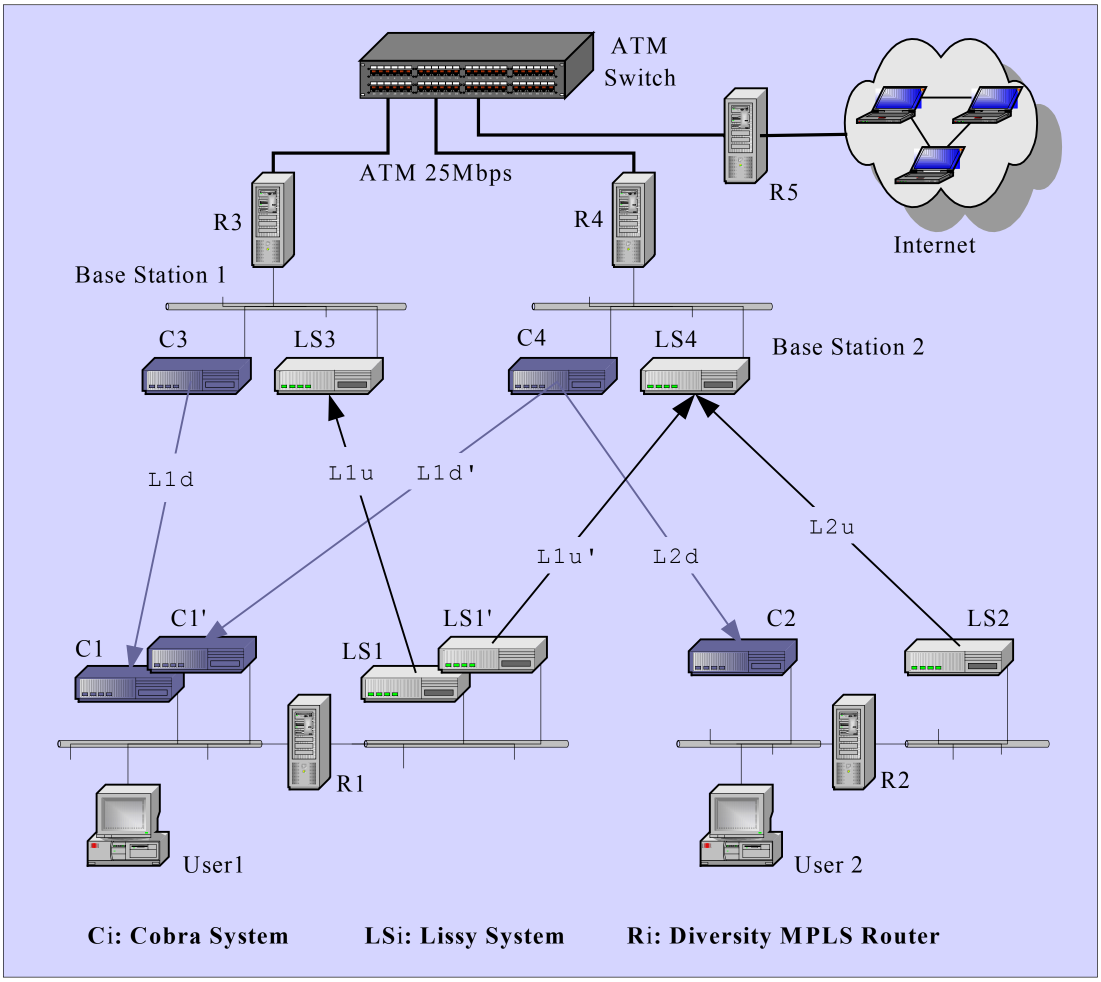


Figure 7.2 General Broadband Wireless Network Configuration

[9] Cobra system is a DVB-S en/de-capsulation system developed by the University of Salzburg, Austria.

[10] Lissy system is a MF-TDMA system developed and proprietary owned by the Joanneum Research Institute, Graz, Austria.

All user PCs and routers are the same PCs as specified in Table 7.1 for the preliminary network configuration. The functionality of the ATM switch and routers is also identical. However, the wired connection is replaced by an RF connection in the general system configuration. The downlink from base station to user site is accomplished by the COBRA system and the return link by the LISSY system.

7.1.6 COBRA DVB-S System

The COBRA system is a standalone DVB-S encapsulation/decapsulation box which runs on a Linux platform. In the base station, it connects via an Ethernet card to the base station LAN. Also attached to the LAN is the LISSY system and the diversity MPLS router that connects the base station LAN to the ATM core network. IP packets coming from either the base station LAN or via the router from the core network are received by the Ethernet card in the Cobra box. The COBRA system performs an "Ethernet to Section" encapsulation and sends data via a DVB parallel interface to the modulator for RF transmitting. In the user site, the Cobra box receives data coming from the DVB-S downlink via an antenna. After de-encapsulating the received data, the Cobra system reconstructs an Ethernet frame and forwards the frame to the user site LAN. The user machine hence receives the IP packets sent via the Cobra system in the base station. In the diversity scenario, a COBRA system with two COBRA boxes in the user site listens to two base stations simultaneously.

7.1.7 LISSY System

The LISSY system is designed as a MF-TDMA (multi frequency - time division multiple access) system with integrated quality of service and bandwidth request mechanism. The user station can request more or less bandwidth from the base station according to its buffer level of the quality of service queues. The requests are centrally processed at the master MF-TDMA station to produce a resource allocation plan which describes all the burst in terms of start time, frequency, coding rate and transmission duration. This control information is distributed via the DVB downlink to all user stations. LISSY connects to the user site LAN or the base station LAN via a 10Mbps Ethernet card. In the user site, LISSY receives the outgoing IP packets by the connected Ethernet card. LISSY breaks up the packets into small cells with Reed Solomon and Viterbi forward error corrections. The cells are then assembled into bursts and transmitted to the base station according to the allocation plan. While in the base station, LISSY receives the bursts in accordance with the allocation plan, corrects the possible code errors, reassembles cells into IP packets and delivers them to the base station Ethernet segment.

7.1.8 STUIF Box

In the diversity user site of the general system configuration, the signal quality of the DVB downlink is monitored by a STUIF Box. The STUIF Box is designed as a tuner and demodulator to receive a DVB-S signal. It provides the DVB transport stream via a synchronous parallel interface (SPI) and an I^2C (Inter-ICs) interface for monitoring and control. The router accesses the STUIF Box and queries the current receiving states via the I^2C bus. The queried states include data lock, frequency lock, transport stream lock, Viterbi bit error and AGC (automatic gain control) level. Based on these states, a diversity decision is made at the router.

7.2 Software Components

To arrive at the ultimate destinations in the diversity network system, packets have to traverse and be processed by many entities including mobility agents, ingress label-switching routers, label-switching routers in the middle of the diversity domain and egress routers. If packets are diverted and there are shadow flows, then the original flows and shadow flows have to be merged. This requires different programs running on the application layer in LINUX systems. At the time this research began, most program components (except some tools discussed in 7.2.3) were not available or not suitable for using in the system configurations as shown in Figure 7.1 and Figure 7.2. Therefore, this section aims to describe the various custom-made software components used in the route diversity system, their purpose and how they were implemented.

7.2.1 Nomadic Access Components

To support nomadic access to the preliminary system and the general network, a mobility agent program runs in the home agent and the foreign agent separately, and a nomadic node program runs in each of the nomadic nodes.

7.2.1.1 Mobility Agent Program

Mobility agent includes home agent and foreign agent. The customised mobility agent program supports both home agent functions and foreign agent functions. The home agent provides home services to the registered nomadic users. It is responsible for the registration and deregistration of nomadic nodes. According to the scheme of integration of Mobile IP with MPLS described in Chapter 4, the mobility agent should send a notification packet to the diversity MPLS router after the home agent registers or deregisters the nomadic node with it. The notification packet will indicate to the diversity MPLS router to establish or teardown a label-tunnel. The label tunnel is a label-switched path from the diversity MPLS router in the nomadic node's home network to the diversity MPLS router in the foreign network. This differs from the Mobile IP protocol that needs to set up an IP-in-IP tunnel to serve the nomadic nodes. When Mobile IP service is integrated with MPLS, the mobility agent needs to support the following functions:

- Function to build and broadcast mobility agent advertisement message within the local segment periodically;

- Function to build and send registration reply messages according to the received registration request messages from a special UDP port - Mobile IP UDP port 434;

- Function to do the keyed MD5 (Riverst 1992) authentication and security verification;

- Function to manage the registered nomadic nodes' information in the mobility agent. This includes insertion, removal and update the nomadic node entry in the nomadic node database which traces all the away nomadic nodes' status.

The diagrams of the mobility agent program are shown in Appendix B. The main states of the mobility agent include *Signal Processing, Agent Solicitation, Register Request, Register with HA, Deregister with HA* and *Receiving Register Reply*. They are described as follows:

In the ***Signal Processing*** state, the mobility agent captures two kinds of signals: one is a termination signal which results in the mobility agent program terminating, and the other one is the timeout signal which results in an agent advertisement packet being broadcasted to the local network segment periodically. When the user wants to terminate the home agent function, some special key-combinations are used and the mobility agent function is terminated. While the mobility agent program is running, it will broadcast agent advertisements to show its existence and the willingness to serve the nomadic nodes. The Mobile IP protocol gives a suggestion of how long the time intervals should be between two consecutive agent advertisements.

In the ***Agent Solicitation*** state, the mobility agent responds to an agent solicitation packet with an agent advertisement sent to the origin of the solicitation packet. This state can occur for both the home agent and the foreign agent when a nomadic node has not heard agent advertisements for a period of time.

In the ***Register Request*** state, the mobility agent decides what services the nomadic node is requesting by parsing the received registration request packets. For security reasons, a nomadic node and home agent authentication association must be established for any registration request and registration reply messages. Therefore any further processing in the *Register Request* state must be based on the clearance of request identification and keyed MD5 authentication, which is the default security algorithm suggested in the Mobile IP protocol by the IETF. When a registration request is rejected by the mobility agent, the reason for rejection will be sent to the nomadic node within a rejected registration reply packet. In the case of a mobility agent acting as a foreign agent, the registration request will be forwarded to the requested home agent. In the case of a mobility agent acting as a home agent, the registration request might be one of two possibilities: registration or deregistration.

In the ***Register with HA*** state, the nomadic node requests to register it with the home agent. The home agent action is quite straightforward: for a node that is not currently registered, a new entry is inserted into the nomadic node database, and the relevant information is updated to the most recent value. For a node that is currently registered, the request is considered as a re-registration request and it is used to extend the service lifetime for the nomadic node. After the registration information is updated in the home agent, an accepted registration reply packet is sent to the foreign agent to inform the nomadic node about the success of registration. The home agent is also responsible for notifying its diversity MPLS edge router to establish a label-tunnel for the delivery of packet destined for the nomadic node, by sending a notification packet to the edge router.

In the ***Deregister with HA*** state, a deregistration request is a registration request with lifetime set to 0 (zero). Deregistration includes removing its entry set from the home agent's nomadic node database; creating correct identification and keyed MD5 authentication fields for the registration reply packet with accept flag; and sending the registration reply packet to the nomadic node. After deregistration, the home agent should not serve the nomadic node anymore, therefore a notification packet is sent to the diversity MPLS edge router in the home network to teardown the established label-tunnel; this will stop the packet being forwarded to the nomadic node by the edge router.

In the ***Receiving Register Reply*** state, the mobility agent acts as a foreign agent. Again for security reasons, any further processing of the registration reply in the foreign agent has to be based on the successful examination of the reply identification and keyed MD5 authentication. For a rejected reply packet, the nomadic node information needs to be removed from the foreign agent, and a notification packet to teardown the label-tunnel is also sent to the diversity MPLS edge router in the foreign network. For an accepted registration reply packet, an entry is inserted into the nomadic node database to track the information of the requesting nomadic node in the foreign agent. A label-tunnel is established for the delivery of packets to the nomadic node after the foreign agent sends a notification packet to the diversity MPLS edge router.

7.2.1.2 Nomadic Node Program

A nomadic node is a normal user machine that runs the nomadic node program to support access to the network when it is away from home. The nomadic node program responds to two kinds of packet: the agent advertisement packet and the registration reply packet received from a mobility agent. Just as in the case of the mobility agent program, a signal processing procedure is needed to respond to the termination and timer signals during the program execution. The design diagrams of the nomadic node program are shown in Appendix B. It includes three states, the *Signal Processing* state, the *Agent Advertisement* state, and the *Register Reply* state, respectively.

The nomadic node enters into the ***Signal Processing*** state when it receives the defined passive signals or an agent solicitation timeout signal. The passive signals are some key-combinations that cause the nomadic node program to be terminated or to stop running. When the nomadic node has not received agent advertisement messages for a period of predefined time, the nomadic node could solicit an agent advertisement message from whoever is the nearby mobility agent by limited-broadcasting an agent solicitation packet to the local network segment.

The ***Agent Advertisement*** state is entered when a nomadic node hears an agent advertisement from the current network. To decide whether to register or deregister with its home agent, the nomadic node first needs to determine where it is. As described in Section 4.2, (integration of Mobile IP with MPLS), the nomadic node could be in one of four possible positions: staying in the home network, staying in the foreign network, moving from one foreign network to another, or returning to home from a foreign network. The nomadic node program processes them as following:

- If the nomadic node stays in the home network, registration to its home agent is not required.

- If the nomadic node stays in a foreign network, it needs to register with the home agent regularly. In this case, the nomadic node builds a registration request packet with correct identification and authentication and sends to the foreign agent; the foreign agent will forward this request to the home agent. The registration request packet has to indicate the requested length of time to be served.

- If the nomadic node moves from one foreign network to another, it needs to reregister with the home agent. A registration request with the new foreign agent address, correct identification and authentication is therefore sent to the new foreign agent and further forwarded to the home agent.

- If the nomadic node returns to home from a foreign network, it needs to deregister with the home agent by sending a registration request with zero-lifetime to the home agent directly.

In the ***Register Reply*** state, the nomadic node first checks the reply identification and MD5 authentication. For a correct reply packet accepted by the home agent, the nomadic node will update its service information (e.g., lifetime, register/deregister status, etc.). For a correct reply packet rejected by the home agent, the nomadic node will try to register again by resending the registration request to the home agent; the time intervals between two consecutive registration tries are calculated in an exponential back-off algorithm.

7.2.2 Diversity MPLS Router Components

The diversity MPLS router program runs on the application layer of each router in the preliminary system configuration and the general system configuration. According to the schemes of route diversity and flow merging proposed in Chapter 5 and Chapter 6, the diversity MPLS router program needs two function components:

1. **Diversity routing function**. This function is responsible for forwarding packets to their destinations in accordance with the diversity routing mechanisms.

2. **Flow merging function**. This function merges an original flow and its shadow flow into one flow at the egress router.

The router consists of a single application program written in the form of a multiple event wait loop based on the *Select* (Stevens 1998) mechanism for Unix event handling. The diversity MPLS router handles events in various states including signals processing state, ARP packet processing state, IP packet processing state and MPLS packet processing state. The diagrams of the router program design are shown in Appendix D.

Signal Processing State: In this state, the passive signal will terminate or stop the running of the routing program. During the running of the diversity MPLS router, the diversion function is activated or deactivated by evaluating the receiving signal quality at the user site. When the diversity condition is changed, a signal is sent to the router program; this will allow the diversity MPLS router to enable or disable the diversity label-switching path in the label-switching table. Upon arrival of the diversion signal, modification or updating to the label-switching table is required.

ARP/RARP Processing State: The router receives all link layer (MAC layer) Ethernet packets by opening the Ethernet devices (e.g. “eth0”) in “raw” mode and sets the devices to promiscuous mode so that all packet on the local Ethernet network can be read and filtered. When an ARP/RARP packet is filtered, the source IP-MAC address pair and/or the destination IP-MAC address pair of the ARP/RARP packet are used to update the MAC address table maintained in the diversity MPLS router. The router tracks any hardware changes (e.g. host up and down, network interface card changes, etc.) in the local Ethernet segment with this MAC address table. In the general system configuration shown in Figure 7.2, the LISSY system requires that the destination MAC address of the packet to be transmitted is the MAC address of the final destined node within the cell. It is also necessary for the diversity MPLS router to give the packet destination MAC address by looking up the local MAC address table.

IP Packet Processing State: The Diversity MPLS router is connected on one side to the local Ethernet network, and its task is to forward IP packets to a suitable next hop via a label-switched path. The router firstly filters all Ethernet traffic on its IP address via the ¼ bridge filter. Local traffic where the destination sub-network address is the same as the source sub-network address is filtered out. Arriving traffic with destination sub-network address same as the local sub-network address is also filtered out. All traffic whose destination sub-network address is different from the local sub-network address is queued for processing by the label switching mechanism. The label-switching process includes: parsing the header of IP packet, obtaining a forwarding equivalence class, mapping the forwarding equivalence class to an outgoing diversity-label, encapsulating the IP packet with the outgoing label, and making diversion label-encapsulation to the original IP packet if the route diversity is enabled. In §6.3, the various aspects of the route diversity protocol are extensively discussed. The process in the diversity MPLS router program follows the protocol described therein.

MPLS Packet Processing State: When the diversity MPLS router receives an MPLS packet, it first looks up the label-switching table to obtain an outgoing label for the packet. If the outgoing label is a normal label, the incoming label of the packet is swapped (replaced) with the outgoing label and the labelled packet is sent out to the next hop. If the outgoing label is a *Null_label*, the packet has arrived at its egress router. In this case the diversity label is removed from the packet, the IP packet is restored and put in different queues for forwarding to its ultimate destination by conventional IP forwarding.

The flow merging function is called before the packet is actually sent to the IP domain. The merged packet is finally forwarded to the ultimate destination. We discussed the scheme of flow merging and the various merging possibilities in detail in Chapter 6. The flow merging function follows this scheme.

7.2.3 Other Application Tools

Developing the testbed described above required an assortment of tools in order to produce the required functions and experiments. This section provides an overview of the software tools used during the process of preparing for the experiments.

During the tests, traffic generation and statistics collection are used to compare the traffic patterns and routing methods. Traffic patterns are generated and collected by TTCP and MGEN (Adamson 1999). TTCP is a widely used benchmarking tool for measuring TCP and UDP performance. It can generate traffic with different packet lengths and is usually used to measure the network throughput. MGEN provides programs for sourcing/sinking real-time IP traffic flows with support for scripted traffic generation program. MGEN transmits, receives and logs time-stamped, sequence numbered packets. Post-test analyses of the log file can assess the network ability under given traffic patterns in terms of packet loss, delay, delay jitter, etc. MGEN has been used to evaluate the capability of the two configured testbeds.

For the evaluation of packet delay or delay jitter, a synchronized system time within the whole testbed is necessary. The Network Time Protocol (NTP) tools developed by Mills *et al* (2002) are used to synchronize the time of computers to another server or reference time source. It provides client accuracies typically within a millisecond on LANs and up to a few tens of milliseconds on WANs (wide area networks) relative to a primary server synchronized to Coordinated Universal Time (UTC). In the testbed shown in Figure 7.1 and Figure 7.2, NTP is used to synchronise all computers to one of the computers. The accuracy of timer tick is more important than the accuracy of time relative to a standard time source like UTC.

It is very useful to gather network statistics "on the wire" during the debugging and refining of the diversity MPLS router program. A network spying tool, Ethereal (Combs *et al* 2002), is used to capture events and gather statistics from a live network, browsing the capture data and viewing detail information for each packet during the experiments.

7.3 Summary

This chapter described the testbed setup for experiments carried out during this research. The preliminary testbed is mainly used to develop the proposed schemes of Integration Mobile IP with MPLS, route diversity and flow merging. The general testbed is to demonstrate these schemes in a more general broadband wireless environment such as the local multipoint distribution system. The system consists of an ATM core network, ATM switch, diversity MPLS router with support of nomadic access, user computers, digital video broadcasting downlink equipment and MF-TDMA uplink equipment. An overview of the mentioned hardware in the two system configurations is given in the part of hardware setup. Following on from the description of the hardware setup of the testbed, the software components developed during the tests are explained in the second part of this chapter. The nomadic access program which supports the diversity MPLS routing is introduced, and the program to implement diversity routing and shadow flow merging are also explained and related to the protocols proposed in the previous chapters. SDL diagrams for the software components are in Appendixes B, C and D.

Chapter 8 Results and Discussion

Abstract

This chapter describes the series of experiments undertaken on the testbed described in the previous chapter. Results are presented in three main sections: the integration of Mobile IP with MPLS, the performance of the diversity MPLS router, and the results of applying the proposed mechanisms in a general wireless broadband network environment. The integration of MIP with MPLS section describes the result of the proposed integration scheme with a comparison of the normal Mobile IP and Mobile IP over MPLS schemes, in terms of the round trip time (RTT) and throughput under different scenarios. The diversity MPLS router test section describes the result of the proposed diversity router and shadow flow merging mechanism in the situation of different application scenarios, in terms of the throughput, route latency, end-to-end delay and packet loss rate, etc. The section of general system application describes the result of applying the diversity router in the real RF environment with the ingredients of noise, interference and packet loss. In each test result, we give the expected explanation. For some tests, like the throughput, the benchmarking methods are also given during the test.

8.1 Results of Different Mobile IP Implementation

8.1.1 Standard Mobile IP

8.1.1.1 Measurement Scenarios

First we examine the properties and results of our standard Mobile IP (MIP) implementation. The results of the standard MIP implementation will act as a benchmark for comparing the results of MIP over MPLS (MIPoverMPLS) and MIP integration with MPLS (MIPintMPLS) solutions and deriving the quantitative conclusions. As explained in Chapter 2, standard MIP uses IP-in-IP (Perkins 1996b) tunnelling protocol to forward packets destined for the mobile node at its home address to its foreign network address. For incoming packets to the node, the home agent must encapsulate them with external IP headers and send them via an IP tunnel to the mobile node; however outgoing traffic from the away mobile node will be delivered to the correspondent node directly from the foreign network, rather than first via the home agent, and therefore forms a triangular route.

Overheads imported from the standard MIP implementation include tunnelling, triangular routing overheads and fragmentation overheads. Tunnelling overhead is caused by the extra processing of packets destined for the mobile node, mainly because of the encapsulation at the home agent and the decapsulation at the foreign agent. Triangular routing overheads cause inefficiency in the home network. The fragmentation overheads occur when the size of an encapsulated packet is larger than the maximum transmission unit (MTU) of a link.

For example, the MTU of an Ethernet link segment is 1500 bytes. The size of an encapsulated packet will increase by at least 20 bytes (i.e. the minimum IP header length). This might cause a packet to become fragmented thus imposing a fragmentation overhead. Because of these overheads, the network performance is then below the performance when a mobile node is in the home network. Traffic throughput from the correspondent node to the mobile node at the foreign network, for instance, will be reduced sharply compared with the throughput to the mobile node at home. The RTT between the correspondent node and the mobile node also increases.

To compare the overhead effects in the standard Mobile IP implementation, the following five network scenarios are considered:

1. A mobile node is in the home network, with data transferred to it from a correspondent node. This ensures that there are no overhead effects on the network performance.

2. A mobile node is in the home network, with data transferred from it to the correspondent node. No extra overheads exist in this scenario. This scenario is similar to Scenario 1, except that the traffic direction is reversed. It is used to verify the link asymmetry by comparison with Scenario 1 and to evaluate the effect of tunnelling by comparison with Scenario 4 (4 below).

3. A mobile node is in a foreign network, with data transferred to it from a correspondent node. Data packets are tunnelled to the foreign network from the home agent, while the acknowledgements are sent to the correspondent node directly from the foreign network. This scenario involves all three overheads: tunnelling, triangular routing and packet fragmentation.

4. A mobile node is in the foreign network, with data transferred from it to the correspondent node. Note that the data traffic is sent directly from the mobile node to the correspondent node, so that there are no tunnelling, fragmentation or triangular routing overheads. The acknowledgements from the correspondent node to the mobile node will however experience tunnelling and triangular routing overheads. Because the packet size of acknowledgements is very small, there is no fragmentation overhead.

   Note that if there is also data from the correspondent node to the mobile node, the acknowledgement will be carried in the data packet and therefore may be fragmented. But in the scenario we are discussing, data is only in one direction, i.e. from the mobile node to the correspondent node, so the acknowledgement will be an individual packet.

   Although the acknowledgement is still via a triangular route in the home agent, its effect to our test is insignificant because firstly the testbed is connected by a very short cable and hence the propagation time is negligible, secondly the acknowledgement packet is much smaller then the data traffic packet so that transferring acknowledgements causes much less loading to the home network and home agent. The overhead is therefore only the tunnelling.

5. As for scenario 3, except the MTU size of the correspondent node is changed to 1460 bytes. In this way, the system will still experience tunnelling overhead and triangular routing overheads, but the fragmentation overhead is removed from the home agent.

From the combination of the above five scenarios, the different overhead effects to the standard Mobile IP implementation can be evaluated. Table 8.1 summarises every kind of overhead effect on the mobile network.

Scenario	MN at	Data Direction		CN MTU (bytes)	Overheads		
		From	To		Tunnelling	Triangle	Fragment
1	Home	CN	MN	1500	No	No	No
2	Home	MN	CN	1500	No	No	No
3	Foreign	CN	MN	1500	Yes	Yes	Yes
4	Foreign	MN	CN	1500	Yes	No	No
5	Foreign	CN	MN	1460	Yes	Yes	No

Table 8.1 Summary of Different Network Scenarios for Mobile IP Test

8.1.1.2 Standard Mobile IP Result

Two performance parameters, RTT and TCP throughput, are chosen for the comparison between different network scenarios described in the previous section.

Table 8.2 lists the RTT measured when the mobile node is moving between the different scenarios. The results are averages of 20 time measurements under different frame sizes using application PING. For the measurement of fragmentation effects caused by the IP-in-IP encapsulation on the RTT, a different measurement method is used instead of using scenario 5.

Frame Size (bytes)	Scenario 1 RTT (ms)	Scenario 2 RTT (ms)	Scenario 3 RTT (ms)	Scenario 4 RTT (ms)
64	0.4	0.5	1.1	1.1
128	0.6	0.6	1.5	1.5
256	0.9	1.0	2.3	2.3
512	1.6	1.7	4.0	4.0
768	2.3	2.3	5.7	5.7
1024	3.0	3.0	7.4	7.4
1280	3.7	3.7	9.1	9.1
1518	4.3	4.4	10.9	10.8

Table 8.2 RTT of Standard MIP in Different Scenarios

Table 8.2 shows that the RTTs in Scenario 1 are nearly the same as in Scenario 2; this is because a PING request and a reply packet include the same amount of bytes information. Whether a packet is sourced from the correspondent node (i.e. Scenario 1) or from the mobile node, the packet receives the same processing. This also explains the similarity of results between Scenario 3 and 4.

The main difference occurs in the results of Scenario 1 and 3 (the two shaded columns in Table 8.2, respectively). In Scenario 1, the mobile node is in the home network and the three overheads do not exist; but in Scenario 3, the mobile node is in the foreign network where triangular routing and tunnelling overheads occur (for the frame size 1518, fragmentation overhead also occurs). We find that when the mobile node is in the foreign network, the RTT is increased by around 150% compared with the mobile node in home network, i.e. the RTT is 2.5 times greater, mostly due to the triangular routing and IP-in-IP tunnelling.

Figure 8.1 shows the RTT corresponding to Scenarios 1 and 3 of Table 8.1. Here we can clearly see the larger RTT when the mobile node is in the foreign network.

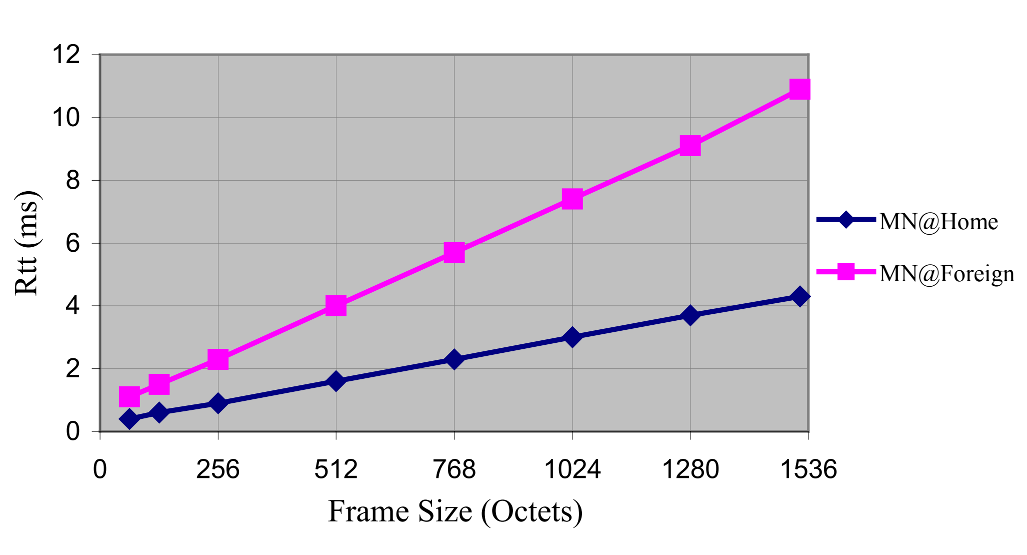


Figure 8.1 Comparison of RTT when MN is in a Home and Foreign Network

To estimate the effects of fragmentation overheads caused by IP-in-IP encapsulation during the forwarding of packets to the mobile node in the foreign network, an alternative measurement method to Scenario 5 in Table 8.1 is used. Here we sent

Ping packets with an encapsulated size equal to the MTU, and Ping packets with an encapsulated size greater than MTU. The first case gives no fragmentation, whilst the second case causes fragmentation.

The actual packet sizes are as follows:

- *No fragmentation overheads after IP-in-IP encapsulation*: using length of ICMP echo data 1452 octets. After the IP-in-IP encapsulation in the home agent, this corresponds to IP packet with length equal to MTU, which is 1500 octets.

  1452(ICMP data) + 8(ICMP header) + 20(IP header) + 20(IPinIP header) = 1500.

- *Fragmentation overheads after IP-in-IP encapsulation*: using length of ICMP echo data length 1454 octets. This corresponds to an IP packet with length 1502 after encapsulation.

The result of the fragmentation overheads on RTT in a standard Mobile IP implementation is given in Table 8.3. Comparing the results of Scenario 3, the fragmentation overhead contributes 0.2 ms to the RTT. i.e. a 1.9% increase. So, the fragmentation overhead effect on the RTT is very small. We can see that the dominant reasons for the increase in RTT are the overheads created by triangular routing and tunnelling.

IP Size (bytes)	Scenario 1	Scenario 2 RTT (ms)	Scenario 3	Scenario 4 RTT (ms)	Comment for Scenario 3, 4
1482	4.4	4.3	10.7	10.7	No Fragment
1484	4.4	4.3	10.9	10.9	Fragment

Table 8.3 Effect of fragmentation on RTT in standard Mobile IP implementation

The next test is about the traffic throughput and it gives a more intuitive explanation of how the different overheads have an impact upon the performance of standard Mobile IP. The results are summarised in Table 9-4. The tests are conducted by means of FTPing a 58.7 Mbytes data file. The results in Table 8.4 are averages of 20 repetitions of file transferring. After each transfer, the FTP application reports the total transfer time and gives the data throughput which is calculated by dividing the file size by transfer time.

Scenario	Transferring Time (sec.)		Throughput (Kbytes/sec.)	
	Average	Standard Deviation	Average	Standard Deviation
1	64.21	1.91	893	26
2	65.79	0.37	870	5
3	163.50	8.03	352	17
4	68.43	0.57	837	8
5	161.80	4.97	354	11

Table 8.4 File Transferring Time and Throughput of Standard Mobile IP

The overall impacts of the three overheads on the standard Mobile IP transfer performance can be obtained by comparing the results of scenario 1 and 3 in Table 8.4. Scenario 1 is the case where the mobile node is in the home network and none of the overheads exist, while in scenario 3 the mobile node is in the foreign network and all overheads exist. It shows that the overheads make the transferring time 155% longer then the normal transferring time when no overheads exist. In terms of the traffic throughput when the mobile node visits a foreign network, it can only achieve 40% of the traffic throughput when the mobile node is in its home network.

