# AN OPTIMIZED FRAMEWORK FOR HEADER SUPPRESSION OF REAL TIME IPv6 TRAFFIC IN MULTIPROTOCOL LABEL SWITCHING (MPLS) NETWORKS

**By**

**IMAD JASIM MOHAMMED**

**Thesis submitted in fulfillment of the requirements**

**for the degree of**

**Doctor of Philosophy**

**August 2011**

## ACKNOWLEDGEMENTS

**بسم الله الرحمن الرحيم**

**{نرفع درجات من نشاء وفوق كل ذي علم عليم "76"} (سورة يوسف)**

I would like to take this opportunity to convey my sincere thanks and deepest gratitude to my supervisor, **Dr. Wan Tat Chee,** for all the help and valuable guidance provided to me throughout my period of research. I consider myself privileged to have had the opportunity to work under his guidance. I'm also grateful to my co-supervisor **Dr. Putra Sumari** for his help and support.

Moreover, I would like to convey my appreciation to **Prof. Sures** (NAv6 Director), **Dr. Andrew Meulenberg** and to **Yung-Wey Chong** (NAv6), all NAv6 center members, the School of Computer Sciences, the Institute of Postgraduate Studies, and the university library for their help and support.

My sincere gratitude also goes to **my parents**, my wonderful wife **Hind**, **brothers**, **sisters**, and our children **Noor, Mohammed, Hajer, and Yaseen**. I thank them for their support, understanding, and encouragement during every step of my study and writing of this thesis.

The favour, above all, before all, and after all, is entirely Allah's, to whom my never-ending thanks and praise are humbly due.

Thank you!

Imad Jasim Mohammed
Penang, Malaysia, March 2011

## DEDICATION

This thesis is dedicated to my mother, father, wife, brothers, sisters and children for their patience and the encouragement they provided during the entire period of the study.

## TABLE OF CONTENTS

## LIST OF TABLES

# LIST OF FIGURES

# LIST OF ABBREVIATIONS

| | |
|---|---|
| ARPANET | Advanced Research Project Agency Network |
| ATM | Asynchronous Transfer Mode |
| BER | Bit Error Rate |
| BS | Base Station |
| CE | Customer Edge |
| CID | Context Identifier |
| CoS | Class of Service |
| CRC | Cyclical Redundancy Checking: |
| CR-LDP | Constrained-based Routing - Label Distribution Protocol |
| CSPF | Shortest Path First algorithm |
| CT | Class Type |
| DestIP | Destination IP |
| DRR | Deficit Round Robin |
| DSCP | Differentiated Service Code Point |
| ECRTP | Enhanced Compressed RTP |
| ERT | Explicit Routing Table |
| EXP | Experimental |
| FEC | Forwarding Equivalent Class |
| FO | First Order |
| FSM | Finite State Machine |
| FTP | File Transfer Protocol |
| GSM | Global System for Mobile Communications |
| HC | Header Compression |
| HD | Header Decompression |
| HTTP | Hyper Text Transfer Protocol |
| IETF | Internet Engineering Task Force |

| | |
|---|---|
| IGP | Internet Gateway Protocol |
| IPHC | Internet Protocol Header Compression |
| IPv6 | Internet Protocol version 6 |
| IR | Initialization and Refresh |
| ISP | Internet Service Provider |
| ITU-T | International Telecommunication Union - Telecommunication Standardization Sector |
| LAN | Local Area Network |
| LDP | Label Distribution Protocol |
| LER | Label Edge Router |
| LIB | Label Information Base |
| LSP | Label Switched Path |
| LSR | Label Switching Router |
| Mbone | Multicast Backbone (Internet) |
| MPHS | Multiprotocol Payload Header Suppression |
| MPLS | Multiprotocol Label Switching |
| native | IPv6 with MPHS |
| NS2 | Network Simulator version 2 |
| OSI | Open System Interconnections |
| PE | Provider Edge |
| PFT | Partial Forwarding Table |
| PHS | Payload Header Suppression |
| PHSF | Payload Header Suppression Field |
| PPP | Point-to-Point Protocol |
| PPS | Packet Per Second |
| PW | Pseudo Wire |
| QoS | Quality of Service |
| RESV | Reservation |
| ROHC | RObust Header Compression |

| | |
|---|---|
| RSVP | Resource Reservation Protocol |
| RTP | Real-Time Transport Protocol |
| SIP | Session Initiation Protocol |
| SLA | Service Level Agreement |
| SO | Second Order |
| SS | Subscriber Station |
| TCP | Transmission Control Protocol |
| TCP | Traffic Conditioning |
| TE | Traffic Engineering |
| TTL | Time To Live |
| tunnel | 6-in-4 with MPHS |
| UDP | User Datagram Protocol: |
| VAD | Voice Activation Detection |
| VoIP | Voice over IP |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WFQ | Weighted Fair Queuing |
| WiMAX | Worldwide Interoperability for Microwave Access |
| without | IPv6 without MPHS |
| WWW | World Wide Web |

