2005

Mobile-IP ad-hoc network MPLS-based with QoS support.

Sasan Adibi
University of Windsor

MOBILE-IP AD-HOC NETWORK MPLS-BASED WITH QOS SUPPORT

by

Sasan Adibi

A Thesis
Submitted to the Faculty of Graduate Studies and Research
through the Department of Electrical and Computer Engineering
in Partial Fulfillment of the Requirements for the
Degree of Master of Science
at the University of Windsor
Windsor, Ontario, Canada

Your file Votre référence
ISBN: 0-494-09836-8
Our file Notre référence
ISBN: 0-494-09836-8

ABSTRACT

The support for Quality of Service (QoS) is the main focus of this thesis. Major issues and challenges for Mobile-IP Ad-Hoc Networks (MANETs) to support QoS in a multi-layer manner are considered discussed and investigated through simulation setups. Different parameters contributing to the subjective measures of QoS have been considered and consequently, appropriate testbeds were formed to measure these parameters and compare them to other schemes to check for superiority. These parameters are: Maximum Round-Trip Delay (MRTD), Minimum Bandwidth Guaranteed (MBG), Bit Error Rate (BER), Packet Loss Ratio (PER), End-To-End Delay (ETED), and Packet Drop Ratio (PDR) to name a few. For network simulations, NS-II (Network Simulator Version II) and OPNET simulation software systems were used

DEDICATION

I dedicate this work to my wife, Negar Rasti, who recently embarked on this journey with me. Her encouragements and calmness were always my guiding light for the duration of my Master's Degree at the University of Windsor. Her patient is most recognized and appreciated.

I also dedicate my work to my mother, Mrs. Shahlah Ejtemai, who always gives boundless supports. Her enthusiasms for my future has always kept me going and her prayers are always with me.

Finally, I would dedicate, not only this work, but also my entire successes in my academic careers, to my beloved father, Late Professor Akbar Adibi, who shined bright in his academic careers. I would consider myself extremely lucky and successful if I could be half of what he was. His permanent presence and effects in my consciousness and dreams are the vital factors in my life and academic careers. He is greatly missed, however his name and offered services will always be recognized and appreciated in the academia.

ACKNOWLEDGEMENT

I would like to thank my supervisor, Prof. Shervin Erfani, for his guidance and support, especially during the last year of my studies.

A special thanks to Prof. Mohsen Guizani for his active role as the external reader.

STATEMENT OF ORIGINALITY

I certify that this thesis, and the research to which it refers, are the product of my own work, and that any ideas or quotations from the work of other people, published or otherwise, are fully acknowledged in accordance with the standard referencing practices of the discipline. I acknowledge the helpful guidance and support of my supervisor, Professor Shervin Erfani. The published papers used in this thesis have been reflected in page 58.

I also certify that the work embodied in this thesis is the result of original research and has not been submitted for a higher degree to any other University or Institution.

TABLE OF CONTENTS

ABSTRACT.....IV

DEDICATION..... V

ACKNOWLEDGEMENTS..... VI

STATEMENT OF ORIGINALITY..... VII

LIST OF FIGURES.....XI

LIST OF ACRONYMS..... XIII

CHAPTER I INTRODUCTION 1
1.1 OSI Model..... 2
1.1.1 Layer 7 – Application Layer..... 2
1.1.2 Layer 6 – Presentation Layer.....2
1.1.3 Layer 5 – Session Layer.....2
1.1.4 Layer 4 – Transport Layer.....3
1.1.5 Layer 3 – Network Layer 3
1.1.6 Layer 2 – Data Link Layer.....3
1.1.7 Layer 1 – Physical Layer.....3
1.2 Detailed Specifications of Layers Four, Three, and Two.....4
1.2.1 Layer 4 – Transport Layer.....4
Services at Transport Layer.....5
1.2.2 Layer 3 – Network Layer.....8
Services at Network Layer.....8
1.2.3 Layer 2 – Data Link Layer.....10
REFERENCES..... 12

CHAPTER II MOBILE-IP AND MANETS..... 13
2.1 Mobile-IPv4 13
2.1.1 Mobile-IPv4 Components.....14
2.1.2 Mobile-IPv4 Mechanism..... 14
2.2 Mobile-IPv6 15
2.3 Mobile-IP Mechanisms contributing to QoS..... 18
2.3.1 Handoff/Handover..... 18
2.3.2 Multihomed Connectivity..... 19
2.3.3 Hierarchical Mobile-IPv6..... 19
2.3.4 Multipath Routing.....20
2.4 Ad-Hoc Protocols and MANETs.....21
2.5 Ad-Hoc Routing Protocols..... 22
2.5.1 Dynamic Source Routing (DSR)..... 24
DSR Mechanism.....25
2.5.2 DSR versus MSR..... 25

MSR Properties....25
2.6 Multipath in Depth for Ad-Hoc Routing Protocols.... 26
2.6.1 Multipath routing in Reactive Protocols.... 26
2.6.2 Multipath Routing in Proactive Protocols.... 26
2.6.3 Multipath Routing in Hybrid Protocols.... 27
2.6.4 Multipath Routing in Hierarchical Protocols.... 27
2.6.5 Multipath Routing in Geographic Position Assisted Routing Protocols.... 28
2.6.6 Multipath Routing in Power-Aware Protocols.... 28
2.6.7 Multipath Routing in Multicasting Protocols.... 29
2.6.8 Multipath Routing in Security Protocols.... 30
2.6.9 Summary of Multipath in Ad-Hoc Routing Protocols....30
REFERENCES.... 32

CHAPTER III QUALITY OF SERVICE (QOS) 34
3.1 Introduction to QoS 34
3.1.1 QoS from User Perspective
Planned QoS.... 34
Achieved QoS....34
User-perceived QoS.... 34
Inferred QoS 34
3.1.2 QoS from Network Perspective 34
Maximum Round-Trip Delay (MRTD)....34
Minimum Bandwidth Guaranteed (MBG).... 35
Bit Error Rate (BER).... 35
Packet Loss Ratio (PER)....35
Packet Drop Ratio (PDR).... 35
End-to-End Delay (EED)....36
Jitter (Variable Delays)....36
3.2 Multiprotocol Label Switching (MPLS)....37
3.2.1 Edge of the MPLS Domain....37
3.2.2 MPLS Domain....37
3.2.3 Features of MPLS....38
3.2.4 Summary of MPLS Mechanism.... 38
3.2.5 Traffic Engineering (TE).... 39
3.2.6 Advantages of MPLS with Mobile-IP.... 39
3.2.7 Summary of MPLS Mobile-IP Mechanism....39
3.2.8 Hierarchical MPLS Mobile-IP....40
3.2.9 IntraFDA versus InterFDA.... 40
3.3 Unique Advantages of MPLS....42
3.3.1 MPLS versus RSVP and DiffServ.... 42
REFERENCES.... 43

CHAPTER IV SIMULATION SETUP, RESULTS AND ANALYSIS 44
4.1 Overhead reduction using MSR on top of MPLS.... 44
4.1.1 Simulation Results and Network Analysis.... 46

4.2 Packet Dropout during Handoff/Handover for an MPLS-Mobile-IP-based System 46
4.3 TCP Retransmission Patterns 50
4.4 Packet Loss Ratio (PLR) in Link Layer Connectivity for Mobile-IP Ad-Hoc Networks 51
4.5 Packet Drop Ratio (PDR) for Mobile-IP Ad-Hoc Routing Protocols with Multipath Capability 52
4.6 Packet Drop Ratio (PDR) for Mobile-IP DSR/MSR on 802.11/MPLS 54
4.7 Conclusions 55
4.7.1 Proposed Scheme 55
4.8 Future Work 56
REFERENCES 57

PUBLISHED PAPERS USED IN THIS THESIS 58
SELECTED BIBLIOGRAPHY 59

APPENDIX 61

(RFC 768 62
RFC 791 62
RFC 792 65
RFC 793 67
RFC 1633 68
RFC 1883 68
RFC 2430 71
RFC 3031 72
RFC 3344 72
RFC 3775 72

VITA AUCTORIS 73

LIST OF FIGURES

1.1 Seven-Layer OSI Model 1

1.2 Logical Link Control (LLC) and Media Access Control (MAC) locations in Data Link Layer 3

1.3 Three-Way Handshaking in TCP 5

1.4 The Layer II and I portions of the 802.11 protocol 11

2.1 Mobile-IPv4 Components and Routing Schemes (RFC 3344) 15

2.2 Mobile-IPv6 Communications using Bi-Directional Tunneling 17

2.3 Mobile-IPv6 Communications using Route Optimization 17

2.4 Handoff/Handover Process in Mobile-IP 18

2.5 A Multihomed Capable Device 19

2.6 A Multihomed Device during the Handoff/Handover Procedure 19

2.7 Hierarchical Mobile-IP Routing 20

2.8 Variety of Mobile Ad-Hoc Routing Protocols 23

2.9 Ad Hoc Routing Protocols Discussed 31

3.1 MPLS Domain Edge Routers 37

3.2 A Typical MPLS Domain 38

3.3 A Hierarchical MPLS Mobile-IP Structure 40

3.4 IntraFDA Movement Update Signaling 41

3.5 InterFDA Movement Update Signaling 41

4.1 Routing overheads versus number of neighbors in a normal non-multihomed transmission environment using DSR 45

4.2 Routing overheads versus number of neighbors in a multihomed transmission environment using MSR 45

4.3 Bandwidth variations around the handoff period for MSR on top of MPLS ... 46

4.4 Handoff/Handover Period for an MPLS-Mobile-IP System with RSVP Provisioning 47

4.5 Analytical RSVP signaling after a handoff 58

4.6 Number of packet dropouts percentage in three different scenarios 49

4.7 Typical Ad-Hoc Mobile-IP Architecture..... 50
4.8 TCP Retransmission Pattern during Mobile-IP activity..... 51
4.9 The PLR pattern during Mobile-IP activity..... 52
4.10 The PDR pattern during handoff..... 53
4.11 The PDR pattern during handoff/handover for MSR/DSR on MPLS.802.11... 54

LIST OF ACRONYMS

ACK:	**Acknowledgement Packet**
ADOV:	**On Demand Distance Vector**
AntHocNet:	**Ant Agents for Hybrid Multipath Routing in Mobile Ad Hoc Networks**
AOMDV:	**On-Demand Multipath Distance Vector Protocol**
ARP:	**Address Resolution Protocol**
ATM:	**Asynchronous Transfer Mode**
BER:	**Bit Error Rate**
CGSR:	**Clusterhead-Gateway Switch Routing**
CLNS:	**Connectionless Network Service**
CN:	**Correspondence Node**
CoA:	**Care-of-Address**
CoL-CoA:	**Co-Located CoA**
CONS:	**Connection-oriented network services**
CRC:	**Cyclic Redundancy Check**
CSMA/CD:	**Carrier Sense Multiple Access – Collision Detection**
DHCP:	**Dynamic Host Configuration Protocol**
DiffServ:	**Differentiated Services**
DLL:	**Data Link Layer**
DSDV:	**Destination-Sequenced Distance-Vector Routing**
DSR:	**Dynamic Source Routing**
DUPACK:	**DUPlicate ACKnowledgment**
EED:	**End-to-End Delay**
FA:	**Foreign Agent**
FDA:	**Foreign Domain Agent**
FEC:	**Forwarding Equivalence Classes**
FSR:	**Fisheye State Routing**
FTP:	**File Transfer Protocol**
GPS:	**Global Positioning System**
HA:	**Home Agent**

HMFR:	**Hierarchical Max-Flow Routing**
HMIP:	**Hierarchical Mobile-IP**
HSR:	**Hierarchical State Routing**
HSR:	**Host Specific Routing**
HTTP:	**Hypertext Transfer Protocol**
ICMP:	**Internet Control Message Protocol**
IEEE:	**Institute of Electrical and Electronic Engineers**
IP:	**Internet Protocol**
ISO:	**Interconnection System Organization**
ITU:	**International Telecommunication Union**
LAR:	**Location Aided Routing**
LLC:	**Logical Link Control**
LSP:	**Label Switch Path**
LSR:	**Label Switch Router**
MAC:	**Media Access Control**
MANET:	**Mobile-IP Ad-Hoc Network**
MAP:	**Mobility Anchor Point**
MLAR:	**Multipath Location-Aided Routing**
M-MANET:	**MPLS-MANET**
MMRAM:	**Multi-Objective Multipath Routing Algorithm for Multicast Flows**
MN:	**Mobile Node**
MPLS:	**Multiprotocol Label Switching**
MPSR:	**Multipath Power Sensitive Routing Protocol**
MRPM:	**Multipath Multicast Routing Algorithm**
MRTP:	**Multi-Flow Real-Time Transport Protocol**
MSR:	**Multipath Source Routing**
MTS:	**Multipath TCP Security**
MTU:	**Maximum Transmission Unit**
NACK:	**Not Acknowledgement Packet**
OSI:	**Open System Interconnection**
PDR:	**Packet Drop Ratio**

PLR:	**Packet Loss Ratio**
QoS:	**Quality of Service**
RFC:	**Request For Comment**
RREP:	**Route Reply**
RREQ:	**Route Request**
RSVP :	**Resource Reservation Setup Protocol**
RTCP:	**Real-Time Transport Control Protocol**
RTP:	**Real-Time Protocol**
SMTP:	**Simple Mail Transfer Protocol**
SNMP:	**Simple Network Management Protocol**
TBRPF:	**Topology Broadcast based on Reverse-Path Forwarding**
TCP:	**Transmission Control Protocol**
TERA:	**Tree Exchange Routing Algorithm**
TTL:	**Time To Live**
TPDU:	**Transport Protocol Data Unit**
UDP:	**User Datagram Protocol**
ZHLS:	**Hierarchical Link State Routing Protocol**
ZRP:	**Zone Routing Protocol**

CHAPTER 1
INTRODUCTION

Tracing the development of Mobile-IP and the need for Quality of Service (QoS) from customer standpoint is driving vendors to integrate existing technologies to integrate with Mobile-IP to offer more services with better quality.

At this fast pace of development in recent years, there is a sense that IP (IPv6 more specifically for better QoS support) is going to be involved more and more in wireless applications. The current IETF standards for mobility (RFC 3344 for IPv4 and RFC 3775 for IPv6) are mostly concerned with a number of micro-mobility issues, however there is still much more to be done as far as QoS is concerned. The deployment of broadband wireless technologies could be the answer in the short run, nevertheless appropriate conventions and protocols to support major changes for QoS are inevitable. Ad-hoc networks, Mobile-IP Ad-Hoc Networks (MANETs) in general, which contains freely moveable nodes in non-infrastructure routing structures, are another example of how existing technologies could open new possibilities for load-sharing and efficient routing in Mobile-IP applications.

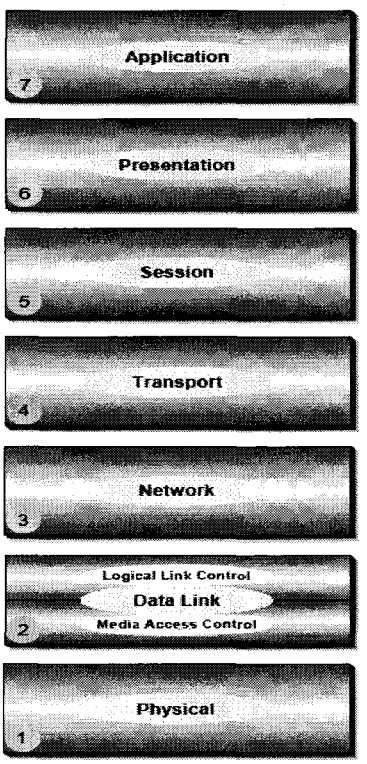


Figure 1.1. Seven-Layer OSI Model

In this section, an overview of the OSI model and services is presented. Seven-Layer OSI (Open System Interconnection) model is a good starting point to tap into the communication systems. By definition [1,7], "the Seven-Layer model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy." The summary of each layer's functionality is given blow [1,2,7,8].

1.1 OSI Model

OSI Model presents a seven-layer architecture (Figure 1.1) for interconnecting heterogeneous devices through various physical networks interconnected. The sub-layers are defined as follows:

1.1.1 Layer 7: APPLICATION Layer

This ***message*** driven layer, provides the interface to the network for the transmission of messages. Such as, FTP (File Transfer Protocol), HTTP (Hypertext Transfer Protocol), TELNET, SMTP (Simple Mail Transfer Protocol), and SNMP (Simple Network Management Protocol) function at this layer.

1.1.2 Layer 6: PRESENTATION Layer

This ***format*** driven layer, provides the data transfer syntax. If required, user-level encryption/decryption, compression/expansion and formats take place at this layer. Messages are broken down and formatted for the receiving application appropriately.

1.1.3 Layer 5: SESSION Layer

This ***dialog*** driven layer, handles dialog control and manages communication sessions by establishing, maintaining, and synchronizing the dialog via hand-shaking, security, and mechanics of an ongoing connection for the transmission of packets.

1.1.4 Layer 4: TRANSPORT Layer

This ***segment*** driven, matches messages to the capabilities and restrictions of the network medium. Messages are divided into segments for transmission and reassembled at their destination. This layer supports flow control, and multiplexing.

1.1.5 Layer 3: NETWORK Layer

This ***datagram*** driven layer, deals with addressing of data delivery, providing the switching and routing technologies, creating logical paths, known as virtual circuits for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as, error handling, congestion control and packet sequencing.

1.1.6 Layer 2: DATA LINK Layer

This ***frame*** driven layer is concerned with providing context to the Physical layer by formatting the bits into frames and assigning a physical address. The data link layer is divided into two sublayers (Figure 1.1): The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.

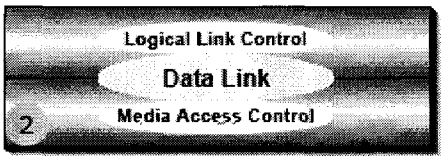


Figure 1.1. Logical Link Control (LLC) and Media Access Control (MAC) locations in Data Link Layer

1.1.7 Layer 1: PHYSICAL Layer

This ***bit*** driven layer deals with the physical structure of a network, connection specifications, and data encoding and decoding for data transfer.

The main focus of this thesis lies between layers 2 and 3. However, to maintain continuity within the Seven-Layer architecture, layers 2 and 4 would also be discussed.

1.2 Detailed Specifications of Layers Four, Three, and Two

1.2.1 LAYER 4: Transport Layer

Transport layer occupies the fourth location on top of the seven-layer OSI model. This layer is concerned with the efficient end-to-end communications between peers. Other aspects of this layer include reliability and data transport, all the way from the source to the destination, independently of the physical network. QoS categories on multiplayer dimensions start to be effective from this layer. Five different classes, as part of QoS definition at the Transport Layer, are defined here [1]:

- **Simple class:** This simple class works with minimal services with only one network connection for each transport connection. The only functions available are for establishment, data transfer with segmenting and error reporting with no multiplexing and only parameters available are address and TPDU (Transport Protocol Data Unit) size.

- **Basic error recovery class:** Similar to the simple class with the exception of network resets, which maintains TPDU sequence numbering and basic transport connections with minimal overheads

- **Multiplexing class:** This class provides a method for multiplexing several transport connections onto a single network connection. The underlying network is assumed to be fully reliable.

- **Error recovery class:** This supports the lower classes and the ability to recover from network disconnect or reset

- **Error detection and recovery class:** This integrates the ability to detect and recover from errors, which occur as a result of the low grade of service with extensive error detection and handling features (i.e., sequence numbering, CRC checking, timeouts, and TPDU retransmissions).

Another category of this layer specifies two major divisions of communications: *Connection-oriented* and *connectionless* communications, which is discussed below:

- **Connection-Oriented versus Connectionless:** Connection-oriented protocols ensure reliable transfer of data with extensive signaling. This, however, adds to the overhead of the frames and makes it less attractive for real-time applications. On the other hand, connectionless protocols lack the reliability and are less complex and faster. An example of connection-oriented protocol is Transmission Control Protocol (TCP) (RFC 793) and a connectionless protocol is User Datagram Protocol (UDP) (RFC 768) (see APPANDIX).