Comparing the results in Scenario 3 and Scenario 5, the effect of fragmentation overheads on the transferring time is 2.6%. The effect of tunnelling can be found by comparing the results in Scenario 2 with Scenario 4 and it is 4.1%. We can then conclude that the overheads caused by triangular routing in the standard Mobile IP implementation is about 148%.

The above result proves that the performance degradation (in terms of transfer time and traffic throughput) is caused primarily by the triangular routing mechanism. The reason is that the network segment of the home agent needs to both receive and forward the packets destined for the mobile node, which effectively decreases the throughput from the correspondent node to the mobile node. For this reason, the routing method in the home agent must be improved by some means—the implementation of integrating Mobile IP with MPLS is one of the solutions to this bottleneck problem.

8.1.2 Results of Mobile IP Over and Integration with MPLS

8.1.2.1 Overheads Analysis

Standard Mobile IP can be used in the MPLS network directly by means of MIPoverMPLS. In this network configuration, the MPLS edge router is seen as the boundary between user network and core network. Differentiating from the standard Mobile IP experiments described in Section 8.1.1, the core network routing mechanism is MPLS instead of a conventional IP forwarding mechanism. Other aspects of network configuration are the same as in the standard Mobile IP experiment, for example, home and foreign agents are still used. Because of this, the overheads affecting the performance of standard Mobile IP also exist in the MIPoverMPLS configuration.

Additionally, there is another overhead caused by the MPLS encapsulating and processing at the ingress router of the MPLS domain. This overhead is called the MPLS overhead. Any packet from the home network to the foreign network will experience MPLS overhead. If the mobile node is away from the home network, packets destined for it will be forwarded over the MPLS domain, and therefore they will experience MPLS overhead on top of the overheads of the standard Mobile IP, i.e. IPinIP encapsulation, fragmentation, and triangular routing overheads. Clearly then, the overall performance of the MIPoverMPLS will not be better than that of the standard Mobile IP network configuration.

Unlike standard Mobile IP and MIPoverMPLS, packets destined for the mobile node in the scheme of MIPintMPLS will be label-switched to the foreign network by the home edge router. Although there is still a home and foreign agent in MIPintMPLS, they are only involved in the process of the mobile node movement registration and notification to the edge label-switching router. The only overhead incurred from the implementation of MIPintMPLS is MPLS overhead.

8.1.2.2 Experiments and Results

The objectives of this experiment are to evaluate the performance of MIPoverMPLS and MIPintMPLS and to give a better solution for the nomadic access support in our diversity MPLS router architecture by comparing different Mobile IP implementation. The scenarios used in the experiments are the same as in Table 8.1.

As in the standard Mobile IP experiments in Section 8.1.1, the RTT of different scenarios are first tested. For the scenarios listed in Table 8.1, the RTT for different frame sizes is measured with a repetition of 20; the results shown in Table 8.5 are the averages of these repeated test data. To simplify the table, only the results of two scenarios are listed which corresponds to the mobile node in the home network and in the foreign network, respectively. The RTT of the standard Mobile IP is also listed in the table for comparison among the three network configurations.

Frame Size (Octets)	Scenario 1 (MN in the home network)			Scenario 3 (MN in the foreign network)		
	Standard MIP RTT (ms)	MIPoverMPLS RTT (ms)	MIPintMPLS RTT (ms)	Standard MIP RTT (ms)	MIPoverMPLS RTT (ms)	MIPintMPLS RTT (ms)
64	0.4	0.4	0.4	1.1	2.4	2.1
128	0.6	0.6	0.6	1.5	2.9	2.5
256	0.9	0.9	0.9	2.3	4.0	3.4
512	1.6	1.6	1.6	4.0	6.1	5.0
768	2.3	2.3	2.3	5.7	8.3	6.6
1024	3.0	3.0	3.0	7.4	10.4	8.3
1280	3.7	3.7	3.7	9.1	12.5	9.9
1518	4.3	4.3	4.3	10.9	14.9	11.4

Table 8.5 Results of RTT for Three Mobile IP Implementations

FTP is used to determine the traffic throughput between a correspondent node and a mobile node in this test. The aim is to estimate what fraction of each overhead contributes to the degradation of Mobile IP performance. As with the throughput test in standard Mobile IP, the tests are conducted by means of FTPing a 58.7 Mbytes data file between the mobile node and the correspondent node. The throughput results are summarised in Table 8.6. The results are the averages of 20 repetitions of file transferring. In order to compare these with standard Mobile IP, the average transfer times of standard Mobile IP in different scenarios are also listed in this table.

Scenario	Standard MIP			MIPoverMPLS			MIPintMPLS		
	Transfer Time (sec)		Throughput (KBytes/s)	Transfer Time (sec)		Throughput (KBytes/s)	Transfer Time (sec)		Throughput (KBytes/s)
	Average	Stdev	Average	Average	Stdev	Average	Average	Stdev	Average
1	64.21	1.91	893	64.58	2.58	888	63.61	1.92	896
2	65.79	0.37	870	65.63	0.28	873	65.74	0.23	872
3	163.50	8.03	352	167.95	6.33	342	77.65	1.07	739
4	68.43	0.57	837	71.16	0.91	805	66.95	0.33	856
5	161.80	4.97	354	171.95	7.34	334	78.51	1.87	729

Table 8.6 Results of FTP for Three Mobile IP Implementation

8.1.2.3 Comparison of MIPoverMPLS with Standard Mobile IP

Table 8.5 shows that the RTT results for Standard Mobile IP and MIPoverMPLS in scenario 1 are identical. This, of course, confirms expectations, because the mobile node is in the home network and no extra processing is required in any of the cases.

However, when the mobile node moves to a foreign network, the situation is different. For MIPoverMPLS, packets have to be encapsulated by both the IPinIP and MPLS and then forwarded to the away the mobile node. This imposes an extra MPLS overhead on top of the existing standard Mobile IP overheads. As a result of the combination of the Mobile IP overheads and MPLS overheads, the RTT between the CN and the mobile node increases. Columns 5 and 6 in Table 8.5 show the results when the mobile node moves to the foreign network. We can see that the RTTs of MIPoverMPLS are larger than that of the standard Mobile IP in the whole range of frame sizes.

By comparing the FTP time of standard Mobile IP and MIPoverMPLS in Table 8.6, the following conclusions can be obtained:

- When the mobile node is in the home network, packets between the mobile node and the correspondent node do not experience MPLS overhead; hence there is only a very small difference of transfer time between standard Mobile IP and MIPoverMPLS. This is shown in scenario 1 and 2.

- When the mobile node is in the foreign network in scenario 3, the MIPoverMPLS takes 4.45s more than the standard Mobile IP to transfer the file from the CN to the mobile node. This is an increase of 2.7% over the same scenario in standard Mobile IP and a 6.9% increase compared with the mobile node in the home network in MIPoverMPLS. This increase is caused by the MPLS overhead in the configuration of MIPoverMPLS.

- The total overhead in MIPoverMPLS is 160% which is obtained by comparing the transfer time between scenario 1 and 3. This is mainly the overhead of standard Mobile IP, (with 6.9% of MPLS overhead).

- From the throughputs of MIPoverMPLS in scenarios 1 and 3, we can see that the throughput of the mobile node in the foreign network can only achieve 38.5% of that of when it is in the home network. Compared with the 40% in standard Mobile IP, the performance of MIPoverMPLS is slightly worse.

- In general the performance of MIPoverMPLS when the mobile node is in the foreign network is worse than that of standard Mobile IP, because of the extra MPLS overhead imposed in the MIPoverMPLS configuration.

8.1.2.4 Comparison of MIPintMPLS with MIPoverMPLS and Mobile IP

Firstly the results in Table 8.5 show that the RTTs of the three different Mobile IP implementations are identical when the mobile node is in the home network (scenario 1). This is because there are no extra overheads for any of the traffic.

Secondly the comparison between column 5 and 7 of Table 8.5 indicates that the RTT of MIPintMPLS is generally greater than that of the standard Mobile IP implementation when the mobile node is in the foreign network. When the mobile node is in the foreign network, packets destined for it traverse the MPLS core network. Thus the MPLS core network imposes more end-to-end latency. We also saw this tendency in the result of MIPoverMPLS.

Thirdly and most importantly, the results in columns 6 and 7 indicate that the RTT of MIPintMPLS is less then that of MIPoverMPLS when both experience the same MPLS core network. The reason is that the MIPintMPLS implementation does not impose overheads like IP tunnelling, triangular routing and fragmentation which are in the MIPoverMPLS implementation. In other words, it is the overheads of standard Mobile IP that makes the performance of MIPoverMPLS worse than that of MIPintMPLS.

The results of file transfer in Table 8.6 indicate that:

- When the mobile node is in the home network (scenarios 1 and 2), the transfer time of the three Mobile IP implementations is very similar. The reason is that the network conditions between the correspondent node and the mobile node are the same in the above scenarios.

- When the mobile node moves to a foreign network, the FTP transfer time of MIPintMPLS only increases by about 22% compared with the transfer time when it is in the home network, while the throughput from the correspondent node to the mobile node achieved 82.5% of that when it is in the home network. This is a great advantage over the standard Mobile IP and the MIPoverMPLS, in which the throughput when the mobile node is in the foreign network can only achieve 40% and 38.5% of that of the mobile node in the home network, respectively.

- With the smaller packet size of scenario 5, the throughput of MIPintMPLS does not improve, compared with the throughput in scenario 3. An obvious fact is that the packet in MIPintMPLS does not suffer the fragmentation caused by IPinIP encapsulation as in standard Mobile IP.

Figure 8.2 is a direct comparison of the throughput for the three mentioned Mobile IP implementations in different scenarios. Clearly, we can see that the MIPintMPLS consistently achieves the best performance in all tested scenarios.

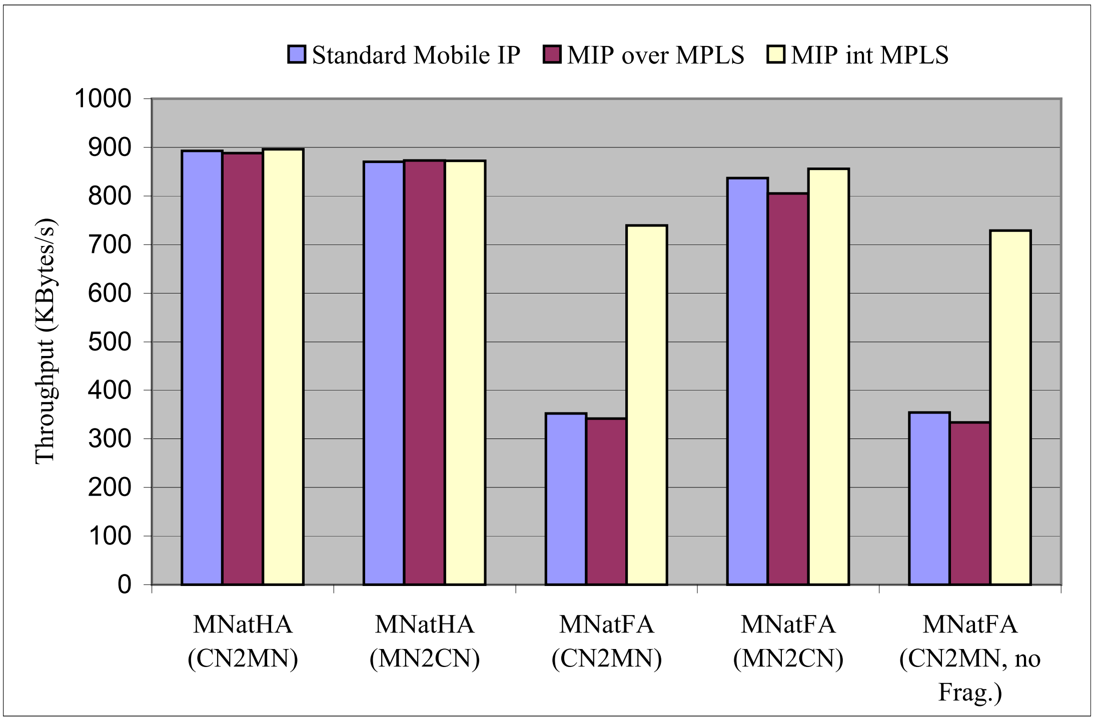


Figure 8.2 Comparison of TCP Throughput for Different Mobile IP Implementation

8.2 Performance of MPLS Diversity Router

The experiments described in this section aim to benchmark the established MPLS diversity router, and to demonstrate the ability of reducing frame loss by using the proposed shadow flow merging scheme.

8.2.1 Benchmarking Tests

8.2.1.1 Throughput of MPLS Diversity Router

The throughput of the MPLS diversity router is the maximum rate at which none of the offered frames are dropped by the router.

Procedure: Send a specific number of frames at a specific rate through the MPLS diversity router and then count the frames that are transmitted by the router. If the count of the transmitted frames is less then the count of offered frames, the rate of the offered stream is reduced and the test is rerun. The throughput is the fastest rate at which the count of test frames transmitted by the router is equal to the number of test frames sent to it.

Parameters: The following parameters are constant in the throughput test and other performance benchmarking:

- The bandwidth between router and core network is 2Mbps. This is in compliance with the testbed setup and requirement of the MF-TDMA return-link of the trial system.
- The duration of each run test is 120s.
- The offered traffic is UDP packet in constant bit rate.
- The frame sizes used in the test are 78[11], 128, 256, 512, 768, 1024, 1280, 1518 octets which are recommended in RFC 2544 (Bradner and McQuaid 1999) in the case of Ethernet connection.

Figure 8.3 displays the throughput of the MPLS diversity router in units of frames/sec when benchmarked with the test procedure and parameters described above. It shows that the throughput for smaller frame sizes drifted more from the theoretical frame rate, while with the increase of frame size the throughput approaches the theoretical throughput (specifically after the frame size 512). This is because the smaller the frame size is, then proportionally more frames will arrive at the router to be processed and transmitted for a certain traffic rate within a certain period of time, which generates heavy processing loads in the router. Consequently the smaller frame size could not achieve the expected frame rate. Notice that the throughput is tested for three different queue lengths – 1000, 500 and 200 respectively, the three curves are overlapped. The graph also shows that there is no significant difference in the throughput among different queue length strategies. The queue length is the total number of packets queued in the router to be processed.

[11] In RFC 2544, the smallest frame size for benchmarking an Ethernet device is specified as 64 octets. The smallest UDP payload which can be generated by application MGEN, used to generate UDP traffic in the experiments, is 32 bytes in which the packet sequence number, timestamp, flow ID and other post-processing information are carried. This makes the smallest frame size in MGEN 78 octets.

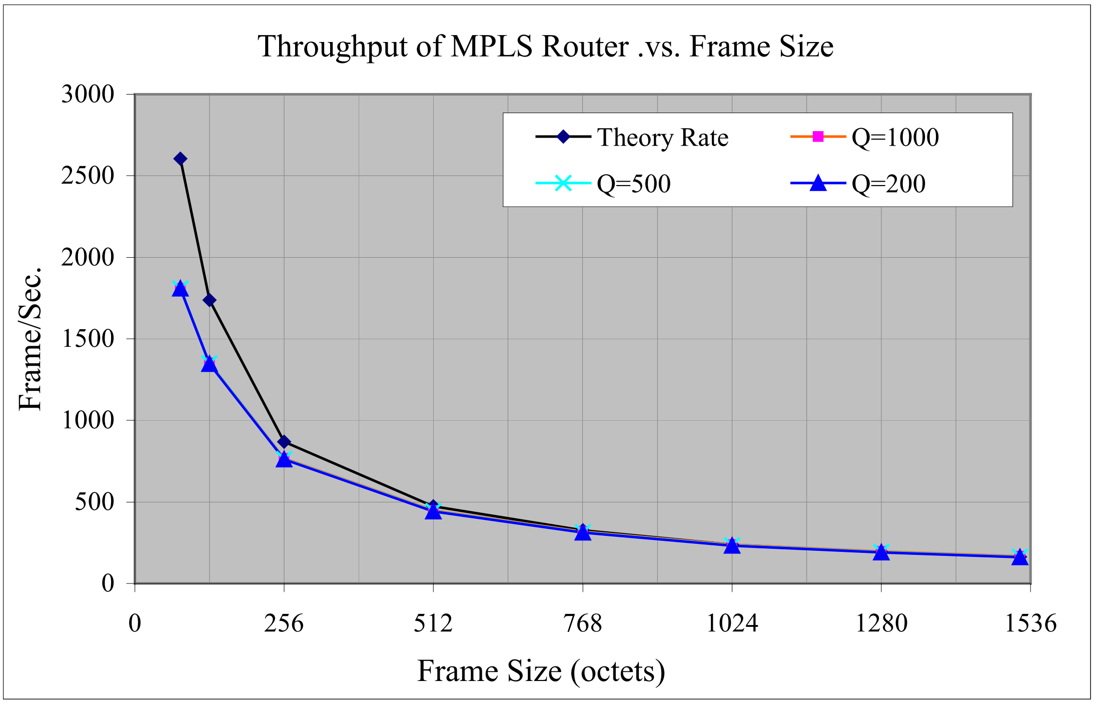


Figure 8.3 Throughput of MPLS Router as the Function of Frame Size

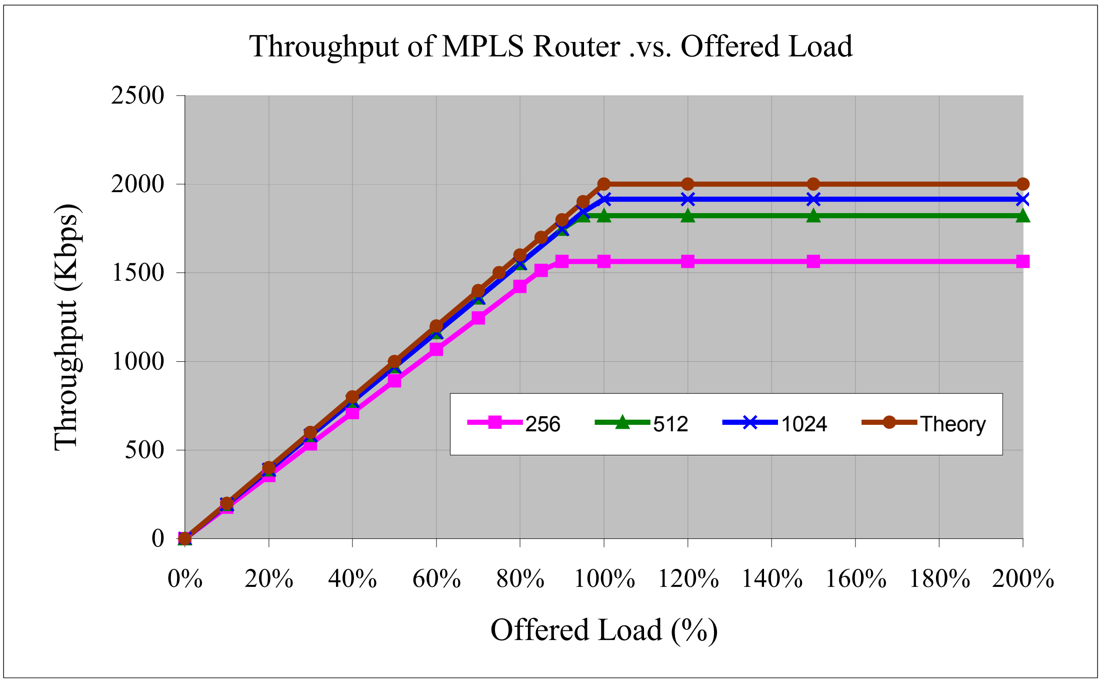


Figure 8.4 Throughput of MPLS Router as Function of Offered Load

Figure 8.4 shows the throughput of the MPLS diversity router as a function of the offered load, which is measured for frame size 256, 512 and 1024 octets. The brown curve is the theoretical throughput under the offered load. The measurement procedure is described as:

- Send the MPLS router frames at a specific percentage of the maximum rate (here it is 2Mbps) and count the frames transmitted by the router. The offered load ranges from 10% to 200% at 10% increases. (Note: as the offered rate reaches maximum throughput, finer granularity is needed to ascertain the absolute value). The duration for each run is 120 seconds. The test is repeated for different frame sizes with the router queue length 1000.

Figure 8.4 shows that for varying frame sizes, the router can process different amounts of offered traffic. As can be seen, the smaller the frame size is, the sooner the maximum processing point is reached. A safe working parameter for the MPLS router is the offered load to be no more then 75% of the maximum rate of the backbone link.

8.2.1.2 Frame Loss Rate

The frame loss rate of the MPLS diversity router is defined as the percentage of frames under steady state (constant) load that were not forwarded due to lack of resources. It can be used in reporting the performance of the MPLS diversity router in the overloaded state. Its measurement procedure is as following:

- Send a specific number of frames at a specific rate through the MPLS router and count the frames that are transmitted by the MPLS router. The frame loss rate is calculated using the following equation:

$$(\text{input\_count} - \text{output\_count}) \times 100 \Big/ \text{input\_count}$$

The first trial is run for the frame rate that corresponds to 100% of the maximum rate of the link from the router to the core network. Repeat the procedure for the rate that corresponds to 90% of the maximum rate used and then for 80% of this rate. The maximum rate is 2 Mbps in this test. This sequence is continued (at reducing 10% intervals) until there are two successive trials in which no frames are lost. The maximum granularity of the trials must be 10% of the maximum rate, a finer granularity is also used at some break-point. The duration of each run is at least 200 seconds. The unit of packet loss rate is the percentage of offered frames that are dropped.

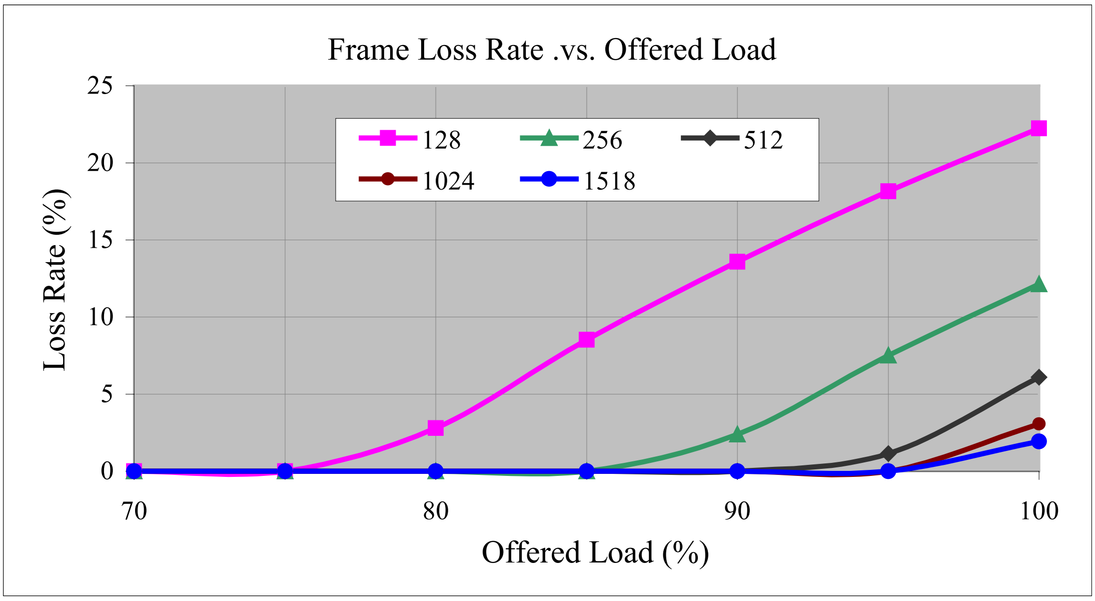


Figure 8.5 Frame loss rate of the MPLS Router as a function of offered load

Figure 8.5 shows the frame loss rate performance of the MPLS router for different frame sizes. The following inferences are made from this:

- When the offered load is low the router is capable of forwarding all the offered frames; therefore the frame loss rate is zero. This remains true when the offered load is less than 75% of the tested maximum rate for all the tested frame sizes. This is to say that there is no frame loss when the router resource utilisation is less then 75%.

- With the offered load increasing, the router resource becomes more fully utilized and frames that are not forwarded by the router will be lost.

- For a certain offered load, the larger the frame size, the less the frame loss rate is, i.e., router resources are utilized more efficiently when frame sizes are averagely large.

8.2.1.3 Latency of the MPLS Router

Latency in the MPLS router measures the time interval beginning with a frame reaching the input port of the MPLS diversity router and ending when the frame is sent to the output port of the router. To measure the latency, the method recommended in RFC 2544 (Bradner and McQuaid 1999) is used. The procedure and parameters are listed as following:

- First determine the throughput for the router at each of the tested frame sizes. Then send a stream of frames at a particular frame size through the router at the determined throughput rate to a specific destination. Each frame has a receiving timestamp and a sending timestamp. Each frame also has a sequence number used as an identification number.

- The stream is 120 seconds in duration for each tested frame size. The number of frames sent within this duration is dependent upon the frame size, for example, the number of frames sent is 217008 for frame size 78 octets and 19632 for frame size 1518.

- An identifying frame after 60 seconds is transmitted and the time at which this frame is received by the router is recorded (timestamp A). The time at which the identifying frame is sent to the output port is recorded (timestamp B).

- The latency is timestamp B minus timestamp A for the specified frame size. The test is repeated at least 20 times with the reported value being the average of the recorded values.

Figure 8.6 displays the result of the measured latency of the MPLS router, which is obtained when the router is configured with queue length 100, 200, 500 and 1000 and the testing stream is UDP protocol at the frame rate of router throughput.

Figure 8.6 shows that the latency steadily increases as the queue length increases. As a store and forward device, the MPLS router queues the frames not being forwarded when the frames reach the router with rate of throughput. The number of queued frames in the front of the tagged frame determines how long the tagged frame will have to wait to be forwarded. This waiting time is the major component of the MPLS router latency and is proportional to the queue length and frame size.

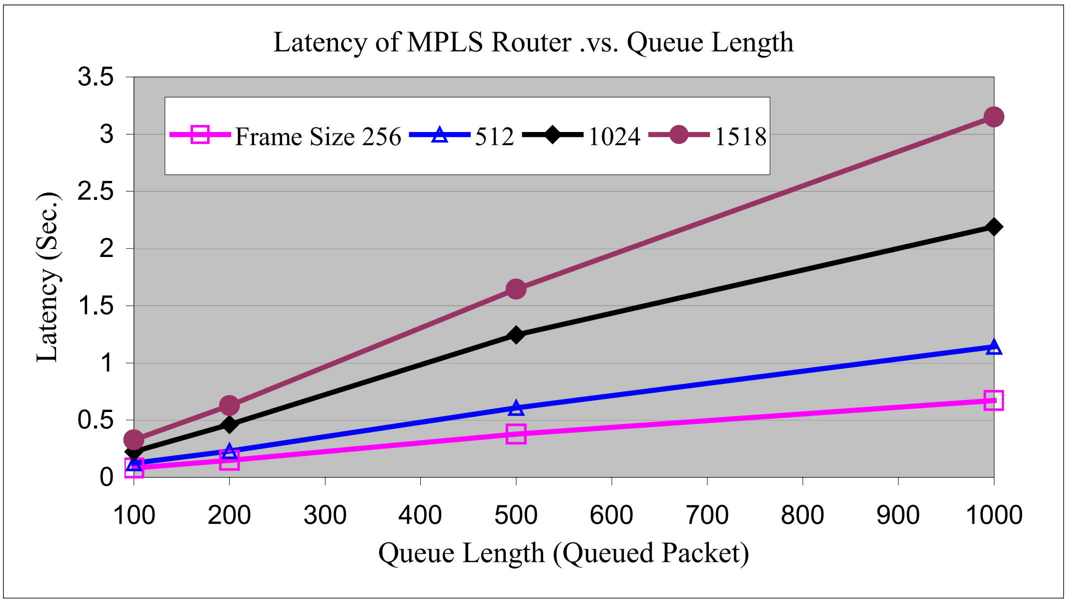


Figure 8.6 Latency of the MPLS router as a function of queue length

8.2.1.4 Burst Traffic

It is convenient to measure the MPLS diversity router performance under steady state load but this is an unrealistic way to gauge the functioning of the router since actual network traffic normally consists of bursts of frames. The size of a burst is the number of frames within the burst. The frames within the burst are transmitted with the minimum legitimate inter-frame gap.

The objective of the burst test is to determine the minimum interval between bursts which the MPLS router can process with no frame loss. During each test the burst size is held constant and the inter-burst interval varied. The burst duration is at least 2 seconds. The test is run with burst size 16, 32 and 64 frames. To generate burst traffic with a specified burst size in this test, a big UDP packet is chosen and chopped into small frames. The result is given in Table 8.7 and it is the average of 20 runs. The burst interval chart is also shown in Figure 8.7.

Frame Size (octets)	Burst Size 16		Burst Size 32		Burst Size 64	
	Burst Interval (ms)		Burst Interval (ms)		Burst Interval (ms)	
	Average	Stdev	Average	Stdev	Average	Stdev
128	10.29	0.02	16.17	0.05	35.19	0.06
256	12.63	0.02	24.76	0.04	53.77	0.15
512	16.76	0.03	33.22	0.05	69.19	0.15
1024	20.67	0.06	40.56	0.09	90.73	0.23
1518	21.46	0.05	40.77	0.13	-----	-----

Table 8.7 Burst Traffic Interval Performance of the MPLS Router

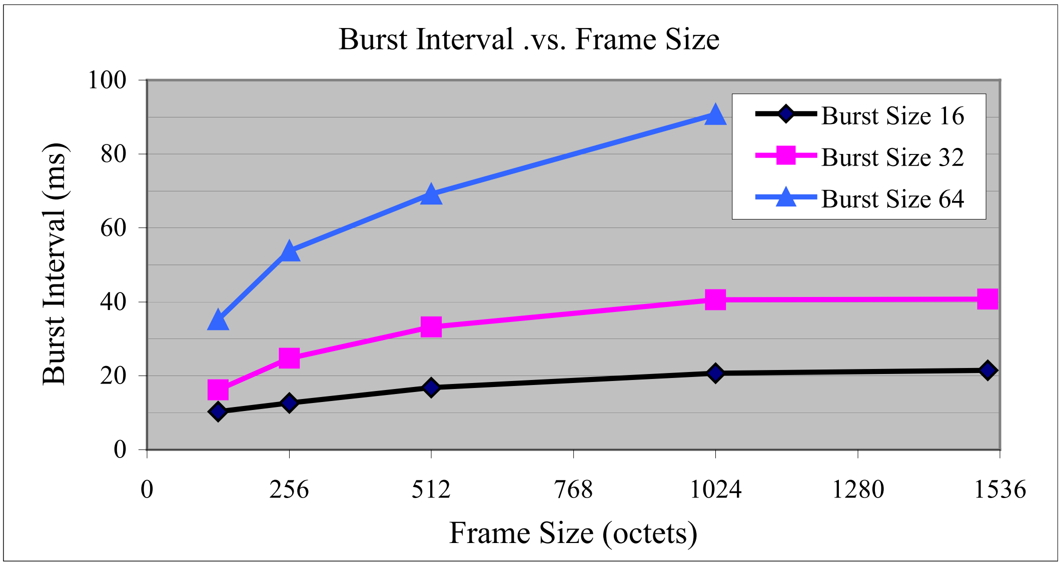


Figure 8.7 Burst Traffic Intervals as Function of Frame Size of the MPLS Router

The result indicates that for a given frame size, the burst interval increases as the burst size becomes greater. The increase is nearly proportional to the burst size. The burst frames have to be queued in the router before they can be processed and forwarded by the MPLS router. When the router is fully utilised, no more new burst blocks can be accepted and processed without frame loss until one whole burst block leaves the router completely. It takes more time to process and forward a burst block with a bigger burst size and therefore the interval between two consecutive burst blocks is longer. The curves in Figure 8.7 shows that for a given burst size, the burst intervals increase more at the small frame size end than at the big frame size end. Actually after the frame size is greater than 1024 octets, the burst intervals increase a little. This is to say that our MPLS router is more sensitive to the small frame sized burst traffic.