# SUATU KERANGKA KERJA TEROPTIMUM BAGI PENINDASAN KEPALA TRAFIK IPV6 MASA NYATA DALAM RANGKAIAN PENSUISAN LABEL MULTIPROTOKOL (MPLS)

## ABSTRAK

Pensuisan Label Multiprotokol (MPLS) dengan IPv6 telah dinyatakan oleh Pasukan Petugas Kejuruteraan Internet (IETF) sebagai mampu diskalakan dan sangat sesuai untuk jenis-jenis trafik yang berlainan seperti VoIP dan Video. Namun, kepala IP yang besar melahirkan overhed kepala yang berlebihan dalam rangkaian MPLS, mengakibatkan kesesakan trafik lalu menjejaskan prestasi rangkaian tulang belakang.

Suatu skema penindasan kepala yang baru, Penindasan Kepala Muatan Multiprotokol (MPHS) dicadangkan dalam tesis ini yang menawarkan penggunaan jalur lebar yang lebih baik bagi MPLS-LSP (Laluan Bersuis Label). Skema yang dicadangkan ini adalah untuk memenuhi ketersediaan yang tinggi bagi rangkaian tulang belakang yang memerlukan skema penindasan yang lebih ringkas. Ianya dibawa merentasi keseluruhan rangkaian tulang belakang, tidak seperti skema yang ada kini yakni, Penindasan Kepala Muatan (PHS) atau Penindasan Kepala Lasak (ROHC), yang kebanyakannya digunakan di rangkaian capaian.

Penyelesaian yang dicadangkan ini membolehkan lebih banyak strim IPv6 masa nyata dan  bukan masa nyata pada tulang belakang yang dibolehkan oleh MPLS, disokong dengan QoS (Kualiti Perkhidmatan) hujung-ke-hujung yang boleh diterima. Tesis ini membentangkan empat sumbangan utama terhadap domain

MPLS. Pertama, MPHS menyokong strim IPv6 asli. Kedua, ia membenarkan strim 6-dalam-4 antara Pinggir Pelanggan (CE-keCE). Ketiga, ia menyokong kewujudan bersama trafik bukan masa nyata seperti trafik Sesawang menggunakan aplikasi berasaskan HTTP (Protokol Pindahan Teks Hiper) dan aplikasi berasaskan FTP (Protokol Pindahan Fail). Akhir sekali, MPHS menyokong LSP Eksplisit.

Keberkesanan MPHS telah diuji menggunakan Simulasi Rangkaian versi 2 (NS2). Hasilnya disahkan menerusi model analitis untuk menunjukkan bahawa ia adalah sebanding dan sepadan dengan hasil daripada model simulasi.

Menggunakan MPHS, pertambahan penindasan yang ketara iaitu 64% bagi trafik IPv6 asli dan 63% bagi trafik 6-dalam-4 dilihat sebagai sebanding dengan skema-skema penindasan yang sedia ada. Penggunaan jalur lebar bagi IPv6 masa nyata dan trafik 6-dalam-4 telah meningkat sebanyak 31%. Seterusnya, lengah bingkisan dalam rangkaian MPLS berkurangan daripada sebanyak 22% apabila MPHS diaktifkan di rangkaian teras. Dari segi kesan MPHS terhadap trafik heterogen, masa tindak balas bagi trafik pelanggan-pelayan berkurangan sebanyak 1.7s (daripada 24.88s kepada 23.14s) bagi trafik Sesawang IPv6, menyingkirkan jatuhan bingkisan bagi data UDP. Truput data TCP meningkat sebanyak 20%, meminimumkan masa lengah dengan begitu berkesan. Selain itu, pengurangan kepelbagaian dalam truput bagi trafik TCP dan UDP dapat dilihat apabila MPHS diaktifkan.