Transport layer protocols are defined by ISO 8072 (OSI transport service), ISO 8073 (OSI transport protocols), and ITU X.214 and X.224 [2].

Services at Transport Layer

The services to be discussed here, which contribute to the QoS, are:

Three-Way Handshaking

TCP differs from UDP in many aspects, one of which is the data handling method. In UDP, datagrams are sent without further provisioning. No guarantee that the receiver has received the packets. In TCP, a socket (a flow-controlled connection with a port number and a destination IP address) is set up and the three-way handshaking makes sure the receiver (Fig. 1.1) has received it.

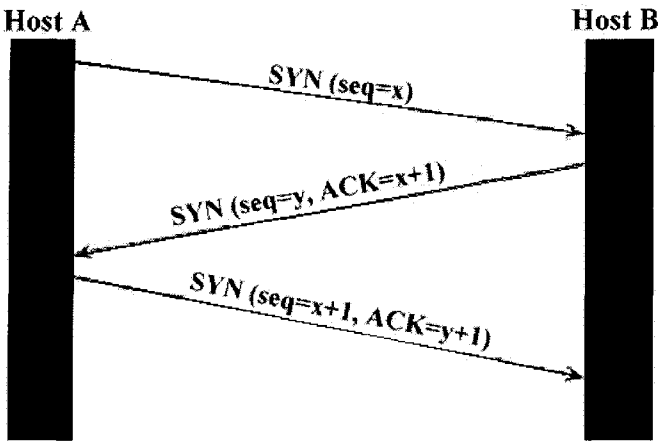


Figure 1.3. Three-Way Handshaking in TCP

Port Numbers

Through port numbers, specific application on the sender's interface could be talking to a specific application on the receiver's interface. Transport layer provides facilities for one-to-one, one-to-many, many-to-one, and many-to-many, simultaneous connectivity through what Session Layer can offer.

Message Segmentation:

This service accepts a message, which can be very large, from the layer above and splits the message, if not already small enough, into smaller units. Then it attaches its own header along with sequence number and other information and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message

Message Traffic Control:

This service informs the sending station to back-off when no message buffers are available and in the case of buffer availability, it tracks the order of packets sent and received using Sequence Number

Message Acknowledgment:

Provides reliable end-to-end message delivery with acknowledgments. This acknowledgement message is very important for the sender to make sure the recipient received the previous message.

Session Multiplexing:

Multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions

Loss and Duplication Control:

TCP, through message acknowledgement, ensures that the recipient has received the messages error-free and through loss and duplication control mechanism, it ensures that no message is lost or received duplicates

Packet Loss Ratio (PLR):

PLR rises when the receiver receives packets with large delays (larger than a margin value) or the packets are lost before reaching the receiver. Packet loss happens when the receiver is unable to receive the packet. In any case, the receiver would generate and send a NACK (Not Acknowledgement) signal to the sender. Too many *retransmissions* would also increase PLR. In this case, retransmissions happen when a packet is not received by the receiver, which a NACK would be generated and sent to the sender or when the ACK (Acknowledgement), generated by the receiver, is not received by the sender. In either case, if the packet is lost or the ACK-NACK is lost, the sender will have to send the packet again. The retransmission pattern is another indicator showing the performance of the transmitting devices and the communication channel.

1.2.2 LAYER 3 - Network Layer

The network layer provides the essential internetwork routing services required for a packet to move one step or more, closer to the destination, based on specific metrics, according to the network protocol. ITUX.213, ISO 8348, ISO 8648, and ISOP 8880 specify network layer requirements.

There are two different categories that specify network layer services: (a) Connection-oriented network services (CONS), such ATM (Asynchronous Transfer Mode), in which physical circuit has to be established before data transmission, and (b) Connectionless Network Service (CLNS) in which packets are switched either on-demand or proactively, such as in IP. These two services work hand-in-hand with connection-oriented and connectionless categories under Transport Layer definition.

Services at Network Layer

The following services, disregards of being CONS or CLNS, are defined at network layer:

Routing

Each routing protocol specifies a set of algorithm in which packets are forwarded to an appropriate route towards the destination. The criteria and method is specific to every individual routing algorithm. Routing protocols are further subdivided into **Distance Vector** routing protocols and **Link-State** routing protocols.

Frame Fragmentation

The transmitting router always needs to specify the capacity of the downstream route. If it determines that the downstream router's maximum transmission unit (MTU) size is less than the frame size with original data length, the router would fragment a frame to fit the MTU size. The correct fragmentation and reassembly at the receiving end will take place at this layer.

Logical-Physical Address Mapping

The translation of logical address or names onto physical addresses takes place within this layer. An example of such a service is given by Address Resolution Protocol (ARP) (RFC 826).

Subnet Usage Accounting

This has accounting functions to keep track of frames forwarded by particular subnet intermediate systems to produce billing information.

Internet Protocol version 4 (IPv4)

IPv4 is based on the Internet standard proposed by RFC 791 and was released in September 1981 (see APPNEDIX).

Internet Protocol version 6 (IPv6)

IPv6 is based on RFC 1883 (updated by RFC 2460) and was released in December 1995 (see APPNEDIX).

Internet Control Message Protocol ICMP

ICMP (RFC 792, see APPENDIX) is on top of IP Layer and is used for informing hosts of problems in delivering IP messages. Problems may be caused by several reasons:

- A host or a router was too busy to process the datagram
- A datagram was discarded because its TTL became 0
- The header checksum did not match
- The requested service or port number was not available on the destination host
- No other communication involved, therefore does not require a transport protocol

1.2.3 LAYER 2 - Data Link Layer

This layer is further sub-layered as Logical Link Layer (LLC) and Media Access Control (MAC) layer. This split is based on the architecture used in the IEEE 802 project, which specifies the following:

- **Logical Link Control (LLC):** Refers to the function required for the establishment and control of logical links between devices on a network (IEEE 802.2) and their relations to the physical addresses
- **Media Access Control (MAC):** Refers to the procedures used by devices to control access to the network medium, such as: CSMA/CD, 802.11.

The other functions related to this layer are: *Data Framing*, which is the final encapsulation of higher-level messages into frames, which are further handled by physical layer. *Addressing*, which is the labelling information for a particular destination with a unique identifier on the same network (MAC address), and the *Error Detection and Handling* through the Cyclic Redundancy Check (CRC).

The Physical Layer and the Data Link Layer are very closely related. The requirements for the physical layer of a network are often part of the data link layer definition of particular technology. For example the DLL tunes the transmit power of the physical layer based on the bit-error rate information from the physical layer [5]. According to reference [3], the implementation considers the cross-layer feedback in the Mobile Node (MN) since it is believed that it would be easier to implement changes on the end-devices than in the network. Also the ultimate goal for improving application performance on wireless devices is the user satisfaction, therefore it is essential to incorporate dynamic user requirements into the protocol stack, such as applying application priorities dynamically. Network interface optimization is also important to minimize power consumption.

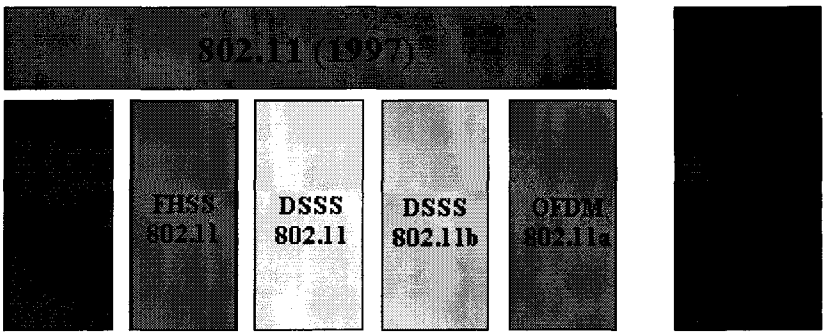


Figure 1.4. The Layer II and I portions of the 802.11 protocol

Figure 1.2 shows the MAC layer and Physical layer interactions of the protocol 802.11, which depicts clear connections between Physical and MAC layers. IEEE 802.11 MAC layer [4] functions not only manage and coordinate the access to the transmission channel, it is also responsible for the authentication and other management and security duties to some extend. [5] Uses the approach of protocol harmonization to reduce energy consumption for the sending process of an IEEE 802.11 WLAN. The results clearly indicate a strong correlation between MAC and the physical layer. A wrongly selected transmission power may result in unnecessary consumed energy. Therefore every MAC protocol needs a fine-tuning according to the underlying physical layer and the channel characteristics. The study concludes that there is an optimal transmission power for every packet size. It also concludes that the packet size should be as large as possible, especially for low BERs. Reference [6] Indicates that physical layer restraints both routing and MAC decisions by altering the directed topology graph.

REFERENCES

[1] Martin John Baker http://www.euclideanspace.com/coms/protocol/osi/layer4/

[2] Sasan Adibi, "Computer Networks. Presentation at the University of Waterloo", Summer 2004

[3] Vijay T. Raisinghani, Sridhar Lyer, "Cross-layer design optimization in wireless protocol stacks", Elsevier Computer Science, Computer Communications 2003

[4] SMC Networks Training, 2003

[5] Jean-Pierre Ebert and Adam Wolisz, "Power Saving in Wireless LANs: Analyzing the RF Transmission Power and MAC Retransmission Trade-Off", European Wireless '99 and ITG Fachtagnung Mobile Kommunikation, October 1999, Munchen, Germany

[6] UlasC. Kozat, IordanisKoutsopoulos, LeandrosTassiulas, "A Framework for Cross-layer Design of Energy-efficient Communication with QoS Provisioning in Multi-hop Wireless Networks", IEEE INFOCOM, 2004

[7] Webopedia Website

[8] David D. Scribner Webpage (http://pages.prodigy.net/dscribner/pub/osi_layers.pdf)

[9] Internet FAQ Archives (http://www.faqs.org/) and throughout this thesis wherever an RFC is described and used

CHAPTER 2
MOBILE-IP AND MANETS

Internet Protocol was invented in early 80s when mobility was not considered, however due to the progress of mobile communications and the urge for Internet connectivity on mobile nodes (MN), researchers tried variety of methods to enable wireless devices to support IP connectivity to the Internet. These resulted in early drafts of Mobile-IPv4, "IP Mobility Support", created by C. Perkins in October 1996 (RFC 2002), which was upgraded by the same author, in August 2002 as, "IP Mobility Support for IPv4 (RFC 3344)". The IPv6 version of IP-Mobility (Mobile-IPv6) "Mobility Support in IPv6, RFC 3775, was created by D. Johnson, C. Perkins, and J. Arkko, in June 2004. Many mobility issues have been considered in IPv6 including [1]: Increase of address space, simplified header, security-mandated, address auto-configuration, destination options. Mobile-IPv6, as well, has been enjoying these features from IPv6 and the structures of mobile-IP infrastructures have been updated to welcome these features.

By 2008, the entire industry has been mandated to switch the Internet Protocol (IP) driven technologies to IPv6 [1]. IPv6, by far, has proven to address many micro-mobility issues and facilitate the mobile-IP operation by its simplified structure and operational units. Therefore Mobile-IPv6 will be the main focus in this thesis. However a quick glance at Mobile-IPv4 will be presented at first.

Definition: Mobile-IP is a set of protocols that enables a mobile node to keep its connectivity to the Internet while moving.

2.1 Mobile-IPv4

This draft specifies an Internet standards track protocol for the Internet community, and divides the entire Mobile-IPv4 scheme into the following sections:

- Agent Discovery (Advertisement, Solicitation and Node Considerations)
- Registration (Authentication, Request and Reply messages
- Routing Consideration
- Security Considerations

2.1.1 *Mobile-IPv4 Components:*

In Mobile-IPv4 (Figure 2.1), four components are defined:

- Mobile Node (MN), which is the actual mobile device (laptop or a cell-phone) with Internet connectivity capability, which moves freely
- Home Agent (HA), where the MN is initially registered and the main server in which serves the MN when it is located in the home network. HA is the permanent address of the MN, when MN is away and reroutes the incoming packets, through encapsulation, to the Foreign Agent, which is the current server, serving MN at the specific point in time
- Foreign Agent (FA), as stated, FA is the router, serving a routing domain in which, the MN is currently passing though its region. FA is responsible for providing a Care-of-Address (CoA) for the MN or registering the MN Co-Located CoA (CoL-CoA) and decapsulating the incoming packets from HA and handing them to MN, and
- Correspondence Node (CN), which is an auxiliary router on the Internet in direct communication with MN through HA and helps forwarding packets from MN to other destinations.

2.1.2 *Mobile-IPv4 Mechanism*

- **Agent Discovery**
  - HA and FA advertise their availability on each link for which they provide service
  - A newly arrived MN sends a solicitation to learn if any prospective agent is present
- **Registration**
  - When MN away from home, it registers its CoL-CoA or its assigned CoA with HA
  - The registration is done with HA either directly or through the FA

    Mobility agents (i.e., FA and HA) advertise their presence via *Agent Advertisement* messages. When FA detected, it acquires a *care-of address* through FA or DHCP

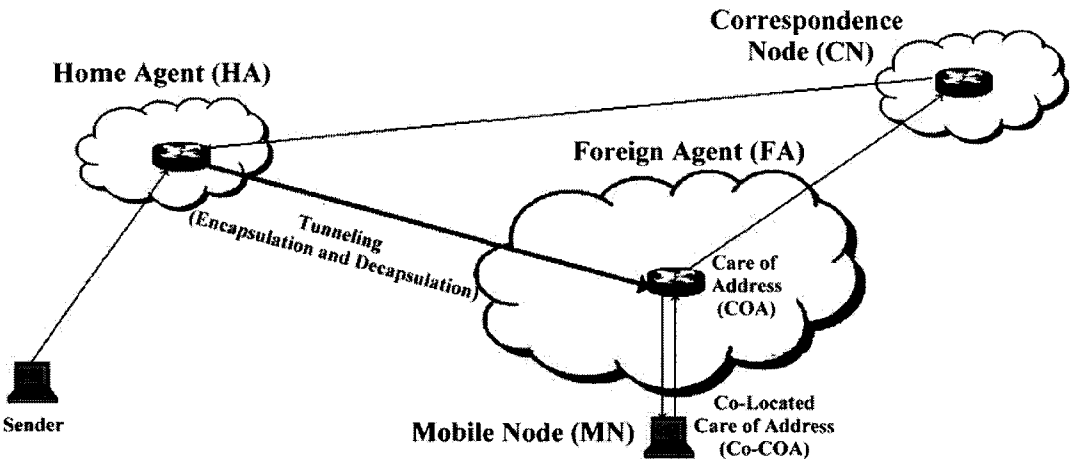


Figure 2.1 Mobile-IPv4 Components and Routing Schemes (RFC 3344)

2.2 Mobile-IPv6

Mobile-IPv6 shares many features with Mobile-IPv4, however the following differences are noticed:

- The deployment of FA in Mobile-IPv6 is optional, however in many proposed schemes using Mobile-IP, similar functional units were proposed. Mobile-IPv6, in general, can operate without the presence of a local router
    - Functional units are: MN, HA, and CN
- The route optimization is an integral part of the protocol
- Prearranged security associates are not mandated as Mobile-IPv6 is able to operate secure enough through route optimization, which also solves the *ingress filtering* problem as well
- Encapsulation and Decapsulation are optional as most packets sent from HA use IPv6 routing header for overhead reduction compared to Mobile-IPv4
- Using IPv6 *Neighbor Discovery* instead of ARP, decouples the Mobile-IPv6 from any particular link layer protocol, thus robustness and independency are assured
- Through the use of *dynamic home agent address discovery* mechanism in Mobile IPv6, triangle routing inefficiencies are eliminated.

The summary of changes compared to Mobility IPv4 is stated below:

- Four new IPv6 destination options are defined:
  - *Binding update option*
  - *Binding acknowledgement*
  - *Binding request, and*
  - *Home address option*
- Two ICMP message are defined for "Dynamic Home Agent Address Discovery":
  - *ICMP home agent address discovery request message*, and
  - *ICMP home agent address discovery reply message*
- Two new IPv4 options for "Neighbor Discovery"
  - *Advertisement interval option*, and
  - *Home agent information option*

In simpler words, the main features of IPv6, which makes IPv6 an attractive network protocol for Mobile-IP applications [1,2] are:

- Foreign Agents (FAs) no more necessary
- Sufficient number of IP addresses
- Simplified header
- Fragmentation based in the sender only
- Mandate security header implementation
- Destination options for efficient routing
- Address auto-configuration
- Avoidance of ingress filtering, and
- Error recovery without soft-state bottleneck

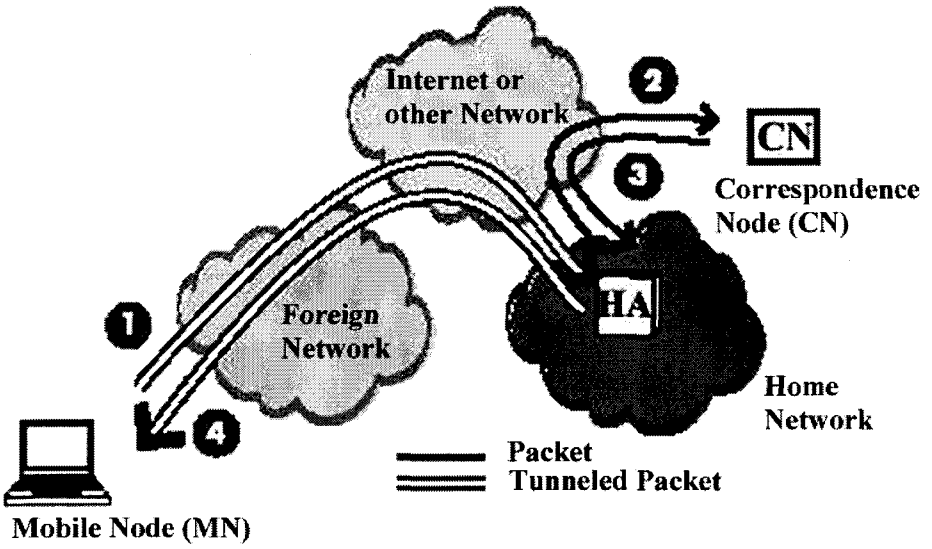


Figure 2.2 Mobile-IPv6 Communications using Bi-Directional Tunneling

Figures 2.2 and 2.3 show the efficient and simplified communication schemes between these three entities using bi-directional tunneling, where HA is in direct communication with MN and CN separately and in Figure 2.3 using route optimization where MN is in direct communication with CN [2]. Reference [2] further specifies the modified ICMP request messages used for Dynamic Home Agent Address Discovery and the protocol overview, which shows improvements in handoff/handover and QoS for Mobile-IPv6, which uses an architecture that integrates InterServ and DiffServ and the extended signaling for Mobile-IPv6 purposes.

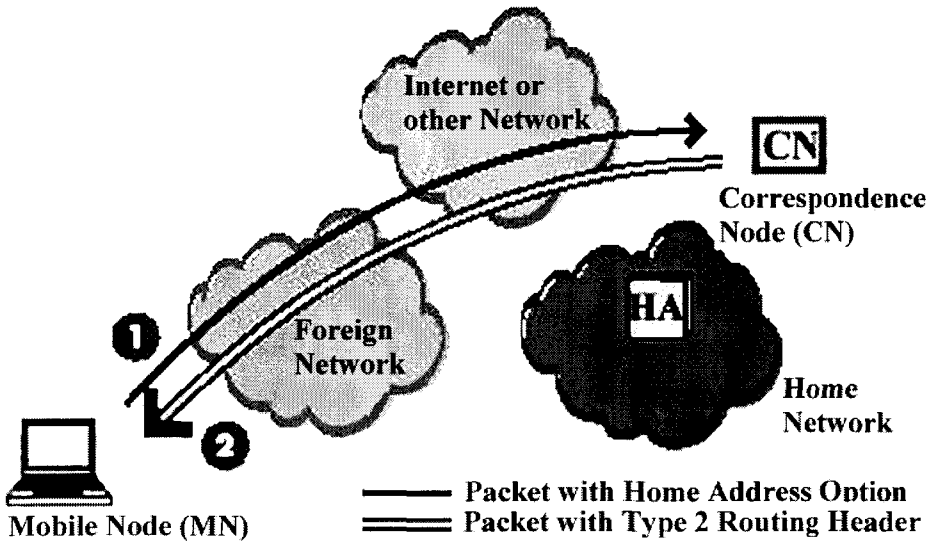


Figure 2.3 Mobile-IPv6 Communications using Route Optimization

2.3 Mobile-IP Mechanisms contributing to QoS

The contribution to QoS is the main concern in this thesis and in this, parts of the mechanisms in which Mobile-IP go through its entire operations, will be discussed, which directly or indirectly contribute to the quality of the service Mobile-IP provide, both to the end-users and from network perspective.