8.2.2 Diversity and Flow Merging Capabilities

Diversity and shadow flow merging capabilities are the major features of the MPLS diversity router with which to provide better service availability in a broadband wireless environment. In this section we design several experiments to simulate the packet loss, and to examine the flow merging capabilities and the benefits derived.

8.2.2.1 Experiment 1: Comparison of Frame Loss Rate

The experiments undertaken in this section concern the ability, when using the MPLS router and shadow flow merging mechanism, to reduce frame loss rate in the case where such a loss happens during the frame transfer from ingress router to egress router. A UDP stream is generated with application MGEN at the source application PC. Each packet is tagged with a timestamp and a continuous sequence number starting from zero. A packet is randomly discarded, whilst making the interval between two discarded packets uniformly distributed and the total number of discarded packets being a certain percentage of the total generated packets. Subroutines for the generation of pseudo-random numbers with a uniform distribution in the range of [0,1] are commonly available. The random packet discarding occurs in either the normal flow, or the shadow flow or both. At the destination application PC, all the received packets are logged and post-processed to check the lost packets, to compute and compare the packet loss rates in different scenarios.

The same experiments are also run using an exponentially distributed packet loss model. Table 8.8 lists one of a set of results which is obtained by sending a 512Kbps CBR UDP stream to the router at 5% random packet discarding rate. The traffic stream lasts at least 120 seconds for each test and the results are the average of 20 repetitions.

When the router works without activating the shadow flow merging in Table 8.8, the frame loss rate at the destination is at a constantly high percentage in column 4 if the uniform distributed frame discarding algorithm is applied. After activating the shadow flow merging mechanism and applying the random frame loss to either the normal or shadow flow, there is only frame loss in the case of small frame sizes and no frame loss in other cases. This is the case that the shadow router is designed to work for. In reality, it is most likely that both flows will lose frames specifically in the wireless environment. This is the last scenario to be evaluated in Table 8.8: in which both flows drop frames randomly, and the frame loss rate at the destination is comparatively much lower after flow merging. The gain of frame loss for shadow flow merging ranges from 4.4 to 16.0. This is calculated by dividing the frame loss rate from two flows with that of one flow without shadow flow merging.

Frame Size (octets)	Number of Total Sent Frames	5% Uniform Distributed Frame Dropping						
		Without Shadow Flow		With Shadow Flow Merging				
		1 Flow Drop		1 Flow Drop		2 Flows Drop		
		No. of Total Lost Frames	%	No. of Total Lost Frames	%	No. of Total Lost Frames	%	Gain
78	98460	4691	4.8	5	0.005	1103	1.1	4.4
128	60000	2858	4.8	1	0.002	471	0.8	6.0
256	30000	1428	4.8	0	0	143	0.5	9.6
512	15000	714	4.8	0	0	46	0.3	16.0
768	10000	476	4.8	0	0	25	0.3	16.0
1024	7500	358	4.8	0	0	20	0.3	16.0
1280	6000	286	4.8	0	0	15	0.3	16.0
1518	5060	241	4.8	0	0	13	0.3	16.0

Table 8.8 Comparison of random frame loss ratio of shadow flow merging

Figure 8.8 shows the frame loss ratio against frame size for the frame drop models of 1% and 2% uniformly distributed frame dropping, Figure 8.9 is for 5% and 10% random dropping respectively. For both figures, it is noticeable that the frame loss ratio of non-shadow flow is higher than the frame loss ratio of with activating the shadow flow when the same random frame drop model is applied. For example, when 2% random frame drop model is applied in Figure 8.8, the curve of non-shadow flow is nearly a flat line and kept at about 2% level; however the curve of with activating the shadow flow (the black one) is less than 0.1%. We also get the conclusion that the frame loss ratio of small frame size is higher than that of the big frame size even if the shadow flow is activated. With the frame size getting bigger, the frame loss ratio is gradually reduced when the shadow flow is activated. This tendency is consistent with the result in Figure 8.5 in which the frame loss ratio of the diversity router is benchmarked against the offered load.

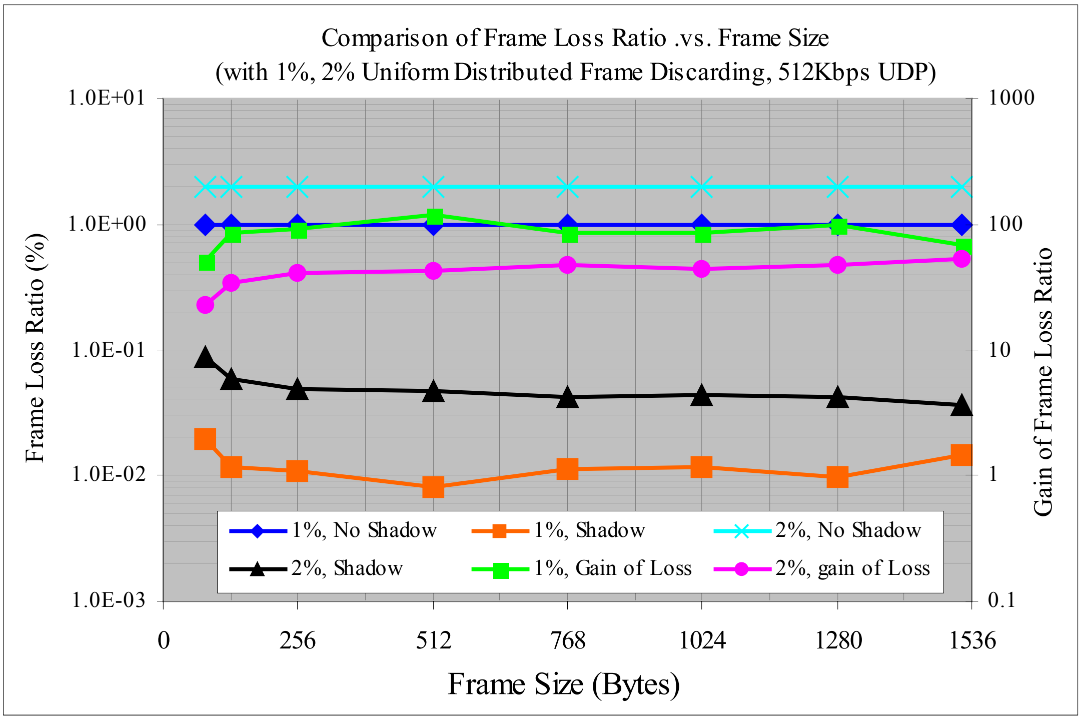


Figure 8.8 Comparison 1 of random frame loss ratio of shadow flow merging

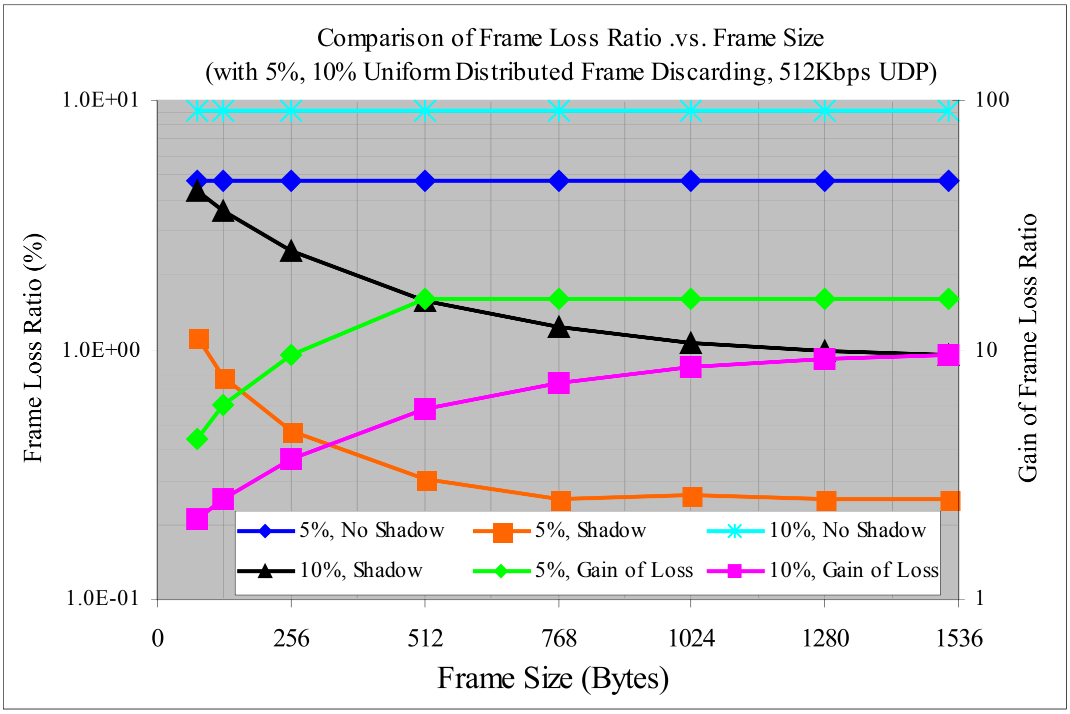


Figure 8.9 Comparison 2 of random frame loss ratio of shadow flow merging

8.2.2.2 Experiment 2: Comparison of End-to-End Delay

This section aims to compare the end-to-end delay of the MPLS diversity router in different application scenarios. The end-to-end delay is the duration of a packet traversing from the source to the destination under normal traffic condition. It is measured by sending a stream of packets from the source machine to the destination machine. The stream duration is at least 120 seconds. In the middle of the stream, a packet with timestamp A is sent from the source and recorded at the destination with timestamp B. The end-to-end delay is the time difference between timestamp A and B. To do this, a network time synchronous application is run to ensure the source and destination have coordinated clocks. To measure the end-to-end delay of the diversity router when frame loss occurs, a random frame discarding algorithm is used to make the interval between two discarded frames distributed exponentially and the total number of discarded packets being a certain percentage of the total generated packets.

The scenarios included in this test are:

- end-to-end delay of a normal flow without frame loss,
- end-to-end delay of a normal flow and a shadow flow without frame loss, and
- end-to-end delay of a normal flow and a shadow flow with frame loss.

The traffic is UDP stream at 512Kbps generated by application MGEN. Each test is run for 120 seconds with 20 repetitions and the result is the average of 20 tests. The result is shown in Figure 8.10.

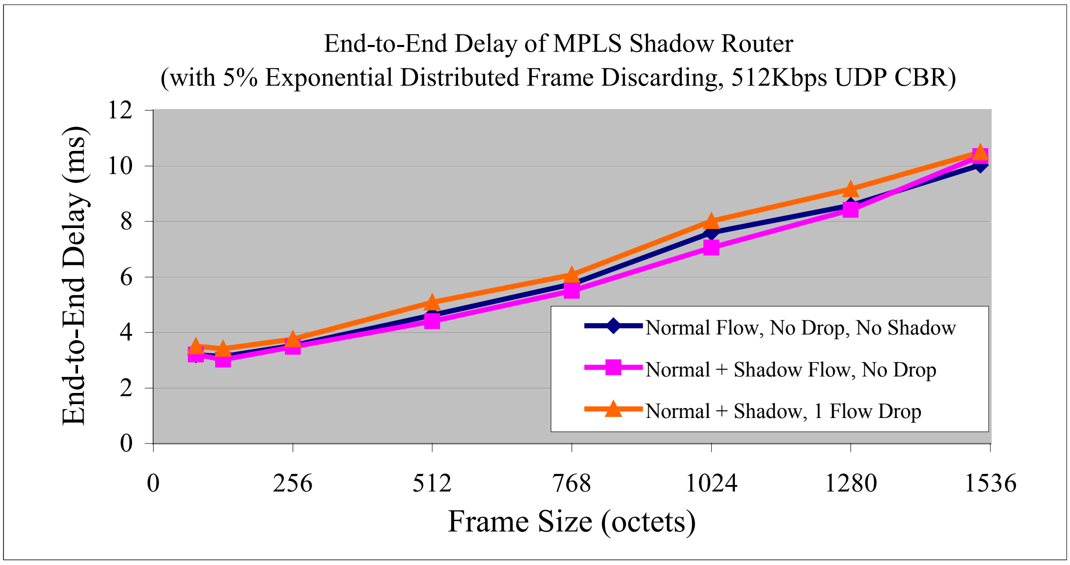


Figure 8.10 Comparison of End-to-End delay of the MPLS Shadow Router

Although the end-to-end delay of the three scenarios is similar, slight differences can be seen in Figure 8.10. In the shadow flow merging mechanism, if two identical packets—one from the normal flow and one from the shadow flow— are received at the egress router, the earlier arrival is the one which will be merged. This will result in the end-to-end delay of the MPLS shadow router being relatively shorter in the case when a shadow flow is activated and no random frame discard occurs on both flows, than in the case when shadow flow is deactivated and there is no frame discard on the normal flow. In Figure 8.10 this is shown by the pink and blue lines respectively. When frame dropping occurs in either the normal flow or the shadow flow, the egress router will use the packet of another flow to merge if it has arrived; otherwise the router will wait the arrival of the dropped packet. This leads to a slightly longer end-to-end delay for the case of frame dropping. The orange line in Figure 8.10 reflects this tendency.

Figure 8.11 shows the end-to-end delay variation during one run of the test. Each point of delay is the average during one second. It clearly shows that the delay of a normal flow without shadow is more dispersed than the delay of normal flow with shadow flow merging in the case of random frame loss. Comparing the two shadow flow merging scenarios, the delay variation of the scenario of one flow drop frame is rarely noticed (pink colour), whilst a few delays are outstanding (yellow colour) although the overall variation is small in the case of both the normal flow and the shadow flow drop frames.

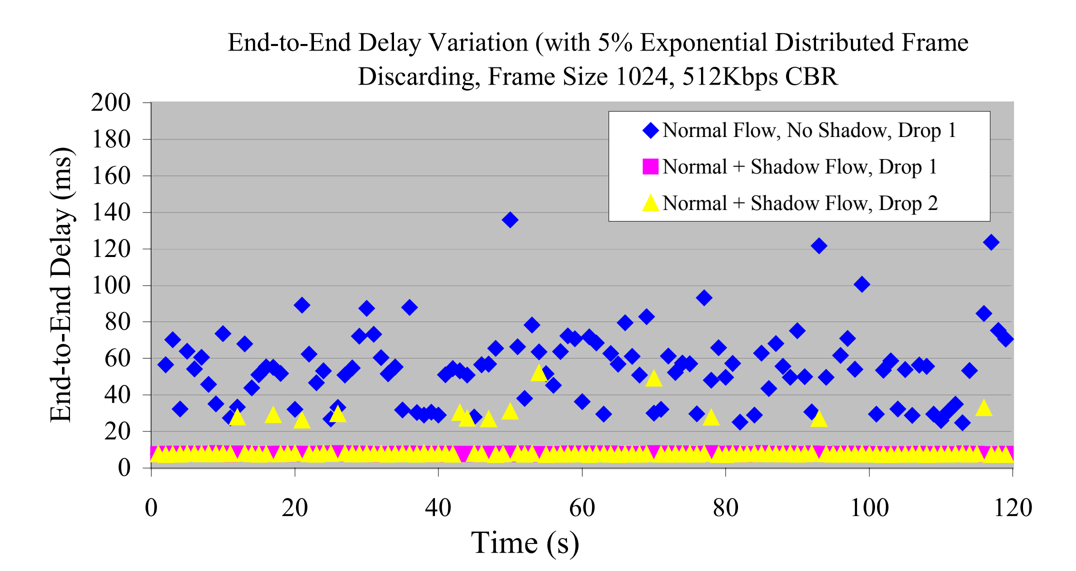


Figure 8.11 Comparison of Delay Variation of MPLS Shadow Flow Router

8.2.2.3 Experiment 3: Comparison of End-to-End Latency

The impact of shadow flow merging on end-to-end latency of the diversity router is compared in this section. The end-to-end latency is the duration of a packet traversing from the source to the destination when the router is injected traffic at the frame rate of throughput. It is measured by sending a stream of packets in the rate of frame throughput from the source machine to the destination machine. The benchmarking frame throughput in Section 8.2.1.1 (see page 106) is used in this experiment. The stream is last 120 seconds. In the middle of the stream, a packet with timestamp A is sent from the source and recorded at the destination with timestamp B. The end-to-end latency is the time difference between time stamp A and B.

The traffic is UDP stream and the duration of each run test is 120 seconds. The tested frame sizes include 78, 128, 256, 512, 768, 1024, 1280 and 1518 octets. No artificial random frame loss is applied on the source traffic in this test. The result shown in Figure 8.12 is the average of 20 repetitions.

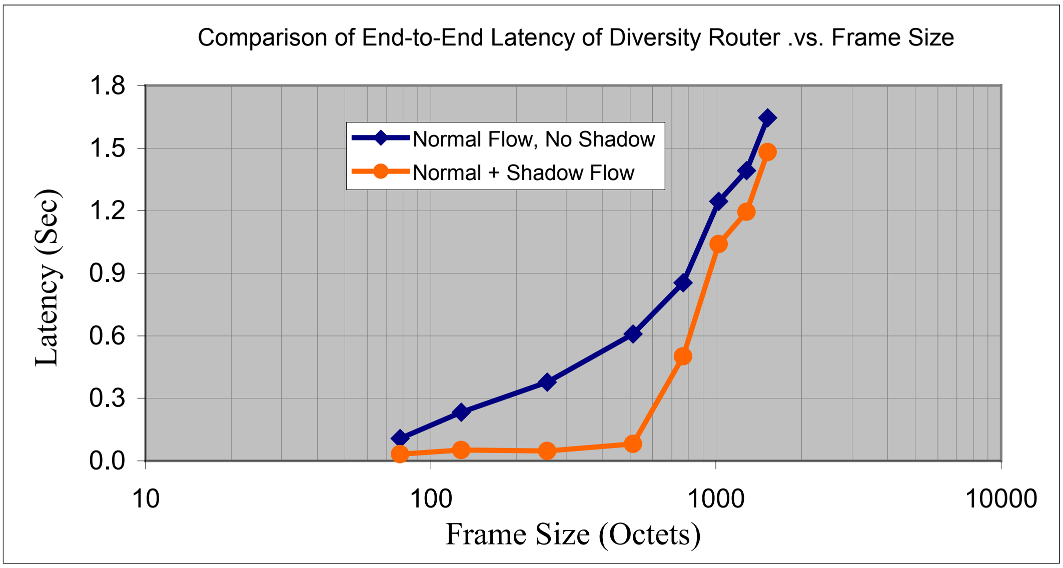


Figure 8.12 Comparison of end-to-end latency of the shadow flow

As we expected, the shadow flow merging mechanism takes the earlier arrived packets for the flow merging, therefore the latency of the merged flow is less than the latency of only the normal flow. Specifically when the router is injected traffic in the rate of frame throughput, its queue is to be full and the end-to-end latency is getting to be large; the end-to-end latency difference, between the case of shadow flow is activated and the case of only normal flow without shadow flow merging, appears to be large (comparing with the end-to-end delay difference when the router works under normal traffic condition such as in Figure 8.10).

8.3 Experiment of diversity in RF environment

This section describes the experiments when the MPLS diversity router is used in a general broadband wireless access system as shown in Figure 8.13 (Figure 7.2, page 83, duplicated here for ease of reading).

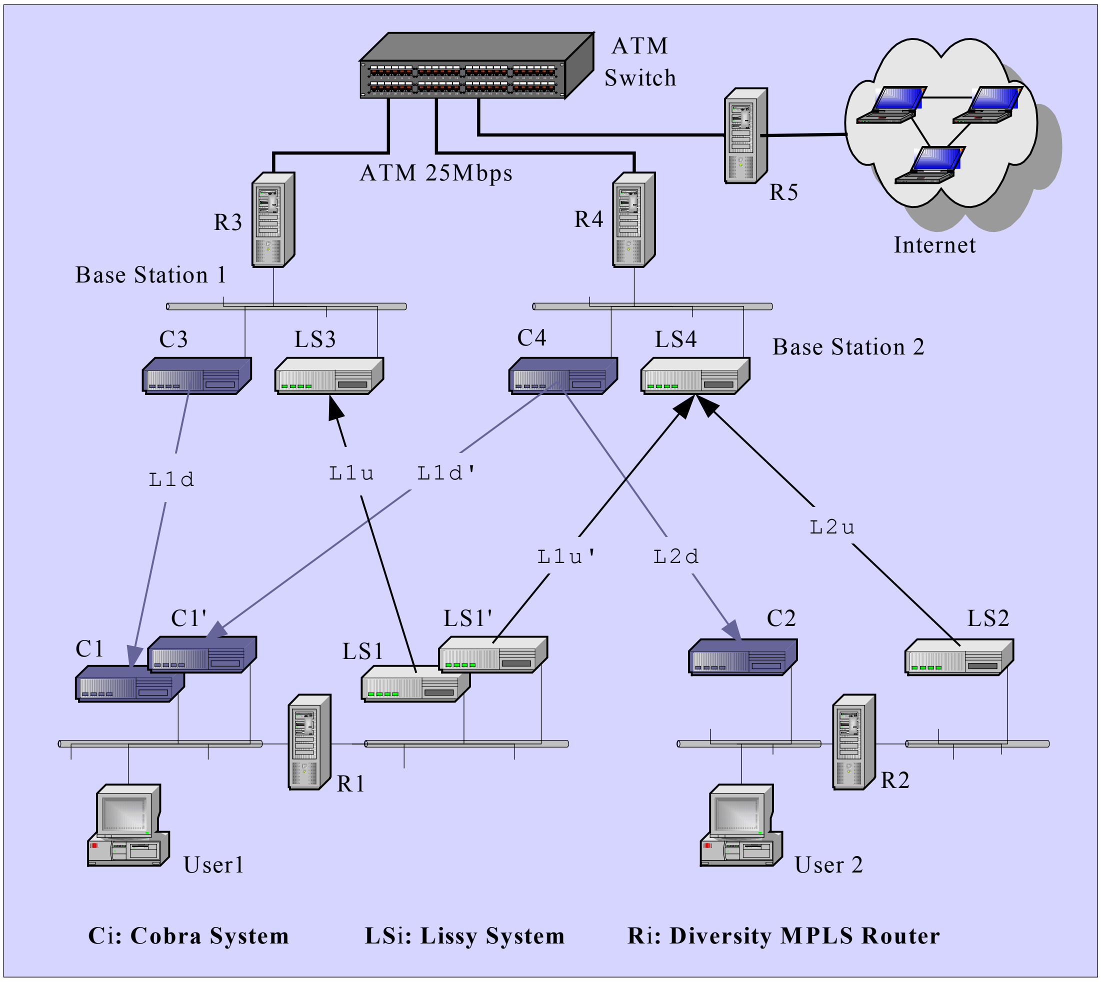


Figure 8.13 Diagram of a general wireless broadband access system

8.3.1 Diversity with Noise and Signal Fading

Diversity is activated when the RF downlink signal is degraded to a certain level which is dependent upon the local weather, geography, requirement of service availability, etc. In the experiment, a *Gaussian* white noise generator is used to adjust the signal to noise ratio and a signal attenuator to simulate the signal fading at the COBRA receiver. The downlink signal level is pre-adjusted to the point at which several dBs attenuation will cause the link failure, so that we can operate the noise generator and signal attenuator to make the RF link swap between normal work state and failure state.

One crucial decision is what parameter is selected as the diversity criteria. One requirement for this parameter is that it should be sensitive to the signal attenuation and noise and effectively indicate the degradation of the link, especially during the time of the link failure. In the configuration of Figure 8.13, the diversity router R1 is able to acquire three parameters – AGC level, lock status and Viterbi error – about the DVB-S receiver via an I^2C bus. The AGC level indicates the receiving signal strength. Experiments show that the quantitative change of the AGC level is not significant with the change of signal attenuation. This smooth behaviour makes the AGC level an unsuitable candidate of diversity criteria. When any lock status is lost, the RF link has already failed. In other words, the lock status is unable to indicate the procedure of link degradation before the link fails.

The Viterbi error in our system indicates the number of bit errors occurring in a unit time (one second). All experiments show that the Viterbi bit error is varied in the range of 0~100 bit/second in the normal work state. When the signal is fading and the link fails, the Viterbi error jumps to a very high level. The choice of Viterbi error as the diversity criteria is hence made because it is more sensitive to signal attenuation and noise than other parameters (for instance, the receiver AGC level or lock status).

The experiments described in this section aim to verify that the diversity function is activated properly when the signal is fading and the RF link is under threat of failure. Figure 8.14 is measured under following parameters:

- Signal to noise ratio: 20dB
- Range of signal attenuation: 0 ~ 12dB in 1dB/step for 60 seconds
- Diversity criteria: Viterbi bit error > 100 bit/second
- Traffic: UDP packets generated by Netmeeting

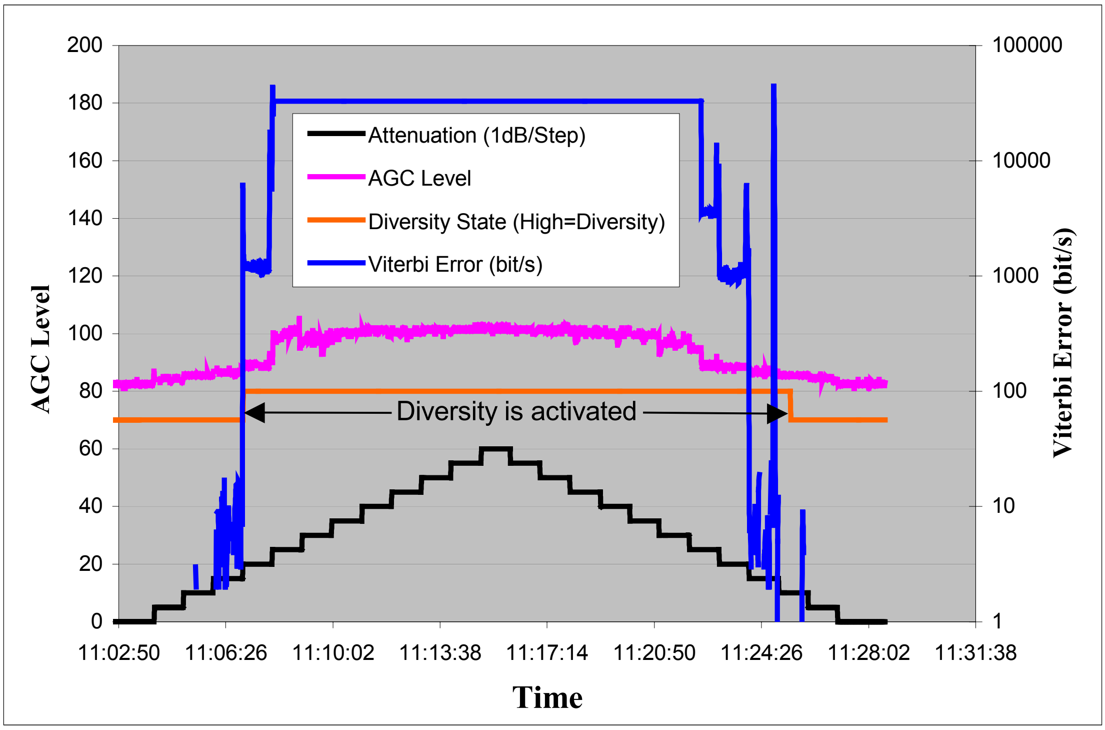


Figure 8.14 Diversity state changing with signal attenuation and Viterbi error (at SNR 20dB, signal attenuation 0~12dB in 1dB/step for 60 seconds)

In Figure 8.14, there is no diversity at the earlier phase because the attenuation is small and there are few Viterbi errors. When the signal attenuation goes from 3dB to 4dB, the Viterbi errors jump to more than 1000 and the diversity function is activated. Further increasing the signal attenuation causes the receiver to lose the lock to the signal and the link to completely fail. During this period, the Netmeeting application is running continuously and without noticeable interruption. The long flat of the Viterbi error curve is because of the Viterbi error register of the Cobra receiver is a constant big number after the link has failed. When the Viterbi error has decreased with the reduction of signal attenuation at the end phase of the experiment, the router checks that the link is back to normal; then it keeps the diversity activated for a further two minutes to ensure that the diversity state is not immediately trigged by the fluctuation of signals. After that, the diversity is turned off and the router returns to normal work state.

Figure 8.15 is measured when the signal to noise ratio is 30dB and other parameters are same as in the above experiment.

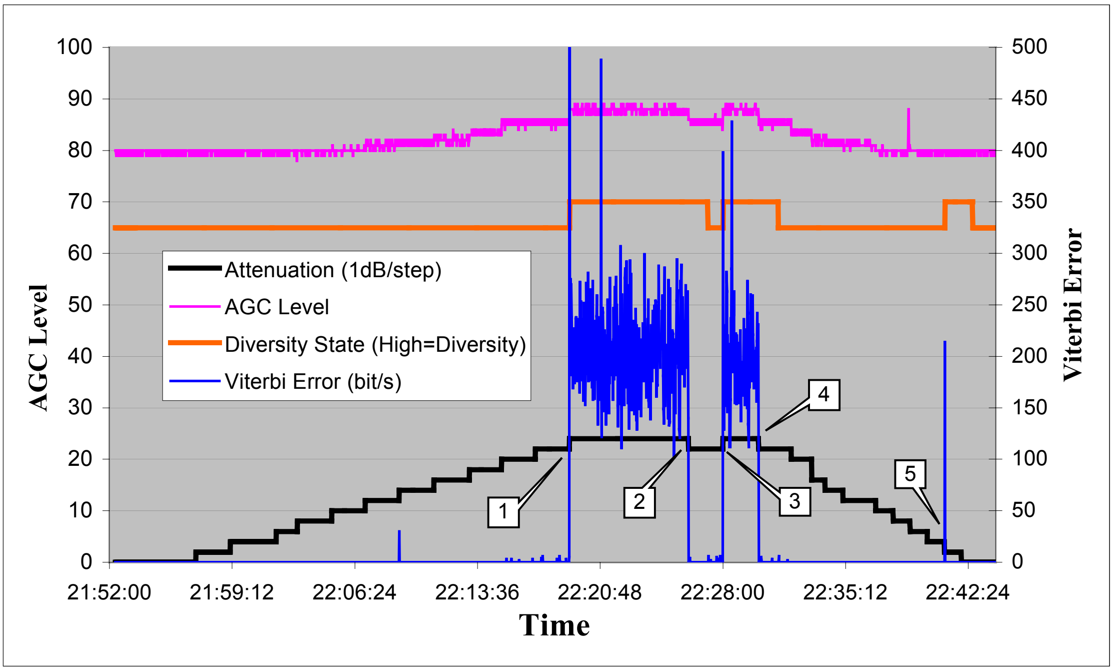


Figure 8.15 Diversity state changing with signal attenuation and Viterbi error (at SNR 30dB, signal attenuation 0-12dB in 1dB/step for 60-120 seconds)

In Figure 8.15, the signal attenuation is still changed at 1dB/step. The five points with callout symbols show the time when the diversity state is changed due to the signal attenuation and the Viterbi bit errors. At point 1, the signal attenuation is changed from 11 dB to 12 dB and thereafter the Viterbi error has a suddenly increase. As the orange line indicated, the diversity is activated at this point. Although the Viterbi error varies in the above of the diversity criteria during the period from point 1 to point 2 and therefore the diversity state is kept at high, the monitoring to the receiver's lock status shows that all the lock status are normal and there are no link failure and data packet loss. If the attenuation is given 1 dB decrease at point 2, the Viterbi error is quickly drop to near zero and the diversity is thereafter deactivated. This procedure is repeated at point 3 and 4 and we get the same result of diversity state change as in point 1 and point 2. While at point 5, the signal attenuation is reduced from 2 dB to 1 dB; there is a sharp glitch in the Viterbi error curve because the signal attenuator lost contact when it is turned from one position to another. The diversity is also activated by this false signal fading condition.

We also tested the diversity state reaction to the fast fading signal under following conditions and the result is shown in Figure 8.16.