# AN OPTIMIZED FRAMEWORK FOR HEADER SUPPRESSION OF REAL TIME IPv6 TRAFFIC IN MULTIPROTOCOL LABEL SWITCHING (MPLS) NETWORKS

## ABSTRACT

Multiprotocol Label Switching (MPLS) with IPv6 has been defined by the Internet Engineering Task Force (IETF) as highly scalable and well suited for different types of traffic such as VoIP and Video. However, large IP headers create excessive header overhead in a MPLS network leading to traffic congestion degrading the backbone network performance.

A new header suppression scheme, Multiprotocol Payload Header Suppression (MPHS) is proposed in this thesis to offer better bandwidth utilization for MPLS-LSP (Label Switched Path). The proposed scheme caters for high availability of the backbone network that requires much simpler compression schemes. It is carried across the entire backbone network, unlike the existing schemes namely, Payload Header Suppression (PHS) or Robust Header Compression (ROHC), that are mainly used at access network.

The proposed solution allows more real-time and non real-time IPv6 streams over MPLS-enabled backbone to be supported with acceptable end-to-end QoS (Quality of Service). This thesis presents four main contributions over a MPLS domain. Firstly, MPHS supports native IPv6 streams. Secondly, it enables 6-in-4 streams between Customer Edges (CE-to-CE). Thirdly, it supports coexistence of non real-time traffic such as Web traffic using HTTP (Hyper Text Transfer

Protocol)-based applications and FTP (File Transfer Protocol)-based applications. Finally, MPHS supports Explicit LSP.

The effectiveness of MPHS was investigated using Network Simulation version-2 (NS2). The results were validated against analytical models to show that it compares and agrees well with the outcome of the simulation model.

Using MPHS, significant suppression gain of **64%** for native IPv6 traffic and **63%** for 6-in-4 traffic were seen as compared to the existing compression schemes. The bandwidth utilization for real time IPv6 and 6-in-4 traffic was improved by **31%**. Subsequently the packet delay in the MPLS network decreased by **22%** when MPHS was activated at the core network. In terms of effects of MPHS on heterogeneous traffic, response time for client-server traffic improved by **1.7s** (from 24.88 to 23.14) for IPv6 Web traffic eliminating packet drop for UDP data. The TCP data throughput was increased by **20%,** effectively minimizing the delay time. In addition, less variation in throughput for TCP and UDP traffic was seen when MPHS was activated.

# CHAPTER ONE
# INTRODUCTION

## 1.1 Background

The growth of the Internet mirrors the rapid development of new protocols, mechanisms and the remarkable increase of Internet users, for data communication and computer networking. This growth, in turn, has been fueled by the exponential growth of the World Wide Web (WWW). Historically the Web has triggered explosive escalation in the Internet due to fast growth of e-mail after ARPANET (Advanced Research Project Agency Network) establishment (Stallings, 2002). The tremendous increase in traffic volume generated from the Web, real-time multimedia, and multicasting applications has motivated researchers to develop new technologies such as Multiprotocol Label Switching (MPLS), and latest techniques such as header compression that can support better Quality of Service (QoS). However, MPLS is one of the technologies that have been used in Internet backbone.

Data packets for real time applications are mainly a comprised form of voice and video, which represent main drivers for QoS implementation and traffic engineering mechanisms in the internet (Meddeb, 2010). Real time application such as Voice over IP (VoIP) having small payloads as compared to their headers results in significant packet processing overheads (Fortuna & Ricardo, 2009). Header compression schemes such as Robust Header Compression (ROHC) and Payload Header Suppression (PHS) were developed for WiMAX defined in IEEE 802.16, where header overhead of real time traffic is the major concern.

MPLS is a routing and forwarding protocol standardized in 2001. The MPLS architecture is defined in (RFC3031, 2001). The traffic engineered MPLS technology is highly distinguished as the modern approach that guarantees the high level of quality and reliability that we expect from telephony services (Juniper, 2007). Explicit label switched path (Explicit-LSP) is one of the MPLS properties that permit the booking of an explicit LSP that is not necessarily the shortest path. Explicit-LSP can be deployed for different situations, like fast restoration path (in failure cases of node/links), for MPLS-Traffic Engineering usage, load balancing, etc. Internet Service Providers have combined the features of MPLS such as speed, Traffic Engineering (TE), QoS, VPN and resiliency with IPv6 features as an alternative transporting facility over the Internet backbone (Griviaud, 2008).