2.3.1 Handoff/Handover

During the operation of MN, it frequently happens when a MN needs to change its point of attachments. This starts from the very moment MN registers its CoL-CoA with the HA. The first thing a MN would do when departing the HA region is to handoff from the HA link and handover its connection to the next available foreign domain. This mechanism repeats itself continually until MN reaches back to its HA region. One of the major issues in this process is, the handoff link (from the Foreign Network 1), normally has to be physically broken before handing-over to the Foreign Network 2 via the handover link. This link breakage contributes to packet loss, bandwidth drop, degradation of QoS and other major quality problems in Mobile-IP applications, especially crucial to real-time applications. This process is depicted in Figure 2.4.

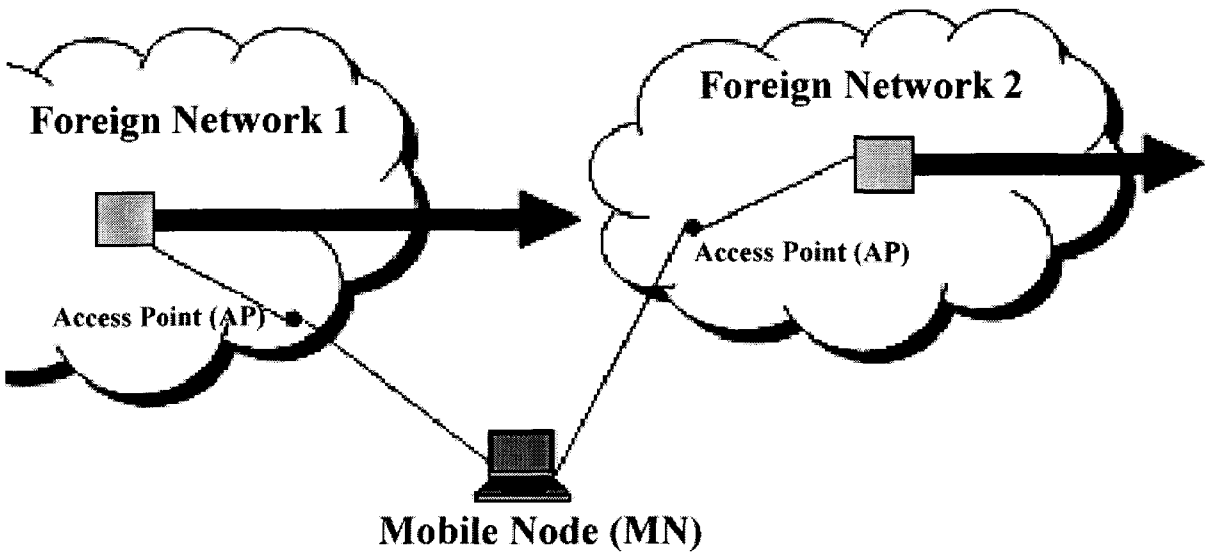


Figure 2.4 Handoff/Handover Process in Mobile-IP

2.3.2 *Multihomed Connectivity*

One of the remedies to link breakage during handoff/handover procedure is the use of multihomed capable devices. Figure 2.5 shows a typical multihomed mobile device.

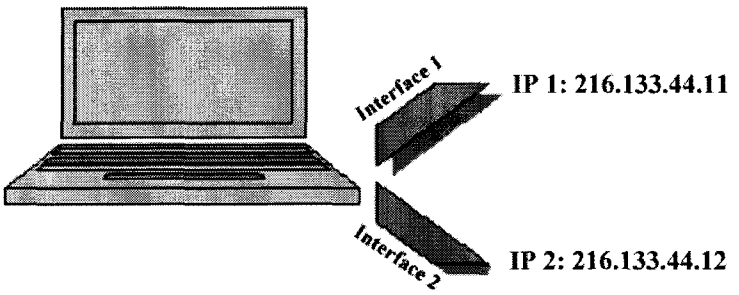


Figure 2.5 A Multihomed Capable Device

Using multihomed devices will facilitate handoff/handover procedure, as shown in Figure 2.6. This will not only preserve at least one link during the handoff/handover process for maintaining QoS, but also, the load sharing, which is crucial for balancing heavy loads, having redundant paths and security issues will also be provided.

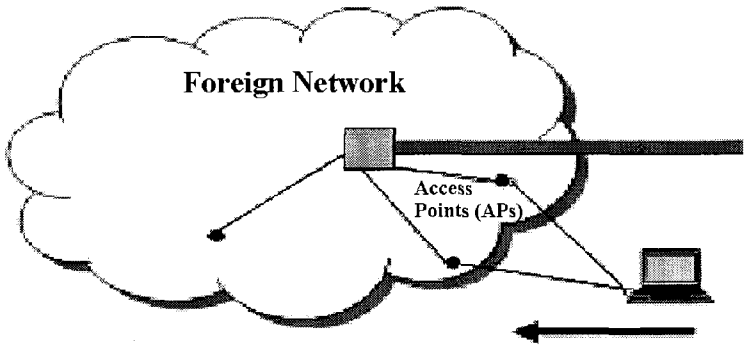


Figure 2.6 A Multihomed Device during the Handoff/Handover Procedure

2.3.3 *Hierarchical Mobile-IPv6*

Hierarchical Mobile-IP (HMIP) as opposed to the flat topology Mobile-IP is a micro-mobility management model. Its purpose is to reduce the amount of signalling between Mobile-IP entities (MN, CN, and HA), especially during the handoff/handover procedure. For this purpose, new components such as mobility anchor point (MAP) and Foreign Domain Agent (FDA, for MPLS-based entities) will be introduced later [4]. These new components perform similar as FA, however their purpose is different. The MN movement falls into two categories, *Local* and *Global*:

- *Local Movement of MN*: As depicted in Figure 2.7, the purpose of a hierarchical Mobile-IP is to keep local movements traffic within the local administration. For example, when MN is changing its access points in Domain 1 (from AP1 to AP2), HA does not have to informed and only MAP1 oversees the process and as long as MN is inside of Domain 1, the packets sent to MN from HA, will be received by MAP1 and MAP1 knows where inside Domain 1 to find MN. This will reduce excessive overhead of registration, acknowledgement, request, and reply messages from MN to HA and back, for local movements
- *Global Movement of MN*: When MN changes the domains, namely, from Domain 1 to Domain 2, at this point, HA needs to be informed and HA has to forward packets destined to MN not through MAP1 but through MAP2. This requires inevitable signalling and handshaking to be done for this transition

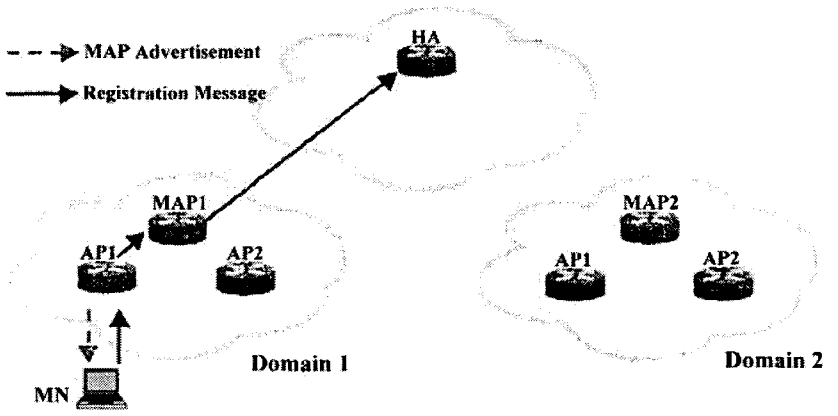


Figure 2.7 Hierarchical Mobile-IP Routing

2.3.4 Multipath Routing

Most routing protocols maintain routing tables to store the next hop towards the desired destination. Many routing protocols preserve a caching mechanism by which multiple routing paths to the same destination are stored. Multipath routing is essential for load balancing and offering quality of service. Other benefits of multipath routing include [3]: the reduction of computing time that routers' CPUs require, high resilience to path breaks, high call acceptance ratio (in voice applications), and better security. Special attention should be given to transport layer protocols as duplicate acknowledgments (DUPACKs) could occur, which might lead to excessive power consumption and congestion. Multipath routing and multihomed connectivity come hand-in-hand and co-exist nicely.

2.4 Ad-Hoc Protocols and MANETs

In addition to cellular networks, ad-hoc network is another network architecture for wireless networks. Ad-hoc network is a non-infrastructure architecture in which nodes can access and offer services from any of the ad-hoc elements located in the wireless range. It is believed that having ad-hoc elements as the main communication elements, will add fidelity to the nature of the communication, as variety of routing protocols, specific to each ad-hoc network scheme, are defined and it is a versatile issue to be able to use a specific routing protocol best suited for the communication needs. Due to the flexible nature of ad-hoc elements, most flexible applications and scenarios are also possible using ad-hoc networks. In general the following properties, specific to ad-hoc networks, are of vital importance in micro-mobility trends [5]:

- Managing local movements without informing the core network
- Decreasing the update traffic for new locations
- Limiting the diffusion of update messages
- Minimizing the delay in the new location update
- Providing superior QoS and support real-time services
- Defining optimal radio resource use
- Supporting paging
- Interacting with Mobile-IP
- Being Radio technology independency
- Insuring robustness and Scalability

Mobile Ad-Hoc Network (MANET): A MANET is defined as a collection of mobile platforms or nodes, which are free to move about arbitrarily as expected in ad-hoc networks. Therefore all the specifications held for mobile-IP and ad-hoc networks would naturally hold for MANETs. To list a few:

- Dynamic topologies
- Dynamic protocols
- Bandwidth-constrained, variable capacity links
- Energy-constrained operation, and
- Limited physical security

2.5 Ad-Hoc Routing Protocols

Ad-Hoc Routing Protocols fall into the following groups:

- **Flat Routing Protocols**
  - Proactive Routing (Table-Driven)
  - Reactive Routing (On-Demand)
  - Hybrid Routing (blend of Reactive and Proactive)

- **Hierarchical (Zone/Cluster-Based) Routing Protocols**
- **Geographic Position Assisted Routing Protocols**
- **Power-Aware Routing Protocols**
- **Security-Aware Routing Protocols**
- **Routing Protocols with Efficient Flooding Mechanisms**
- **Multicasting Routing Protocols**
  - Geographical Multicast (Geocasting)
  - Tree-Based
  - Mesh-Based
  - Zone Routing
  - Associativity-Based
  - Differential-Destination
  - Weight-Based
  - Preferred Link-based

The first three groups (Flat "Proactive, Reactive, and Hybrid", Hierarchical, and Geographical Position Assisted) are of particular important. Hierarchical MANETs specially use the hierarchical Mobile-IP structures for their routing schemes. Figure 2.8 shows these three categories and the related routing protocols.

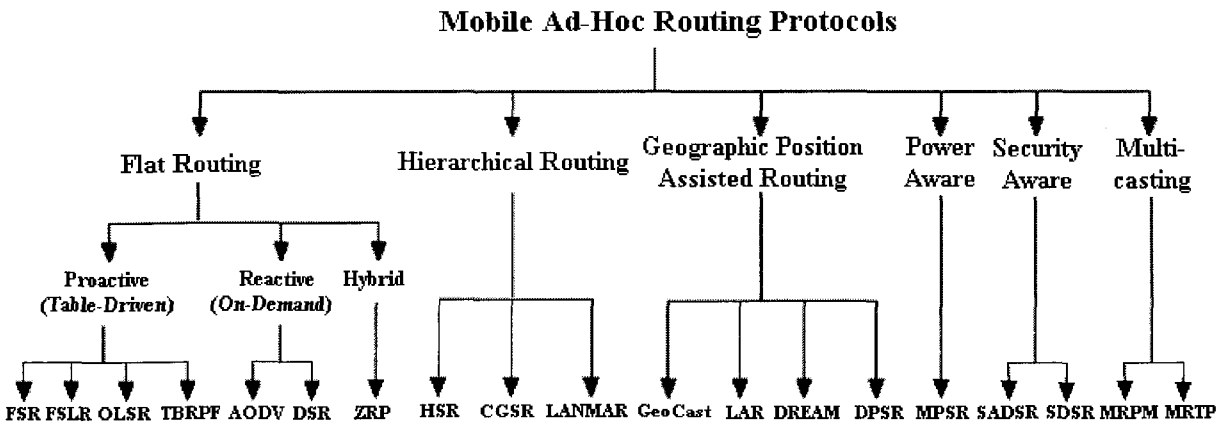


Figure 2.8. Variety of Mobile Ad-Hoc Routing Protocols

It is shown (Figure 2.8) that, ad-hoc routing protocols fall into three major vertical and two horizontal categories. The vertical categories are: *Flat, Hierarchical,* and *Geographic Position Assisted Routing.* Horizontal categories are: *Reactive (On-Demand)* and *Proactive (Table-Driven).* Reactive (on-demand) protocols create routes only when the packet is ready to be sent. Therefore routes to the destinations are not known before the packets are ready to be routed. When a node requires a route to destination, it initiates route discovery process starting from the transmitting node. This process completes once the best route is found from all possible route permutations. Examples of this category are: Ad Hoc On Demand Distance Vector (ADOV), and Dynamic Source Routing (DSR).

Proactive protocols, on the other hand, are table-driven and nodes continuously search for routing information within a network to complete the routing tables. Therefore when a packet is ready to be routed, the route is already known. This makes routing fast, however maintaining large tables is difficult. Examples of this category are: Fisheye State Routing (FSR) and Topology Broadcast based on Reverse-Path Forwarding (TBRPF).

The vertical category is comprised of *Flat, Hierarchical,* and *Geographically Position Assisted Routing.* In flat routing, all ad hoc elements are of the same level, while in hierarchical routing protocols, there is grouping of individual elements or clusters to perform tasks while others wait until the task is handed over to the next level. Examples of this category are: Host Specific Routing (HSR) and Clusterhead-Gateway Switch Routing (CGSR). The last category uses the position of nodes "i.e., Global Positioning System (GPS)" for an efficient routing, i.e., Location Aided Routing (LAR).

2.5.1 *Dynamic Source Routing (DSR)*

DSR is one of the most important routing protocols. In one of our simulations, we consider DSR and one of its flavors, MSR (Multipath Source Routing). The main attributes of DSR are:

- **Quick Adaptation:** The protocol adapts quickly to routing changes and network dynamics, specially when host movement is frequent, unlike other distant vector protocols
- **Little Overhead:** Requires little or no overhead during periods in which hosts move less frequently
    - Based on simulations, the packet overhead is less than %1 of the total traffic [23]
    - Source Routing causes the sender to determine the complete sequence of nodes through which to forward the packet, the list of this route is explicitly in the header
    - No periodic router advertisement
- The protocol is based on *Distant Vector* routing protocols
    - Each router broadcasts to each of its neighbor routers, its view of the distance to all hosts and shortest path is calculated based on metrics
    - **Route discovery:** The cache of DSR is based on dynamic route finding
    - **Battery preserve:** Preserving the battery energy is based on the fact that DSR does not send and receive advertisements on regular bases. This is where DSR is different than conventional *distant vector* protocols
    - **Bi-directional:** In DSR, bi-directional transmission is not required because every thing is based on broadcasting

DSR Mechanism

- A *Source Route* has to be constructed in the packet header giving all the hops the packet should go through to the destination
- All hops update their *route caches* when they receive new information
- *Route discovery* is issued when a hop receives a packet with no destination entry. Each route discovery is consisted of the following information:
    - *Route request*
    - *Route reply*
    - *Route record*
    - *Route ID*: This is a vital information in order to distinguish between multiple *route requests* received, i.e., <initiator address, *route id*>

- While waiting for the *route discovery* reply, DSR performs normal operation and buffers the unknown destination packet in its buffer
- The monitoring of the wellness of routes is done by *route maintenance*

2.5.2 DSR versus MSR

MSR is an extension of the DSR protocol. It consists of a scheme to distribute traffic among multiple routes in a network, while using the same route discovery process as in DSR with the exception that multiple paths can be returned, instead of only one route. Upon receiving a packet for routing, if the destination has no entry in the cache, MSR initiates a route discovery by flooding a **RREQ *(Route Request).*** Once the RREQ reaches the destination, a **RREP *(Route Reply)*** will reverse the route in the route record of the RREQ and traverse back through this route. Each received route is given a unique index and stored in the cache. Independency between paths is very important, therefore *disjoint* paths are preferred.

MSR Properties

To summarized MSR properties, MSR:

- MSR is a flat-topology and re-active protocol (on-demand), an extension of DSR
- Appropriate paths calculated between nodes
- Efficient packet forwarding on calculated paths
- Effective end-host usage of multiple paths
- **Provides multiple paths from a source to a destination**
- Provides loop-free paths
- **Provides disjoint paths**
- **Traffic load is distributed (based on delay; lower delay means more traffic for a specific time)**
- Complete route(s) known at source

2.6 Multipath in Depth for Ad-Hoc Routing Protocols

2.6.1 Multipath routing in Reactive Protocols

On-demand routing protocols are inherently attractive for multipath routing, because of faster and more efficient recovery from route failures. *MSR "Multipath Source Routing Protocol"* [6] is an example of such protocols that supports multipath routing. MSR is a direct descendant of DSR. By incorporating the multipath mechanism into DSR and employing a probing based load-balancing mechanism, the throughput, end-to-end delay, and drop-rate have been improved greatly. The drawback of MSR would be the processing overload of originating the packets, which could become more negligible as the processing power of computers increase day-by-day. Another routing protocol offering multipath routing in this category is the *AOMDV "On-Demand Multipath Distance Vector Protocol"* [7], that extends the single path AODV protocol to compute multiple paths. There are two parts in AOMDV contributing to multipath routing, one of which is the notion of an advertised hop-count to maintain multiple loop-free paths at each nodes and the other is the modification of route discovery mechanism in the AODV protocol for link-disjoint multiple paths from source and intermediate nodes to the destination. Under wide range of mobility traffic scenarios, AOMDV offers a significant reduction in delay and up to 20% reduction in the routing load and the frequency of route discoveries.

2.6.2 Multipath Routing in Proactive Protocols

Proactive routing algorithms, such as DSDV "Destination-Sequenced Distance-Vector Routing" [8], maintain route updates among all nodes all the time. In fact, many proactive protocols tend to offer shortest path to each destinations. This is done by continuously monitoring the network topology. Unlike reactive routing algorithms, proactive routing protocols are capable of repairing broken routes in a short time. This is done by collecting network topology continuously. The drawback of DSDV however is the requirement of parameters such as the periodic update interval, maximum value of the "settling time" for a destination and the number of update intervals, which may become known before a route is considered stale. These parameters will likely represent a tradeoff between the latency of valid routing information and excessive communication overhead [10]. Another example of proactive routing protocol is discussed in [9]. *TERA "Tree Exchange Routing Algorithm"* is an extension to standard distance vector routing

algorithms, which is based on multipath. This paper discusses the necessary modifications to enable multipath routing. This modification does not require any additional messages, therefore no extra cost is incurred to add multipath capability to the scheme.