- Signal to noise ratio: 20dB
- Range of signal attenuation: 0 ~ 12dB within 5 seconds and 12 ~ 0dB within 5 seconds
- Diversity criteria: Viterbi bit error > 100 bit/second
- Traffic: UDP packets generated by Netmeeting

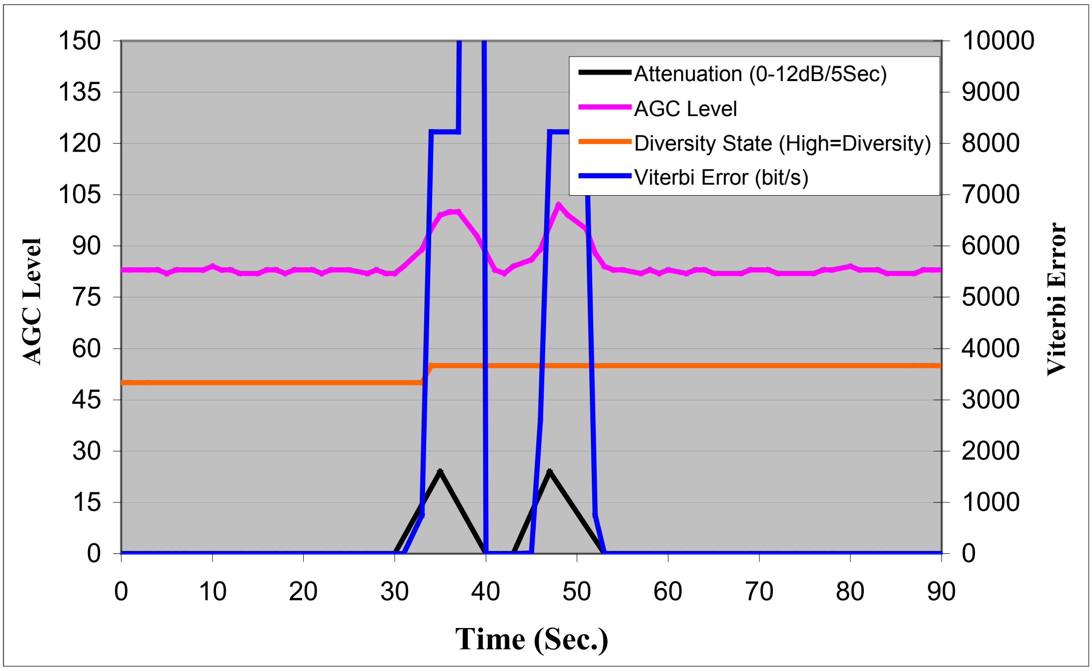


Figure 8.16 Diversity state reaction to fast signal fading (at SNR 20dB, signal attenuation at 12dB/5seconds)

The result in Figure 8.16 indicates that the fast signal fading can also activate the diversity, provided that the Viterbi error has been changed simultaneously and sufficiently. One experiential requirement of the diversity in EMBRACE is that the diversity should react to up to 10dBs signal fading within a time gap of 5 seconds. The result in this test ensures that the diversity can be activated when such a signal fading occurs.

As a comparison to the effect of diversity, the router was also set to work in a non-diversity state. During the signal attenuation and link failure period, the non-diversity Netmeeting lost pictures and just stacked there, thus proving that route diversity does provide higher service availability, as predicted.

8.3.2 Comparison of Frame Loss Rate

In this section, we designed two experiments to compare the benefits of diversity and shadow flow merging when the link is made to fail during transfer of different types of traffic.

In the first experiment, a comparison is made of the UDP frame loss rate when the diversity mechanism is activated, against when it is not. The results shown in Table 8.9 are obtained using the following parameters:

- Traffic: UDP at 256Kbps CBR, duration 120 seconds for each frame size
- Signal to noise ratio at the receiver: 20dB
- Diversity criteria: Viterbi bit error > 100 bit/second
- Signal attenuation: 0 ~ 6dB in 1dB/step for 2 seconds

Frame Size (Octets)	Total Frames	Diversity is deactivated		Diversity is activated	
		Number of Lost Frames	Loss Rate (%)	Number of Lost Frames	Loss Rate (%)
128	47964	12484	26.0	12686	26.000
256	18728	343	1.8	27	0.140
512	8440	167	2.0	5	0.059
768	5448	102	1.9	2	0.037
1024	4022	78	1.9	1	0.025
1280	3188	66	2.1	1	0.031
1470	2763	50	1.8	2	0.072

Table 8.9 Comparison of frame loss for diversity and no-diversity in link failure

The result in Table 8.9 is also shown in Figure 8.17. To make the chart display the frame loss improvement as clear as possible in the range of frame size, the point of frame size 128 is not shown in this diagram. Otherwise the big number of frame loss in frame size 128 will suppress the other points to undistinguishable.

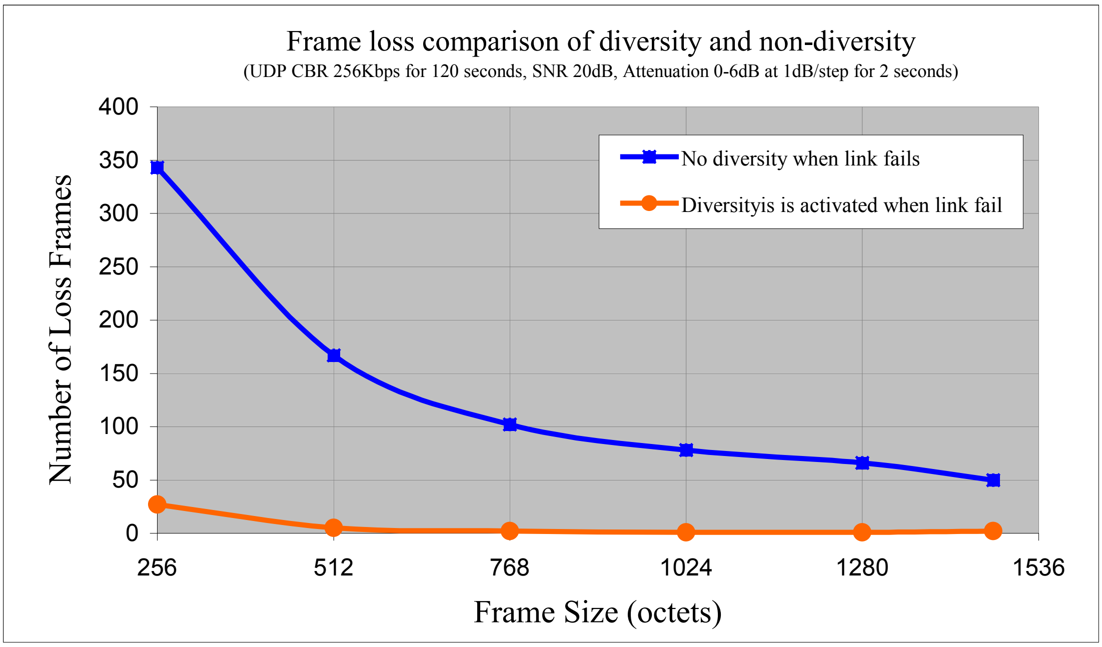


Figure 8.17 Comparison of frame loss for diversity and no-diversity in link failure

When the signal attenuation varies from 0 to 6dB, the Cobra receiver experiences link failure and the data path between user station and base station is broken. If the route diversity function is not activated, packets transmitted to the user are completely lost during the link failure; whilst in the case of router diversity being activated, data will be sent to the user in a shadow flow. Table 8.9 and Figure 8.17 clearly indicate that the number of lost packets, when diversity is activated, is significantly less than the number of lost packets when diversity is not activated. However Table 8.9 also indicates that the frame loss is not improved when the frame size is small (e.g. frame size 128 octets) after activating the diversity. It shows that for the small frame-sized packet, the diversity router is not performed as well as it is for the large frame-sized packet. This result is in consistent with the benchmarking of frame loss rate in Section 8.2.1.2 (see Figure 8.5, page 110) and comparison of random frame loss for the diversity router in Section 8.2.2.1 (see Figure 8.8 and Figure 8.9, page 116).

In the second experiment, TCP throughput is used to compare the benefit of diversity against the non-diversity. In the testbed of Figure 8.13, TCP traffic is transmitted from user 2 to user 1 for 30 seconds. First the TCP throughput of normal link, in which there is no signal fading and no packets loss, is measured; this is the best TCP throughput the system can achieve in any case. Then the TCP throughput is measured when the signal is faded during the transmission of TCP packets. The RF signal is faded in the same way as in the previous experiment. When the signal is so weak that the link fails between the user station and the base station, packet loss occurs. Unlike UDP transfer, TCP will back off and slowly start again to restore the lost packets if diversity is not activated. Consequently the TCP throughput of non-diversity is much lower than that of the normal link. If the diversity is activated, the lost packets are still delivered to user 1 via the shadow flow; therefore the TCP throughput of diversity does not suffer from the TCP back-off and slow-start mechanism, it is expected to match the TCP throughput of the normal link.

The results in Table 8.10 show the differences of TCP throughputs between diversity and non-diversity. All the results are averages of 20 repetitions. It shows that the TCP throughput of diversity is as good as in the normal working state and the TCP throughput of non-diversity is the worst.

	Normal link (No fading, no link failure, no packet loss)		Diversity (Fading, one link failure, packet loss)		No Diversity (Fading, one link failure, packet loss)	
TCP Throughput (Kbps)	Mean	Stdev	Mean	Stdev	Mean	Stdev
	555.7	2.3	556.2	1.1	261.6	20.5

Table 8.10 TCP throughput of diversity and non-diversity when link failure occurs

8.3.3 Verify Diversity Function by Other Services

With the implemented general wireless broadband access network testbed, the following applications were run to verify the functions of the route diversity and the shadow flow merging mechanism[12]:

- Ping
- Telnet
- WWW
- FTP
- Netmeeting
- VoIP

[12] For acceptable performance with these applications, we would expect to require a long term measurement with the RF connection in various signal fading and noise circumstances.

Except for Netmeeting and VoIP which are run between the two cells of our wireless network (see Figure 8-11), the peers of other applications are in the wider Internet environment. We found that during the phase of RF signal fading and normal link failure, as the consequence of inserting attenuation and *Gaussian* white noise, all applications ran smoothly and normally without noticeable service interruption.

8.4 Summary

This chapter presents the experiments undertaken on the testbed described in Chapter 7, using the protocols described in Chapter 4, 5, and 6.   The experiments are in three sets.

The first set of experiments revealed the disadvantages of standard Mobile IP when used in the proposed MPLS diversity router and a need to improve the performance of Mobile IP implementations in the MPLS network. The overheads and their impact upon the application of Mobile IP in shadow MPLS router are analysed. Traffic throughput is the main bottleneck when using Mobile IP in the MPLS diversity router. Experiments show that the simplest way of using Mobile IP in the MPLS diversity router, MIPoverMPLS, achieves less than 40% of the original traffic throughput. Alternatively by using the proposed integration of Mobile IP with MPLS, results indicate that the MPLS diversity router achieves the highest performance in terms of traffic throughput.

In the second set of experiments, the performance of MPLS diversity router and the use of shadow flow merging to reduce frame loss rate are tested. The throughput, frame loss rate, latency, and burst interval of the MPLS diversity router are measured against different frame sizes and network configurations, along with the description of benchmarking methods. For diversity measurement and shadow flow merging ability, the experiments concentrate on the improvement of the frame loss rate and the influence in end-to-end delay, by comparing different combinations of normal flow and shadow flow frame loss models. The results reveal the gain of frame loss rate that can be achieved by using the diversity and shadow flow merging mechanism.

The final set of experiments were conducted in the real RF environment and integrated with the DVB-S downlink system, MF-TDMA uplink system and ATM core network. Noise and signal fading are applied to the system to make it lose data packets and the results showed that the diversity plan and shadow flow merging mechanism perform acceptably well in reducing the frame loss rate and improving the service availability. Clearly the successful use of diversity and shadow flow merging to reduce data loss in these experiments proves that the protocols in this thesis are beneficial.

Chapter 9 Conclusions

Abstract

This thesis has presented a route diversity protocol and shadow flow merging mechanism for the support of nomadic access and route diversity with multiprotocol label switching on the broadband wireless access network. It is used to improve service availability and network reliability. In this final chapter a synopsis of the thesis is presented, followed by a discussion and conclusion of the results. The final section describes the future works and possible research and application of the route diversity protocol.

9.1 Thesis Summary

The work presented in this thesis is a solution to support nomadic access and improve service availability in a broadband wireless access network. It is the author's contribution to the EMBRACE project and mainly includes the following:

- A mechanism of integration Mobile IP with MPLS to support nomadic access with improved performance in broadband wireless access network. In this mechanism, the mobility agents are not responsible for tunnelling traffic to the mobile nodes anymore; instead they only keep on tracing the movements of the mobile nodes and let the label switching routers forward traffic to the mobile nodes by means of the notification message exchange.

- A diversity protocol and shadow flow merging mechanism to counteract the signal fading and improve the service availability during system outage, which, besides sending a packet on its normal path, also duplicates the packet and sends it on a separate, diverted labelled path when the normal path is under threat of failure. The shadow flow merging mechanism is responsible for merging the normal flow and shadow flow together and delivering the merged packet to its destination.

Although there are many requirements for a broadband wireless system, providing higher service availability and supporting services to users at anytime and anywhere are of most concern because of the following factors:

- The services in a wireless broadband system are more susceptible to impairment by buildings, vegetation and terrain, attenuation, and interference on the propagation channel. Accordingly the service availability and system performance can drop dramatically. In the worst case, the services are completely unavailable.

- After a user has moved to another service area, connection to the user's home network is changed and service is usually unavailable unless the system supports nomadic access.

These factors determine how well the users are served. IETF has defined Mobile IP (RFC 2002 - Perkins 1996a) to support host mobility in the wider Internet. In Chapter 2 the Mobile IP protocol was described, taken from RFC 2002, and the functions and protocol details summarised, along with a brief introduction to several earlier host mobility trials. It was the intention to acquaint the reader with supporting nomadic access in broadband wireless network in this research, before a detailed description to the method of improving throughput was given in later chapters.

The specification and application of MPLS have been and still are being defined and standardised. In Chapter 3 an explanation of MPLS packet forwarding was given, with a description of the MPLS label format and MPLS applications. MPLS has many advantages over conventional IP packet forwarding. Its typical applications include traffic engineering, quality of service routing, flow merging, and traffic tunnelling.

This research seeks to solve the problem of improving service availability and supporting nomadic access in a broadband wireless access network. Thus the protocol of route diversity, shadow flow merging mechanism, and integration of Mobile IP with MPLS are proposed in this research. It is at this point that Chapter 1-3 is important and may be regarded as setting the scene for this research.

This thesis proposed the integration of Mobile IP with MPLS to support nomadic access to broadband wireless access system. In this integration plan, the home agent and the foreign agent are still existed but only to help the mobile node's registration.

The basic principle of the integration is to assign an outgoing label at the home label switching router for the mobile node; the assigned label is the same value as the label from the home agent to the foreign agent. When the mobile node is registered with the mobility agents, a notification message is exchanged between the mobility agents and the edge routers; the edge routers use this notification to refresh the label switching entry of the mobile node. Packets destined for the mobile node are label-switched to the foreign network to which the mobile node is currently connected. Compared with the normal Mobile IP implementation, one of the advantages of the integration is that a higher throughput from the correspondent node to the mobile node can be achieved.

Improving the service availability in the broadband wireless access system is the main research element. This thesis proposed the protocol of route diversity and shadow flow merging mechanism to solve this problem. The *shadow flow* and *diverted path* are defined in Chapter 5. Route diversity involves four phases: the signal detection and diversity decision phase, the diversion phase, the normal path and diverted path coexistence phase and the restoration phase. The considerations of each phase during the diversity are explained.

Route diversity is based on label switching. When diversity happens, a diverted path is established. The normal path and diverted path are different label-switched paths. Packets requiring diversity are duplicated and sent on both the normal path and diverted path with different route diversity labels. The route diversity protocol requires that the label-switching table in a diversity-enabled router is modified to adapt the router state changing amongst the four phases.

Forwarding duplicated packets along the diverted path forms a shadow flow in the route diversity protocol. The egress router will receive two identical packets, one is from the original path and one is from the diverted path. The shadow flow merging mechanism, which is presented in Chapter 6, is, as its name implies, responsible for merging the shadow flow with the original flow to form a single flow. The values of label fields in normal flows are set differently to the label fields in shadow flows. It is in this chapter that the disciplines of how to assign values for different fields in the route diversity label are given. The shadow flow merging algorithm is based on the calculation of the sequence numbers in the original flow label and the shadow flow label. The merging algorithm is illustrated with three different merging examples which summarised the possible merging scenarios in our route diversity protocol.

Chapter 7 explained the testbed on which the integration of Mobile IP with MPLS, the route diversity protocol and the shadow flow merging algorithm are implemented and their functions verified. The experiments conducted, their results and analysis were delivered in Chapter 8. The test results of the implementation of Mobile IP integration with MPLS are reported first. The results are compared with the results of standard Mobile IP implementation and Mobile IP over MPLS implementation. With five different data transfer scenarios, the overheads and their impacts to the MPLS diversity router are analysed. Traffic throughput from a correspondent node to the mobile user is the main bottleneck in supporting of nomadic access in the testbed. The experiments show that MIPintMPLS achieves the highest throughput among the three compared implementations.

The performance of route diversity and shadow flow merging mechanism was evaluated with the measurement of throughput, latency, burst interval and frame loss rate. The improvement of service availability was finally verified in a broadband wireless access network with RF environment. This involved DVB-S downlink system and MF-TDMA uplink system. By applying *Gaussian* white noise and signal attenuation to the downlink, a service outage was simulated. To compare the benefits of diversity and shadow flow merging with a non-diversity network, the frame loss rate and traffic throughput were measured during the service outage time. Several frequently used applications in the Internet, for example, WWW, FTP, Telnet, and Netmeeting, were also tested in the testbed during the service outage time. Despite the normal path being completely unavailable during the service outage time, the experiments proved that all the services were still fully available by applying the route diversity and shadow flow merging protocol.

9.2 Conclusion

This thesis achieves three progressive goals. The first is the development of a route diversity protocol and shadow flow merging mechanism that could improve the service availability and supports nomadic access in wireless access environment and MPLS domain. The second is the development of a nomadic access mechanism that integrates Mobile IP with MPLS – MIPintMPLS, with a better throughput performance in the MPLS domain. The third, which builds on the previous two, is to apply the proposed protocol and mechanism in the general broadband wireless system and to prove that the developed protocol improves the service availability in the service outage time.

Service in wireless access systems can be impaired by buildings, vegetation, rain, snow and interference on the propagation channel, etc. This may cause data packet loss and even link failure when the impairment is severe. How to improve the service availability, therefore, is an important concern in the wireless access system. The first aim of this research is to improve the service availability.

The route diversity protocol uses an alternative link—a diverted path—to protect the wireless access system from the data packet loss and link failure. In this protocol, the wireless access network is seen as an MPLS domain and inside an IP domain, the normal path and diverted path are different label-switched paths, and the packet is forwarded to different label-switched path according to its diversity label. Packets arriving at the edge of this domain are first duplicated; the original packet is forwarded along the normal path and forms the normal flow, whilst the duplicated packet is forwarded along the diverted path and forms the shadow flow. The normal flow and shadow flow have different diversity labels. When these two flows arrive at the egress diversity router finally, they are merged into one flow. With the shadow flow being forwarded along the diverted path, the possibility of success delivering packets through the wireless access network is improved during the period when there is imminent risk of the wireless link failing, and also during the period when the link has actually failed.

The normal IP routing mechanism uses a destination IP address longest-match to determine the path along which the packet is going to be forwarded. This does not allow for a packet to be forwarded onto another path other than the longest-match path. If a packet is lost during transfer along the longest-match path, it is lost permanently. Without retransmission, there is no way to restore the packet. In wireless access networks, even retransmission could not restore the packet when the link fails. In the context of reducing packet loss and improving service availability during the service outage time, a route diversity protocol is more suitable for wireless access network than the normal IP routing mechanism.

The experiments of packet loss rate comparison in Section 8.2.2 further showed the benefits of using route diversity protocol. It revealed that the use of the protocol produced a gain in the packet loss rate when the random packet loss is presented in the testbed. If both the normal link and the diversity link lose packets randomly, then the loss rate of route diversity is much less than that of the non-diversity; the gain is within the range of 4.4 ~ 16 times. Using a route diversity protocol, the improvement of end-to-end delay variation is also observed.

As the protocol was applied in the general wireless access network that includes DVB-S downlink subsystem and MF-TDMA uplink subsystem, the advantages of route diversity in improving service availability were verified throughout. This is the third progressive goal achieved in this research. To determine whether diversity is needed to activate, the quality of the wireless link is monitored dynamically. The criteria to judge the link quality and activate diversity can be very different according to different requirements and conditions. One essential requirement for the diversity criteria is that it should be sensitive and effective to indicate the degradation of the link, especially during the time of the link failure.

There are several candidates: the DVB-S receiver's AGC level, lock status and Viterbi error for the diversity criterion. The AGC level indicates the receiving signal strength and its feature of smooth change with the signal fading makes it an unsuitable candidate of the diversity criteria. While the lock status is an indication of link failure, it does not help to judge whether the link quality is currently degrading. Experiments show that the Viterbi error is more sensitive to signal fading or link degradation and can also indicate the state of link failure effectively. Based both on these analysis and experiments, the Viterbi error is selected as the diversity criteria. The diversity algorithm maintains a four states' finite state machine to change the diversity states among the four diversity phases.

Experiments in the wireless access network revealed how the diversity states change with signal fading, AGC level and Viterbi error during the period of downlink failure by inserting signal attenuation and Gaussian white noise to the downlink signal. Running different applications, for example, the frequently used FTP and WWW, during the period of downlink failure can give a direct comparison of effects of diversity and non-diversity. The capability of reducing data packet loss and improving service availability by diversity protocol in the general wireless access network is further verified by measuring UDP frame loss rate when the diversity protocol is used during the period of downlink failure. A significant reduction of frame loss, when the diversity protocol is applied in the wireless network, is observed.

To support nomadic access to the broadband wireless network, the IETF Mobile IP was imported and implemented in the testbed. With improving the overall performance of the system in mind and having a united routing mechanism, another progressive goal—the integration of Mobile IP with MPLS, was implemented and tested in this research. The integration scheme did not change the architecture of the mobile IP network, but did change the functions of the mobile IP entities. The home agent and the foreign agent still exist, but only function with the registration of mobile node movement with the mobility agent. There is no need for the home agent capturing, encapsulating with IPinIP and forwarding the packets destined for the mobile node.

Compared with other implementations of mobile IP in the testbed, for example, the standard Mobile IP and Mobile IP over MPLS, one major benefit of the integration of Mobile IP with MPLS is that when the mobile node is in the foreign network, the traffic throughput from a correspondent node to the mobile node is improved significantly. In the standard MIP and MIPoverMPLS implementation, experiments show this throughput was less than 40% of the throughput when the mobile node is in the home network; whilst in the MIPintMPLS scheme, the throughput achieves 82.5%. A consistently better throughput performance in MIPintMPLS is also observed for all of the investigated traffic transfer scenarios.

As a whole, the work described in these chapters has dealt with the problems of supporting nomadic access and improving the service availability in broadband wireless access network and achieved the objectives. It involves a considerable scope of development and application. Although much work, for example, very long term testing to prove its effectiveness in rain or snow signal fading, remains to be done, the preliminary application of the research into a general wireless access network is very successful and encouraging.

It is worth noticing that all the measurement results, performance, and the derived conclusions are limited to the network testbeds which are set up for this research, and therefore may be not interpreted as universally suitable.

9.3 Future Directions

The work presented in this thesis is the first step in implementing diversity with MPLS to support nomadic access to and improve service availability of a broadband wireless access network. Although the results show significant improvements over non-diversity implementation in the performance of nomadic access throughput and service availability, several features of the route diversity and shadow flow need further investigation.

One such case is the investigation of very long term improvement of service availability with diversity in wireless access network. Without a long-term observation and study, it is impossible to depict the characteristics of diversity in the wireless environment where signal fading and interference on the transmission channel caused by terrain, buildings, vegetation, rain, snow, etc., are presented. Although we prove the effectiveness and usefulness of the protocol by inserting signal attenuation and noise to the channel, there is no result from the rain and snow fading directly. Despite the installation of the broadband wireless system in the mountain area of Norway being scheduled, as shown in Figure 8-2 and Figure 9-11, it did not happen until this thesis was written. The long-term investigation involves much work and needs the cooperation of all partners of the consortium. Only after this investigation, can the diversity protocol be further modified in terms of improving service availability of broadband wireless access network.

Another feature of the diversity protocol is that several parameters can be used as the diversity criterion. In this research the Viterbi error is chosen as the criterion because of its steep changing between the link state transition of failure and normal. Other parameters such as the receiving signal strength and the receiver's lock status can also be chosen. The argument is which one is better or more reasonable. Using signal strength seems reasonable, but our observation shows that some times the link has already failed despite a strong signal indication. If using lock status as the criterion, the argument is that when any lock status is lost, the data link has also failed; so that the diversity could not protect the system during the period when the link is going to fail. The Viterbi error is lower in normal working state and has a steep rise near the critical point at which the link is going to fail. This requires the diversity to react to the Viterbi error changing quickly. It seems unrealistic to have a united diversity criterion standard. Clearly a model of selecting diversity criterion in different situations is needed and this requires further studying.

In the architecture of diversity protocol presented in this thesis, the diversity wireless access network is seen as an MPLS domain inside an IP domain, the diversity label is a one-layer flat structure. If the diversity wireless access network is sat inside another bigger MPLS domain, a scalable multiple-layer diversity label stack structure is needed to pass the external MPLS labelled packet through the diversity domain. This has not been implemented and certainly needs to be done properly for the application of the diversity protocol in the wider Internet.

The diversity protocol could be potentially used in many other areas such as traffic engineering and security. Recent research by Huang *et al* (2002) proposed using a path protection mechanism to build a reliable MPLS network. In the 1+1 path protection mechanism of that research, the recovery path is fully reserved and carries the same traffic as the working path. This protection mechanism is very similar to the shadow flow mechanism in this thesis. In the context of traffic engineering, the diversity protocol can be used to share traffic load among different paths. For example, when the traffic requires more path resources than the path can provide, a certain amount of traffic can be diverted to an alternative path and delivered to the destination by diversity protocol. The diversity protocol and shadow flow merging mechanism can also be used in the secure transfer of traffic, for instance the data can be partly delivered via one path and partly via another different path. Interception or eavesdropping the traffic from either of the two paths does not help the attacker or eavesdropper to get the whole image of traffic. All of these could be applications of the diversity protocol worthy of further exploration.

Reference

Adams, C. (2000), Koudelka, O. *Constraints for the IBC 2001 LMDS Demonstration.* Unpublished EMBRACE Working Document. Oxford: Rutherford Appleton Laboratory. June.

Adams, C. (ed). (2001a). *Prototype IP implementation for MPEG-2 transport stream down link delivery and MF-TDMA up link*. Unpublished EMBRACE Deliverable Document D5. Oxford: Rutherford Appleton Laboratory. May.

Adams, C. (2001b), Shi, X. *Route diversity in an interconnected LMDS network.* Proceedings of IST Mobile Communications Summit 2001. Barcelona. September. Pages 561-566. ISBN: 84-931132-3-9.

Adamson, B. (1999). *The MGEN Toolset*. URL: http://manimac.itd.nrl.navy.mil/MGEN/. August.

Almesberge, W. (1999). *Linux Network Traffic Control - Implementation Overview.* URL: ftp://icaftp.epfl.ch/pub/people/almesber/tcio-current.ps. April

Awduche, D.O. (1999). *MPLS and Traffic Engineering in IP Networks.* IEEE Communications Magazine, Vol 37 No 12. December. Pages 42-47. ISSN: 0163-6804

Awduche, D.O. (2001a), Berger, L., Gan, D.H., Li, T., Srinivasan, V., Swallow, G., *RSVP-TE: Extensions to RSVP for LSP Tunnels*. Internet Draft, draft-ietf-mpls-rsvp-lsp-tunnel-09.txt. August.

Awduche, D.O. (2001b), Chiu, A., Elwalid, A., Widjaja, I., Xiao, X. *Overview and Principles of Internet Traffic Engineering*. Internet Draft, draft-ietf-tewg-principles-01.txt. October.

Bhagwat, P. (1996), Perkins, C. and Tripathi S. Network Layer Mobility: *An Architecture and Survey.* IEEE Personal Communications, Vol 3 No 3. June. Pages 54-64. ISSN:

Blake, S. (1998), Black, D., Carlson, M., Davis, E., Wang, Z., Weiss, W. *An Architecture for Differentiated Services*. RFC 2475. December.

Braden, R. (1989). *Requirements for Internet Hosts – Communication Layers*. RFC 1122. October

Bradner, S. (1991). *Benchmarking Terminology for Network Interconnection Devices*. RFC 1242. July.

Bradner, S. (1999) and McQuaid J. *Benchmarking Methodology for Network Interconnect Devices*. RFC 2544. March.

Chen, T.M. (1999) and H.Oh, T. *Reliable Services in MPLS*, IEEE Communication Magazine, Vol 37 No 12. December. Pages 58-62. ISSN: 0163-6804.

Chua, K.C. (1999), Li, Y.Z., Foo, C.C. *On a Linux implementation of mobile IP and its effects on TCP performance*, Computer Communications, Vol 22 Issue 6. April. Pages 568-588. ISSN: 00140-3664.

Cisco System. (2000). *Introduction to MPLS.* White Paper. P/N 78-10672-01. April.

Combs, C. (2002). *Ethereal-Sniff the glue that holds the Internet together*. URL: http://www.ethereal.com/. January.

Craig, K.H. (ed). (1999). *Propagation planning procedures for LMDS*. CRABS (ACTS 215) Deliverable Report D3P1B. Available at: http://www.telenor.no/fou/prosjekter/crabs/d3p1b.pdf

Craig, K.H. (2000) and Tjelta, T. *Cellular radio access for broadband services: propagation results at 42 GHz*. Telektronikk, Special Issue on Broadband Radio Access. Vol 96 No 1. Pages 36-44. ISSN: 0085-7130.

Deering, S. (ed). (1991). *ICMP Route Discovery Messages*. RFC 1256. September.

Deering, S. (1998), Hinden, R. *Internet Protocol, Version 6 (IPv6) – Specification*. RFC 2460. December.

Dixit A. (1996) and Gupta, V. *Mobile-IP for Linux (ver 1.00).* May. URL: http://anchor.cs.binghamton.edu/~mobileip/MIP100/DOC/mip-doc.v100.ps.

Embrace Consortium (1999). *Description of work*. Unpublished proposal for EU IST project Efficient Millimetre Broadband Radio Access For Convergence and Evolution. September 1999.

Fore Systems, Inc. (1997a). *ATM Management Interface (AMI) Manual*. MANU0021-01. March.

Fore Systems, Inc. (1997b). *ForeRunner ATM Switch Configuration Manual.* MANU48-01. March.

Hanks, S. (1994), Li, T., Farinacci, D. and Traina, P. *Generic Routing Encapsulation (GRE)*. RFC 1701. October.

Huang, C. (2002), Sharma, V., Owens, K., Makam, S. *Building reliable MPLS networks using a path protection mechanism*. IEEE Communication Magazine. Vol 40 No 3. March. Pages 156-162. ISSN: 0163-6804.

Huitema, C. (1996). *IPv6: The New Internet Protocol*. Upper Saddle River, New Jersey: Prentice-Hall, Inc. ISBN: 0-13-241936-X.

Ioannidis, J. (1993) and Maguire, G.Q. *The Design and Implementation of a Mobile Internetworking Architecture*. Proceeding of Winter USENIX. San Diego, CA. January 25-29. Pages 491-502.

Jacobson, V. (1990). *Compression TCP/IP Header for Low-Speed Serial Links*. RFC 1144. February.

Jamoussi, B. (ed). (2001). *Constraint-Based LSP Setup using LDP*, Internet Draft, draft-ietf-mpls-cr-ldp-05.txt. February.

Johnson, D.B. (2000) and Perkins, C. *Mobility Support in IPv6*. Internet Draft, draft-ietf-mobileip-ipv6-14.txt. July.

Joanneum Research. (2001), TUCR, Ericsson and University of Salzburg. *Prototype equipment for the base station and user terminal*. Unpublished EMBRACE Document D6. June.