Typically Internet backbone networks suffer from high load traffic and congestion at edge routers. This bandwidth consumption for packet headers is higher as compared to access network in Wireless, WiMAX or satellite networks. For example, as stated in (RFC4247, 2005), for a real-time application such as VoIP over a WAN, packet headers for 300 million calls per day could consume of about 20-40 Gbps.

Currently there are limited comparative studies between compression and suppression schemes in terms of complexity analysis. Compression schemes are mainly compressing IP header field to less number of bits using encoding and decoding techniques. Suppression schemes work by stripping out an IP header field at the sender node and then restoring the field at the receiver node. No work has been done on implementation of header suppression for IPv6 and 6-in-4 over MPLS for real time applications. Moreover, Multi-Ingresses and Multi-Egresses in MPLS domains need to be addressed compared to mobile to edge router connection. Further, most compression techniques focuses mainly on wireless and satellite technologies, leaving out other network technologies such as MPLS.

## 1.2 Problem Statement

One of the most critical aspects in transmitting real time streams over IPv6 networks is the increase in header size in relation to the small payload size compared to IPv4 that represents extra overhead (or successive headers overhead problem). These overheads are considered additional costs in terms of complexity metrics such as time complexity for packet header processing, storage resources such as queuing requirement, and transmission bandwidth requirements. As a result these overheads might contribute negatively in the network performance (QoS) and increase the probability of traffic congestion problem. In terms of QoS parameters, real time applications are very sensitive to the delay and jitter.

In a data stream, most of the fields in the packet header would be the same from the first packet to the last packet. In real time applications such as VoIP, the header overhead problem defined above will be seen in every packet in such a data stream. For example, encapsulated data packet consuming a total of 93 bytes where 60 bytes for RTP/UDP/IPv6 header and 33 bytes for voice data (using GSM 6.0 codec). The header occupies more than half (actually 64%) of the packet size. This overhead problem could be reduced using header suppression scheme that is proposed in this thesis.

## 1.3 Research Motivations

The following are the motivations for current research:

- The increase in interest over the implementation of MPLS as an efficient transport technology for telecommunication industry.

- The need to investigate the effect on performance of large header sizes relative to small data payload for IPv6 Internet Backbone infrastructure using MPLS technologies.

- The choice of suitable header reduction scheme to reduce the header overhead for real time data flow.

## 1.4 Objectives

The overall objective of this thesis is to enhance the efficiency of packet processing in terms of QoS metrics such as bandwidth utilization, throughput, delay, jitter, and packet drop for real time applications. To achieve the above objective, the specific objectives are defined as follows:-

1) To perform a qualitative functional comparison between existing header compression schemes (e.g. PHS and ROHC) with the proposed framework for the MPLS-enabled backbone.

2) To propose a new framework that enhances the QoS performance of real time applications in the MPLS-based backbone by incorporating overhead reduction techniques.

3) To analyze the proposed framework using an end-to-end queuing model and study its effect on real time IPv6 traffic by simulation to obtain more statistics regarding the performance.

4) To investigate the interaction of overhead reduction for real time IPv6 traffic with non real-time traffic such as web traffic using the HTTP protocol, as well as data transfers using FTP protocol.

## 1.5 Scope

The scope of this work (Figure 1.1) is limited to IPv6 client networks for real time traffic, multiple mixed IPv4/IPv6 domains with MPLS support, 6-in-4 tunneling approach, and one real time codec using, **Global System for Mobile Communications** (GSM).