2.6.3 Multipath Routing in Hybrid Protocols

Hybrid routing protocols incorporate the merits of both on-demand and proactive routing protocols. An example of this category is *Zone Routing Protocol "ZRP"*, which is similar to a cluster with the exception that each node acts as a cluster head and a member of other clusters. The routing zone forms a few mobile ad hoc nodes within one, two or more hops away where the central node is located. The fact that both reactive and proactive schemes are found in the functionality of hybrid routing protocols, better performance is expected. However, due to hierarchical nature of the schemes more memory will be required compared to the identical reactive or proactive scheme [10]. Reference [11] describes another hybrid algorithm, *AntHocNet "Ant Agents for Hybrid Multipath Routing in Mobile Ad Hoc Networks"*, an ACO algorithm for routing in MANETs. The route setup of this scheme is performed by reactive algorithm and the route probing and exploration are done by proactive scheme. The related simulation experiments show that AntHocNet can outperform AODV in terms of delivery ratio and average delay, especially in more mobile and larger networks. Scalability is also promising in this scheme. However, relatively large amount of overhead could be mentioned as a drawback and also less adaptability to the network situation.

2.6.4 Multipath Routing in Hierarchical Protocols

Hierarchical routing protocols tend to avoid excessive overhead by limiting the local traffic to the local management and only global movements are reported between zones/hierarchical layers. This, on the other hand, increases the complexity of the routing schemes. In [12] a technique is proposed to reduce the computational complexity of max-flow routing, based on a hierarchical decomposition of the network (*Hierarchical Max-Flow Routing "HMFR"*). Max-flow routing forwards packets in such a way that the impact of failures is minimized. However, the computational complexity of max-flow routing is quite high, making it not reasonable for moderate size networks.

Other hierarchical routing protocols such as *Hierarchical State Routing "HSR", Zone-based Hierarchical Link State Routing Protocol (ZHLS),* and *Clusterhead Gateway Switch Routing (CGSR)* also fall under the same category.

2.6.5 Multipath Routing in Geographic Position Assisted Routing Protocols

There are presently several ad hoc routing algorithms such as; *Multipath Location-Aided Routing "MLAR"*, which is a multipath routing version of LAR; that uses position information (2D or 3D) to make routing decisions at each node. The proposed algorithm in [13] uses a 3D approach, which is a new hierarchical, zone-based 3D routing algorithm based on GRID by Liao, Tseng and Sheu [14]. The approach proposes a replacement of LAR with Multipath LAR (MLAR) in GRID. It is expected to have significant performance differences in 3D and as to whether single or multi-path algorithms should be used in a particular scenario. The simulation results demonstrate the performance benefits of MLAR Over LAR and AODV in most mobility situations. AOMDV delivers more packets compared to MLAR, however it does it at a cost of more frequent flooding to control packets and thus higher bandwidth usage than MLAR.

2.6.6 Multipath Routing in Power-Aware Protocols

The fact that ad hoc nodes are battery operated and have limited energy resources, make energy efficiency a key concern in the operation of such networks. Further studies have shown that the subsystem communication consumes a large fraction of total energy and therefore solutions for energy efficient communication are of great interest. Energy and power related issues are primarily physical layer topics and their effects on efficient routing open a new door into *Cross-Layer* issues, which are relatively new topics.

An interesting insight of power-aware ad hoc protocols has been presented in [15] in which optimization at the network layer is of major concern. The research is classified into three categories based on the different aspects and they address: power control, routing, and sleep mode (stand-by) control.

This paper further tries to investigate open issues of cross-layer, one of which is the understanding of the bottleneck, which is possibly because of topology discovery overhead, the routing protocol overhead, the actual transmission of data and the idle radio listening. Wireless contention, measuring available power, and CPU overhead are also said to contribute as well.

Multipath Power Sensitive Routing Protocol "MPSR" [16] is another ad hoc routing protocol with interest in power-aware communication. MPSR shows how an efficient heuristic-based multipath technique can improve the mean-time-to-node-failure and maintain the variance in all the nodes power as low as possible. MPSR is a flat topology in which every node is treated equally and stability and end-to-end delay reduction are of critical concern. The simulation results show performance optimized in MPSR protocol compared to the *Dynamic Source Routing "DSR"*.

2.6.7 Multipath Routing in Multicasting Protocols

Multicast Routing Protocols are of great interest as the demand for such communication is on the rise. *Multipath Multicast Routing Algorithm "MRPM"* [17] is an example of this category. In MERM, a method chooses the next hop when multiple equal cost next hops are present. Through the simulation, it was investigated that this quick distributed dynamic algorithm can manage network resources efficiently.

Multi-Flow Real-Time Transport Protocol "MRTP" [18] is another example of a mesh-based ad hoc-based protocol that offers multipath routing for multicast application. It is based on *Real-Time Protocol "RTP" and Real-Time Transport Control Protocol "RTCP"*. RTP itself is a multicast-oriented protocol for real-time applications. MRTP is motivated by the observations of effective path diversity in combating transmission errors in ad hoc networks, and effective data partitioning techniques in improving the queuing performance of real-time traffic. The simulation results show performance improvement in lost packets per frame and buffer management.

Multi-Objective Multipath Routing Algorithm for Multicast Flows "MMRAM" [19] proposes a multi-objective traffic-engineering scheme using different distribution trees to multicast several flows. MMRAM tries to combine maximum link utilization, hop count, total bandwidth consumption, and total end-to-end delay into a single aggregated flow. This combination makes MMRAM an attractive candidate for *Multiprotocol Label Switching "MPLS"*. This multi-tree routing protocol uses a multicast transmission with load balancing.

2.6.8 *Multipath Routing in Security Protocols*

Security has gained a lot of attentions recently and many attempts in proposing end-to-end security schemes have been carried out, one of which is by the use of multipath routing. The scheme presented in [20] tries to tackle the security issue by presenting trust and key management models for intrusion detection and prevention. The existence of multiple paths between nodes in an Ad hoc network is exploited to increase the robustness of transmitted data confidentiality. The proposed algorithm is tested against time for intrusion detection and robustness.

Another multipath routing algorithm for data security enhancement, *Multipath TCP Security "MTS"*, is discussed in [21]. In MTS, the source node chooses the available routes adaptively rather than testing the "stored routes" one by one exhaustively. Simulation results show that the algorithm provides a reasonably good level of security and performance. Compared to AODV and DSR, MTS has a better number of participating nodes and highest interception ratio. The average end-to-end delay between MTS, AODV and DSR shows that beyond speeds of 1.7 m/s, MTS delay drops rapidly and performs better in respect to the other two routing protocols.

So far, security options for ad hoc elements from the transport layer point of view was discussed, however the security option could be implemented in the application running on wireless nodes. The reference [22] shows a scheme in which a secret message is divided into multiple shares and through the use of multipath routing, the shares can be delivered to the destination via multiple paths. This enhances data confidentiality in a mobile ad hoc network and is expected to reduce the message compromising and eavesdropping probability. This is done by the distribution of a secret among multiple independent paths while it is transmitted across the network. As drawbacks, it shows that multipath routing causes more collision among correlated routes themselves thus degrades network performance such as packet delivery ratio.

2.6.9 *Summary of Multipath in Ad-Hoc Routing Protocols*

Figure 2.9 shows the different routing protocols discussed in this section and details of which protocol belongs to which group.

Protocols	Reactive	Proactive	Hybrid	Hierar.	Geog.	Power	Security	Multicast
DSR	✓							
MSR	✓							
AODMDV	✓							
AODV	✓							
DSDV		✓						
TERA		✓						
HMFR				✓				
ZRP			✓					
ANT.NET			✓					
HSR				✓				
ZHLS				✓				
CGSR				✓				
MLAR					✓			
MPSR						✓		
MRPM								✓
MRTP								✓
MMRAM								✓
MTS							✓	

Figure 2.9 Ad-Hoc Routing Protocols Discussed

REFERENCES

[1] D. J. Wilson, R. Dragnea, "IPv6 in Fixed and Mobile Networks", Technology White Paper, Juniper Networks Press, November 2004

[2] K. Zhigang, J. Ma, L. Jun and H. Jianping "Mobile IPv6 and some issues for QoS"

[3] C. Siva Ram Murthy and B. S. Manoj, "Ad Hoc Wireless Networks Architecture and Protocols", Prentice Hall 2004

[4] V. Vassiliou, H. L. Owen, D. Barlow, J. Sokol, H. P. Huth, "M-MPLS: Micro-mobility-enabled Multiprotocol Label Switching", 2003

[5] Tin-Yu Wu, Ching-Yang Huang, Han-Chieh Chao, "A survey of Mobile-IP in cellular and Mobile Ad-Hoc Network environments", Ad Hoc Networks Journal, 2003

[6] Lei Wang, Lianfang Zhang, Yantai Shu and Miao Dong, "Multipath Source Routing in Wireless Ad Hoc Networks", CCECE 2000, 7-10 March 2000

[7] Mahesh K. Marina S. R., "On-demand Multipath Distance Vector Routing in Ad Hoc Networks", 9th International Conference on 11-14 Nov. 2001

[8] Charles Perkins and Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing for Mobile Computers", In Proceedings of the Symposium on Communication Architectures and Protocols, ACM SIGCOMM, 1994

[9] Ralph Jansen, Sven Hanemann and Bernd Freisleben, "Proactive Distance-Vector Multipath Routing for Wireless Ad Hoc Networks", Proceedings of 10th Symposium on Communicati-ons and Vehicular Technology, Eindhoven, Netherlands, SCVT 2003

[10] Shafinaz Buruhanudeen, "Overview of Ad Hoc Routing Protocols", University of Bradford, UK, Nov. 2002

[11] Frederick Ducatelle, Gianni Di Caro and Luca Maria Gambardella, "Ant Agents for Hybrid Multipath Routing in Mobile Ad Hoc Networks", Wireless On-demand Network Systems and Services, 2005. WONS 2005. Second Annual Conference on 19-21 Jan. 2005

[12] Stephan Bohacek, Joòao P. Hespanha, Chansook Lim, Katia Obraczka, "Hierarchical Max-Flow Routing", To be presented at the 2005 IEEE GLOBECOM, Nov. 2005

[13] Soumendra Nanda, Robert S. Gray, "Spatial Multipath Location Aided Ad Hoc Routing", Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on 2004

[14] W. H. Liao, Y. C. Tseng, and J. P. Sheu, "GRID: A Fully Location-Aware Routing Protocol for Mobile Ad Hoc Networks", Telecommunication Systems, Vol. 18, no. 1,2001, pp. 37-60

[15] Sushant Jain, "Energy Aware Communication in Ad-hoc Networks", Technical Report UW-CSE 03-06-03

[16] Anand Prabhu Subramanian, Anto A J, Janani Vasudevan and Narayanasamy P, "Multipath Power Sensitive Routing Protocol for Mobile Ad hoc Networks", WONS2004, Madonna di Campiglio, Italy, January 2004

[17] Zhang Baoxian, LiuYue and Chen Changiia, "A Multipath Multicast Routing Algorithm", Com-munications, 1999. APCC/OECC '99. Fifth Asia-Pacific Conference Volume 2, 18-22 Oct. 1999

[18] Shiwen Mao, Dennis Bushmitch, Sathya Narayanan, and Shivendra S. Panwar, "MRTP: A Multi-Flow Realtime Transport Protocol for Ad Hoc Networks", Vehicular Technology Conference, 2003, 6-9 Oct. 2003

[19] Ramon Fabregat, Yezid Donoso Meisel, Jose L. Marzo, Alfonso Ariza, "A Multi-Objective Multipath Routing Algorithm for Multicast Flows", 2004 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'04)

[20] Souheila BOUAM. Jalel BEN-Othman, "Data Security in Ad hoc Networks Using MultiPath Routing", Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on Volume 2, 7-10 Sept. 2003

[21] Zhi Li; Yu-Kwong Kwok, "A New Multipath Routing Approach to Enhancing TCP Security in Ad Hoc Wireless Networks", Parallel Processing, 2005. ICPP 2005 Workshops. International Conference Workshops on 14-17 June 2005

[22] Wenjing Lou; Wei Liu; Yuguang Fang, "A Simulation Study of Security Performance using Multipath Routing in Ad-Hoc Networks", Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003

[23] David B. Johnson, David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", 1996

CHAPTER 3
QUALITY OF SERVICE (QOS)

3.1 Introduction to QoS

Internet backbone of today, considers the fact that data is delivered as a single "best effort" class of service, rather than "how" it is delivered [1]. Both "if" and "how" are of QoS concerns. QoS is the measure of how good a service is, as presented to the user. It is expressed in user understandable language and manifests itself in number of parameters, with either subjective or objective values.

3.1.1 QoS from User Perspective

From provider-user perspective, QoS could be divided into four definitions:

- *Planned QoS*: Or what the Internet Service Provider (ISP) intends to offer and what users expect to receive
- *Achieved QoS*: The actual QoS delivered
- *User-perceived QoS*: The QoS perceived by human users, which may differ from the achieved, and
- *Inferred QoS*: The quality determined by the ISP, resulting from user opinion studies

From protocol point of view, there are two QoS approaches, *Integrated Services (InterServ)* for per flow and *Differentiated Services (DiffServ)* for aggregated traffic [2].

3.1.2 QoS from Network Perspective

The QoS parameters in a mobile-IP application are:

Maximum Round-Trip Delay (MRTD):

Routing Trip Delay (RTD) is the time that takes for a packet to travel from one point on the network to the other point in the network and back to the same location and MRTD is the maximum possible value for RTD. In the mobile-IP application this refers to the lengthiest path in the scheme, which is the distance between MN and Home Agent (HA). Our method for measuring

this value is the time between *Binding Request* from MN reaches HA and plus the time the *Binding Reply* is sent back from HA to the MN [3]:

$$MRTD = BindingRequest\ [MN, HA] + BindingReply\ [HA, MN]$$

Minimum Bandwidth Guaranteed (MBG):

MBG is a very important parameter for QoS. It shows the worst-case scenario in respect to the bandwidth. MBG is an application specific parameter and is often set as a percentage of the maximum bandwidth possible. Protocols, such as MPLS and ATM offer MBG.

Bit Error Rate (BER):

BER is a measure of how reliable the link is and how fault tolerant the communication is. It is specified by number of error bits in a bulk of data or the probability of error taking place and depending on specific physical-layer specifications, BER can be anywhere from 10^{-5} to 10^{-12}. In mobile-IP, the worst-case scenario happens during handoff/handover process.

Packet Loss Ratio (PER):

PER parameter is a multi-layer QoS parameter. From transport-layer, network-layer down to link-layer and physical layer all could contribute to the value of PER. In our study, the effect of the link-layer connectivity, which is affected by the handoff/handover process, will be depicted. The value of PER is in form of percentage and ranges from 0.1% to 5%.

Packet Drop Ratio (PDR):

PDR is a measure of the robustness of the receiver, its buffer-full protection, and error-free reception. During handoff/handover, PDR could rise due to routing inefficiency and buffer overflow.

End-to-End Delay (EED):

The overall EED shows the performance of each node, the processing times and the average distance between nodes. EED is a subjective parameter, that is, for specific applications, the value of EED should fall less than specific values for acceptable QoS. For normal voice applications, EED should be less than 300 msec [4] and for high quality voice in mobile-IP (VoIP over wireless link), EED should be less than 150 msec [5].

Jitter (Variable Delays):

Jitter happens due to the variation of queue lengths and variations in processing times for reordering and reassembling packets that arrive out of sequence and correct order. The latter is mostly due to multipath routing. The effect of jitter is in the order of 10^{-3} in a high performance mobile-IP system.

The focus of this thesis is to investigate compare these QoS parameters in different schemes and compare the results with the proposed scheme and point out the superiorities. For this, we continue on the proposed scheme and introduce Multiprotocol Label Switching (MPLS) protocol and how it can be integrated with Mobile-IP to support QoS.

3.2 Multiprotocol Label Switching (MPLS)

MPLS is a packet forwarding protocol that is capable of layer III-to-Layer II routing mapping. The essence of this protocol is to assign packet flows to label switched paths (LSPs). Packets are classified at ingress router or the label edge router (LER), based on forwarding equivalence classes (FECs) [6,7]. FECs summarize essential information about the packet such as; destination, precedence, VPN membership, QoS information and the route of the packet chosen by traffic engineering (TE).

3.2.1 Edge of the MPLS Domain

Layer III analysis is performed only once, at the "*Ingress*" (see Figure 3.1). The Layer III header is mapped into a fixed-length (20-bit) header, called a "*label*". At each router across the network, only the label need be examined and at the end of the network, an Edge LSR, called "*Egress*", swaps the label out.

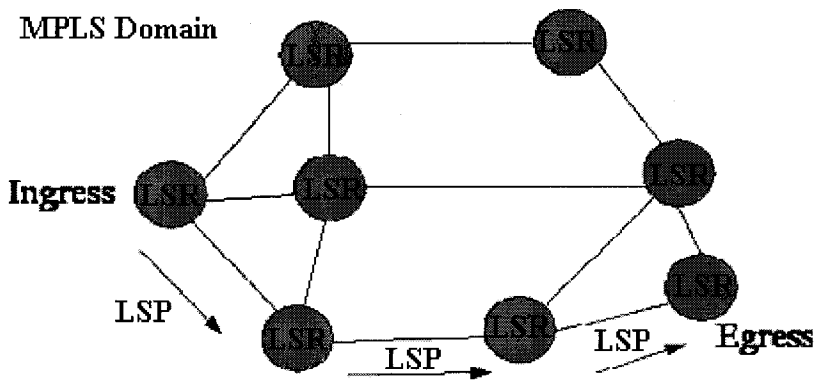


Figure 3.1 MPLS Domain Edge Routers

3.2.2 MPLS Domain

Figure 3.2 shows a typical MPLS Domain with Ingress and Egress at the edge of the domain and FECs-LSPs providing efficient routing from the entrance to the exit of the domain and each LSR responsible of fast switching the incoming packets according to the label specifications.

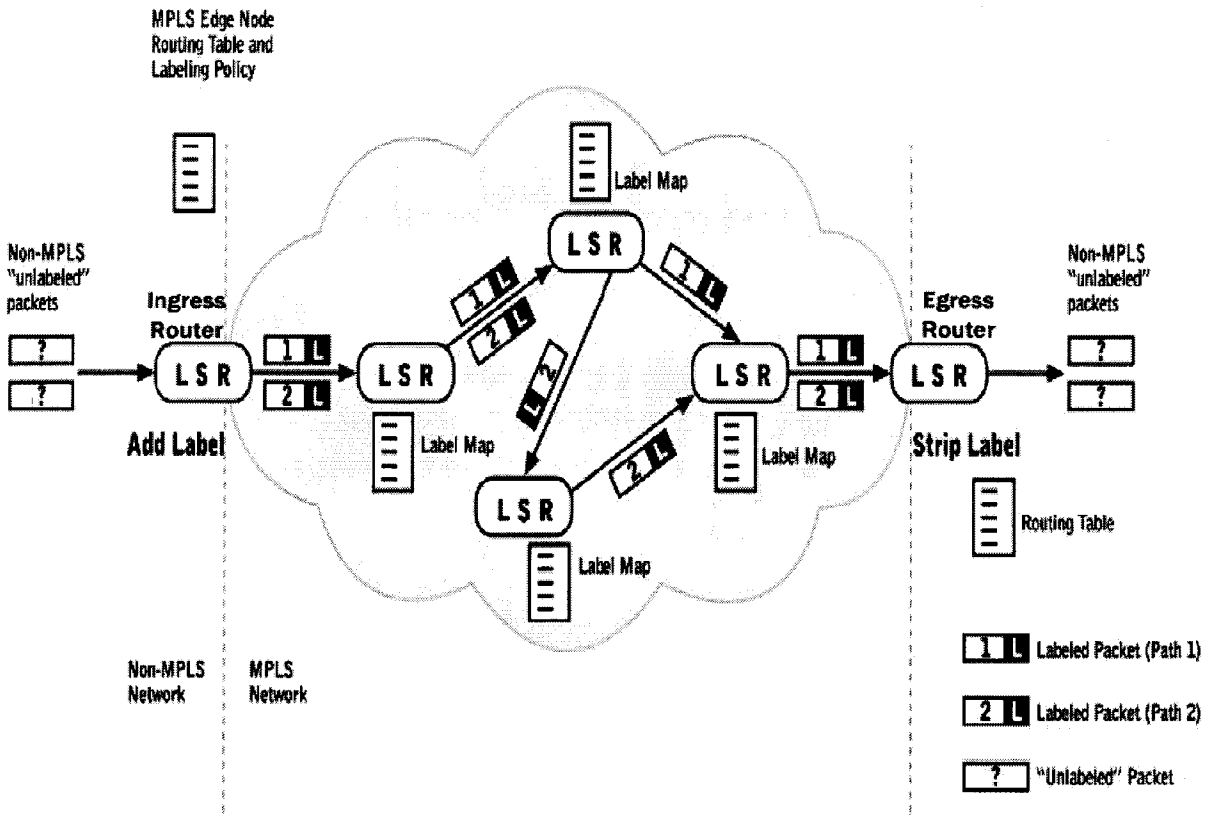


Figure 3.2 A Typical MPLS Domain

3.2.3 *Features of MPLS*

MPLS benefits from both, *Circuit-Switched* network attribute, such as ATM, which can provide *Minimum Bandwidth Guaranteed*, and from *Packet-Switched* network attribute, such as IP. After all, connections are not physically setup (Virtual Connections) and data is still packetized. The other reason for migrating to MPLS is the fact that, functionally speaking, MPLS works at the layer II and can integrate wide variety of protocols on to the Link Layer. It is *Highly Reliability*, and it *Supports Quality of Service.*

3.2.4 *Summary of MPLS Mechanism*

In MPLS, traffic is aggregated into groups called *FEC* (*Forwarding Equivalence Classes*). FECs are assigned to specific *Label Switched Path* (*LSP*) and *Traffic-Engineering* (TE) can be implemented to assign *high-priority FECs* onto *high-quality LSPs* and *lower-priority FECs* onto *lower-quality LSPs.* This way QoS is implemented using MPLS

3.2.5 *Traffic Engineering (TE)*

TE is the assignment of particular treatment to groups of traffic with similar identifier as opposed to single-flow treatment for IP-based traffic. In fact we have two types of data flows:

- **Per flow**: Typically a flow has very fine granularity and reflects a single interchange between hosts, such as a TCP connection. Data is treated per flow and no groups are data could be treated once for all, such as, IntServ.
- **Per Aggregated flow:** Is a number of flows that share forwarding state and a single resource reservation along a sequence of routers, such as in DiffServ. TE supports Per Aggregated flow.