Kleinrock, L. (2000). *On some Principles of Nomadic Computing and Multi-Access Communications.* IEEE Communications Magazine, Vol 38 No 7. July. Pages 46-50. ISSN: 0163-6804.

Kyas, O. (1996). *ATM Networks.* (2nd ed). London: International Thomson Computer Press. ISBN: 1-85032-303-8.

Lawrence J. (2001). *Designing Multiprotocol Label Switching Networks.* IEEE Communication Magazine, Vol 39 No 7. July. Pages 134-142. ISSN: 0163-6804.

Li, T. (1999). *MPLS and the Evolving Internet Architecture*. IEEE Communication Magazine. Vol 37 No 12. December. Pages 38-41. ISSN: 0163-6804.

Loktu, H. (ed). (1999). *Specification of next-generation LMDS architecture*. CRABS (ACTS 215) Deliverable Report D2P1B. Available at: http://www.telenor.no/fou/prosjekter/crabs/d2p1b.pdf

Mills, D.L. (2002). *The Network Time Protocol (NTP) Distribution*. URL: http://www.eecis.udel.edu/~ntp/ntp_spool/html/index.htm

Myles, A. (1995), Johnson, DB. and Perkins, C. *A Mobile Host Protocol Supporting Route Optimization and Authentication*. IEEE Journal on Selected Areas in Communications. Vol 13 No 5 June. Pages 839-849.

Norbury, J. (2000). *Toward the next generation LMDS systems architecture*. Telektronikk Special Issue on Broadband Radio Access. Vol 96 No 1. Pages 17-27. ISSN: 0085-7130.

Nordbotten, A. (2000). *LMDS Systems and their Application.* IEEE Communications Magazine, Vol 38 No 6. June. Pages 150-154. ISSN: 0163-6804.

Perkins, C. (1993). *Providing Continuous Network Access to Mobile Hosts Using TCP/IP*. Computer Networks and ISDN Systems. Vol 26. Pages 357-369.

Perkins, C. (ed). (1996a). *IP Mobility Support*. RFC 2002. October.

Perkins, C. (1996b). *IP Encapsulation within IP*. RFC 2003. October.

Perkins, C. (1996c). *Minimal Encapsulation within IP*. RFC 2004. October

Perkins, C. (1997). *Mobile IP: Design Principles and Practices*. Massachusetts: Addison-Wesley Publishing Company. ISBN: 0-201-63469-4.

Perkins, C. (ed). (2002). *IP Mobility Support for IPv4, revised*. RFC 3220. January.

Ren, Z. (2000), Tham, CK., Foo, CC., Ko, CC. *Integration of Mobile IP and MPLS*. Internet Draft: draft-zhong-mobile-ip-mpls-01.txt. July.

RFC 791. (1981). University of Southern California. *Internet Protocol*. RFC 791. September.

Riverst, R.L. (1992). *The MD5 Message-Digest Algorithm*. RFC 1321. April.

Rosen, E. (2001a), Viswanathan, A. and Callon, R. *Multiprotocol Label Switching Architecture*. RFC 3031. January.

Rosen, E. (2001b), Tappan, D., Fedorkow, G., Rekhter Y., Farinacci, D., Li, T., Conta,A. *MPLS Label Stack Encoding*. RFC 3032. January.

Rubini, A. (1998). *Linux Device Drivers.* Sebastopol, CA: O'Reilly & Associates. February. ISBN: 1-56592-292-1.

Schmidt, M. (2002), Koudelka, O., Ebert, J., Schlemmer, H., Adams, C., Shi, X., Linder, H. and Stering, W. *The EMBRACE System Demonstrator.* Proceedings of IST Mobile & Wireless Telecommunications Summit 2002. Greece. June. Pages: ISBN:

Semeria, C. (1999). *Multiprotocol Label Switching – Enhancing Routing in the New Public Network*. White Paper P/N: 200001-002, Juniper Networks Inc. September.

Shi, X. (2000), Adams, C. and Smith, A. *Diversity and Nomadic Access to a Broadband Wireless IP Network.* Proceedings of Multi-Service Network 2000 Conference. Abingdon. July. URL:http://www.acu.rl.ac.uk/msn2000/Cos2000proceedings.html

Shi, X. (2001) and Adams, C. *An MPLS Approach to the Route Diversity and QoS in EMBRACE.* Unpublished Embrace TechReport. March.

Stevens, W.R. (1998). *Unix Networking Programming, Volume 1*. (2nd ed). Upper Saddle River, NJ: Prentice Hall PTR. ISBN 0-13-490012-X.

Solomon, J.D. (1998). *Mobile IP – The Internet Unplugged*. New Jersey: Prentice Hall PTR. ISBN: 0-13-856246-6.

Tanenbaum, A.S. (1996). *Computer Networks*. (3rd ed). Upper Saddle River, New Jersey: Prentice-Hall, Inc. ISBN: 0-13-394248-1.

Taylor, M. (1996), Waung, W. and Banan, M. *Internetwork Mobility – The CDPD Approach*. Upper Saddle River, New Jersey: Prentice-Hall, Inc. ISBN: 0-13-209693-5.

Teraoka, F. (1993) and Tokoro, M. *Host Migration Transparency in IP Networks: The VIP Approach*. Computer. Communication Review, ACM. January. Pages 45-65.

Teraoka, F. (1994), Uehara, K., Sunahara, H. and Murai, J. *VIP: A Protocol Providing Host Mobility*. Communications of The ACM. Vol 37 No 8. August. Pages 67-75. ISSN:

Tjelta, T. (2000), Nordbotten, A., and Loktu, H. *Broadband radio access for multimedia services*. Telektronikk, Special Issue on Broadband Radio Access. Vol 96 No 1. Pages 2-10. ISSN: 0085-7130.

Trillium Co. (2001). *Multiprotocol Label Switching (MPLS).* Published in The International Engineering Consortium. URL:http://www.iec.org

Varshney, U. (2000) and Vetter Ŕ. *Emerging Mobile and Wireless Networks.* Communications of the ACM, Vol 43 No 6. June. Pages 73-81. ISSN: 0001-0782.

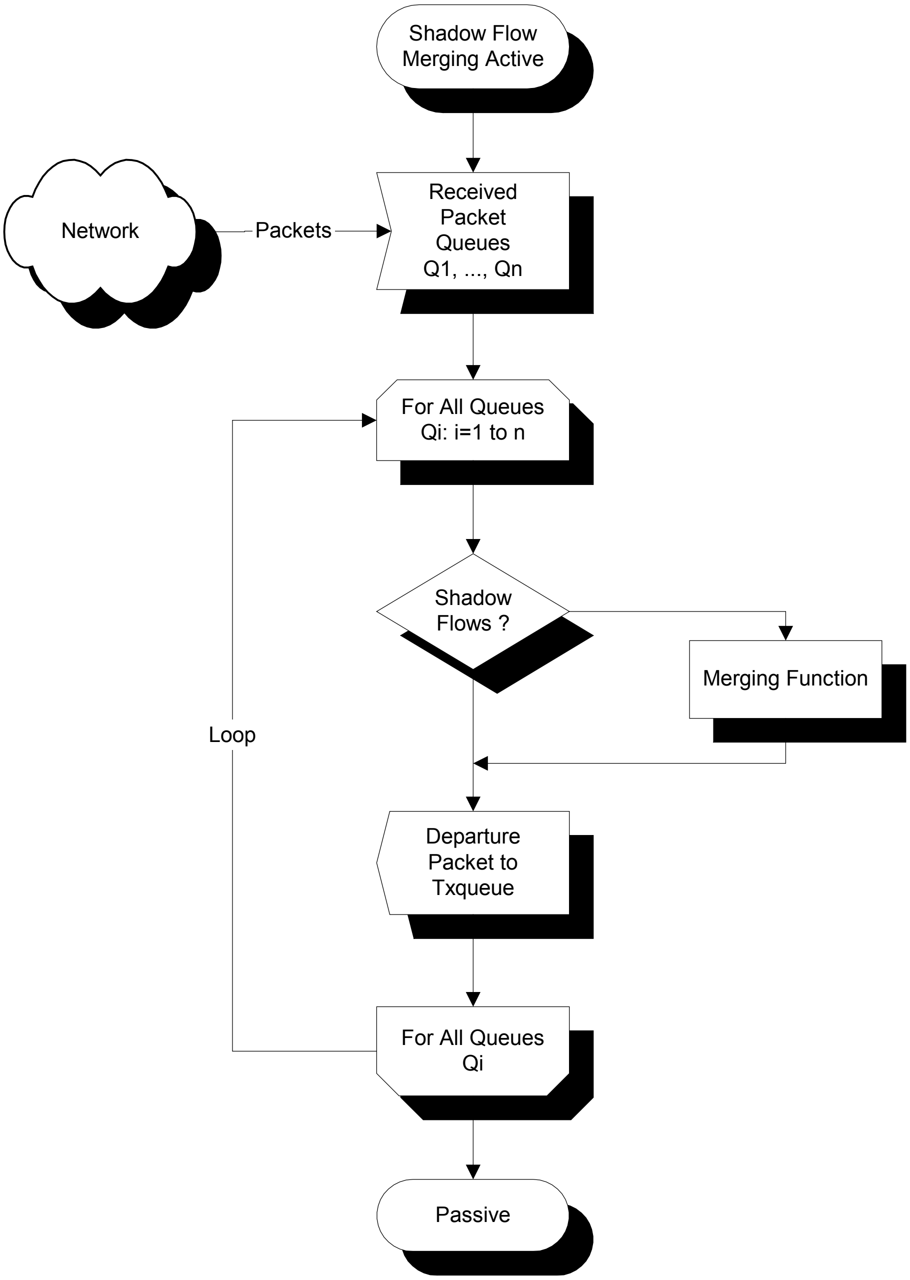
Williams, B. (2000). *Quality of Service, Differentiated Services and Multiprotocol Label Switching.* Ericsson Inc. White Paper. EN/LZT 108 3225 R2. URL: http://www.ericsson.com/iptelephone

Xiao, X. (2000), Hannan, A., Bailey, B. and Ni LM. *Traffic Engineering with MPLS in the Internet*, IEEE Network, Vol 14 No 2. March/April. Pages 28-33. ISSN: 0890-8044.

Appendix A

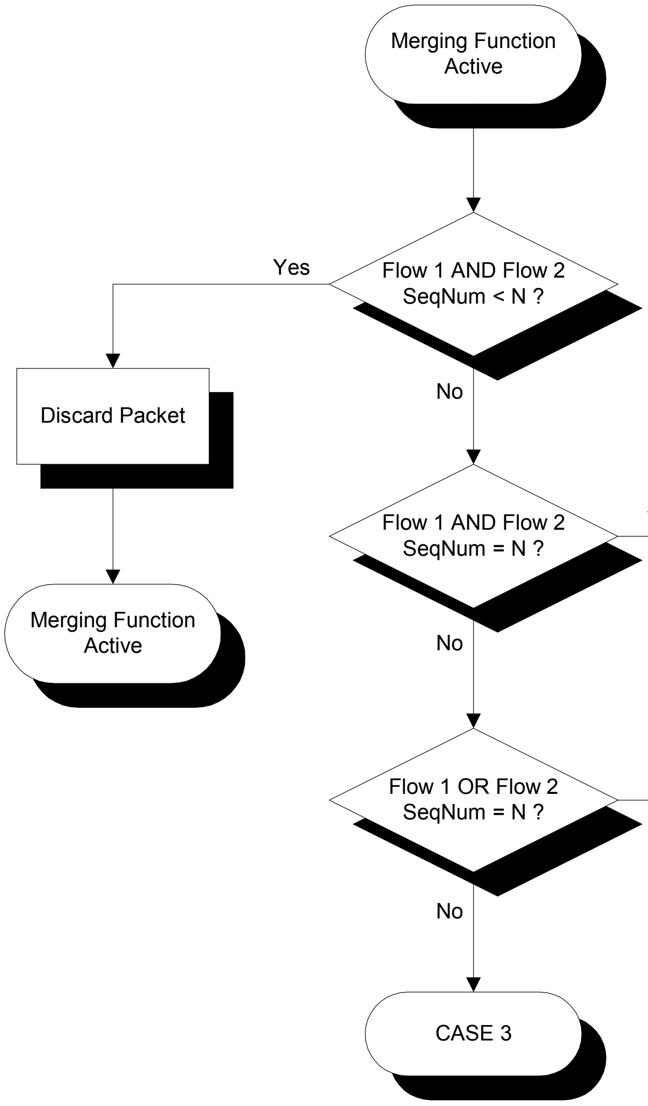
SDL Diagrams for the Shadow Flow Merging Algorithm

Level 1 – High Level Design



Shadow Flow Merging Active
Network
Packets
Received Packet Queues Q1, ..., Qn
For All Queues Qi: i=1 to n
Shadow Flows ?
Merging Function
Loop
Departure Packet to Txqueue
For All Queues Qi
Passive

Level 2 - Merging Function

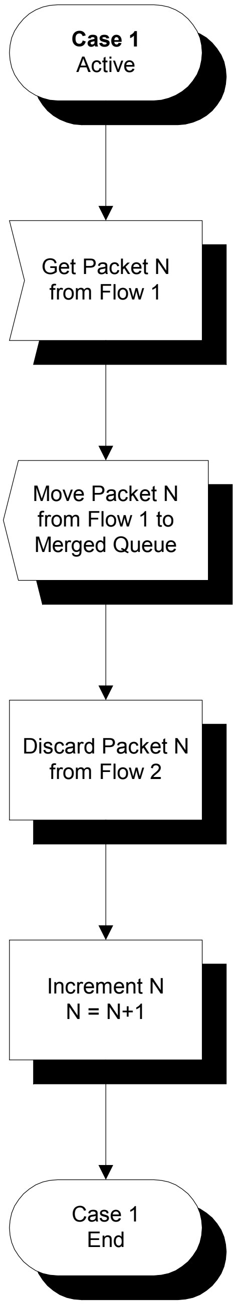


Case 1: Processing when packet N is available for both flow

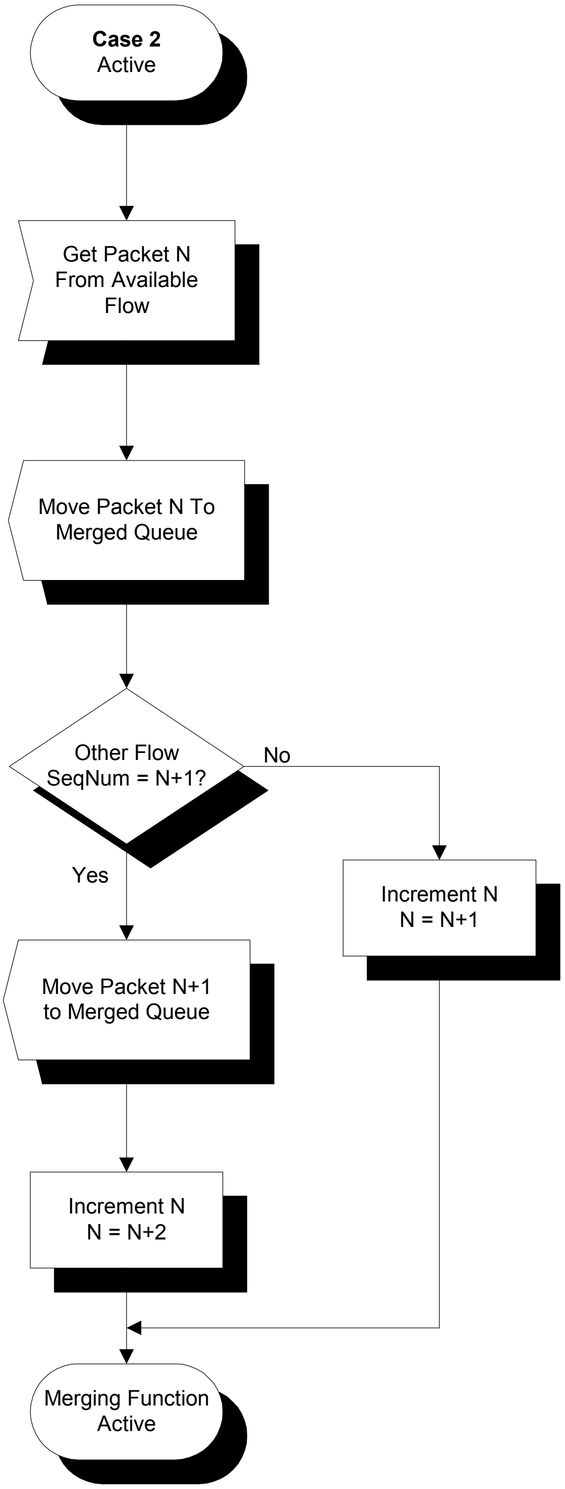
Case 2: Processing when packet N is only available in one flow

Case 3: Processing when packet N is not available in either flow

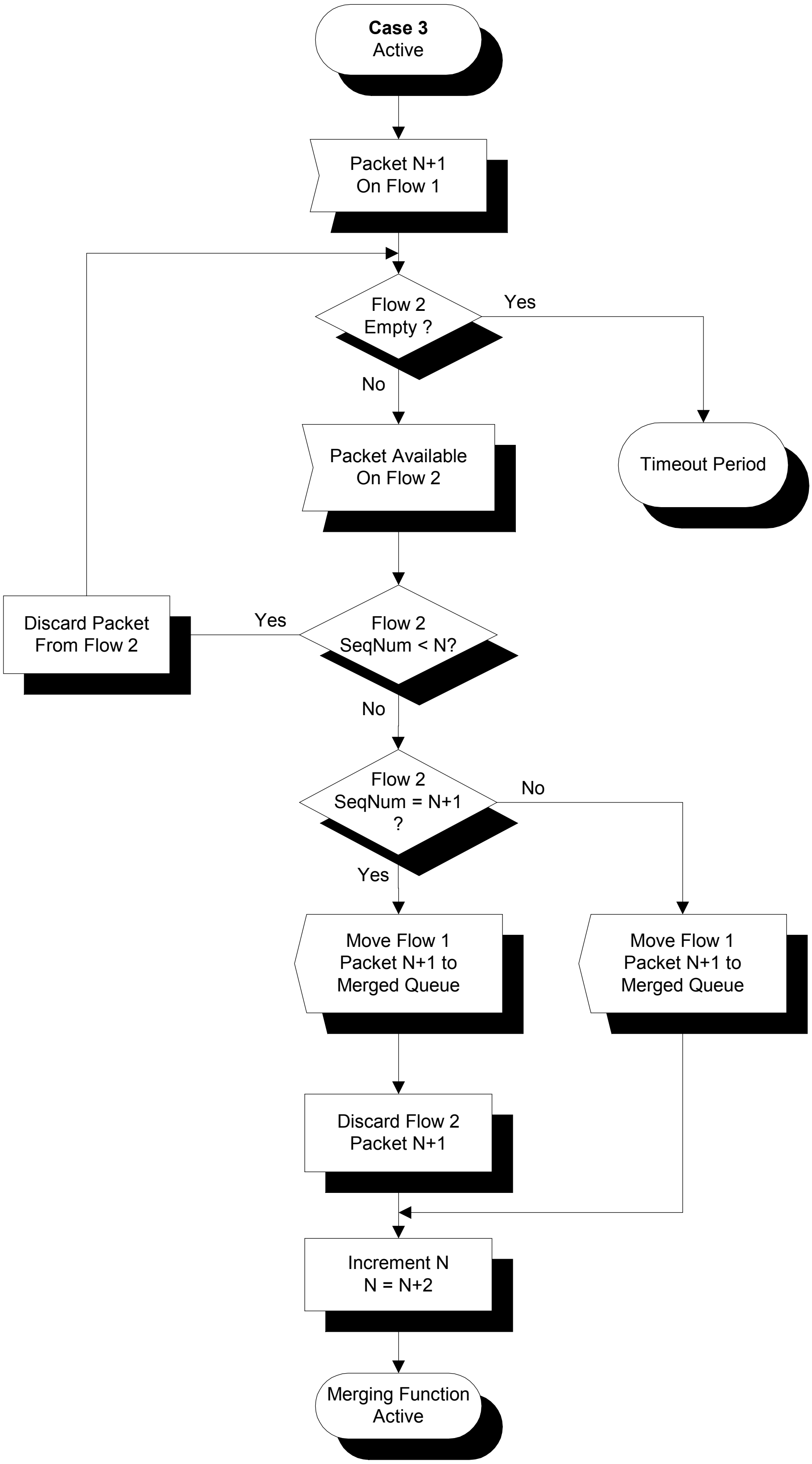
Level 2.1 – Case 1


Case 1
Active
Get Packet N from Flow 1
Move Packet N from Flow 1 to Merged Queue
Discard Packet N from Flow 2
Increment N
N = N+1
Case 1
End

Level 2.2 – Case 2

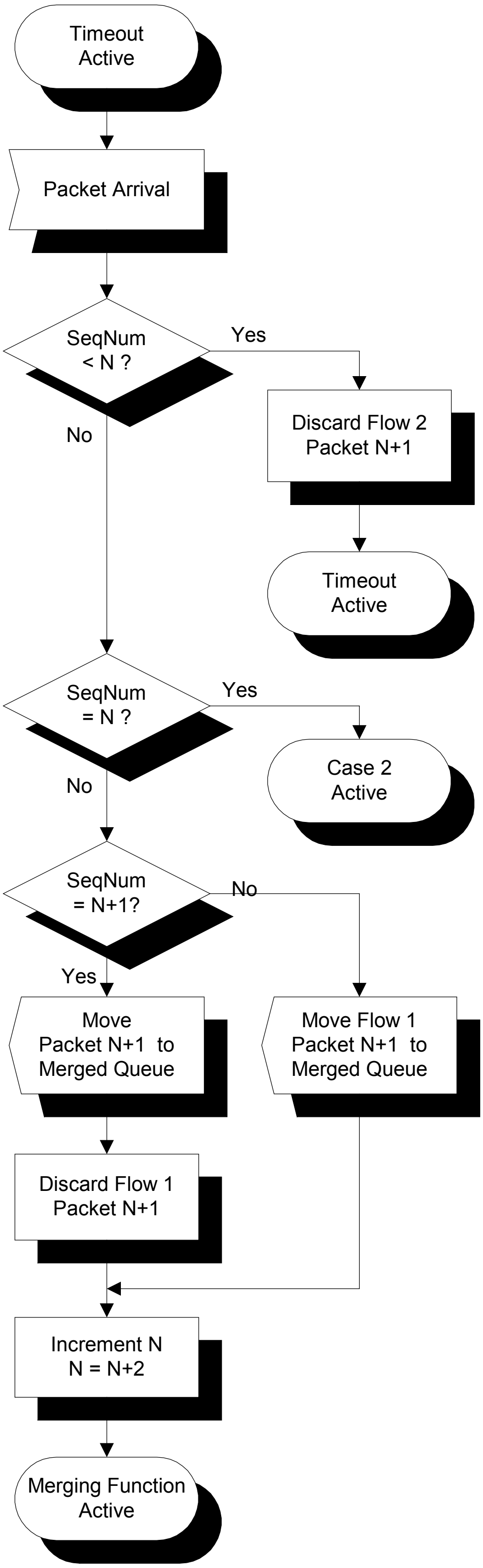


Level 2.3 – Case 3

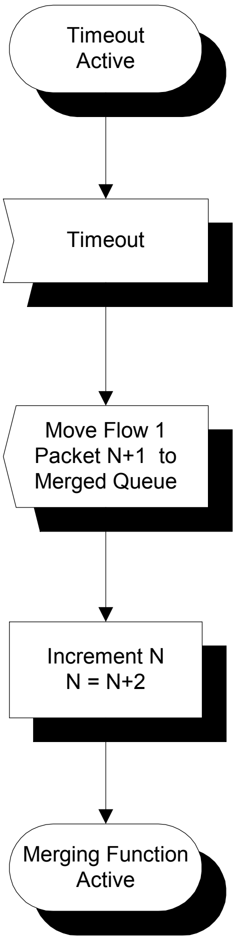


Level 2.3 (a) (b) – Timeout Period

2.3 (a) Packet Arrival during Timeout



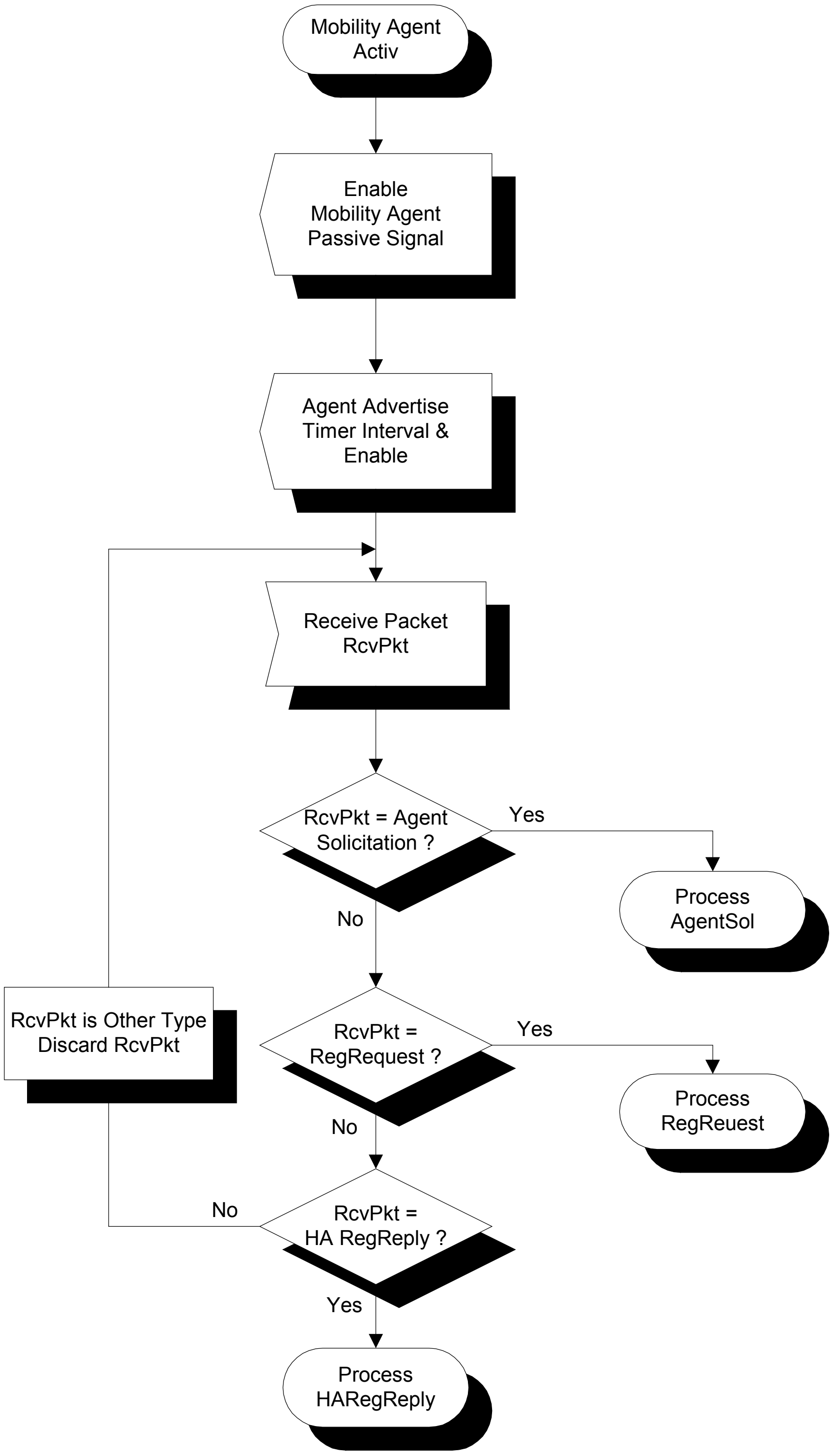
2.3 (b) No Packet Arrival during Timeout



Appendix B

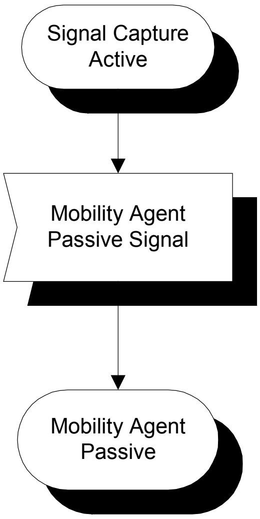
SDL Diagrams for Mobility Agent with MPLS

Level 1 – High Level Design

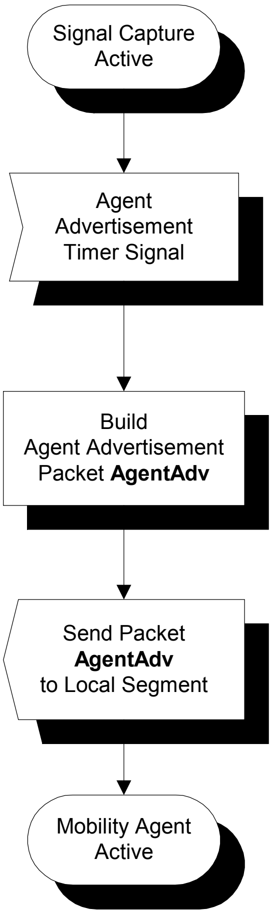


Level 2.1 Signal Processing

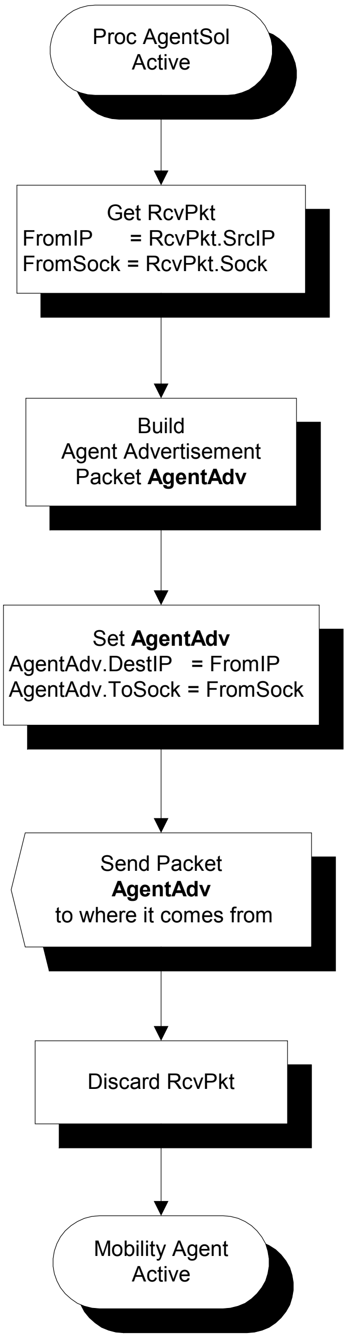
2.1 (a) Exiting Signal



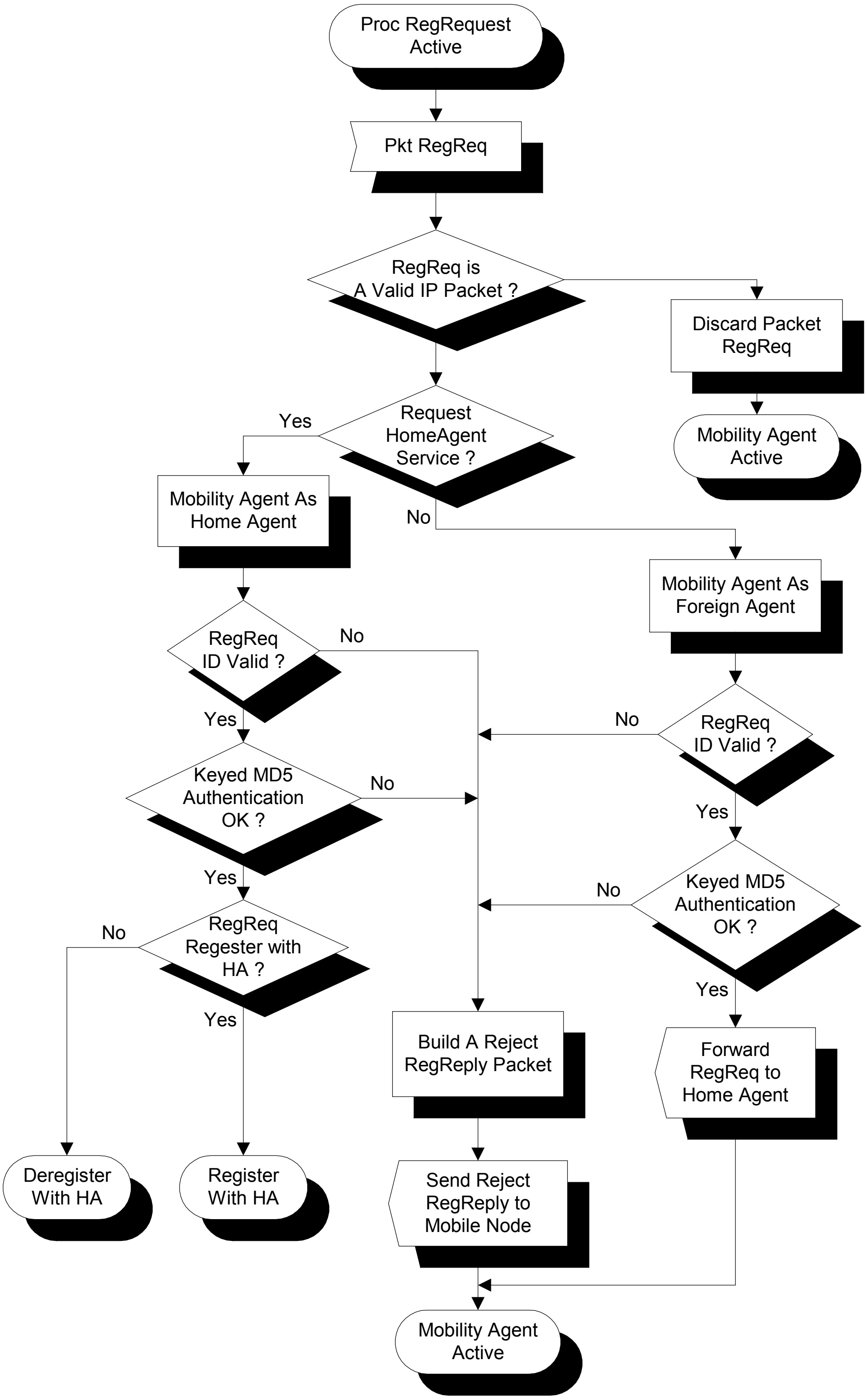
2.1 (b) Agent Advertisement Timer Signal