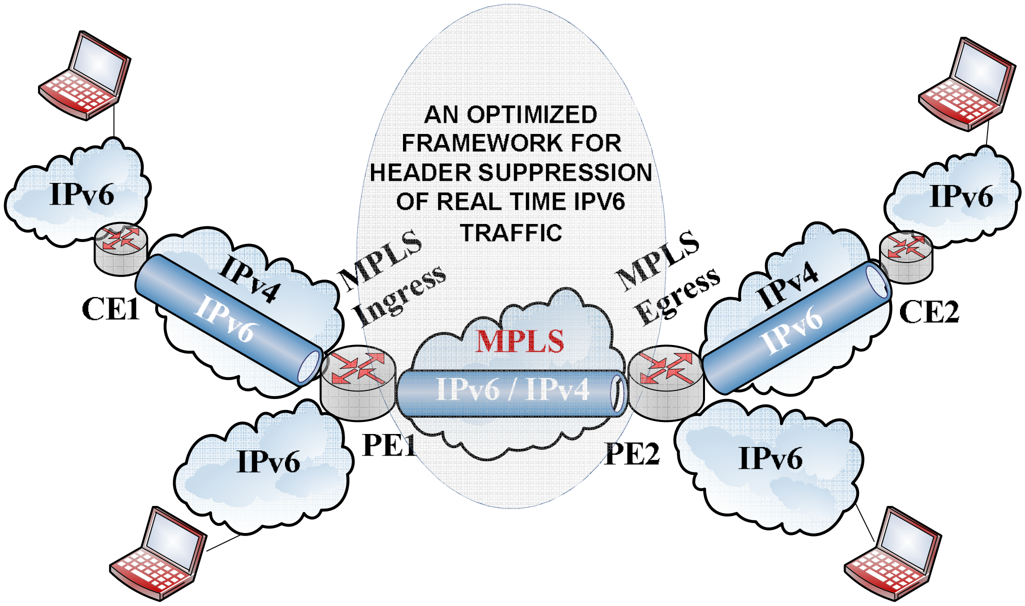

Figure 1.1: Thesis Scope

## 1.6 Research Framework

Fig 1.2 depicts complete research framework of the thesis.

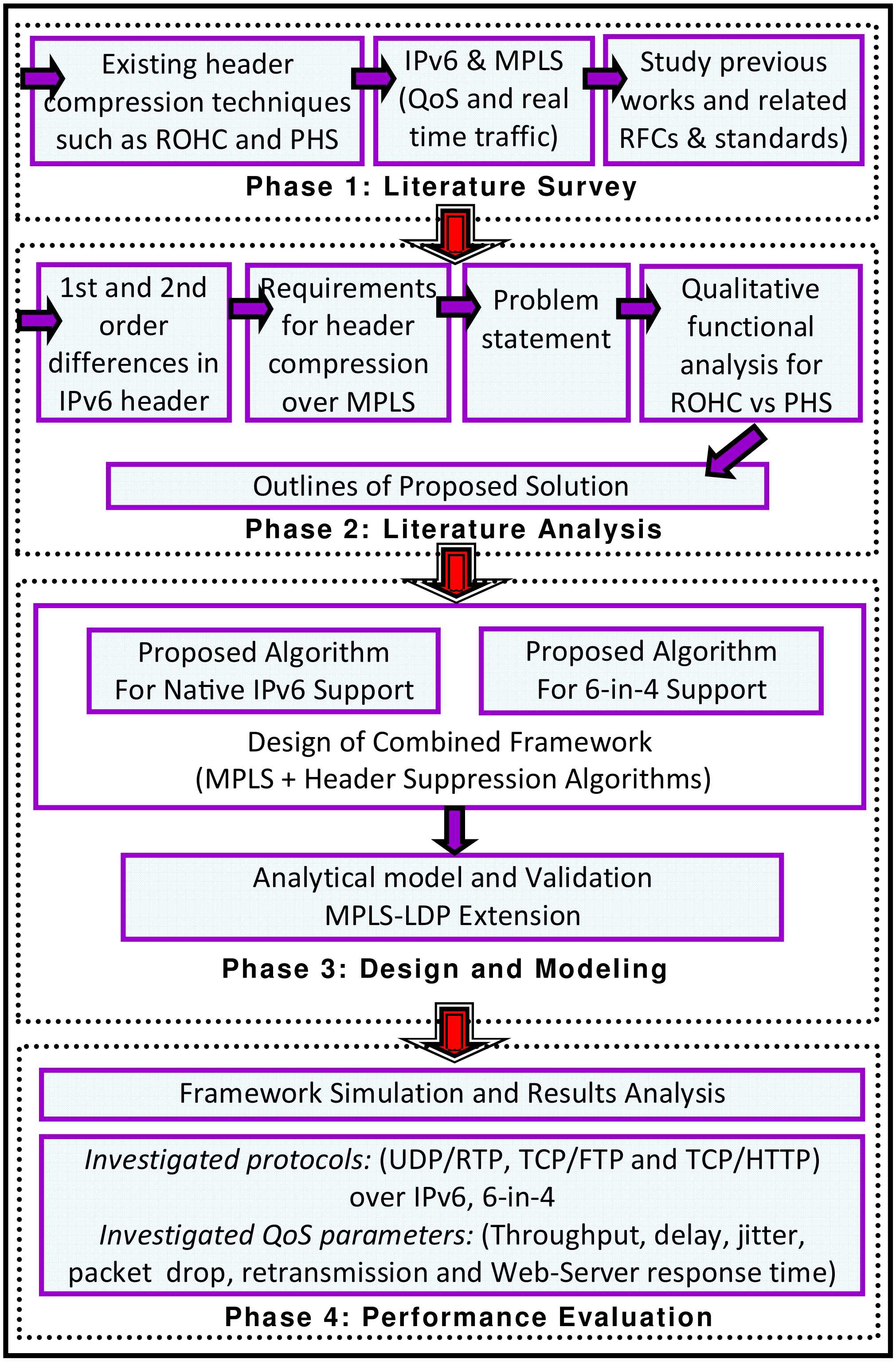
Existing header compression techniques such as ROHC and PHS
IPv6 & MPLS (QoS and real time traffic)
Study previous works and related RFCs & standards)
Phase 1: Literature Survey
1st and 2nd order differences in IPv6 header
Requirements for header compression over MPLS
Problem statement
Qualitative functional analysis for ROHC vs PHS
Outlines of Proposed Solution
Phase 2: Literature Analysis
Proposed Algorithm For Native IPv6 Support
Proposed Algorithm For 6-in-4 Support
Design of Combined Framework (MPLS + Header Suppression Algorithms)
Analytical model and Validation MPLS-LDP Extension
Phase 3: Design and Modeling
Framework Simulation and Results Analysis
Investigated protocols: (UDP/RTP, TCP/FTP and TCP/HTTP) over IPv6, 6-in-4
Investigated QoS parameters: (Throughput, delay, jitter, packet drop, retransmission and Web-Server response time)
Phase 4: Performance Evaluation