3.2.6 *Advantages of MPLS with Mobile-IP*

The integration of MPLS with Mobile-IP is an excellent match. Routing optimization and necessary tunneling could be done using label-switching. The features making MPLS attractive for Mobile-IP usage are:

- Fast Switching
- Small State Maintenance
- Highly Scalability
- Connection-Oriented QoS
- Guaranteed Minimum Bandwidth
- Guarantee of Maximum Delay
- Precedent Routing for Specific Data Type
- Hierarchical MPLS Mobile-IP is possible
- Reduction of Overhead
- QoS guaranteed LSP setup
- Smooth handoff support

3.2.7 *Summary of MPLS Mobile-IP Mechanism*

An LSP from HA to the FDA is established during registration request and reply process. Encapsulation is done based on MPLS Ingress functionality of the HA and the Care-of Address (CoA) of the MN is the FEC of this LSP.

3.2.8 *Hierarchical MPLS Mobile-IP*

The integration of Mobile-IP with MPLS in a hierarchical topology will have the least reduction of overhead due to the nature of hierarchical topologies. The highest level of overhead, again, happens during the handoff/handover procedure. As mentioned for Hierarchical Mobile-IP scheme (Chapter 2, Figure 2.7), handoff/handover procedures are divided into two categories, local movements and global movements. The Mobile Anchor Points (MAPs) were introduced in Chapter 2 and for MPLS-based structures, a new entity called, Foreign Domain Agent (FDA), is used, which is similar to MAP with MPLS capability. Figure 3.3 shows the topology.

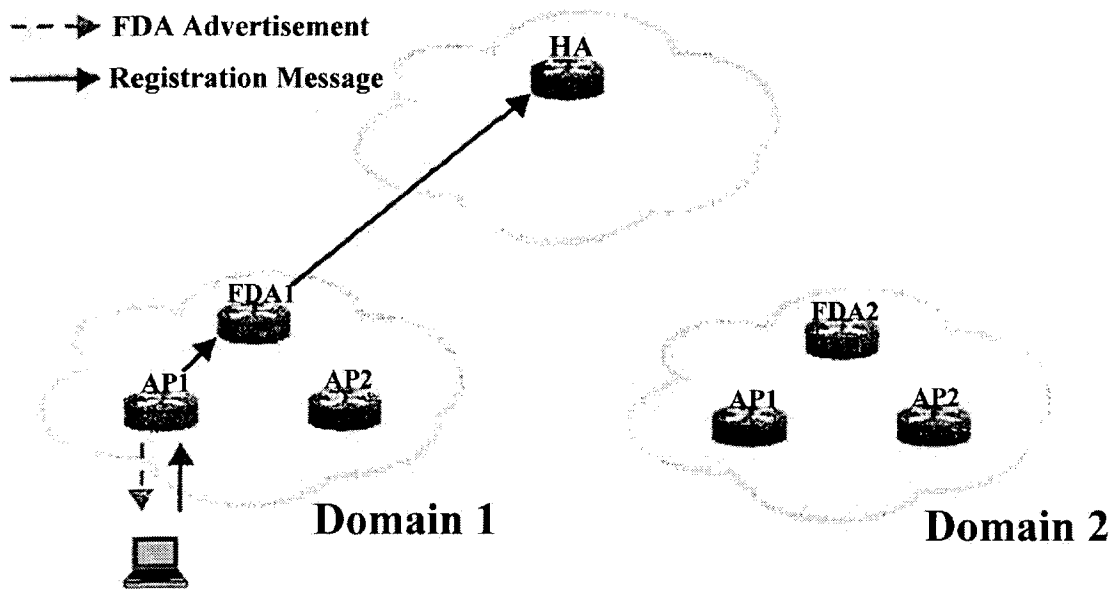


Figure 3.3 A Hierarchical MPLS Mobile-IP Structure

3.2.9 *IntraFDA versus InterFDA*

During local movements, similarly as suggested in ordinary hierarchical Mobile-IP, here the FDA1 manages the location updates of MN inside the FDA1 domain. Hence no further updates required between HA, FDA1, and MN. The signaling scheme is shown in Figure 3.4. The local movement is called *IntraFDA* movement.

During global movement, *InterFDA*, handoff/handover takes place between FDA1 and FDA2 and HA is informed of the global change. Figure 3.5 shows the *InterFDA* movement.

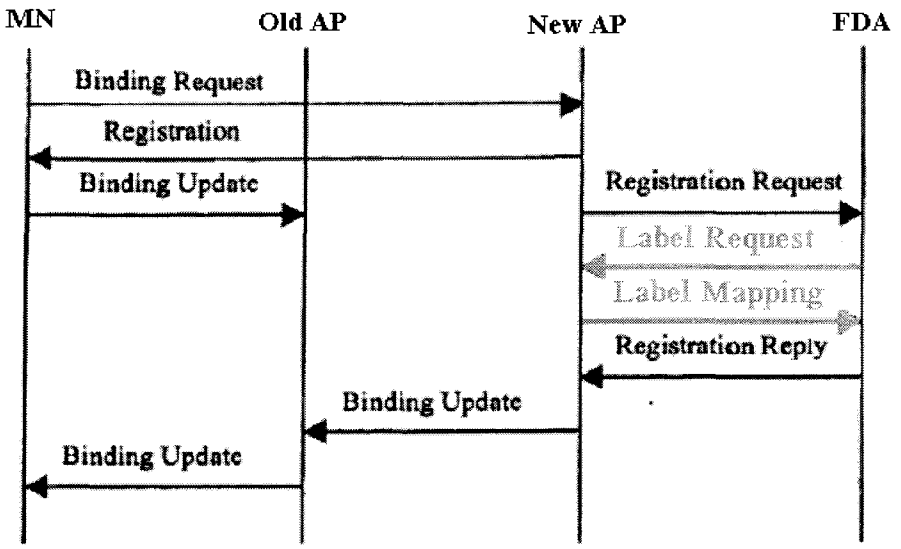


Figure 3.4 IntraFDA Movement Update Signaling

As it can be noticed, orange lines represent pure MPLS messages (Label Request and Label Mapping). MPLS messages are assisted by RSVP (Resource Reservation Setup Protocol, RFC 2205).

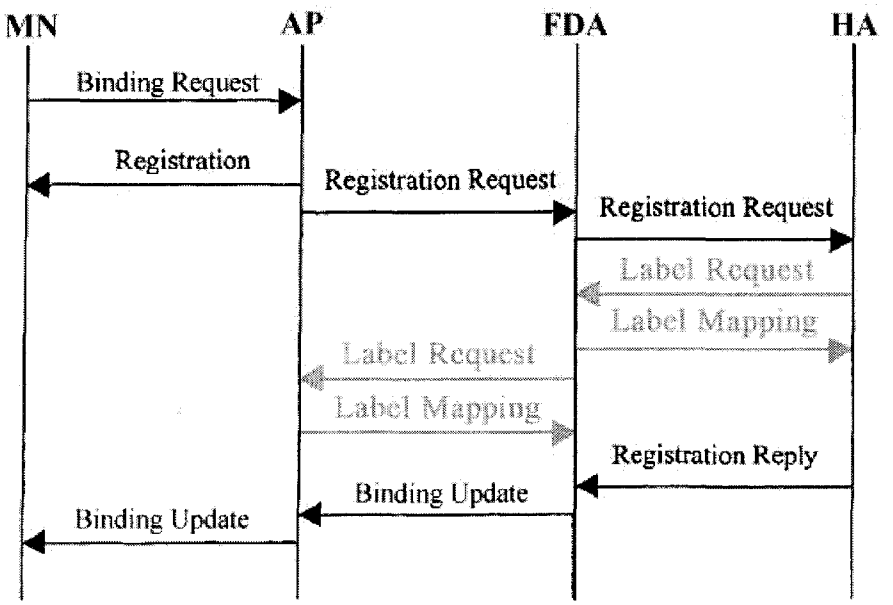


Figure 3.5 InterFDA Movement Update Signaling

3.3 Unique Advantages of MPLS

MPLS, as mentioned, offers many fine attributes, which contribute to a better QoS. Now the question is, is MPLS the only answer? To what extend does the integration of MPLS with Mobile-IP increase the QoS? "How much better" will Mobile-IP work with MPLS compared to other protocols, which offer QoS? These comparative questions will be answered in this and next sections.

3.3.1 MPLS versus RSVP and DiffServ

To answer these questions, let's look at all the alternatives to MPLS. There are two other alternatives to MPLS, which are: **RSVP** and **DiffServ**.

- **RSVP:** The Resource Reservation Setup Protocol (RFC 2205) installs state associated with resource reservations for individual flows originated/destined to hosts. RSVP is used by a host, on behalf of an application data stream, to request a specific QoS from the network for a particular data stream or flows. The problem with RSVP is the fact that no aggregated data treatment is available, only per flow treatment. This feature lacks the scalability issue immensely and therefore TE (Traffic Engineering) cannot be applied to RSVP alone, which makes it a poor quality candidate for Mobile-IP applications. However the messaging structure of RSVP will be used in MPLS protocol[8]

- **DiffServ:** Which stands for Differentiated Services (as described in RFC 2430), is an aggregated traffic treatment protocol. Therefore, traffic-classes through the use of traffic-trunks, can apply identical treatment to aggregated data flows, as opposed to a single-flow treatment in RSVP. Meanwhile RSVP is again used in DiffServ structure because RSVP creates and maintains distributed state for information other than pure resource reservation. However the problems with DiffServ are summarized as follows:
    - DiffServ still works at layer III, which makes it slower than MPLS and also technology dependent of the Link Layer protocol
    - It lacks proper network provisioning for Mobile-IP environments, and
    - Lacks dynamic configurations needed for a dynamic nature of Mobile-IP system [9]

REFERENCES

[1] QoS in the Internet, Centre for Telecommunications Research, King's College London

[2] Sasan Adibi, "Mobile-IP Ad-hoc Networks with QoS Support", M.A.S. Second Seminar, University of Windsor, August 2005

[3] Abhishek Roy, Kalyan Basu, Sajal K. Das, "Performance Modeling of Wireless Voice over IP" IWDC 2002

[4] Sasan Adibi, Mohammad Naserian, Shervin Erfani, "A Fast Handover M-MANET", CCECE 2005

[5] Hiroshi Esaki, "Multi-Homing and Multi-Path Architecture Using Mobile IP and NEMO Framework", 2004

[6] V. Vassiliou, H. L. Owen, D. Barlow, J. Sokol, H. P. Huth, "M-MPLS, 2003

[7] S. Adibi, M. Naserian, S. Erfani, "Mobile-IP MPLS-Based Networks", CCECE 2005, Saskatoon

[8] Analysis of the RSVP Protocol:
"Marc Greis", Internet Task Force Engineering – Draft, 2001

[9] An Analysis of the DiffServ Approach in Mobile Environments:
"Torsten Braun", Proceedings of 1st Workshop on IP Quality of Service for Wireless and Mobile Networking (IQWiM), Alemanha, April 1999

CHAPTER 4

SIMULATION SETUP, RESULTS AND ANALYSIS

In this chapter, which contains data gathered from our simulation results, we present various simulation setups for testing different mechanisms for QoS support.

4.1 Overhead reduction using MSR on top of MPLS

In this simulation we compared two identical networks with identical component structures and traffic patterns [1,2]:

- Network 1:
  - Radio Transmission Range: 250 m
  - Network Layer Protocol: IPv6 on top of *DSR*
  - Devices using non-Multihomed capability
  - Medium Access Control Protocol: *802.11b*
  - Traffic Capacity: 2-7 Mbps
- Network 2:
  - Radio Transmission Range: 250 m
  - Network Layer Protocol: IPv6 on top of *MSR*
  - Devices using Multihomed capability
  - Medium Access Control Protocol: *MPLS*
  - Traffic Capacity: 2-7 Mbps

To monitor the overhead generated by both networks we use less than 100 Ad-Hoc nodes moving inside the wireless range. The testbed is simulated using OPNET. OPNET is an object-oriented simulation tool developed by OPNET Technologies Inc.

Using OPNET, Figure 4.1 shows the overhead respect to the number of neighbors for Network 1. Figure 4.2 shows the same for Network 2. Figure 4.3 shows the bandwidth variations of before, during and after the handoff/handover procedure.

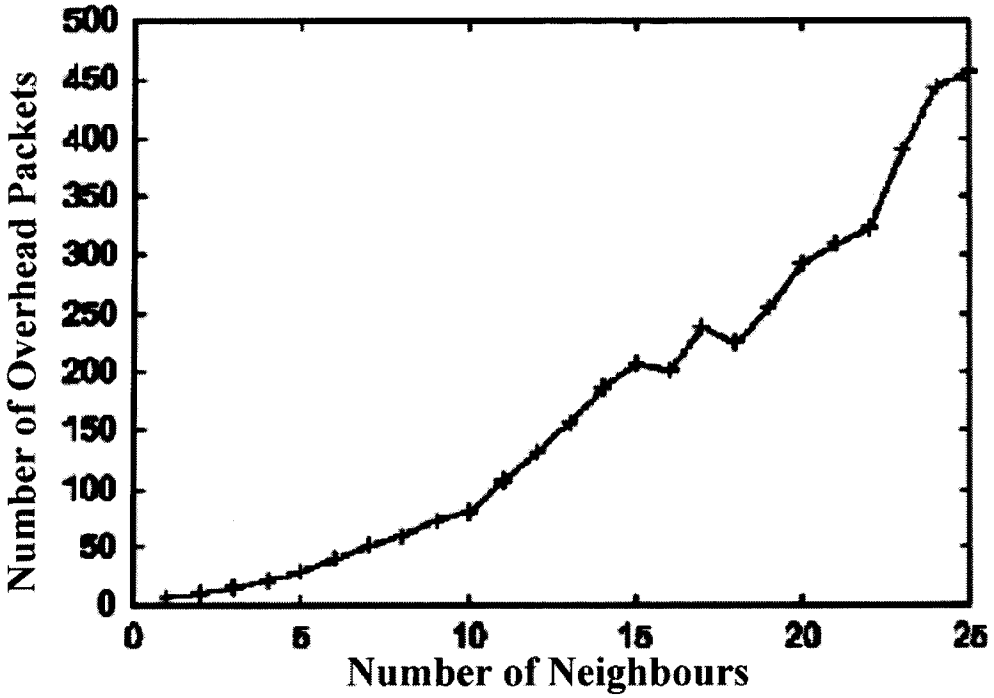


Figure 4.1 Routing overheads versus number of neighbors in a non-multihomed transmission environment using DSR

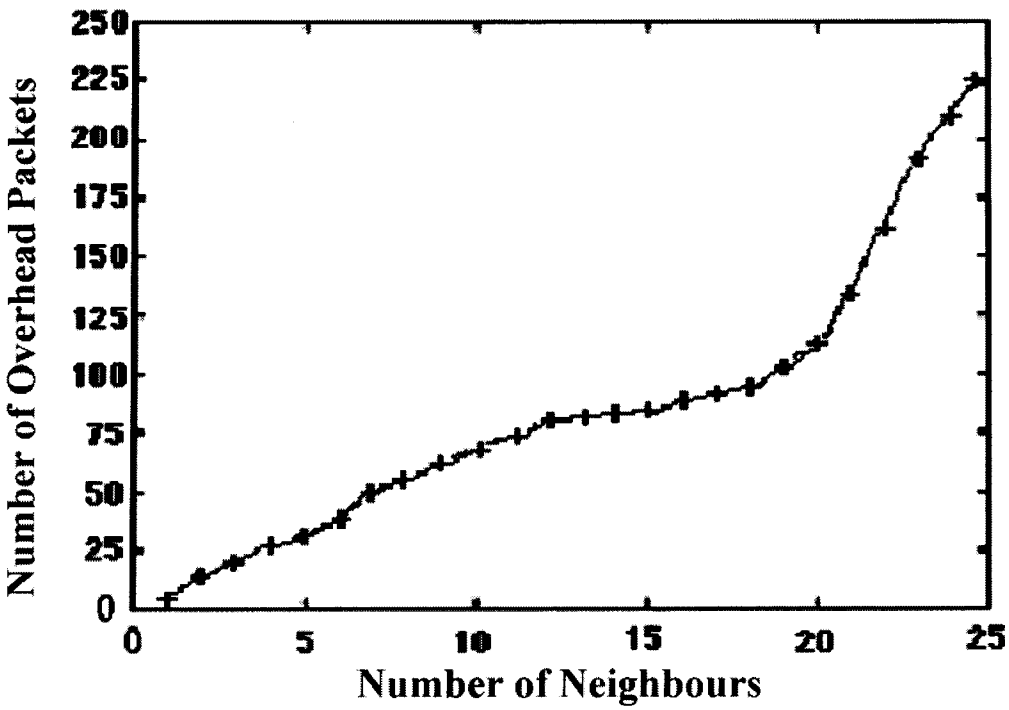


Figure 4.2 Routing overheads versus number of neighbors in a multihomed transmission environment using MSR

Figures 4.1 and 4.2 show that the number of overhead drops at least 40% in Figure 4.2 compared to Figure 4.1. There is an optimal number of neighbors, after which the number of overhead increases dramatically. According to Figure 4.2, this optimal number of neighbors is 20.