Signal Capture Active
Agent Advertisement Timer Signal
Build Agent Advertisement Packet **AgentAdv**
Send Packet **AgentAdv** to Local Segment
Mobility Agent Active

Level 2.2 Processing Agent Solicitation

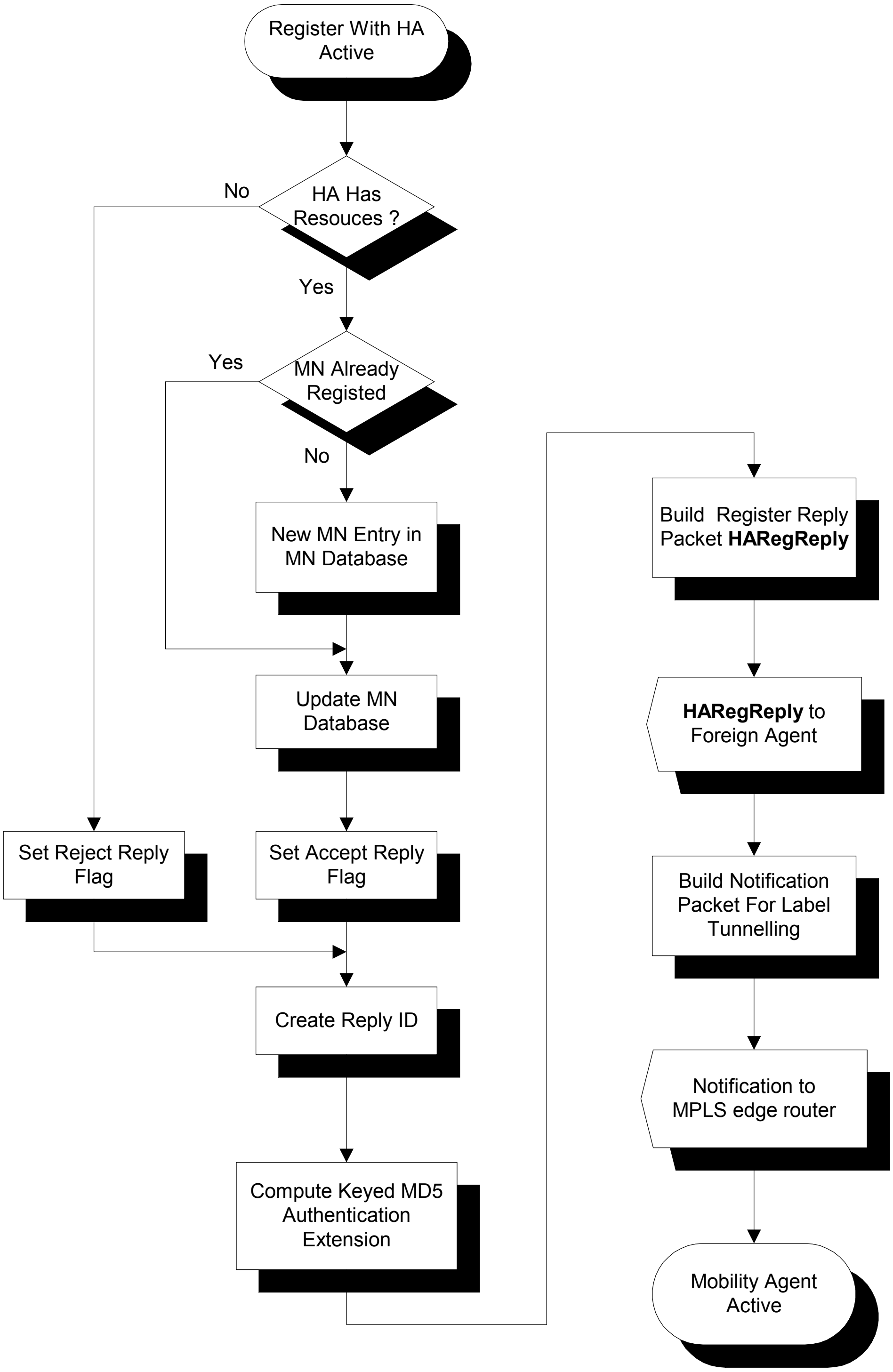


Level 2.3 Processing Register Request

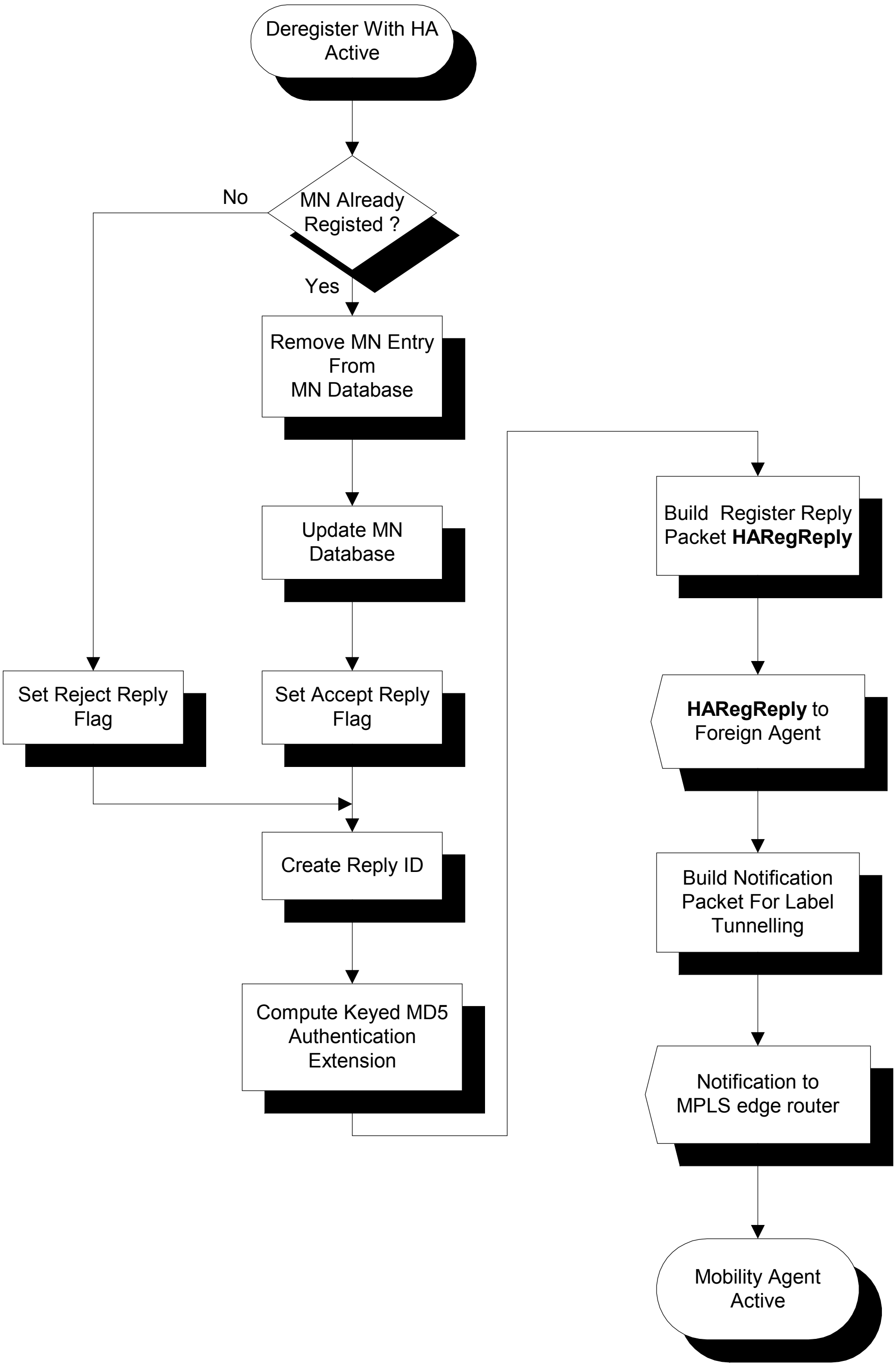


Proc RegRequest Active
Pkt RegReq
RegReq is A Valid IP Packet ?
Discard Packet RegReq
Mobility Agent Active
Yes
Request HomeAgent Service ?
No
Mobility Agent As Home Agent
Mobility Agent As Foreign Agent
RegReq ID Valid ?
No
Yes
Keyed MD5 Authentication OK ?
No
Yes
RegReq ID Valid ?
No
Yes
Keyed MD5 Authentication OK ?
No
Yes
RegReq Regester with HA ?
No
Yes
Build A Reject RegReply Packet
Forward RegReq to Home Agent
Deregister With HA
Register With HA
Send Reject RegReply to Mobile Node
Mobility Agent Active

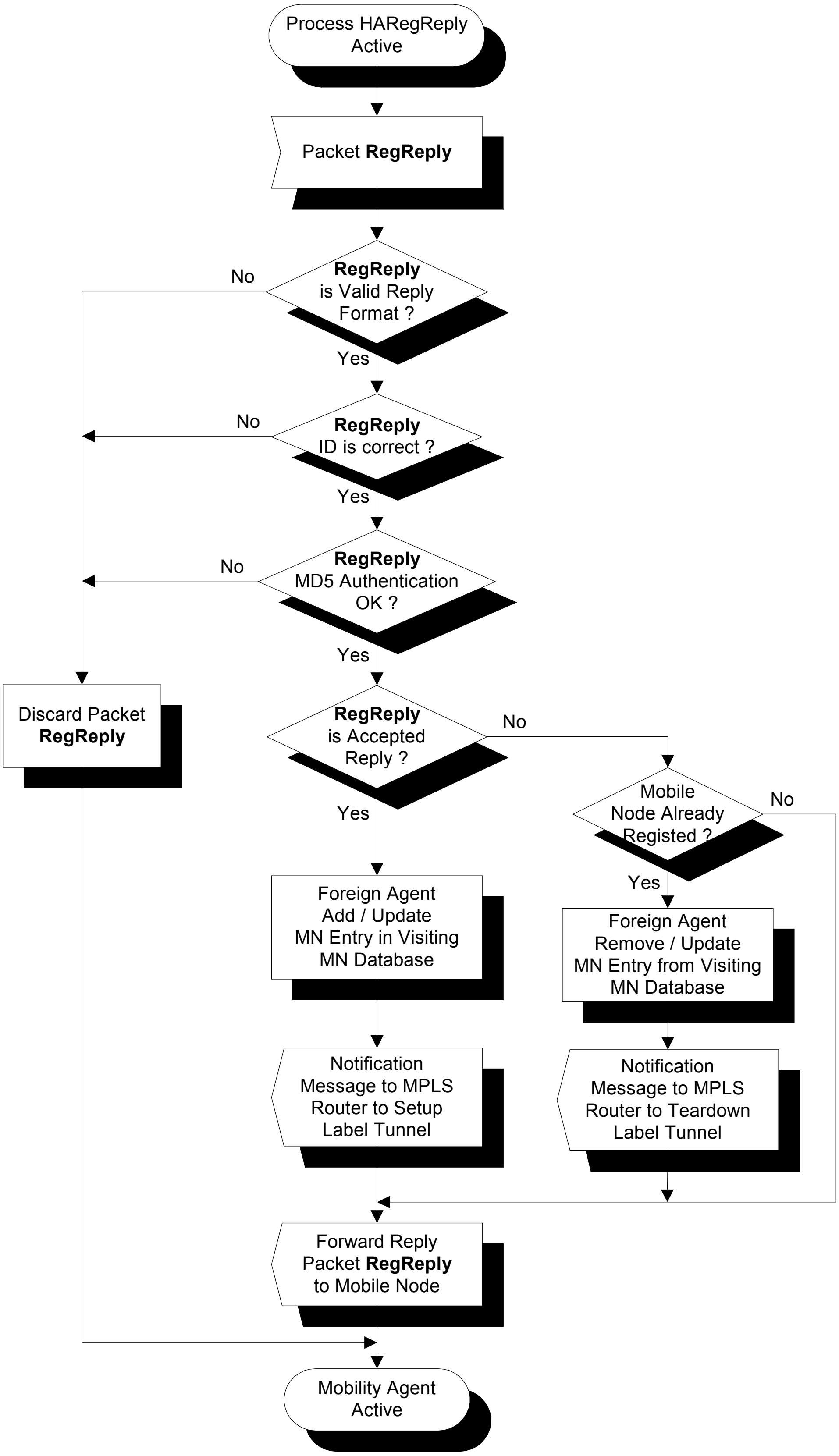
Level 2.3.1 Register With HA


Register With HA Active
No
HA Has Resouces ?
Yes
Yes
MN Already Registed
No
New MN Entry in MN Database
Update MN Database
Set Reject Reply Flag
Set Accept Reply Flag
Create Reply ID
Compute Keyed MD5 Authentication Extension
Build Register Reply Packet HARegReply
HARegReply to Foreign Agent
Build Notification Packet For Label Tunnelling
Notification to MPLS edge router
Mobility Agent Active

Level 2.3.2 Deregister With HA


Deregister With HA Active
MN Already Registed ?
No
Yes
Remove MN Entry From MN Database
Update MN Database
Set Reject Reply Flag
Set Accept Reply Flag
Create Reply ID
Compute Keyed MD5 Authentication Extension
Build Register Reply Packet HARegReply
HARegReply to Foreign Agent
Build Notification Packet For Label Tunnelling
Notification to MPLS edge router
Mobility Agent Active

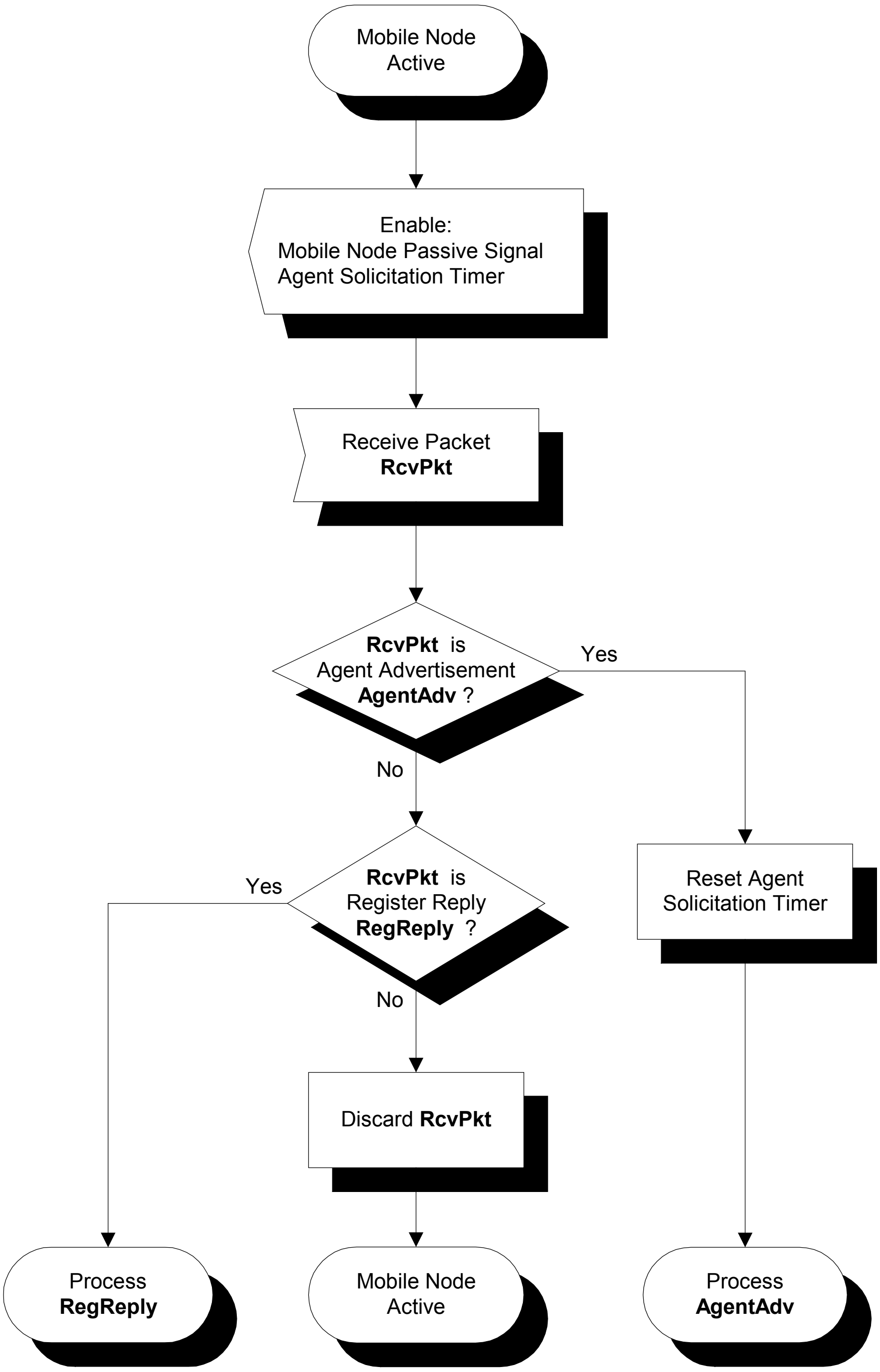
Level 2.4 Process Receiving Register Reply


Process HARegReply Active
Packet RegReply
RegReply is Valid Reply Format ?
No
Yes
RegReply ID is correct ?
No
Yes
RegReply MD5 Authentication OK ?
No
Yes
Discard Packet RegReply
RegReply is Accepted Reply ?
No
Yes
Mobile Node Already Registed ?
No
Yes
Foreign Agent Add / Update MN Entry in Visiting MN Database
Foreign Agent Remove / Update MN Entry from Visiting MN Database
Notification Message to MPLS Router to Setup Label Tunnel
Notification Message to MPLS Router to Teardown Label Tunnel
Forward Reply Packet RegReply to Mobile Node
Mobility Agent Active

Appendix C

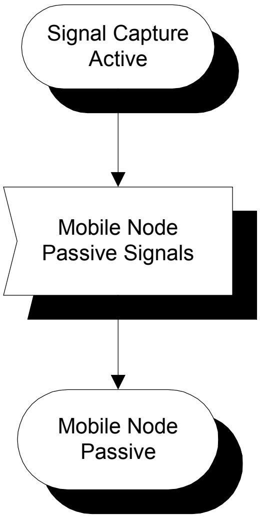
SDL Diagrams for Mobile Node with MPLS

Level 1 – High Level Design

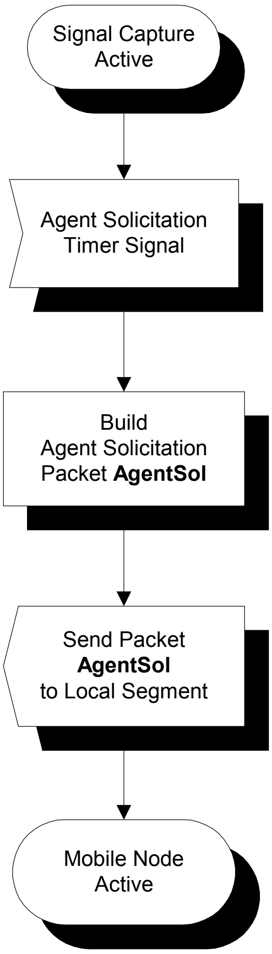

Mobile Node Active
Enable: Mobile Node Passive Signal Agent Solicitation Timer
Receive Packet RcvPkt
RcvPkt is Agent Advertisement AgentAdv ?
Yes
No
RcvPkt is Register Reply RegReply ?
Yes
No
Reset Agent Solicitation Timer
Discard RcvPkt
Process RegReply
Mobile Node Active
Process AgentAdv

Level 2.1 Signal Processing

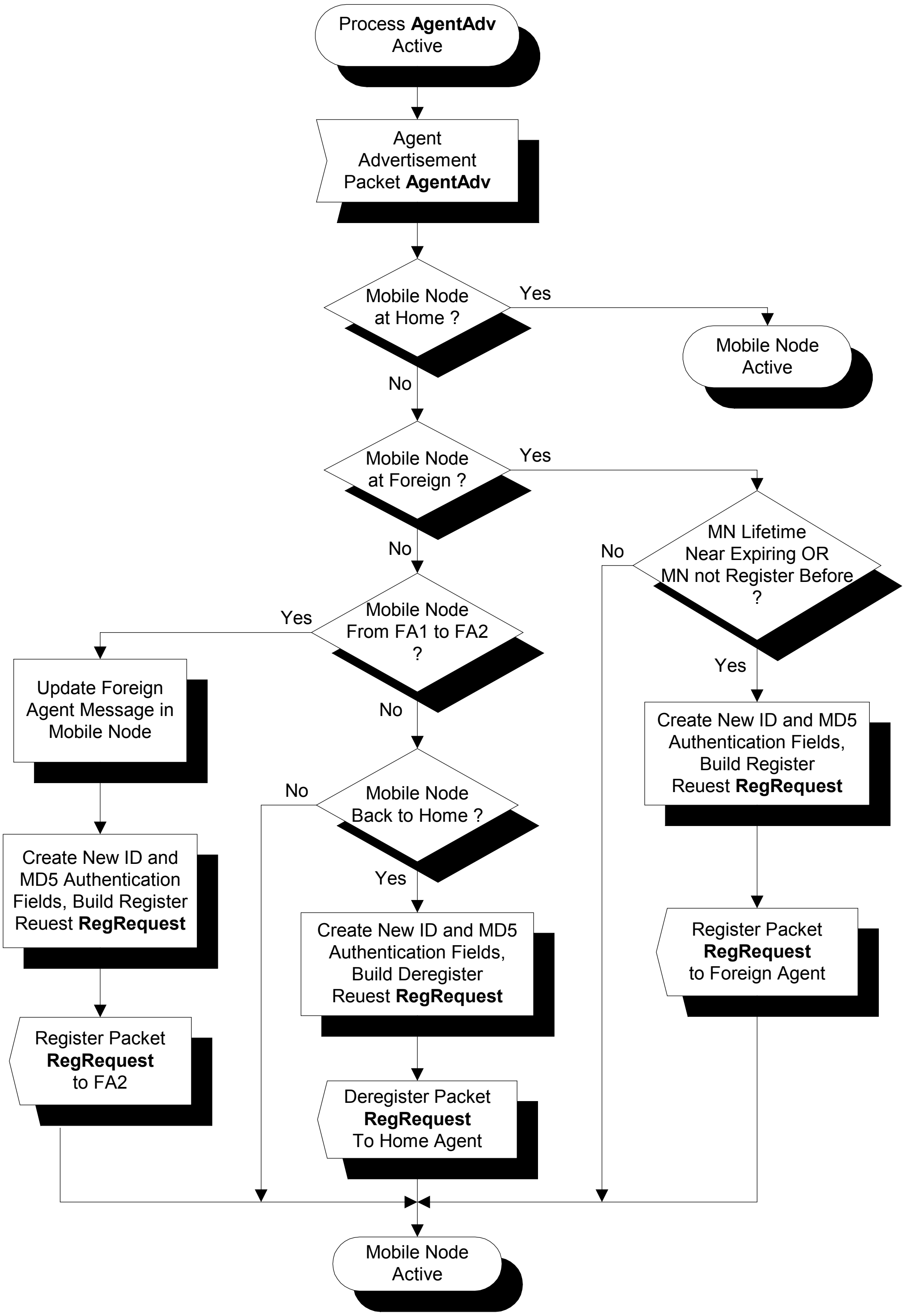
2.1 (a)   Exiting Signal



2.1 (b) Agent Solicitation Timer Signal

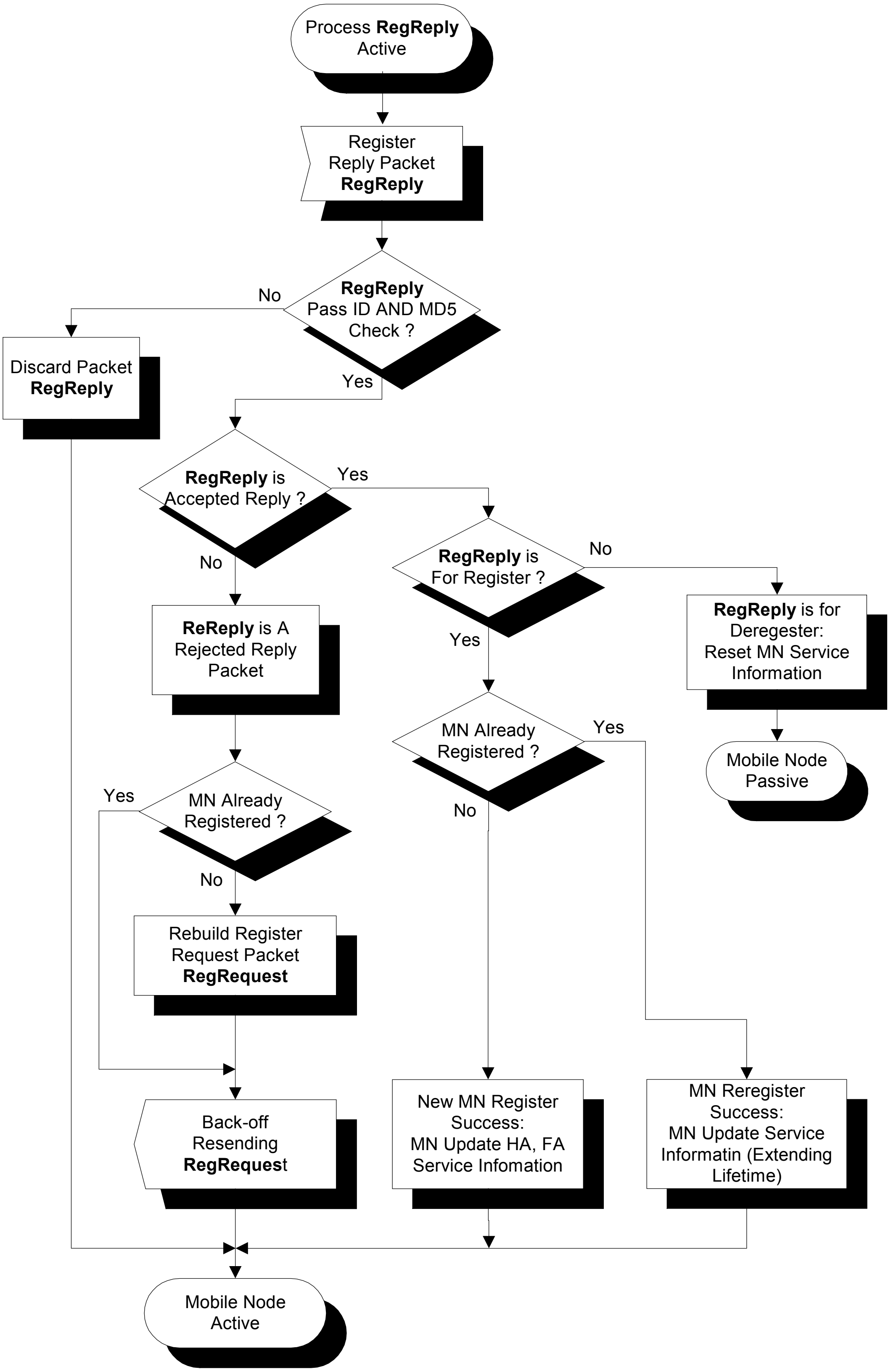

Signal Capture Active
Agent Solicitation Timer Signal
Build Agent Solicitation Packet AgentSol
Send Packet AgentSol to Local Segment
Mobile Node Active

Level 2.2 Process Agent Advertisement



Process **AgentAdv** Active
Agent Advertisement Packet **AgentAdv**
Mobile Node at Home ?
Yes
Mobile Node Active
No
Mobile Node at Foreign ?
Yes
MN Lifetime Near Expiring OR MN not Register Before ?
No
No
Mobile Node From FA1 to FA2 ?
Yes
Update Foreign Agent Message in Mobile Node
Yes
Create New ID and MD5 Authentication Fields, Build Register Reuest **RegRequest**
No
Mobile Node Back to Home ?
No
Create New ID and MD5 Authentication Fields, Build Register Reuest **RegRequest**
Yes
Register Packet **RegRequest** to Foreign Agent
Create New ID and MD5 Authentication Fields, Build Deregister Reuest **RegRequest**
Register Packet **RegRequest** to FA2
Deregister Packet **RegRequest** To Home Agent
Mobile Node Active