Figure 1.2: Research Framework

## 1.7 Thesis Organization

This thesis is organized into seven chapters.

**Chapter 1** presents the preamble and objectives of this thesis. It starts by presenting a background discussion for the header compression schemes for real time applications and overview for MPLS-IPv6 technology with our research motivations and objectives.

**Chapter 2** extensively covers the literature survey and discusses the most current and related works in header compression research field and MPLS technology. The researcher will also discuss properties of IPv6 header, QoS models, and requirements for header compression over MPLS. Functional analysis for ROHC and PHS is introduced. The reasons of choosing payload header suppression for MPLS framework are discussed.

**Chapter 3** covers the methodology discussion on how the proposed solution was designed. The new header suppression algorithm (MPHS) for MPLS is introduced in this chapter. Functional comparisons for MPHS versus PHS and ROHC using finite state machines (FSM) are introduced. Justifications and consideration for MPHS are also described in this chapter.

**Chapter 4** introduces an end-to-end analytical model for MPHS. It verifies the model by comparing the model and simulation results. It discusses the model in terms of QoS components such as delay, throughput and packet drop.

**Chapter 5** introduces the simulation environment for MPHS in terms of design and analysis. In addition, it states simulation parameters, scenarios for MPHS experiments, and QoS performance metrics used, while simulation results, analysis and discussion for experiments are presented in **Chapter 6**.

**Chapter 7** introduces the research findings; research conclusion, and the possible future work for this study.

# CHAPTER TWO
# LITERATURE REVIEW

## 2.1 Introduction

This chapter introduces the work related to header compression, real time traffic requirements, MPLS technology, IPv6 and 6-in-4 header specification and principles for QoS. It produces a functional comparison for PHS versus ROHC in terms of complexity. The work includes major and minor research domains originating from QoS IPv6 header compression and supersession (Figure 2.1). In addition, it discusses the most related works in terms of QoS performances, advantages, limitations, and outlines the justification for proposed framework.