4.1.1 Simulation Results and Network Analysis

The simulations were run for two different variables with the following parameters:

- For Network 2, the LSP setup method was for two sets of traffic, Data-Driven Bi-Directional and Controlling Signals
- Total number of mobile nodes in each RAN: variable between 20 to 100 nodes

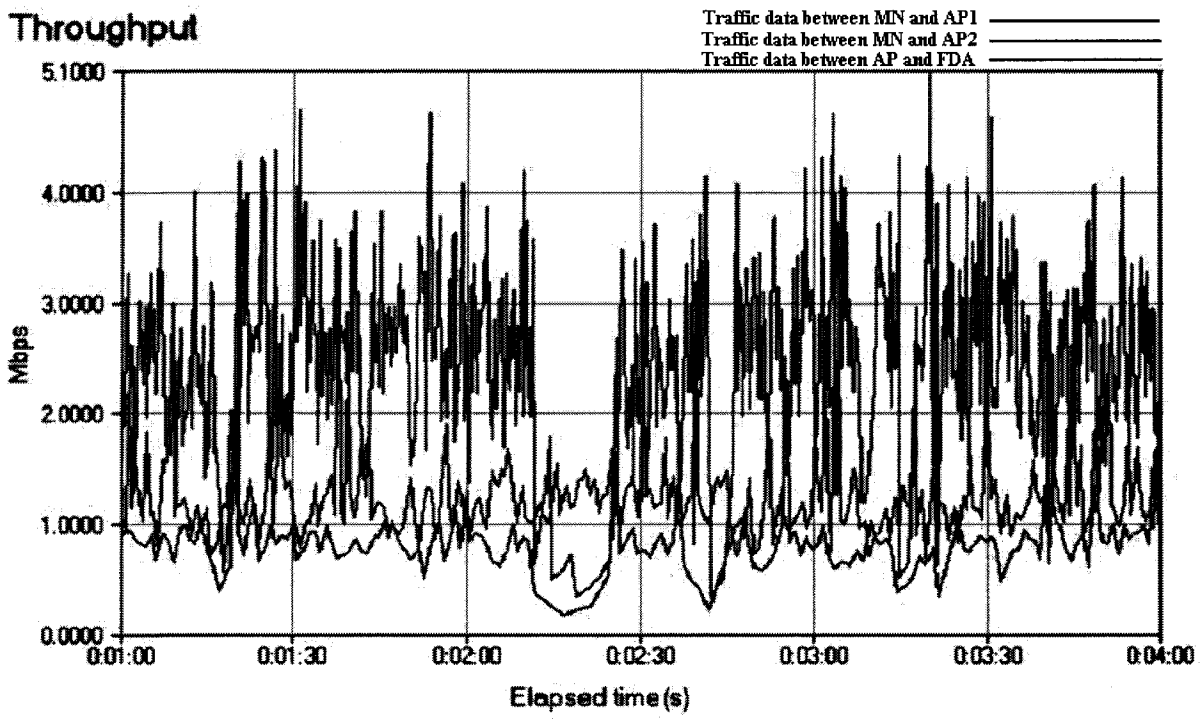


Figure 4.3 Bandwidth variations around the handoff/handover period for MSR on top of MPLS

- Simulation results show:
  - Effective number of neighbors and number of hops
    - As it can be seen, using MSR on top of MPLS reduces the number of overhead dramatically
  - Minimum Bandwidth during Handoff/Handover

- The bandwidth during the handoff/handover period (2 sec – 2.5 sec) degrades, however the link is not broken and connectivity is maintained. The minimum bandwidth is guaranteed to be above 1 Mbps, which is in an acceptable range

4.2 Packet Dropout during Handoff/Handover for an MPLS-Mobile-IP-based System

Here we investigate the nature of handoff/handover and its effect on the percentage of dropped packets due to the packets being lost and/or receivers' buffers being full, which disallows the receiver to receive more new packet. Figure 4.4 shows the architecture by which the testbed was established [3].

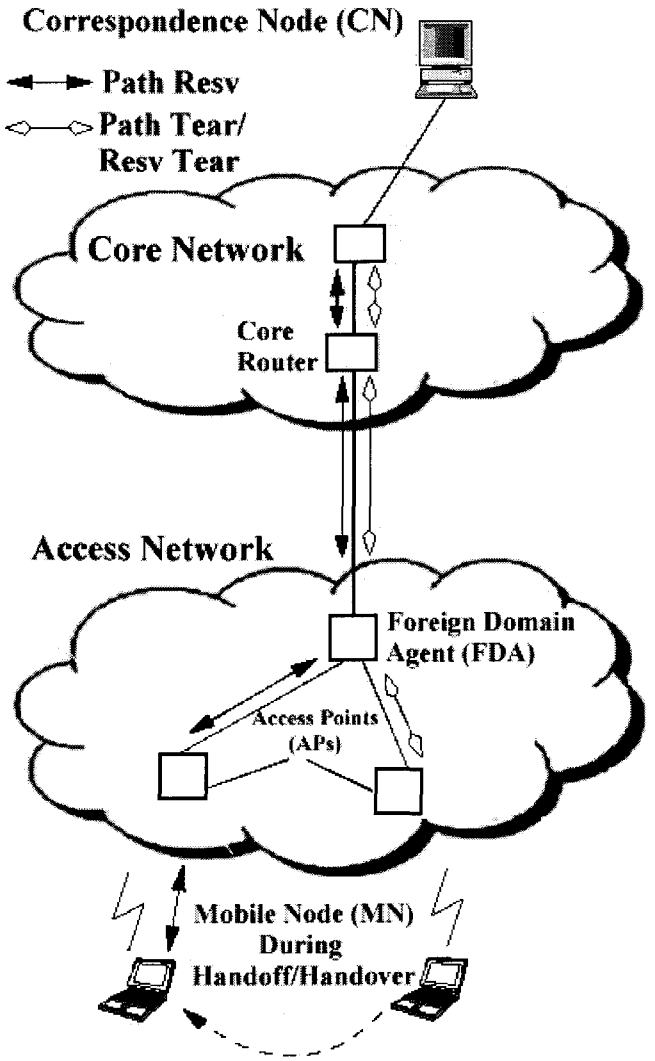


Figure 4.4 Handoff/Handover Period for an MPLS-Mobile-IP System with RSVP Provisioning

In this case RSVP governs the data flow scheme for QoS supports for MPLS signaling, either to minimize delays and packet dropouts or maintaining guaranteed bandwidth throughout the whole operation of MN from leaving the home network, roaming through different foreign networks, engaging in handoffs and finally returning to the home network. During this handoff, the established RSVP session needs a new round of RSVP signaling exchange. RSVP creates a soft session state in every intermediate router that passes the traffic flow. Each session is uniquely identified by the session object, which is constructed by the triplet "DestAddress, DestPort, Protocol ID". Thus the downlink and uplink reservation need re-establishment a new Path state needed to be re-generated. The soft-state property of RSVP-TE enables the application of soft-state location management on the MNs within the Mobile-IPv6 MPLS domain. The FDA sends a new RSVP message, with a LABEL_REQUEST object, to the current FDA. The HA, instead of the current FDA receives the PATH message containing a LABEL-REQUEST object, it responds with a RESV message that contains a LABEL object on the behalf of the MN. The interactions between MN, old FDA, new FDA, domain routers, HA and CN are presented in Figure 4.5.

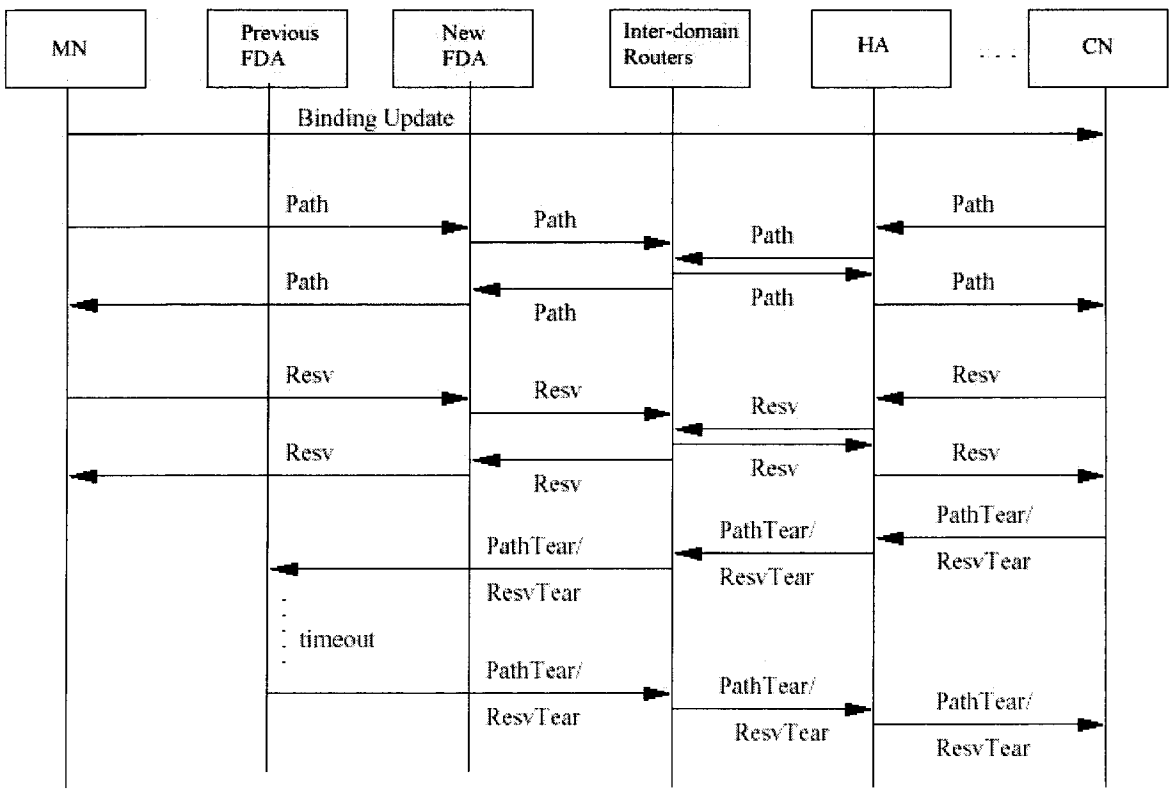


Figure 4.5 Analytical RSVP signaling after a handoff

In this section, a testbed was setup to investigate the packet dropout in three different scenarios. In the first scenario a MN was set to abandon a cellular region and enter a new region. In this case a flat topology ad-hoc network was used without the presence of RSVP and MPLS. A multimedia streaming audio/video conveying audio/video traffic ranging from 4 to 7 Mbps was the traffic load between MN and the APs. In the second scenario the same traffic was used with the presence of MPLS technology and in the third scenario RSVP was employed as well with and without optimal number of access points. Using OPNET simulation and related parameters in each scenario, the results were plotted in Figure 4.6.

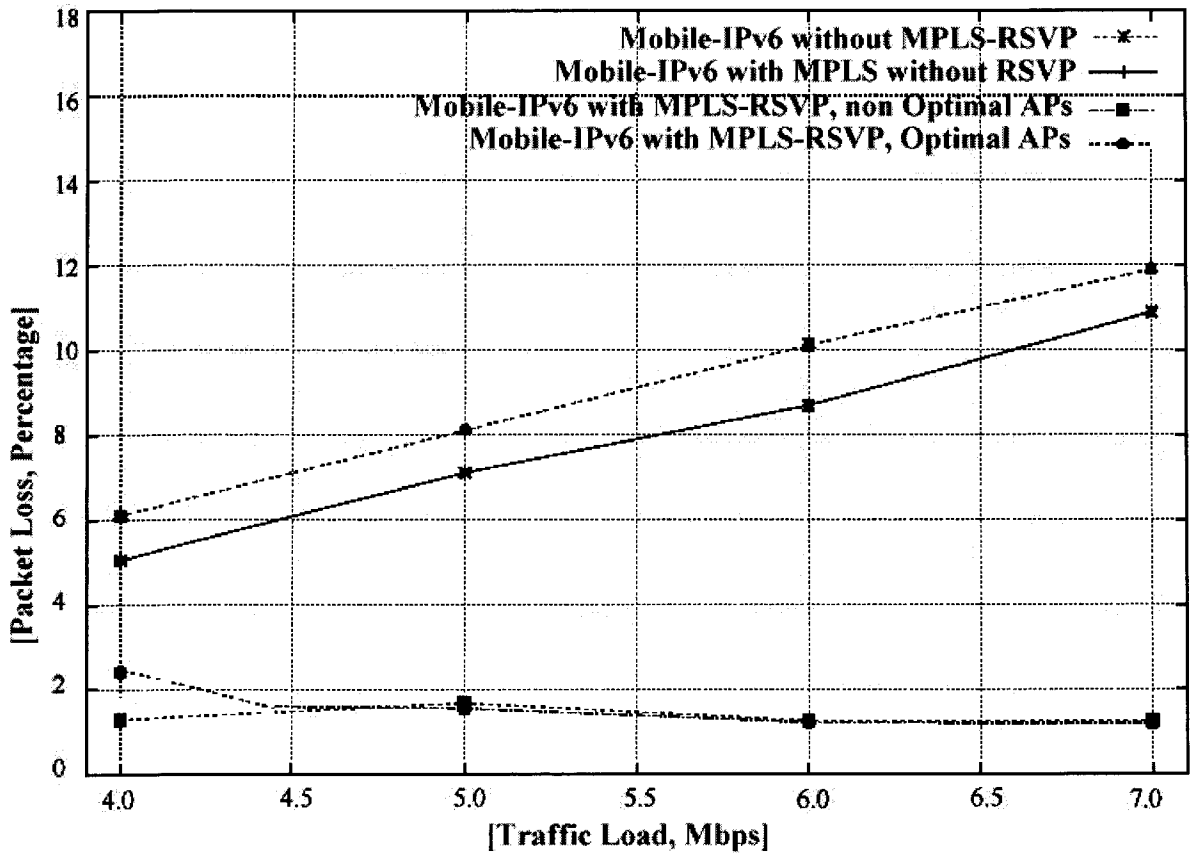


Figure 4.6 Number of packet dropouts percentage in three different scenarios

We realized there is an optimal number of APs, which minimizes the number of packet drops per unit of time. In our case, for traffic load of 4-7 Mbps the optimal number of APs, which associates with the best error rate, is three APs per FDA domain.

4.3 TCP Retransmission Patterns

Figure 4.7 shows an ad-hoc mobile-IP architecture with essential entities such as; HA, NC, hosts, and ad-hoc elements and optional entities such as; Access Points and ad-hoc manager.

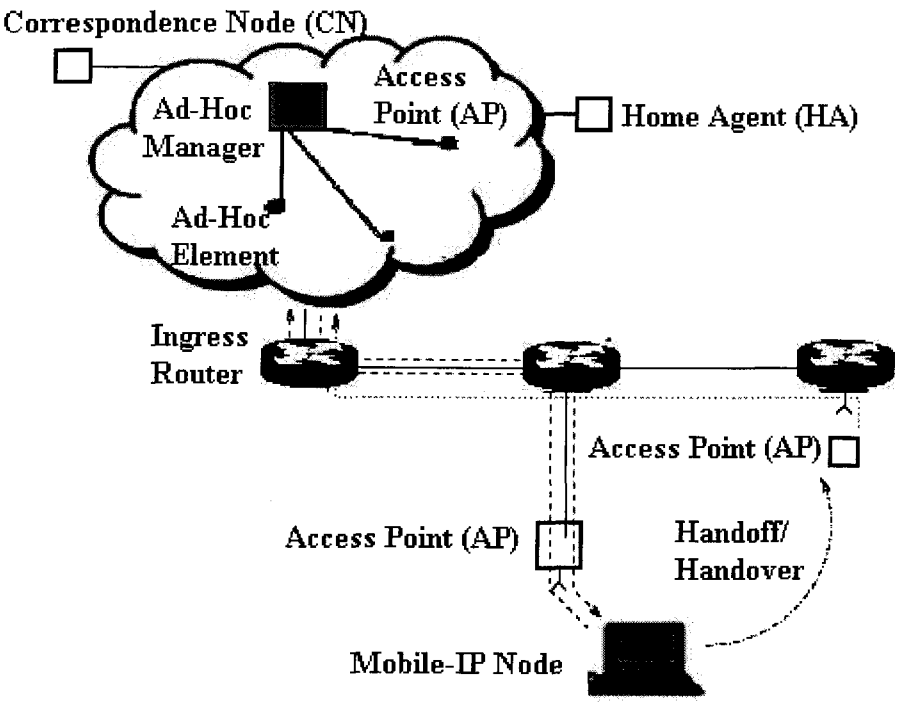


Figure 4.7 Typical Ad-Hoc Mobile-IP Architecture

The following specifications were used in the simulator:

- Traffic rate of the channel is set to 2 Mbps
- Ad-Hoc elements use dynamic source routing (DSR) protocol for routing
- For traffic generation we use FTP over TCP for all the flows in the network

The simulation shows the retransmission pattern in the course of mobile-IP movements and special consideration should be applied to the handoff/handover procedure. Figure 2 shows this pattern. As depicted in Figure 4.8, between the 3rd and the 4th seconds the first handoff/handover happens and there we have a slight degradation of the connection due to the physical occurrence of handoff. The number of retransmissions rises to 3 in the worst case. The same happens between 8th and 9th seconds.

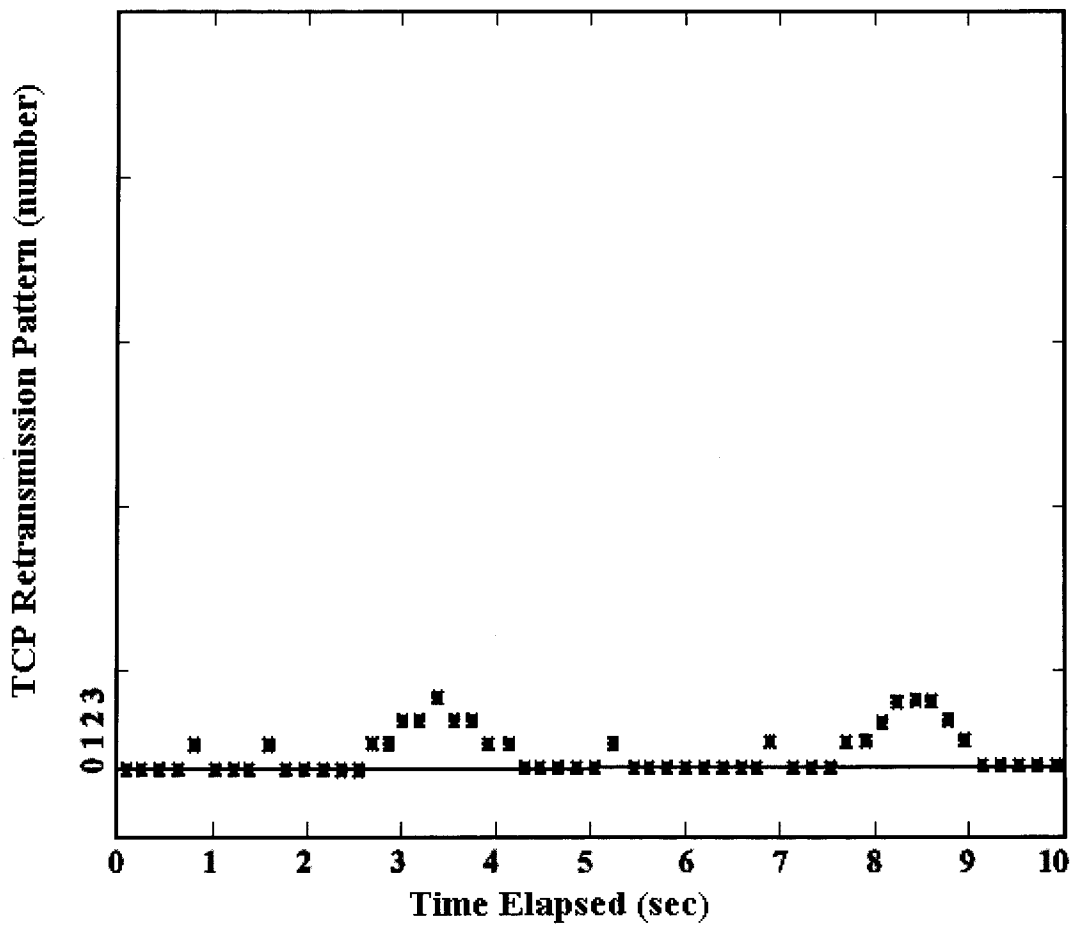


Figure 4.8 TCP Retransmission Pattern during Mobile-IP activity

4.4 Packet Loss Ratio (PLR) in Link Layer Connectivity for Mobile-IP Ad-Hoc Networks

A testbed was setup to calculate the Packet Loss Ratio (PLR is the parameter measuring the QoS associated to the performance of specific routing protocol) in three ad-hoc routing protocols, DSR, HSR, and OLSR. OPNET was used and the following parameters were set during the simulation [5]:

- Traffic rate of the channel is set to 2 Mbps
- For traffic generation, FTP over TCP was used
- Simulation was run for 5 seconds
- The handoff/handover takes place during the 1.2 and 4.3 seconds

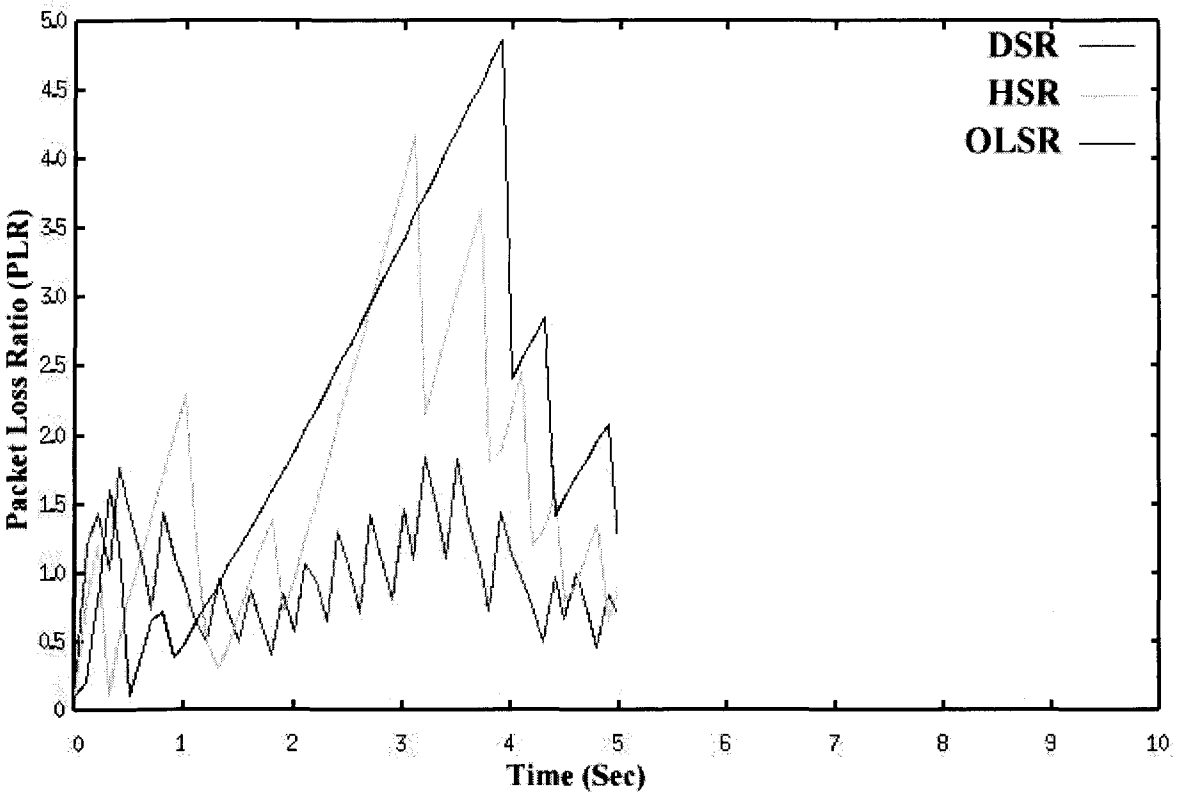


Figure 4.9. The PLR pattern during Mobile-IP activity

The simulation (Figure 3) shows the performance comparisons between DSR, OLSR and HSR during handoff/handover mechanism for the course of mobile-IP movements. This shows that the performance of DSR is relatively the best as it has a built in mechanism for route discovery specially developed for on-demand routing protocols. The performance of OLSR tends to worsen during the handoff/handover period.

4.5 Packet Drop Ratio (PDR) for Mobile-IP Ad-Hoc Routing Protocols with Multipath Capability

The Packet Drop Ratio (PDR), which is one of the parameters contributing to Quality of Service (QoS), was simulated [6] for a number of ad-hoc routing protocols, namely; Multipath Source Routing (MSR), Destination-Sequenced Distance-Vector Routing (DSDV), Hierarchical Max-Flow Routing HMFR), and Multipath Location Aided Routing (MLAR). For this, a testbed

on OPNET was established to compare the QoS offered by four of the routing protocols. The wireless node uses the following traffic information:

- Traffic rate between Mobile Node to the Access Point is set to 2 Mbps
- For traffic generation, FTP over TCP is used
- Simulation was run for 8 seconds
- The handoff/handover takes place during the first second
- PDR measures the QoS associated to the performance of specific routing protocol

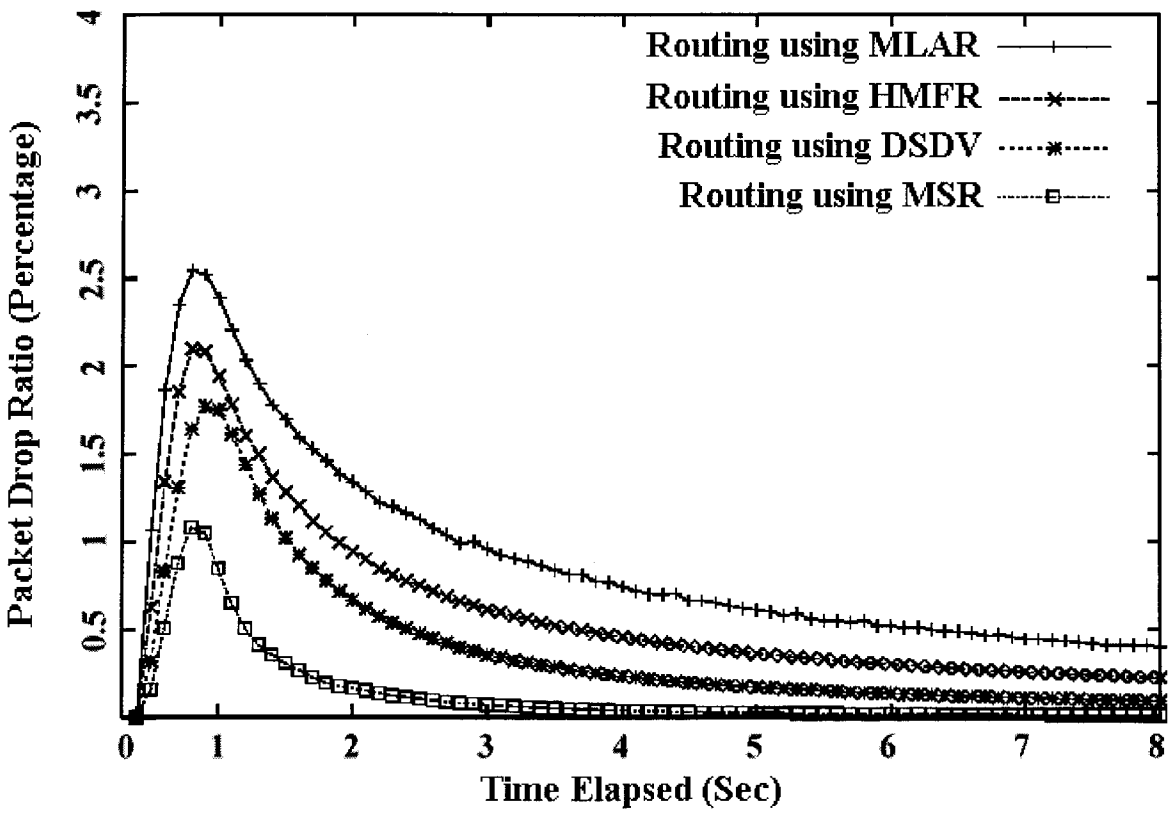


Figure 4.10. The PDR pattern during handoff

The simulation (Fig. 4.10) shows the performance comparisons between MSR, DSDV, HMFR, and MLAR during handoff/handover mechanism for the course of mobile-IP movements. This shows that the performance of MSR is relatively the best as it has a built-in mechanism for route discovery, specially developed for on-demand routing protocols. The performance of MLAR is measured to be the worst due to the inefficiency of geographical position assisted routing for small cells.

4.6 Packet Drop Ratio (PDR) for Mobile-IP for DSR/MSR on 802.11/MPLS

Similar testbed, as in 4.5, has been adopted using OPNET to compare the PDR in a network environment with DSR-IPv6 and MSR-IPv6 on top of 802.11 and MPLS. The results are reflected in Figure 4.11. Wireless nodes uses the following traffic information:

- Traffic rate between Mobile Node to the Access Point is set to 2 Mbps
- For traffic generation, FTP over TCP is used
- IPv6 with DSR or MSR is the network layer protocol
- 802.11 or MPLS is the MAC layer protocol
- Simulation was run for 8 seconds
- The handoff/handover takes place during the first second

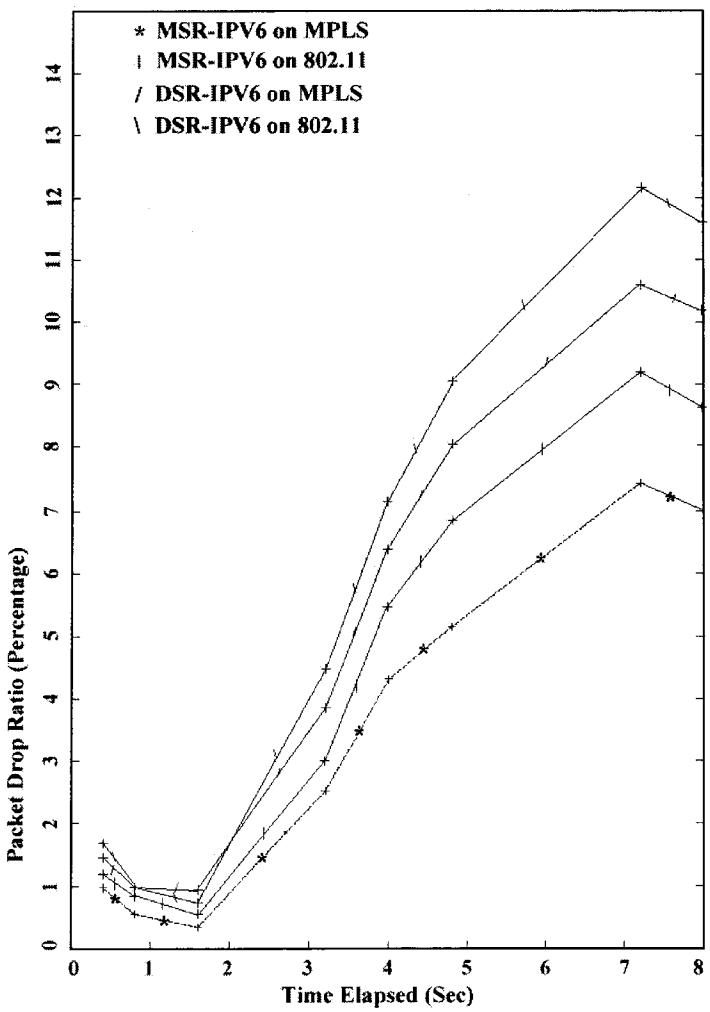


Figure 4.11. The PDR pattern during handoff for MSR/DSR on MPLS/802.11

4.7 Conclusions

In this thesis, the behavior of MPLS-based Mobile-IP system, under various network protocols was tested and special attention was given to the handoff-handover period for QoS monitoring. QoS parameters presented by the proposed architecture, as well as architectures proposed by others, was in-stake during the handoff-handover period.

Those parameters under investigation were:

- Minimum Bandwidth Guaranteed (MBG)
- Packet Loss Ratio (PLR)
- Packet Drop Ratio (PDR)
- Effect Number of Neighbours
- Effect Number of Access Points (APs), and
- TCP Retransmission Pattern

Through extensive simulations, the proposed architecture is proven to guarantee QoS parameters, within minimum accepted value ranges.

4.7.1 Proposed Scheme

Support of QoS for Mobile-IP Ad-Hoc Routing Protocols was investigated, with the following suggestions and proposals:

- Using multihomed MN with MSR routing protocol on top of MPLS, the number of overhead drops
- This overhead is further decreased when MANET using multihomed MN-MPLS-Integrated with FDA is used
- QoS parameters were the main focus of the simulations and these testbed settings ensured approved parameter ranges
- For the worst case scenario "handoff/handover", QoS was maintained

4.8 Future Work

For future work, we suggest further simplification of the Mobile-IP and Ad-Hoc network mechanisms. For this cross-layer approach should be investigated and optional fields in all the involved protocols should be used for Cross-Layer information transfer between components. For Next Generation Networks (NGNs), we suggest that there should be an Increase in the network capability to support future demands of QoS parameters for more efficient handoffs and handovers. The possibility of removing the need for global handoffs/handovers, other schemes, such as, Umbrella Coverage should be investigated.

Finally, new ad-hoc protocols, which are updated frequently, should be investigated to check for more efficient cooperation with MPLS.

REFERENCES

[1] Sasan Adibi, "MSR ANALYSIS IN MICRO-MOBILITY NETWORKS", CCECE 2005, May 1-4 Saskatoon, Canada

[2] Sasan Adibi, Mohammad Naserian, Shervin Erfani, "A FAST HANDOVER M-MANET WITH QOS SUPPORT", CCECE 2005, May 1-4 Saskatoon, Canada

[3] Sasan Adibi, Shervin Erfani, "MOBILE AD-HOC NETWORKS WITH QOS AND RSVP PROVISIONING", CCECE 2005, May 1-4 Saskatoon, Canada

[4] Sasan Adibi, Shervin Erfani, "TCP Connectivity Analysis in Mobile-IP Ad-Hoc Networks", INTERNATIONAL SYMPOSIUM ON COLLABORATIVE RESEARCH IN APPLIED SCIENCE (ISOCRIAS), Vancouver BC, Canada, October 7-9 2005

[5] Sasan Adibi, Shervin Erfani, "Link Layer Connectivity in Mobile-IP Ad-Hoc Networks", to appear on WCNC 2006

[6] Sasan Adibi, Shervin Erfani, "A Comparison Study of Multipath Routing in Flat, Hierarchical, and Geographic Assisted Networks", to appear on RWS 2006

PUBLISHED PAPERS USED IN THIS THESIS

1. **"Mobile Ad-Hoc Networks with QoS and RSVP Provisioning"**, *Sasan Adibi and Shervin Erfani, CCECE Saskatoon, May 1-4 2005*
2. **"Link Layer Connectivity in Mobile-IP Ad-Hoc Networks"**, *Sasan Adibi and Shervin Erfani, to appear on WCNC 2006*
3. **"A Fast Handover M-MANET with QoS Support",** *Sasan Adibi, Mohammad Naserian, Shervin Erfani, CCECE Saskatoon, May 1-4 2005*
4. **"Mobile-IP MPLS-Based Networks",** *Sasan Adibi, Mohammad Naserian, Shervin Erfani, CCECE Saskatoon, May 1-4 2005*
5. **"MSR Analysis in Micro-Mobility Networks",** *Sasan Adibi, Mohammad Naserian, Shervin Erfani, ISNG 2005 Las Vegas, April 2-4 2005*
6. **"Multipath Source Routing Analysis in a Mobile-IP Ad-Hoc Network",** *Sasan Adibi, Mohammad Naserian, Shervin Erfani, CCECE Saskatoon, May 1-4, 2005*
7. **"TCP Connectivity Analysis in Mobile-IP Ad-Hoc Networks",** *International Symposium on Collaborative Research in Applied Science (ISOCRIAS), University of British Columbia, Vancouver Canada, October 7-9, 2005*

SELECTED BIBLIOGRAPHY

MOBILE-IP

Performance Evaluation of Two Layered Mobility Management using Mobile IP, "Jin-Woo Jung, Hyun-Kook Kahng, Ranganathan Mudumbai, Doug Montgomery", **Globcom 2003**

Mobile IP - Enabling Mobility for the 3G Wireless Internet, "Paresh Jain and Rakesh Kelkar", **Technology Review# 2003-02**

Effect of the label management in Mobile IP networks, "Yen-Wen Chen, Zhong-Jian Yan", **AINA '03**

Providing Differentiated Services to Mobile IP Users, "Torsten Braun and Günther Stattenberger", **LCN 2001**

QoS in Mobile-IP version 6, "Z. KAN, D. ZHANG, R. ZHANG, J. MA", **ICII 2001**

Qos Support in Mobile IP Version 6, "Hemant Chaskar and Rajeev Koodli", Nokia Research Center, RFC 3583

IP VERSON 6

IP version 6, "Geoff Huston", **ICANN 2002**

Advanced Routing Suite: IPv4 and IPv6 Testing and Interoperability, "IP Infusion", 2002¨QoS in Mobile-IP version 6, "Zhigang KAN, Dongmei ZHANG, Runtong ZHANG, Jian MA", ICII 2001

Qos Support in Mobile IP Version 6, "Hemant Chaskar and Rajeev Koodli", Nokia Research Center, RFC 3583

RFC 3775 – Mobility Support in IPv6, "D. Johnson, C. Perkins, J. Arkko", June 2004

MPLS

Minimizing re-routing in MPLS networks with preemption-aware, "Balazs Szviatovski, Aron Szentesi, Alpar Juttner", Computer Communications 2002

Restoration by path concatenation: fast recovery of MPLS paths, "Yehuda Afek, Anat Bremler-Barr, Haim Kaplan, Edith Cohen, Michael Merritt", Distributed Computer 2002¨Formulation of the Traffic Engineering Problems in MPLS based IP Networks, "Girish, M., Zhou, B., and Hu, J.Q.", ISCC 2000

QoS Implementation for MPLS Based Wireless Networks, "Subramanian Vijayarangam and Subramanian Ganesan", ASEE April 2002¨Cell Switched IP for MPLS", "Chuck Semeria", Juniper Networks Whitepaper 2002

MPLS label space for optical packet switched networks, "M. J. Reed", IEEE 2003

APPENDIX

UDP (RFC 768)..... 62
IPv4 (RFC 791)..... 65
ICMP (RFC 792)..... 67
TCP (RFC 793)..... 68
IntServ (RFC 1633)..... 68
IPv6 (RFC 1883)..... 71
DiffServ (RFC 2430)..... 72
MPLS (RFC 3031)..... 72
Mobile-IPv4 (RFC 3344)..... 72
Mobile-IPv6 (RFC 3775)..... 72

RFC 768 (RFC768)

User Datagram Protocol

J. Postel
ISI
28 August 1980

User Datagram Protocol

For More Information Refer to: http://www.faqs.org/rfcs/rfc768.html

---

RFC 791 (RFC791)

INTERNET PROTOCOL (IP)
DARPA INTERNET PROGRAM
PROTOCOL SPECIFICATION

September 1981

IP Header

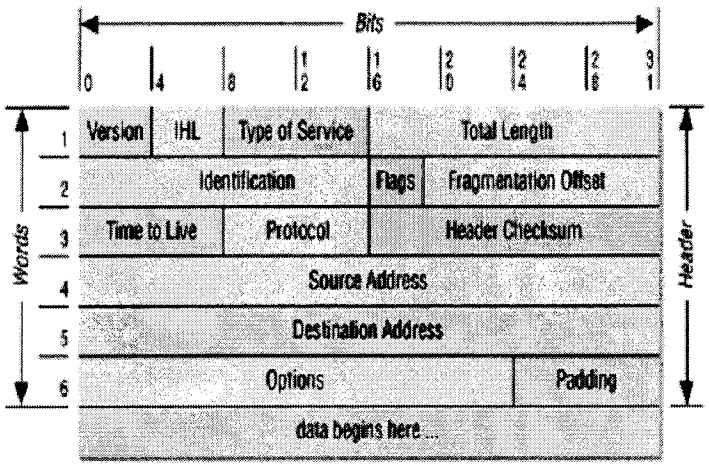


Figure 1.2 IPv4 Frame

IP frame specifications are summarized as follows:

Version, 4 bits = 0100
IHL = Internet Header Length, 4 bits
Type of Service, 8 bits
Total Length, 16 bits
Identification, 16 bits

Flags, 3 bits
Fragmentation Offset, 13 bits
TTL, 8 bits
Protocol, 8 bits
Header Checksum, 16 bits
Source and Destination Addresses, 16 bits each
Options, Variable
Padding, Variable
Data, Variable