Level 2.3 Process Register Reply

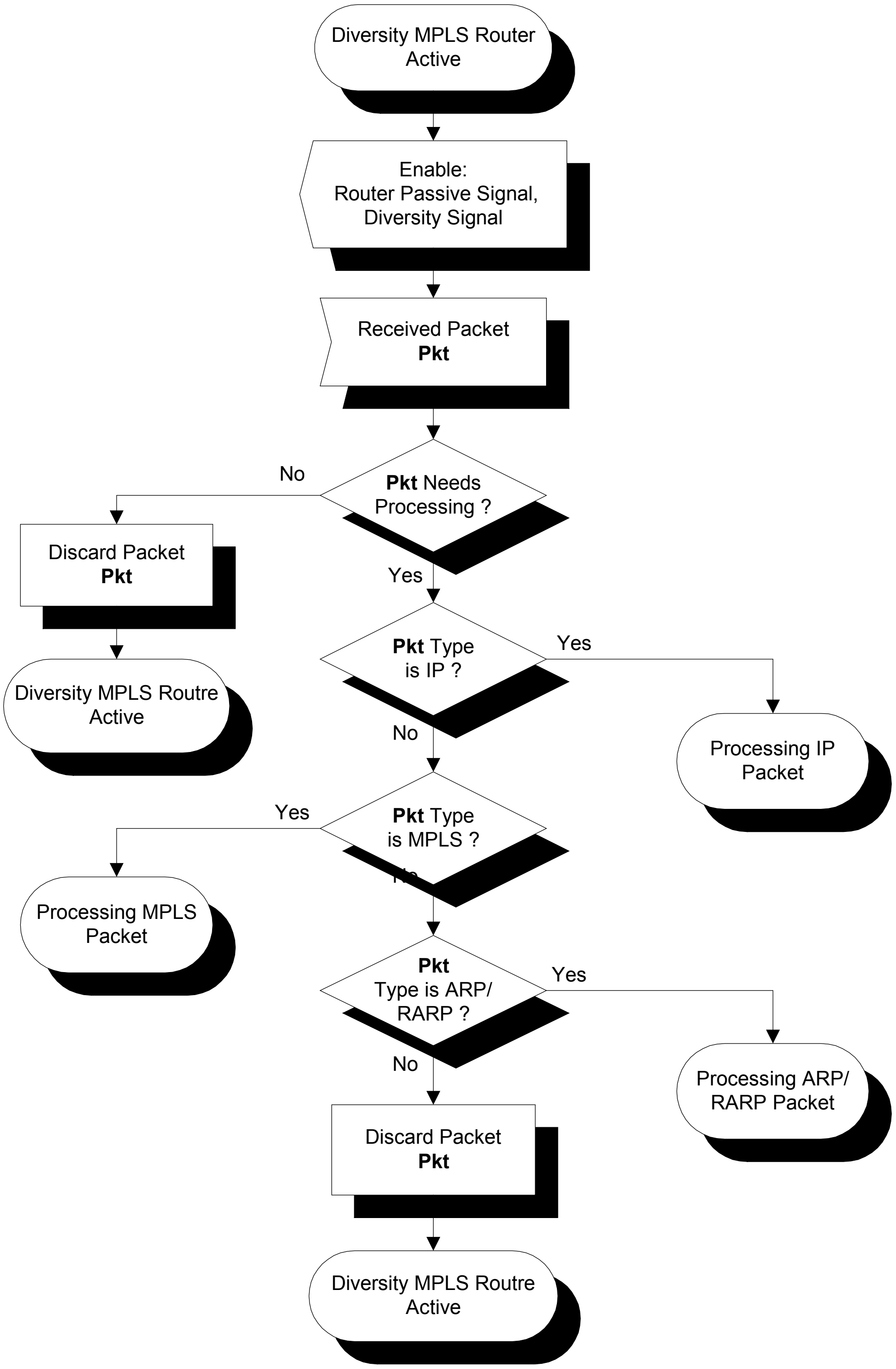


Process RegReply Active
Register Reply Packet RegReply
RegReply Pass ID AND MD5 Check ?
No
Yes
Discard Packet RegReply
RegReply is Accepted Reply ?
Yes
No
RegReply is For Register ?
No
Yes
ReReply is A Rejected Reply Packet
RegReply is for Deregester: Reset MN Service Information
Mobile Node Passive
MN Already Registered ?
Yes
No
MN Already Registered ?
Yes
No
Rebuild Register Request Packet RegRequest
Back-off Resending RegRequest
New MN Register Success: MN Update HA, FA Service Infomation
MN Reregister Success: MN Update Service Informatin (Extending Lifetime)
Mobile Node Active

Appendix D

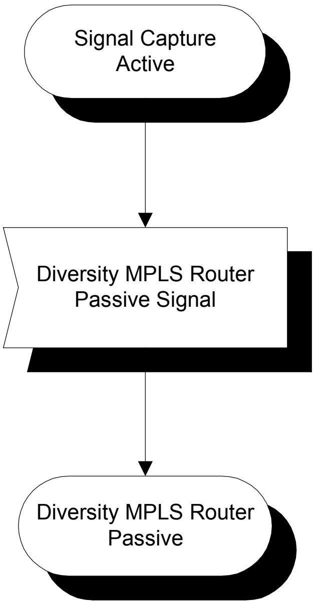
SDL Diagrams for Diversity MPLS Router

Level 1 – High Level Design

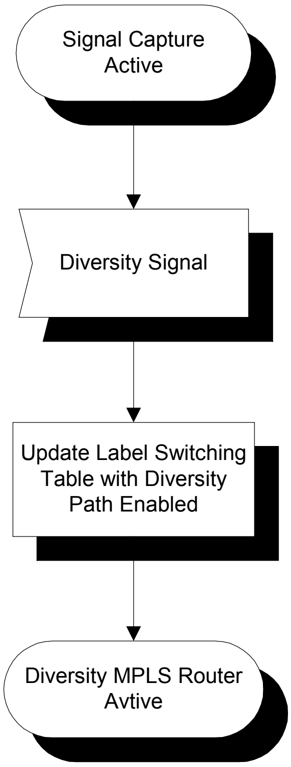

Diversity MPLS Router Active
Enable: Router Passive Signal, Diversity Signal
Received Packet **Pkt**
Pkt Needs Processing ?
No
Discard Packet **Pkt**
Diversity MPLS Routre Active
Yes
Pkt Type is IP ?
Yes
Processing IP Packet
No
Pkt Type is MPLS ?
Yes
Processing MPLS Packet
No
Pkt Type is ARP/ RARP ?
Yes
Processing ARP/ RARP Packet
No
Discard Packet **Pkt**
Diversity MPLS Routre Active

Level 2.1 Signal Processing

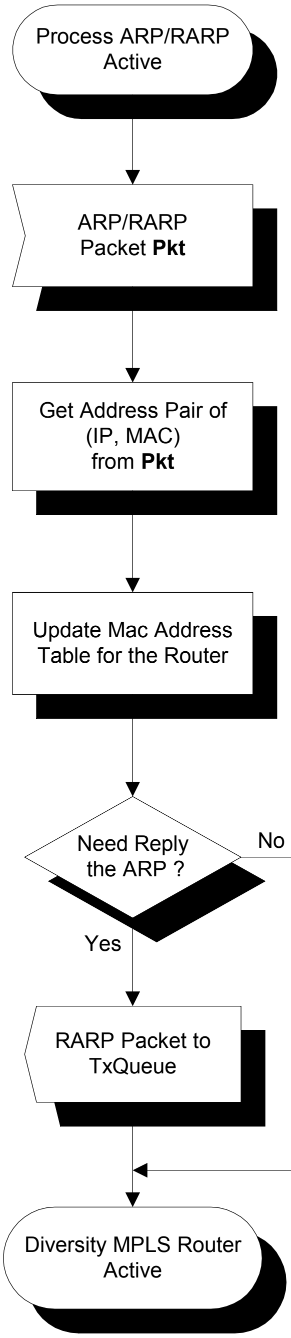
2.1 (a) Exiting Signals


Signal Capture Active
Diversity MPLS Router Passive Signal
Diversity MPLS Router Passive

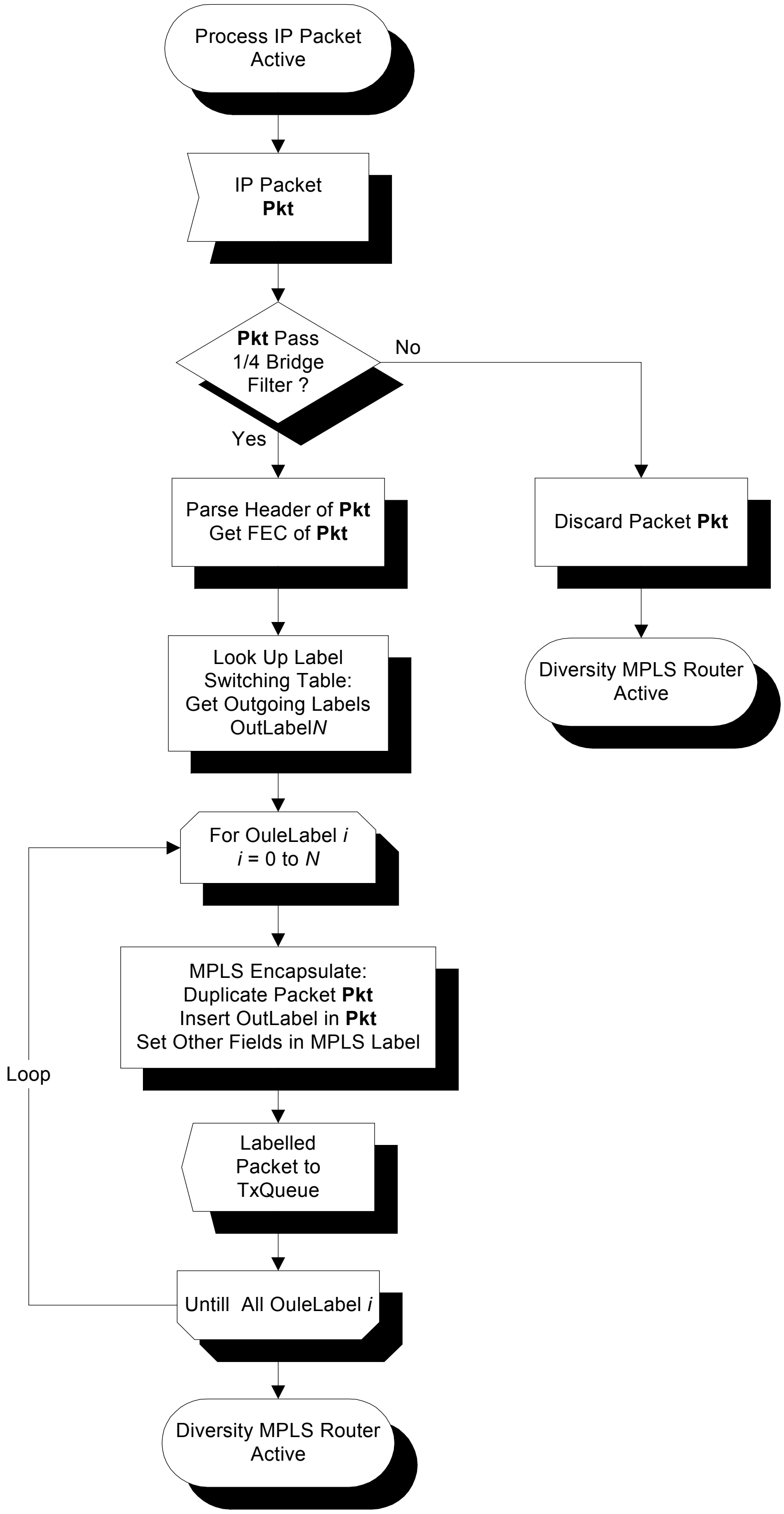
2.1 (b) Diversity Enabling Event


Signal Capture Active
Diversity Signal
Update Label Switching Table with Diversity Path Enabled
Diversity MPLS Router Avtive

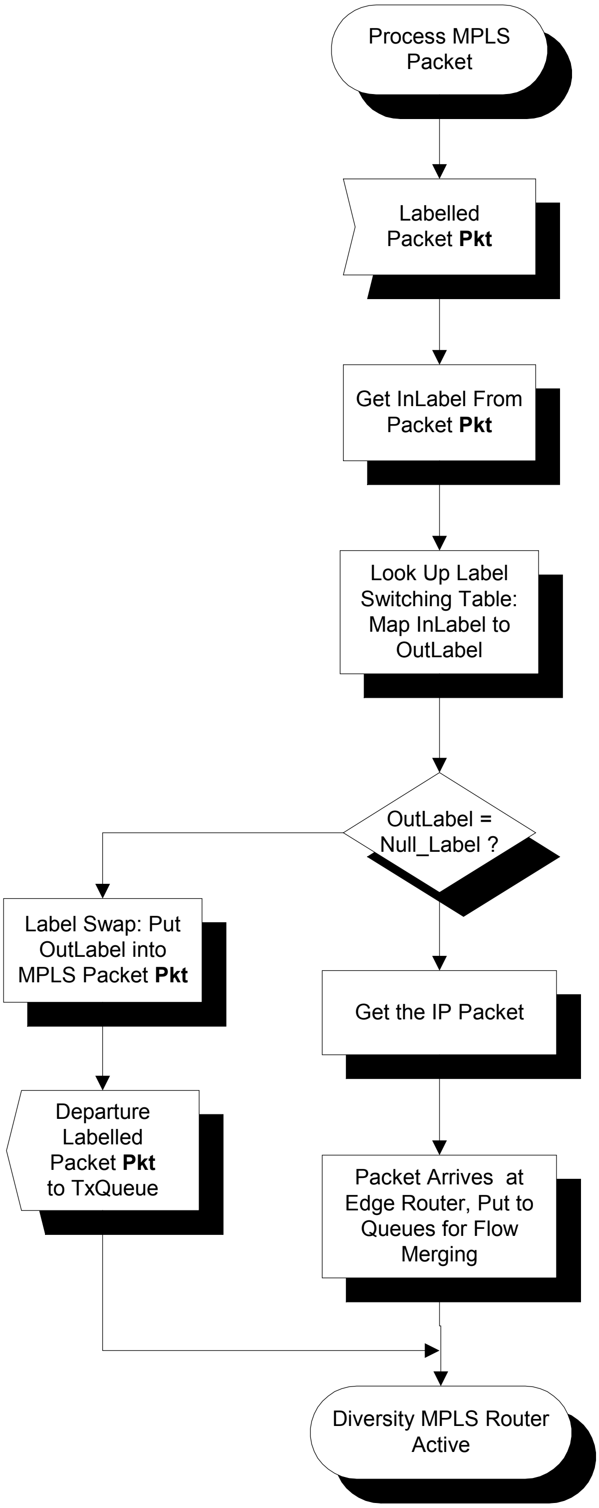
Level 2.2 Processing ARP/RARP Packet


Process ARP/RARP Active
ARP/RARP Packet Pkt
Get Address Pair of (IP, MAC) from Pkt
Update Mac Address Table for the Router
Need Reply the ARP ?
No
Yes
RARP Packet to TxQueue
Diversity MPLS Router Active

Level 2.3 Processing IP Packet


Process IP Packet Active
IP Packet **Pkt**
Pkt Pass 1/4 Bridge Filter ?
No
Yes
Parse Header of **Pkt** Get FEC of **Pkt**
Discard Packet **Pkt**
Diversity MPLS Router Active
Look Up Label Switching Table: Get Outgoing Labels OutLabel*N*
For OuleLabel *i* *i* = 0 to *N*
MPLS Encapsulate: Duplicate Packet **Pkt** Insert OutLabel in **Pkt** Set Other Fields in MPLS Label
Loop
Labelled Packet to TxQueue
Untill All OuleLabel *i*
Diversity MPLS Router Active

Level 2.4 Processing MPLS Packet



Process MPLS Packet
Labelled Packet **Pkt**
Get InLabel From Packet **Pkt**
Look Up Label Switching Table: Map InLabel to OutLabel
OutLabel = Null_Label ?
Label Swap: Put OutLabel into MPLS Packet **Pkt**
Get the IP Packet
Departure Labelled Packet **Pkt** to TxQueue
Packet Arrives at Edge Router, Put to Queues for Flow Merging
Diversity MPLS Router Active

Appendix E

Publications

Route Diversity in an Interconnected LMDS network
Published in: Proceeding of IST Mobile Communications Summit 2001. Barcelona, September 2001. Pages 651-656. ISBN: 84-931132-3-9.

Diversity and Nomadic Access to a Broadband Wireless IP Network
Published in: Proceeding of Multi-Service Networks 2000. Cosener's House, Abingdon, July 2000.

Route Diversity in an Interconnected LMDS Network

Christopher Adams, Xiyu Shi

Rutherford Appleton Laboratory, Cranfield University
chris@buck.ac.uk, x.shi@rl.ac.uk

The use of alternative base stations for clients of a star LMDS network can improve the accessibility of a user station in a number of rain fade situations.

The scheme described, monitors the down stream power level and sets up a duplicate traffic stream to a second base station when the detected signal level falls below a pre-established level. These two streams are called "shadow flows" and they only exist for a short time whilst the fade conditions are assessed. One of the "shadow flows" will normally be closed down when either the fade has recovered or has been confirmed.

It is hoped that the rate of fade will be such that starting up "shadow flows" on a small fade margin will give enough time for the route to be well established before the fade becomes bad enough to provoke serious bit errors and hence packet loss. This has still to be established by the long-term trials, which will occur towards the end of the project, but initial experiments on our test bench are encouraging.

I. Introduction

LMDS cellular networks using 40 GHz range offer the possibility of considerable potential bandwidth for network providers. Unfortunately rain at these frequencies can cause heavy signal fades possibly resulting in bit errors, even after coding. Path diversity attempts to counteract heavy fading due to localised rain by providing another RF path to a different base station. The use of alternative paths in the former ACTS project CRABS [Craig99] has been shown to produce a significant decrease in outage time in some configurations. This ability to switch traffic to another cell when fade conditions prevent the current base from being used is an essential part of the EMBRACE project.

EMBRACE is a star network with the up link path using MF-TDMA from individual clients stations whilst the down link from the base station uses a continuous mode transmission based on the DVB-S transport stream.

II. Embrace IP Networking

In the EMBRACE network all traffic apart from broadcast digital television is carried in IP packets. Broadcast digital television is carried as "raw" MPEG-2 in a DVB-S transport stream whereas all other traffic is embedded in IP and MAC layer packets in either Ethernet, DVB-S or MF-TDMA formats.

The network allows IP packets to be transmitted on the up link to the base station using both multiple frequencies and time division slots, MF-TDMA. Traffic arriving at the base station is sorted into:

- local traffic destined for a different user station within the same cell,
- traffic destined to other LMDS cells within the same network,
- traffic destined for other sub-networks within the internet as a whole.

The base station transmits IP packets, destined for the current cell, embedded in a continuous DVB-S transmission broadcast to all the user stations.

LMDS cells are connected together by a core or backbone network. This is based on a mesh of logical ATM paths, VCs (Virtual Circuits) that provide interconnectivity and also provide some quick routes for priority traffic.

The network also provides Quality of Service (QoS) guarantees based on the traffic class in the Type of Service (TOS) field of the IP header. The guarantees are maintained by using priority traffic classes within the MF-TDMA and DVB-S controllers, using MPLS (Multi-Protocol Label Switching) [Rosen01] routing within the LMDS cell interconnection network, and also by diversity routing.

III. Path Diversity Enabled Client

Figure 1 shows the path diversity scheme in diagrammatic form. Site 1 has a diversity capability but site 2 does not. The core network is only shown here as a connection from each site to an ATM switch which is also connected to the Internet as a whole.

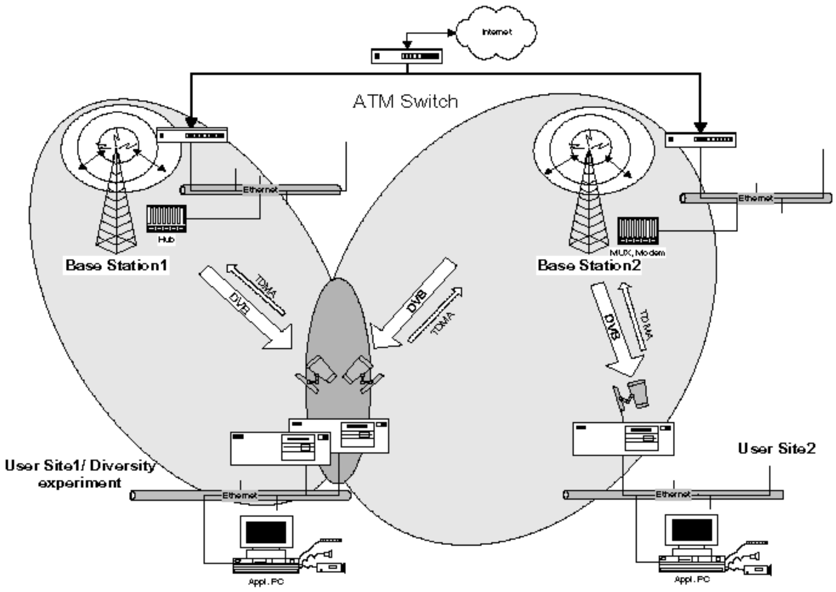


Figure 1- Path Diversity

The DVB-S down link hardware consists of a demodulator/decoder attached to a DVB-S transport stream card embedded in a Linux PC. A special fade detecting PC able to read registers in both demodulators via an I^2C bus, is attached to the network. . Several registers in the demodulator have to do with receive power level and error conditions either with or without coding. The “raw” amplitude of the QPSK signal is currently read and compared against previous values. If the signal is lower than a preset level then path diversity is turned on.

IV. The ATM Core Network

In Figure 2, the arcs with arrows at both ends indicate a pair of ATM Permanent Virtual Circuits, PVCs. These circuits are terminated in the special EMBRACE MPLS/IP routers which connect the base station in each cell to the backbone or core network. These routers have the responsibility of routing the IP packets, according to their QoS requirements in [Adams01], to the correct destination router. The thick lines indicate special PVCs for carrying priority traffic between selected routers. The decision on which particular route is chosen in the router is defined by tables specifying both the IP destination and the TOS byte in the IP header. (TOS is normally used to specify quality of service requirements.)

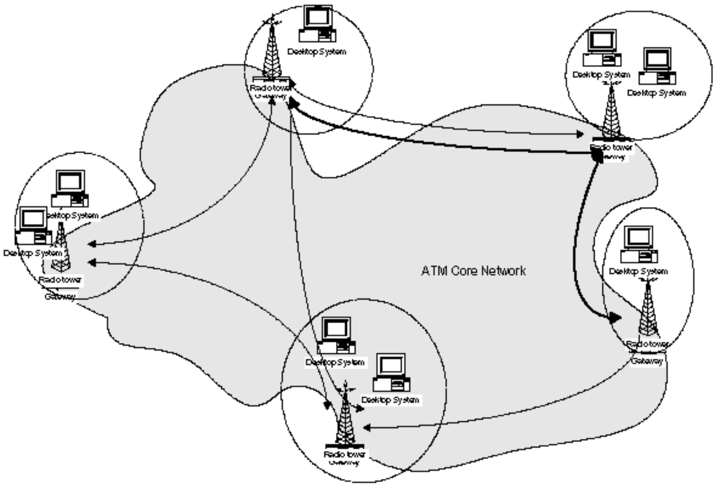


Figure 2 - Logical ATM Core Network

V. Multi-Protocol Label Switching, MPLS, in Embrace

MPLS is designed to handling the routing of information from an entrance router to an MPLS exit router; this is known as the MPLS domain in [Rosen01]. The packets that are routed may be of any sort—IP packets, Ethernet frames, IPv6 or even AAL5 blocks. The routing of packets is independent of the underlying packet protocol that is being routed. MPLS routing has several advantages over ordinary IP routing:

- Packets of any type can be routed.
- Packets are routed very quickly by merely swapping their input label to the output label. This is the same mechanism used by ATM switching.
- More than one path can be established between an entrance and an exit router.
- Multiple paths can be used for traffic load balancing.
- Different paths can be used for different types of priority traffic.
- Different paths can be used for path diversity when avoiding rain fades.

In the standard MPLS format, MPLS headers are inserted between the level 2 header and the level 3 packet [Xiao00]. In our case there are two distinct ways of carrying the MPLS header.

- The header is carried at the end of an Ethernet frame between the last data byte of the level 3 data and the level 2 CRC. (That is, just before the CRC.)
- The header is carried at the front of an ATM AAL5 block and just before the IP packet embedded in the AAL5 block. There is no level 2 header in this case.

These two mechanisms have been adopted for reasons of processing speed and minimum data handling overhead. Figure 3 shows the specialised MPLS field used in the Embrace experiment.

Path A unique label field which is used in the label swapping.
Sequence number A monotonically increasing number which identifies the particular packet coming from the router with Router ID.
Router ID A unique identifier of the entrance router
Stack A push down stack of labels (not used)
TTL A Time To Live down counter to prevent loops

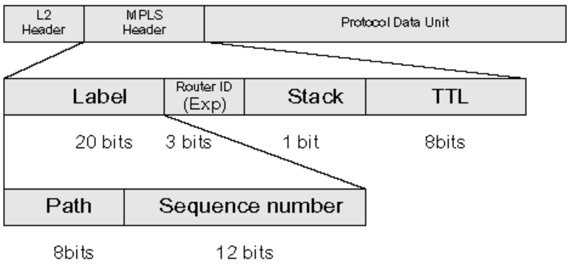


Figure 3 – MPLS Header and Packet Format

VI. Fade Detection and Labelling

Figure 4 shows the fade detector connected to two Ethernet segments. Incoming Ethernet frames are inspected to determine whether the embedded IP packet requires diversity switching. If this is required then the fade process is invoked.

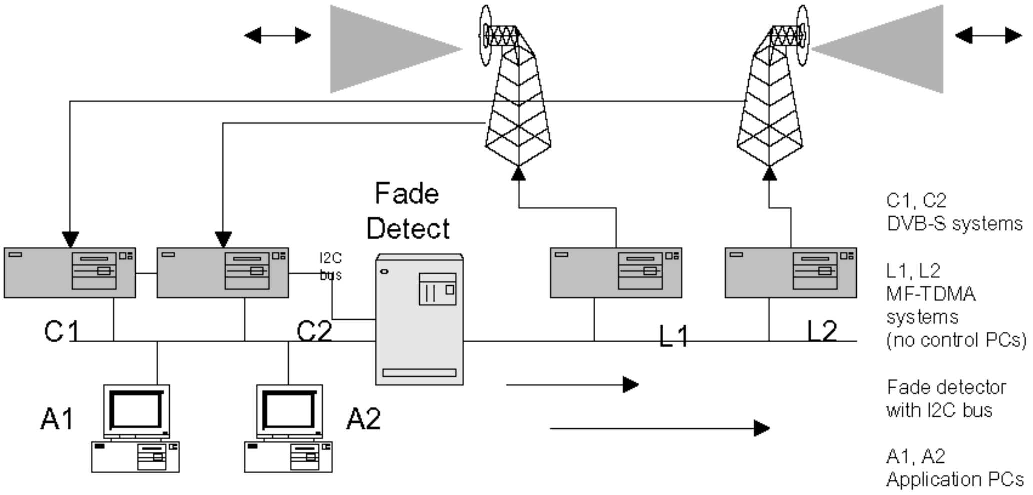


Figure 4 – Fade detection Arrangement

- The fade detection system consists of a Linux PC fade detection process that regularly reads the status of the two decoder systems. The registers on the decoder cards are read over the I^2C bus. Currently the digital amplitude of the QPSK signal is used to determine the amount of fade. Other error rates after coding provide little information on the signal strength.

- If the fade process notices a significant fade in the signal from the current base station then the fade control station attempts to set up a second and simultaneous path to the second base station.
- The fade station causes the current packet stream to be duplicated and sent down a second MPLS path.
- If fade is not indicated then the fade station only produces a single MPLS stream to the exit router.
- The fade station acts as a MPLS entrance router for both diversity and non-diversity traffic.
- An MPLS path (shadow flow) is closed down either if both links are not in fade and hence diversity is not required, or if one of the links is in heavy fade. This causes the fading site's shadow flow to be closed and the stream will default to a single flow over the MPLS routing network.

VII. Fade Data Flow

Outgoing IP traffic from, say, A2 (Figure 4) goes to the fade detector over one of the two Ethernets. A process in FD takes the incoming IP packet and inspects the fade status. If it is necessary to form a shadow flow then a bit is set in the MPLS header and two distinct MPLS labels are attached to the packet and a copy and the packets sent to stations L1 and L2 on the second Ethernet. This is easy to do as the MF-TDMA system works in promiscuous mode. The sequence number in the MPLS label is incremented every time a packet is received at the fade detector, thus there will be two packets in the MPLS network with different labels but with the same sequence number. MPLS streams with different labels will have different sequences.

Incoming MPLS "shadow" traffic streams at the exit MPLS router are combined together using the following algorithm. (MPLS streams are specified as being "shadows" if they have the same entrance router and exit router, but different MPLS labels.)

- The current sequence number offset between the two streams is calculated by observing the arrival of a number of MPLS packets
- Buffers on each path provide storage of packets on each path which is necessary to adjust the arrival time of each stream
- The buffers are arranged so that both streams appear to have simultaneous arrival times and can be read at the same time
- If a packet (sequence number N) is not available from the first channel (N+1 is present but not N) then the process takes the packet (sequence number N) from the second channel if available. If it has not arrived it waits for a short time,
- If a packet is absent from both streams the process goes back to the top of the loop looking for packet with sequence number N+1 on the first channel.

These rules combine two streams if the delay is constant or slightly varying. It is necessary to re-measure the time offset between the two streams on a regular basis if the overall delay is greatly varying.

The exit MPLS router provides a stream of outgoing IP packets which will be as close to the original IP stream as possible when taking account of packet losses.

VIII. Fade Shadow Flow Preliminary Results

Figure 5 shows a typical result of an actual measured performance on the MPLS test bed taken at a particular constant bandwidth. There is clearly a great improvement especially when the number of packets per second is relatively small or the packet size is relatively large.

Figure 6 shows the improvement in delay due to taking the first packet arriving on each stream. This was an unexpected result. The graph uses a log scale and the delay due to the actual transmission times dominates the delay for large packet size. These experiments used a particular constant bandwidth, 2Mbit/s.

(The network currently has a small, but non-zero, UDP loss rate of about 1% near the maximum virtual channel rate due to packet handling overheads and this was used as the error process in this case. Further experiments will use an artificial error generator.)