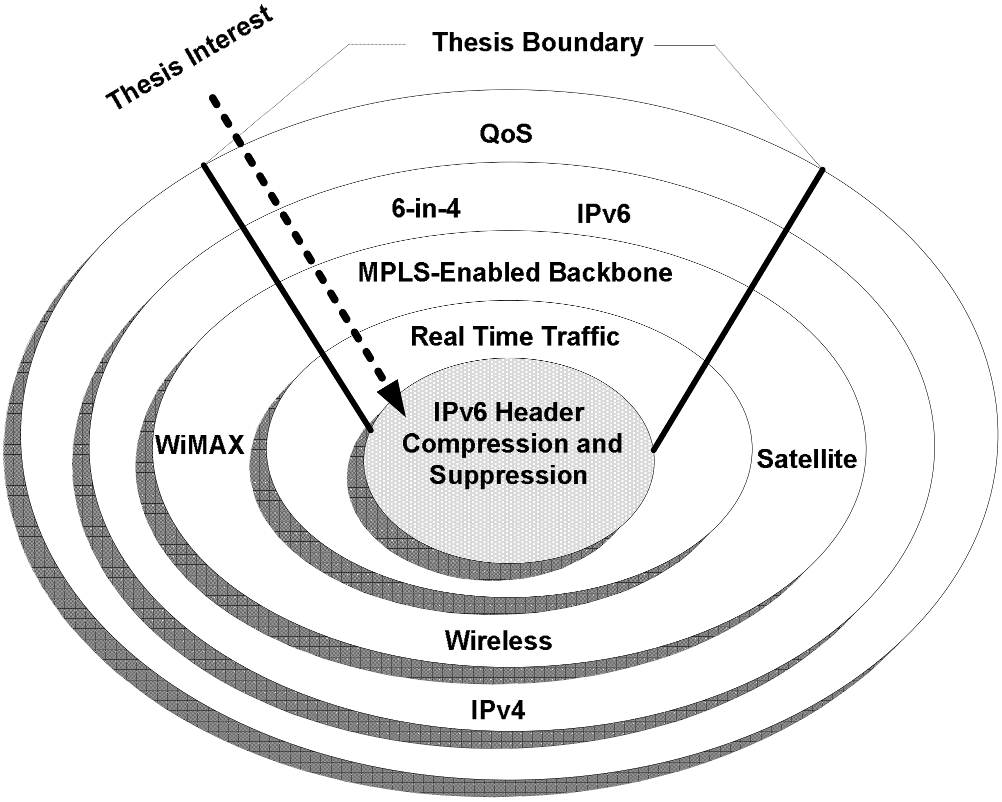

Figure 2.1: Thesis Interest & Boundary

## 2.2 QoS Models, Mechanisms and Metrics

Internet QoS efforts are aimed to expand the base services of a network to a number of selectable service responses which are distinguished from the best-effort service by supporting superior service level. The expanded services are distinguished by providing a predictable service response, despite varying network traffic load such as the number of concurrent traffic flows (RFC2990, 2000). In terms of quality of service, metrics such as delay, jitter, packet loss, throughput, service availability, and per flow sequence preservation, measures the service quality that IP Traffic experiences.

Real time applications which are mainly voice and video packets representing main drivers for QoS implementation and traffic engineering mechanisms in the internet (Meddeb, 2010). It needs to fulfill certain requirements to achieve end to end QoS metrics. For instance, less than 200ms latency is recommended for voice conversation, at about 30ms jitter is preferred, and below 1 percent packet loss ratio is recommended (Szigeti & Hattingh, 2004).

In terms of OSI (Open System Interconnection) model, Real Time Protocol (RTP) is a transport layer protocol commonly used to transport digitally encoded stream of Voice over IP (VoIP) (RFC3550, 2003) and video over IP. The delivery of the VoIP bearer stream from sender to receiver is a dealing function of RTP which uses one of the signaling protocols such as Session Initiation Protocol (SIP) (RFC3261, 2002) to setup the VoIP session and to determine the codec format used.

Various types of codecs are used to compress and transmit the VoIP packets of real time applications, and most of these codecs produce small packet sizes. Properties of VoIP codec's vary in bandwidth requirements, call delivery quality and complexity. In addition, some codecs use compression to reduce the required bandwidth for a VoIP call, and consequently can be divided into lose and lossless codec's based on compression quality (Evans & Filsfils, 2007). Voice datagram(s) (Taylor, et al., 2005) are on the order of 20 bytes while IPv6/UDP/RTP headers are on the order of 100 bytes. GSM codec is considered as VoIP codec for this thesis.

### 2.2.1 Network QoS Requirements for VoIP Applications

VoIP applications are defined by different Service Level Agreement (SLA) metric parameters such as (Evans & Filsfils, 2007). The formula for each of the following QoS metric is defined in **Chapter 5**.

`

#### 2.2.1.1 Delay

Delay is an expression of how much time it takes for a packet of data to get from one designated source to destination. The interactive conversational speech is the main impact factor for one-way end-to-end delay. For example ITU-T recommendation on mouth-to-ear delay was specified in G.114 which uses the E-model and suggested that delay around 150 ms will satisfy for most VoIP applications/users. As the delay increases, the satisfactory level decreases. It will become unacceptable once the delay value passes the 400 ms threshold (delay levels are shown in Table 2.1). The mean opinion score MOS "is a well established scheme, which provides a numeric measure of the quality of a voice call at the destination" (Evans & Filsfils, 2007).