Detailed frame specifications are stated as follows:

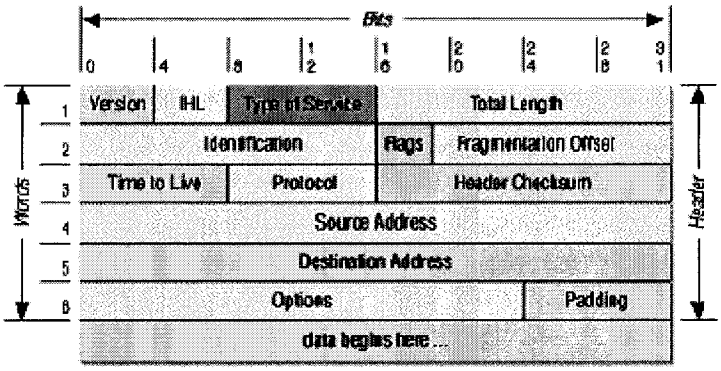


Figure 1.3 Type of Service (ToS) in IPv4 Frame

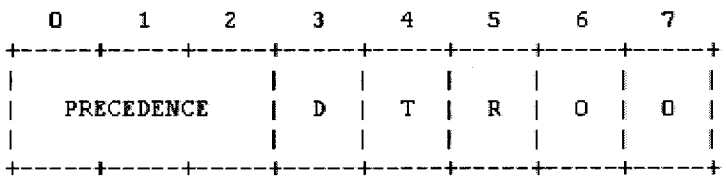


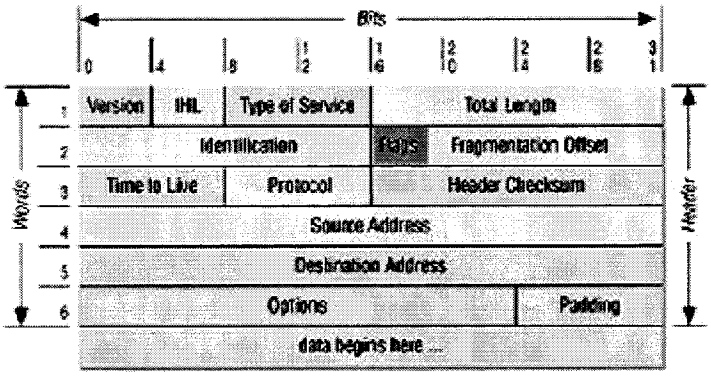
Figure 1.4 Precedence in IPv4

Type of Service (Figures 1.3 and 1.4), 8 bits

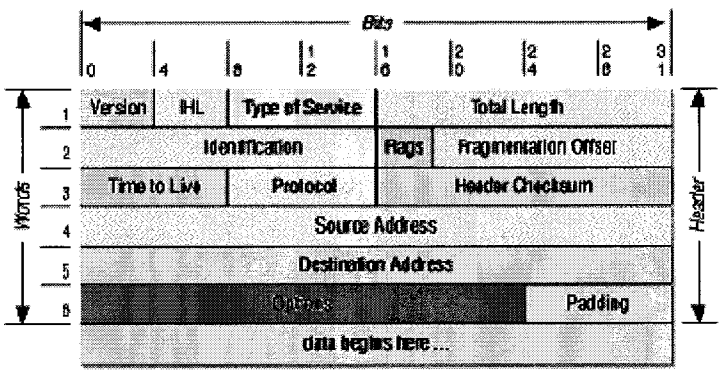
Bits 0-2:	Precedence	
Bit 3:	0 = Normal Delay,	1 = Low Delay
Bit 4:	0 = Normal Throughput,	1 = High Th.
Bit 5:	0 = Normal Reliability,	1 = High Rel.
Bits 6-7:	Reserved for Future Use	

Precedence

111 -	Network Control:	Precedence 7 (High)
110 -	Internetwork Control	Precedence 6
101 -	CRITIC/ECP	Precedence 5
100 -	Flash Override	Precedence 4
011 -	Flash	Precedence 3
010 -	Immediate	Precedence 2
001 -	Priority	Precedence 1
000 -	Routine	Precedence 0 (Low)

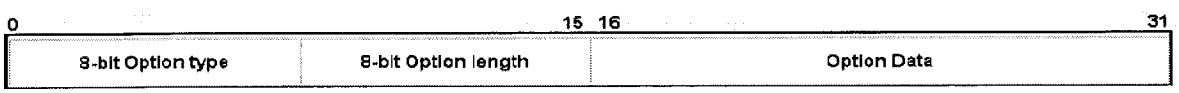


Flags: 3 bits
Bit 0
Reserved
Bit 1
The fragment bit. A value of 0 means packet may be fragmented while a 1 means it cannot be fragmented. If this value is set and the packet needs further fragmentation, an ICMP error message is generated
Bit 2
This value is set on all fragments except the last one since a value of 0 means this is the last fragment



Options: Variable

Options include:
Security and handling restrictions
Record route - Each router records its IP address
Time stamp - Each router records its IP address and time
Loose source routing - Specifies a set of IP addresses the datagram must go through.
Strict source routing - The datagram can go through only the IP addresses specified



Bit 0: Copied Flag: a 0 indicates that the options are to be copied to all fragments

Bits 1-2: Option class. The option classes are as follows:

00 - Control: Normal operation of IP **01 - Reserved**

10 - Debugging and measurement: For special functions such as time stamp, etc

11 - Reserved

Bits 3-7: Option number

The value of these bits combined with the copied flag and option class actually defines what the option is: If the bits 3-7 are:

03H (3 Dec), it indicates "Record Route", RFC 791

Used to record the hops in which the packet travels to the destination

83H (131 Dec), it indicates "Lose Source Route", RFC 791

Forces the packet to pass through the path given by the source with an option to skip one or more hop if necessary

89H (137 Dec), it indicates "Strict Source Route", RFC 2113

Forces the packet to pass through the path given by the source strictly. That is if a hop listed was not ready for passage, the packet is discarded and an error code is generated

For More Information Refer to: http://www.faqs.org/rfcs/rfc791.html

---

RFC 792 (RFC792)

Internet Control Message Protocol (ICMP)

Network Working Group J. Postel
Request for Comments: 792 ISI

September 1981
Updates: RFCs 777, 760
Updates: IENs 109, 128

INTERNET CONTROL MESSAGE PROTOCOL

ICMP Frame

-IP Version always 4

-IHL always 5 for ICMP

-Type of Service always 0

-Total Length

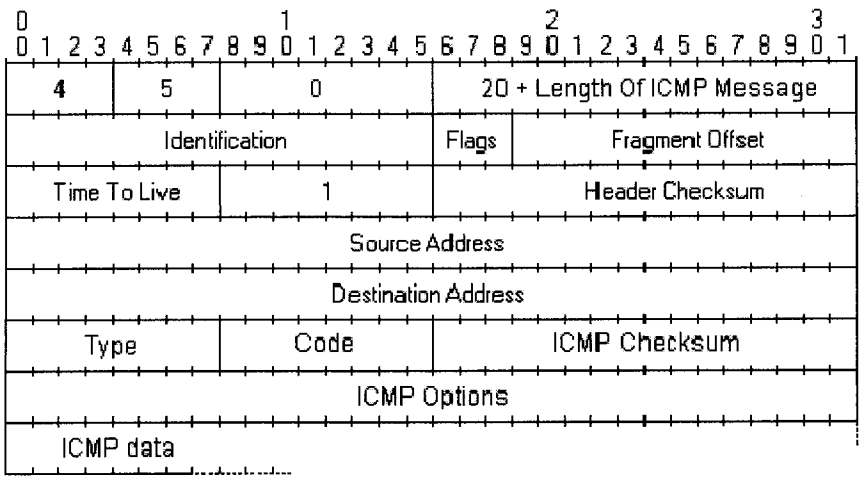
20 (for IP) + ICMP

-Identification

Assigned by the sender to aid in assembling fragments of a datagram. Can be any semi random value

-Flags

The sending host or router will probably always make this value 0




```
ICMP Frame
      -Fragmentation Offset = 0
ICMP messages are very short, no need to be fragmented
      -TTL
Should be high enough
      -Protocol = 1
Indicating ICMP
      -Header Checksum
Checksum is calculated on the IP header only
      -Source Address
Source IP Address
      -Destination Address
Destination Address
```

```
⊟IP: ID = 0x959; Proto = ICMP; Len: 92
   IP: Version = 4 (0x4)
   IP: Header Length = 20 (0x14)
   IP: Precedence = Routine
   IP: Type of Service = Normal Service
   IP: Total Length = 92 (0x5C)
   IP: Identification = 2393 (0x959)
 ⊞IP: Flags Summary = 2 (0x2)
   IP: Fragment Offset = 0 (0x0) bytes
   IP: Time to Live = 128 (0x80)
   IP: Protocol = ICMP - Internet Control Message
   IP: Checksum = 0x519A
   IP: Source Address = 134.171.73.42
   IP: Destination Address = 134.171.73.45
   IP: Data: Number of data bytes remaining = 72 (0x0048)
⊟ICMP: Echo: From 134.171.73.42 To 134.171.73.45
   ICMP: Packet Type = Echo
   ICMP: Echo Code = 0 (0x0)
   ICMP: Checksum = 0x7C7B
   ICMP: Identifier = 9221 (0x2405)
   ICMP: Sequence Number = 0 (0x0)
   ICMP: Data: Number of data bytes remaining = 64 (0x0040)
```

ICMP Frame

```
      -Type of Service
      0 Echo Reply
      3 Destination Unreachable
      4 Source Quench
      5 Redirect
      8 Echo
      11 Time Exceeded
      12 Parameter Problem
      13 Timestamp
      14 Timestamp Reply
      15 Information Request
      16 Information Reply
-Code = 0
      This is a sub-code, telling the ICMP type what to do
-ICMP Checksum
      Calculated over the IP data (excluding the IP Header)
```

For More Information Refer to: http://www.faqs.org/rfcs/rfc792.html

---

RFC 793 (RFC793)

Transmission Control Protocol (TCP)

September 1981

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

by

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

For More Information Refer to: http://www.faqs.org/rfcs/rfc793.html

---

RFC 1633 (RFC1633)

Integrated Services (IntServ) in the Internet Architecture: an Overview

Network Working Group
Request for Comments: 1633
Category: Informational

R. Braden
ISI
D. Clark
MIT
S. Shenker
Xerox PARC
June 1994

For More Information Refer to: http://www.faqs.org/rfcs/rfc1633.html

---

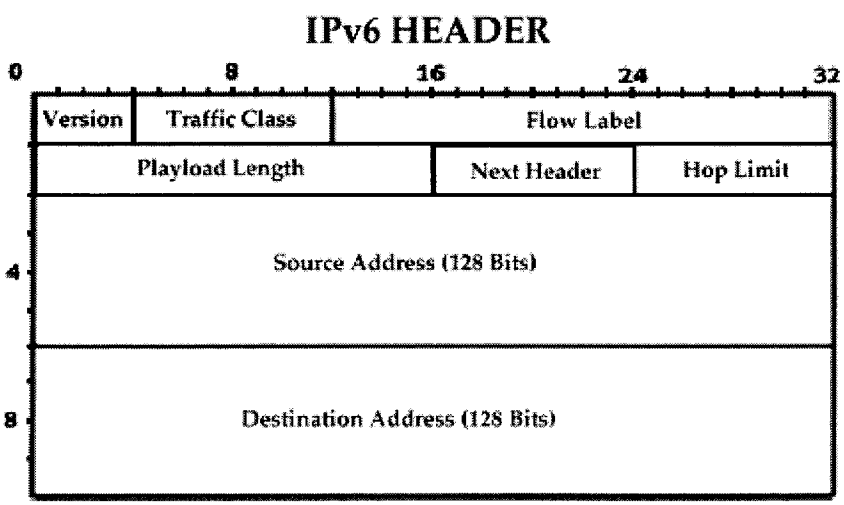
RFC 1883 (RFC1883)

Internet Protocol, Version 6 (IPv6) Specification

Network Working Group
Request for Comments: 1883
Category: Standards Track

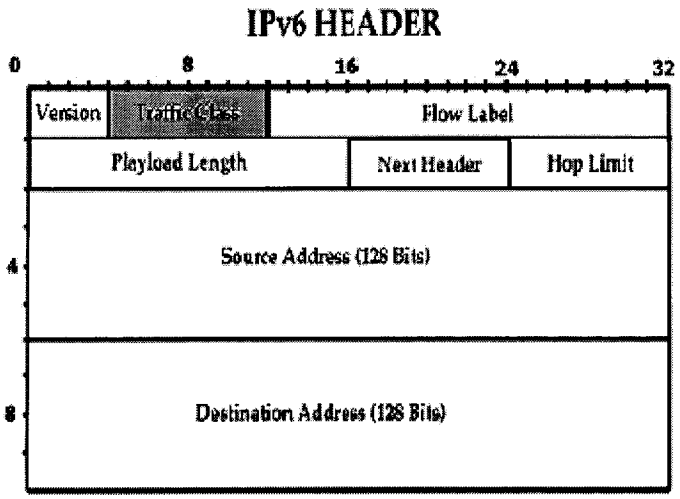
S. Deering, Xerox PARC
R. Hinden, Ipsilon Networks
December 1995

Internet Protocol, Version 6 (IPv6)
Specification

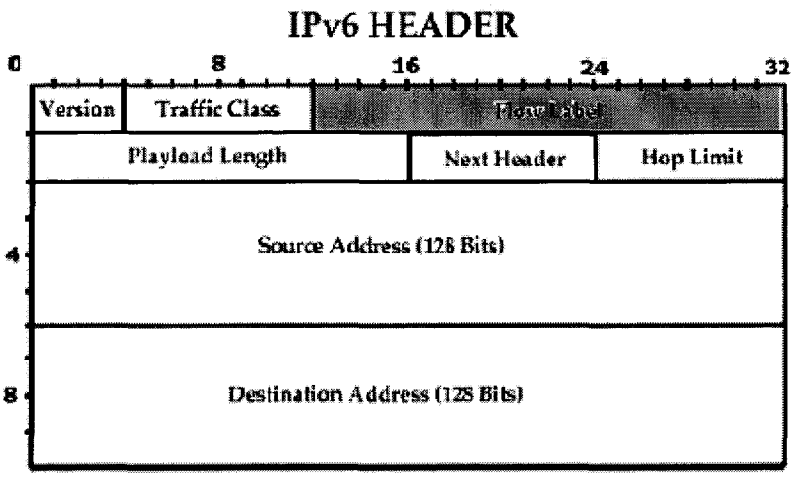


Version, 4 bits = 0110
Priority (Traffic Class), 4 bits
Flow Label, 24 bits
Payload Length, 16 bits
Next Header, 8 bits
Hop Limit, 8 bits

Source Address, 128 bits
Destination Address, 128 bits



Traffic Class (Priority), 4 bits 16 cases
- IPv6 splits the traffic into two categories
    Congestion-Controlled
        May be arbitrarily delayed if the network is congested
        0-7 are related to congestion-controlled
            "0" No priority specified
            "1" Background traffic - e.g. news
            "2" Unattended data transfer - e.g. E-mail
            "3" Reserved
            "4" Attended bulk data transfer - e.g. FTP
            "5" Reserved
            "6" Interactive traffic - e.g. remote logins
            "7" Control traffic - ICMP, SNMP, Routing Information
    Non-Congestion Controlled
        Related to data that cannot be sensibly delayed and should, rather, be discarded, such as real-time audio/video. There's no priority of congestion controlled over the non-congested

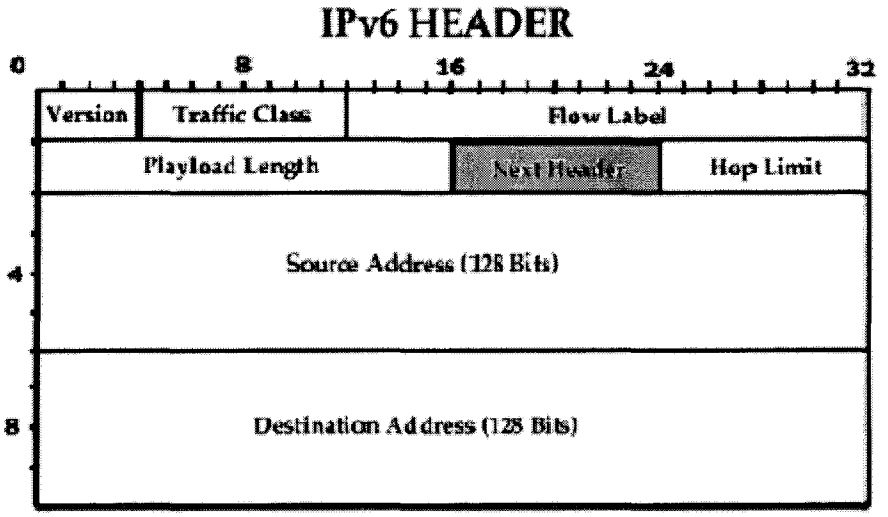


Flow Label Bit Format (RFC 1809 and 3697)

- The Flow Label is a pseudo-random number between 000001 and FFFFFF
- The zero Flow Label is reserved to say that no Flow Label is being used
- All datagrams with the same (non-zero) Flow Label must have the same Destination Address,
  Hp- by-Hop Options header, Routing Header and Source Address contents
- The notion is that by simply looking up the Flow Label in a table, the router can decide how to route and forward the datagram without examining the rest of the header

Flow Label:

- Used to identify a traffic flow
- Provides support for the capability of routing traffic specific to a particular flow via a particular route as this value is visible to all intermediate routers
- Flow labels are still rather experimental



0	Hop-by-Hop Options Header
4	Internet Protocol
6	Transmission Control Protocol
17	User Datagram Protocol
43	Routing Header
44	Fragment Header
45	Interdomain Routing Protocol
46	Resource Reservation Protocol
50	Encapsulating Security Payload
51	Authentication Header
58	Internet Control Message Protocol
59	No Next Header
60	Destination Options Header

For More Information Refer to: http://www.faqs.org/rfcs/rfc1883.html

---

RFC 2430 (RFC2430)

A Provider Architecture for Differentiated Services (DiffServ) and Traffic Engineering (PASTE)

Network Working Group
Request for Comments: 2430
Category: Informational

T. Li
Juniper Networks
Y. Rekhter
Cisco Systems
October 1998

For More Information Refer to: http://www.faqs.org/rfcs/rfc2430.html

---

RFC 3031 (RFC3031)

Multiprotocol Label Switching (MPLS) Architecture

Network Working Group
Request for Comments: 3031
Category: Standards Track

E. Rosen
Cisco Systems, Inc.
A. Viswanathan
Force10 Networks, Inc.
R. Callon
Juniper Networks, Inc.
January 2001

Multiprotocol Label Switching Architecture

For More Information Refer to: http://www.faqs.org/rfcs/rfc3031.html

---

RFC 3344 (RFC3344)

IP Mobility Support for IPv4 (Mobile-IPv4)

Network Working Group
Request for Comments: 3344
Obsoletes: 3220
Category: Standards Track

C. Perkins, Ed.
Nokia Research Center
August 2002

IP Mobility Support for IPv4

For More Information Refer to: http://www.faqs.org/rfcs/rfc3344.html

---

RFC 3775 (RFC3775)

Mobility Support in IPv6 (Mobile-IPv6)

Network Working Group
Request for Comments: 3775
Category: Standards Track

D. Johnson
Rice University
C. Perkins
Nokia Research Center
J. Arkko
Ericsson
June 2004

Mobility Support in IPv6

For More Information Refer to: http://www.faqs.org/rfcs/rfc3775.html

---

VITA AUCTORIS

NAME:	Sasan Adibi
PLACE OF BIRTH:	Tehran, Iran
YEAR OF BIRTH:	1970
EDUCATION:	Alborz High School, Tehran, Iran 1986-1990
	Amirkabir University of Technology, Tehran Iran 1991-1995 B.Sc.
	Brunel University, Western London, UK 1997-1999 M.Sc.
	University of Windsor, Windsor, Ontario 2002-2005 M.Sc.