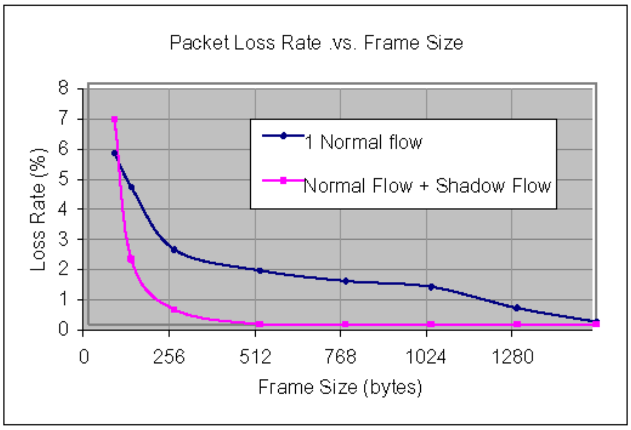


Figure 5 – Comparison of Packet Loss Rate

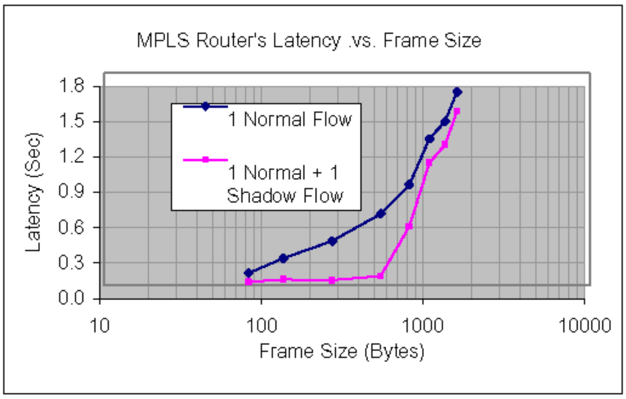


Figure 6 – Comparison of Packet End-to-End latency

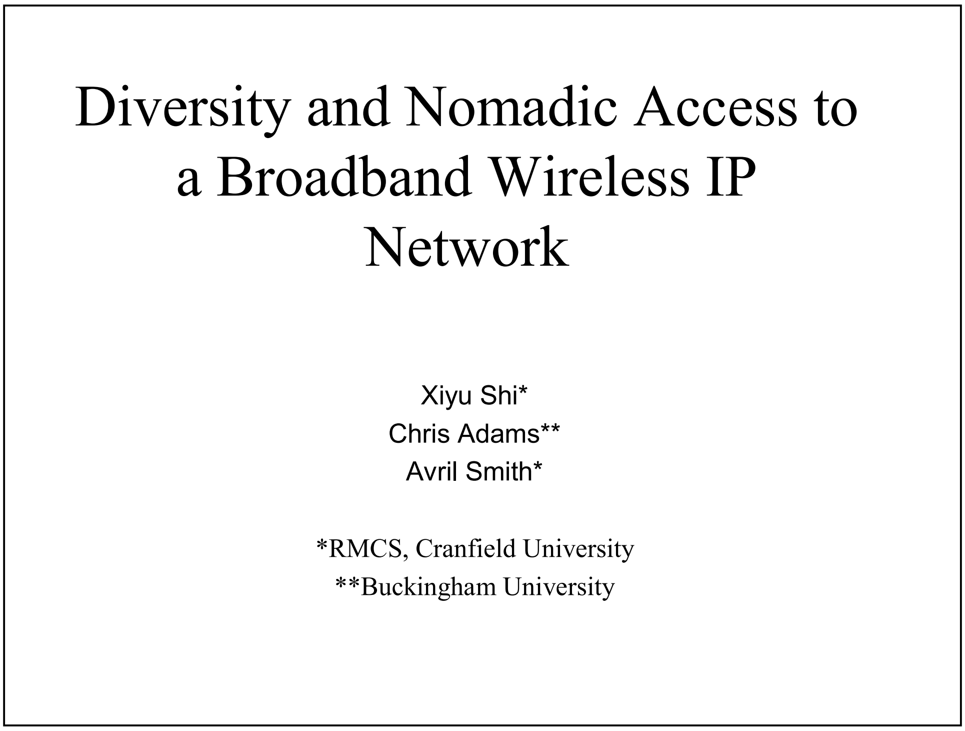
References

[Adams01] Chris Adams, "Prototype IP Implementation for MPEG-2 transport stream down link delivery and MF-TDMA up link", *EMBRACE Deliverable Doc. D5*, 29th May, 2001

[Craig99] K. H. Craig, "Propagation Planning Procedures for LMDS", *CRABS Deliverable Report D3P1B*, http://www.telenor.no/fou/prosjekter/crabs/d3p1b.pdf, 13 Jan., 1999

[Rosen01] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture", *RFC 3031*, Jan. 2001

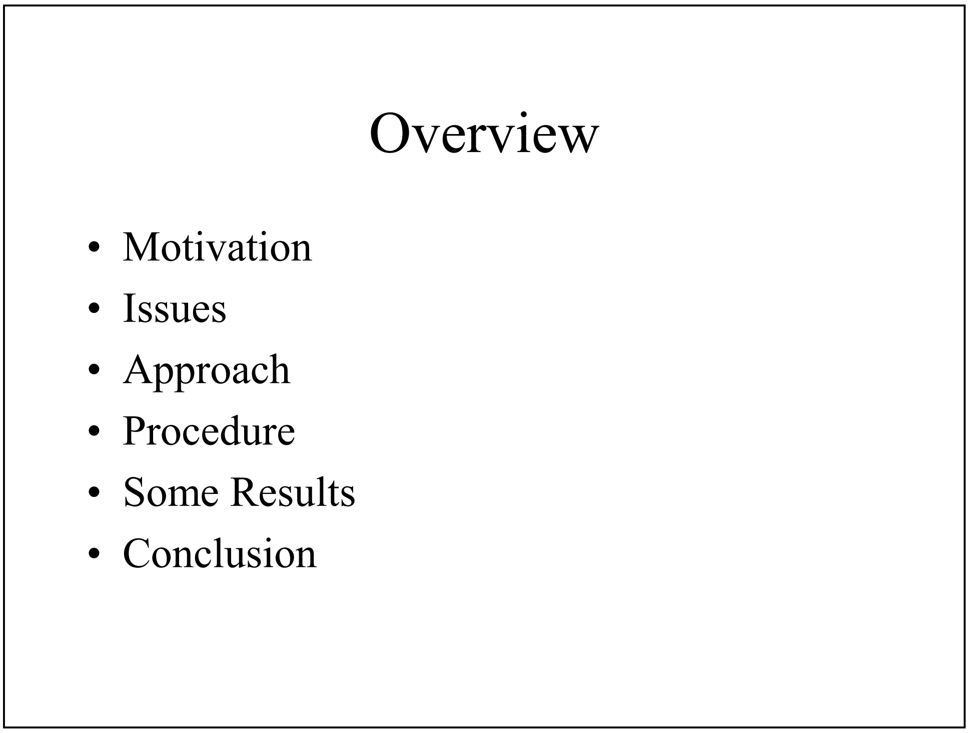
[Xiao00] Xipeng Xiao, Alan Hannan, et al, "Traffic Engineering with MPLS in the Internet", *IEEE Network*, Vol. 14, No.2, March/April 2000



Diversity and Nomadic Access to a Broadband Wireless IP Network

Xiyu Shi*
Chris Adams**
Avril Smith*

*RMCS, Cranfield University
**Buckingham University

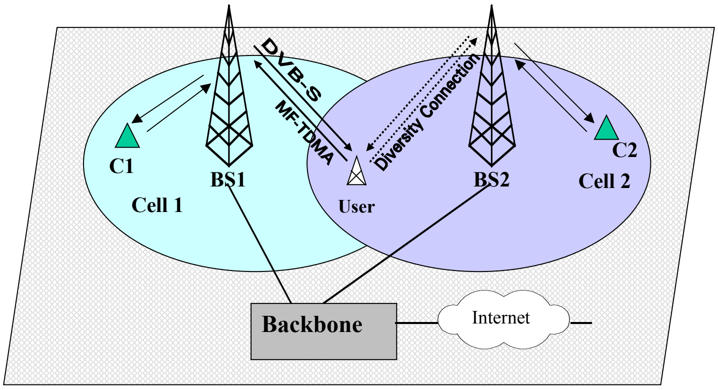


Overview

- Motivation
- Issues
- Approach
- Procedure
- Some Results
- Conclusion

Motivation

- Consider the following Broadband Wireless Access Network

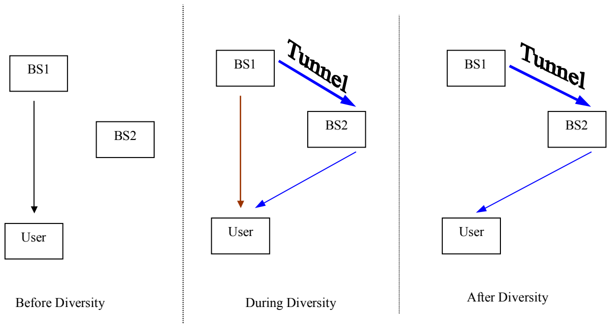


Features and Problems

- Features
  - User registers and Connects to one Base Station (e.g. BS1--Home)
  - All traffic be carried over IP
- Problems
  - Nomadic access to the network
  - Link between BS1 and User can be affected by:
    - Buildings
    - Attenuation by rain, sleet, snow
    - Interference…

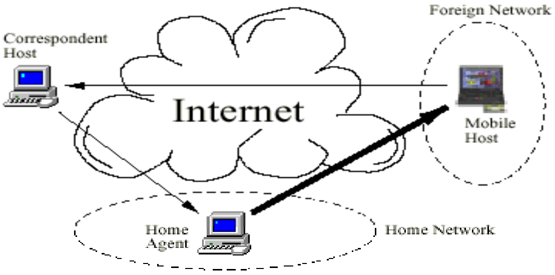
A Simple Diversity Solution

- Diversity
  - Definition
- Diversity Procedure



The Mobile IP Approach

- The basic Mobile IP model

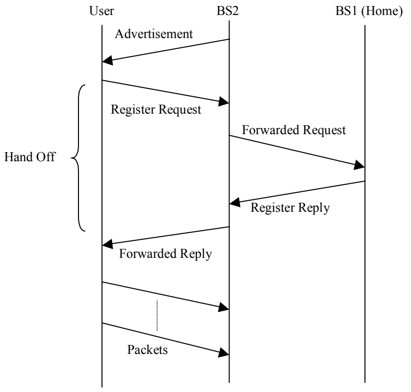


- Implementation: Mobile IP + Simulcasting

Route Establishment

- Procedure
  - User made the diversity decision
  - User received mobility agent advertisement from a nearby base station
  - User send a request to its home BS via the nearby BS
  - User received a reply from home BS to grant the diversity (and nomadic ?) access
  - User uses the new BS to connect to Home BS

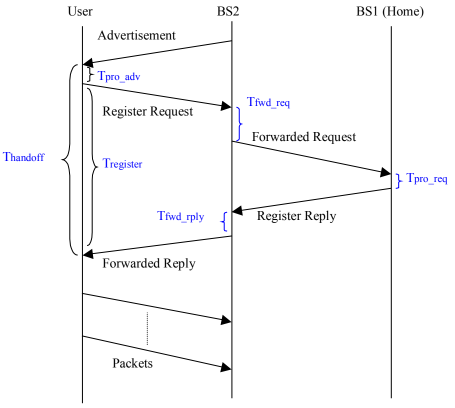
- Time sequence

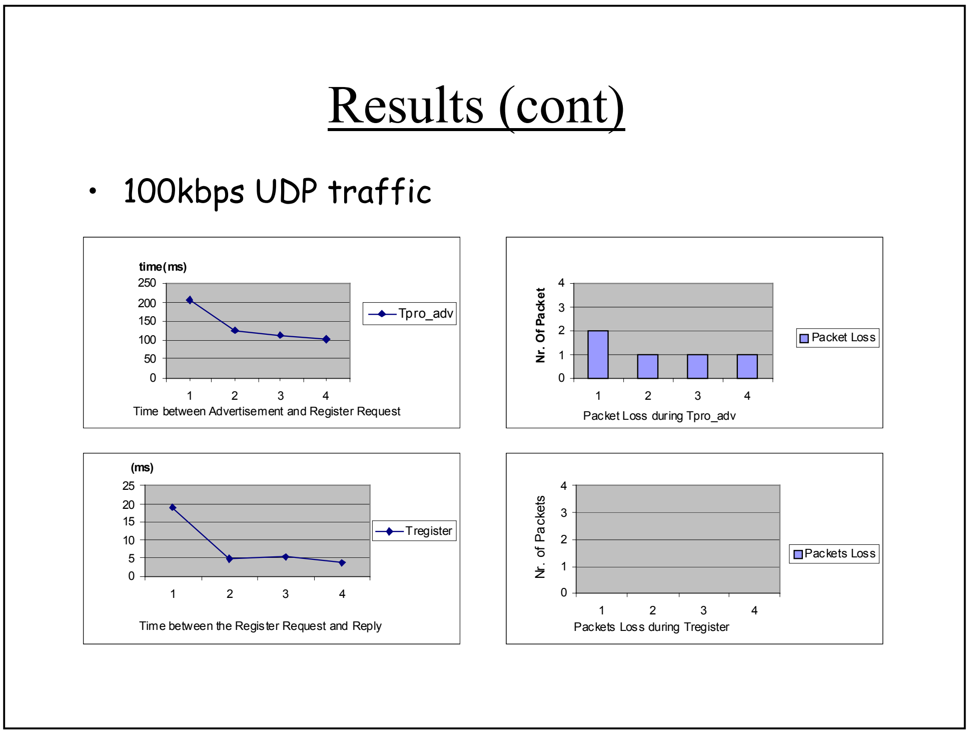


Results

- Parameters
  - Hand off time
  - Packet loss during hand off
- $T_{handoff} = RTT + T_{pro\_adv} + T_{fwd\_req} + T_{pro\_req} + T_{fwd\_rply}$
- Typical value
  - $RTT = 1.5ms$
  - $T_{register} < 10ms$
  - $T_{handoff}$: 0.1~0.9s

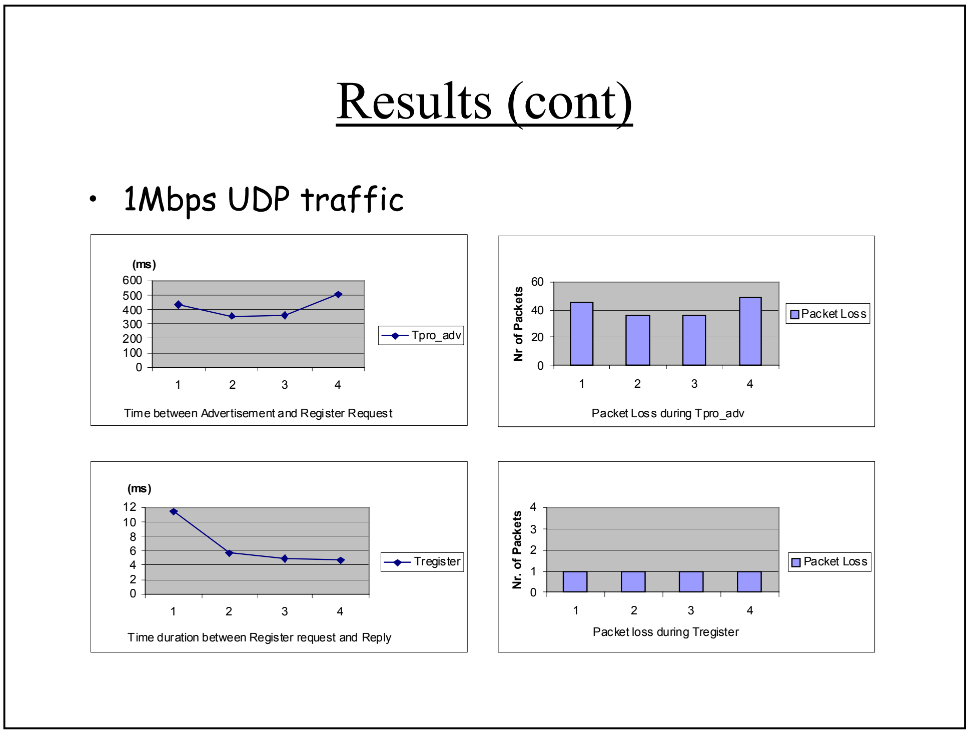
- Times during the user handoff





Results (cont)

- 100kbps UDP traffic

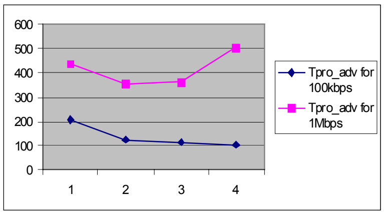


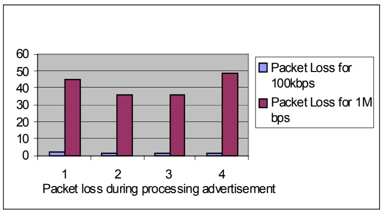
Results (cont)

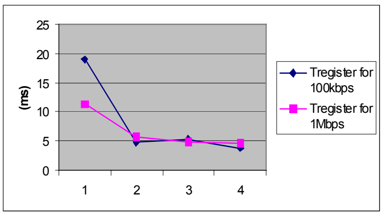
- 1Mbps UDP traffic

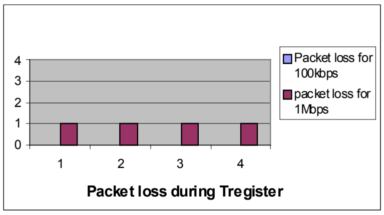
Results (cont)

- Comparison









Conclusion

- With IP diversity, packets are duplicate delivered to the user. This ensures the packet loss is at a low level during hand off
- Support user nomadic access
- Higher availability and reliability
- Other approach
  - DiffServ
  - Specific connection protocol for radio access

Appendix F

Pictures of System Configuration

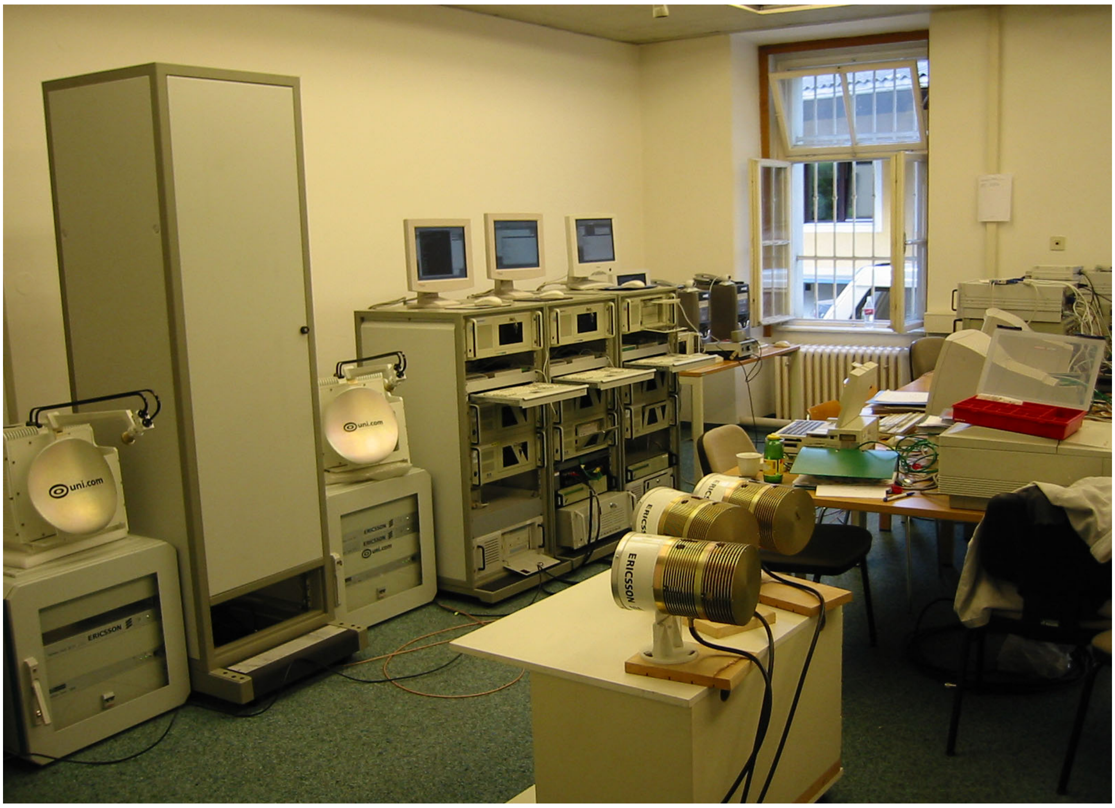


Figure F. 1 Diagram of System

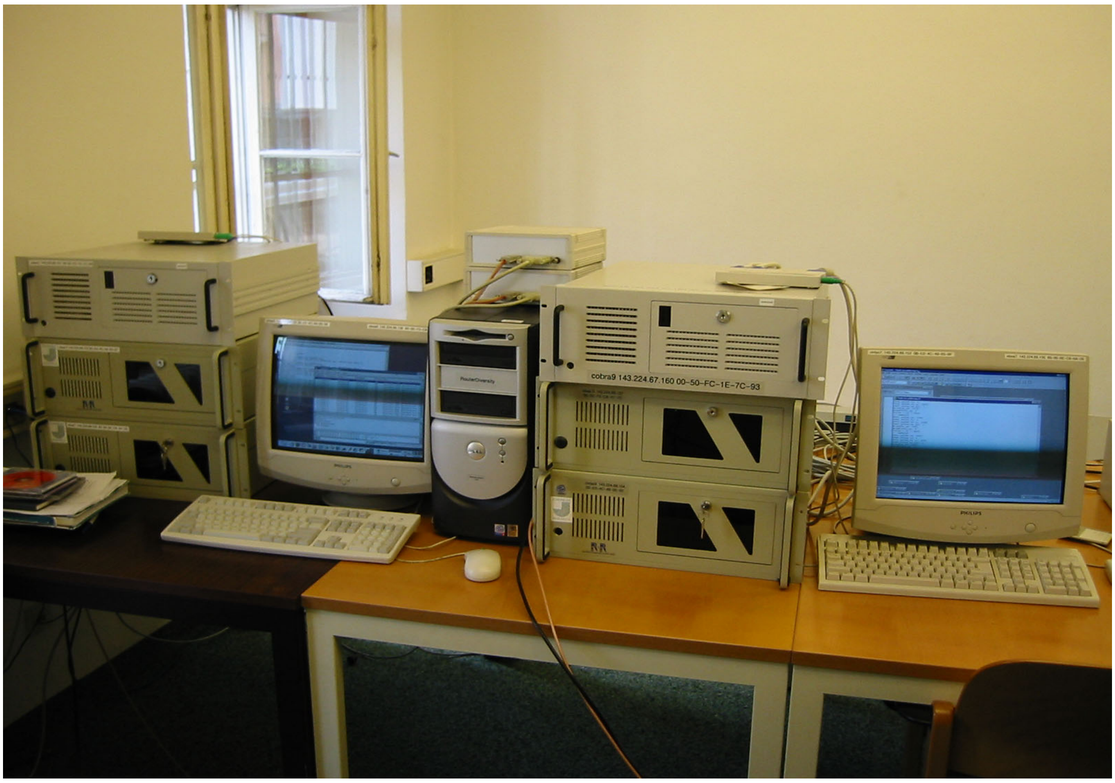


Figure F. 2 Configuration of diversity router

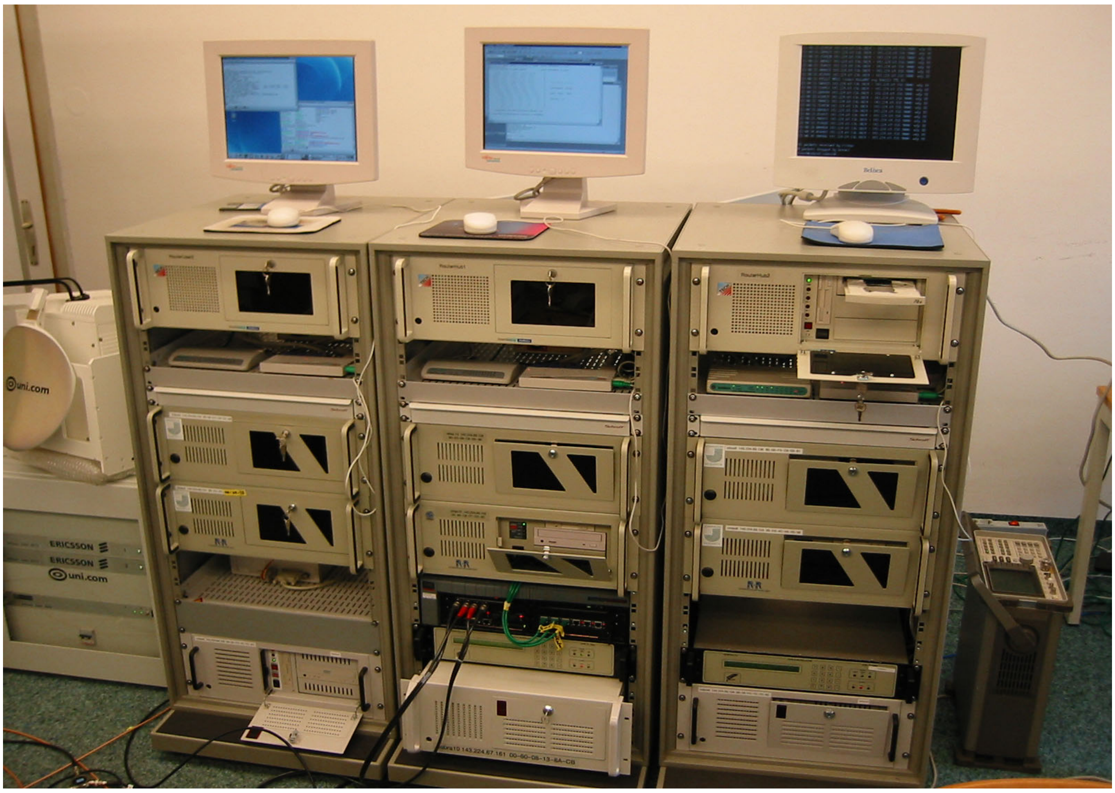


Figure F. 3 Configuration of routers at the user site and base station

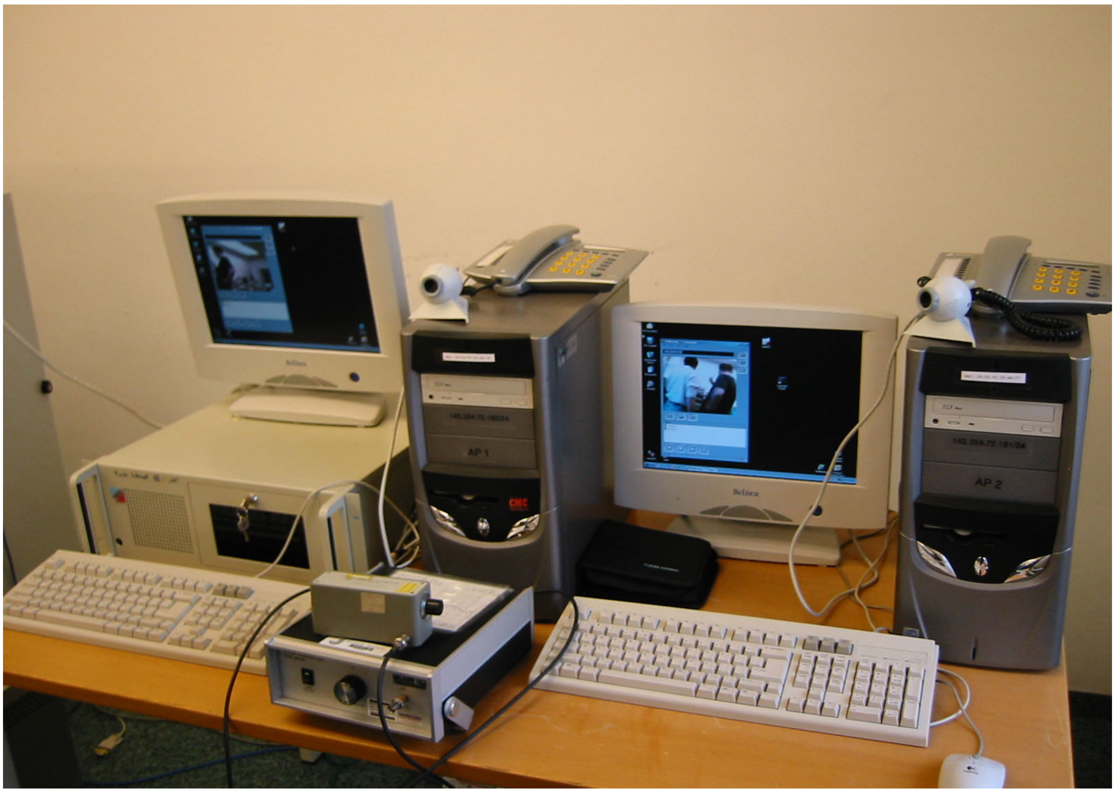


Figure F. 4 Application PCs running netmeeting

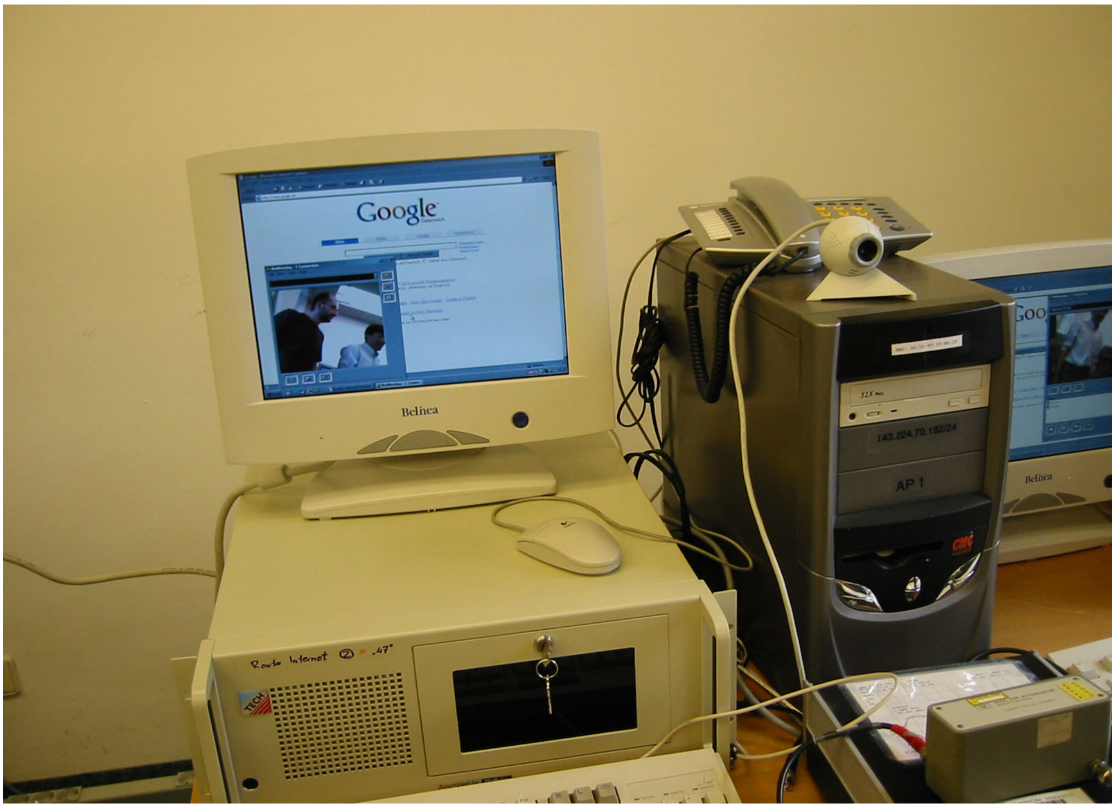


Figure F. 5 Connected to the Internet

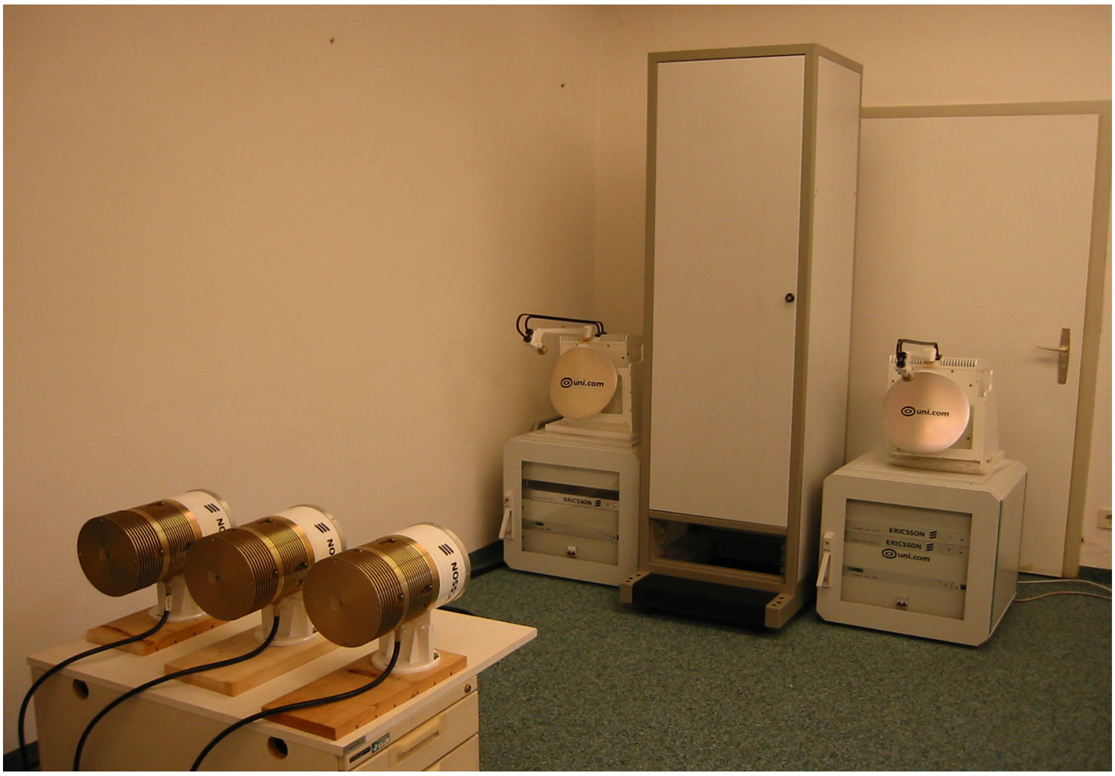


Figure F. 6 The RF Indoor/Outdoor Unit and Antenna