TABLE 2.1: ITU G.114 Determination of the Effects of Absolute Delay by the E-model (Evans & Filsfils, 2007)

| Ear-to-mouth | R factor | Objective MOS |
|---|---|---|
| **Delay < 150 ms** | 80 – 89 | 5 |
| **150 ms < delay < 250 ms** | 70 - 79 | 4 |
| **250 ms < delay < 325 ms** | 60 - 69 | 3 |
| **325 ms < delay < 425 ms** | 50 – 59 | 2 |
| **Delay > 425** | 90 - 100 | 1 |

Network delay which impacts the VoIP call is one component of the end-to-end delay. In order to satisfy VoIP application requirements, the network QoS design should consider the maximum delay values mentioned above and apportion the budget to various network delay components (such as propagation delay through the backbone such as MPLS backbone, scheduling delay due to congestion, access link serialization delay, and end-system delay due to VoIP codec and jitter buffer).

#### 2.2.1.2 Jitter

It is the parameter that characterizes the variation of network delay. In practice de-jitter buffers (which is used at the destination end-systems to remove jitter or delay variation by converting delay variation to constant delay), and play-out buffers are used to control delay variation.

#### 2.2.1.3 Packet Drop

This QoS parameter is calculated from the difference between the sending number and receiving number of packets Packet drop could happen as a result of traffic congestion, lower layer errors, network element failures, or loss in the application end-systems.

#### 2.2.1.4 Throughput

It is referred to as the amount of data (packet payload) moved successfully from one place (source) to another (destination) in a given time period. Average bandwidth used for a call can be reduced by using various techniques such as Voice Activation Detection (VAD) (which uses silence suppression techniques), and/or header compression techniques such as ROHC or PHS. Goodput is another QoS metric that exclude protocol overhead of transport, network and data link layers from the throughput (Yoo, 2010).

### 2.2.2 QoS Models

In terms of QoS models, (Wallace., 2004) Cisco developed QoS features and categorized them into one of the following three models (Figure 2.2).

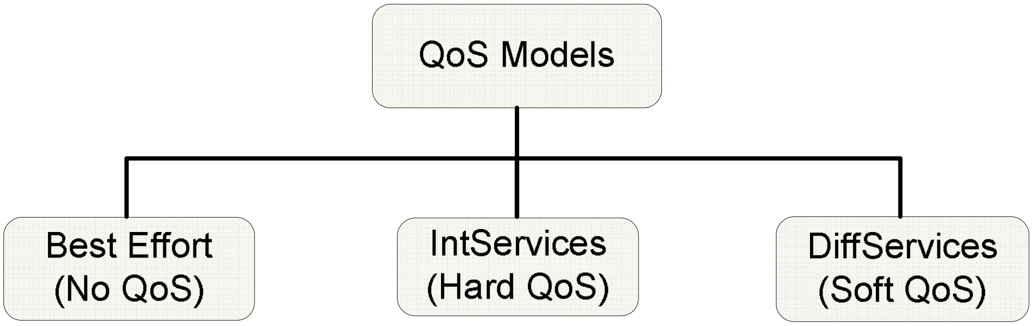

Figure 2.2: QoS Models (Wallace., 2004)

#### 2.2.2.1 Best Effort (No QoS)

Best Effort is the traditional datagram model. No differentiation between elastic and inelastic streams exists in this model which contributes to unpredictable services.

#### 2.2.2.2 Integrated Services (Hard QoS)

IntServ Architecture was defined in (RFC1633, 1994) It is characterized by guaranteeing per-flow QoS and strict bandwidth reservations. IntServ requires signaling for path reservation using Resource Reservation Protocol defined (RFC2205, 1997). Path/RESV messages require admission control and must be configured on every router along the path, and work well on small-scale. The main disadvantages of this model are scaling with large number of flows and requiring devices to retain state information.

#### 2.2.2.3 Differentiated Services (Soft QoS)

DiffServ architecture is defined in (RFC2475, 1998). It is scalable, well supportive to large flows through aggregation, and defines per-hop behavior (PHB). It is capable to create Traffic Conditioning (TC) meaning when edge nodes perform TC such as MPLS ingress nodes, it allows core routers to do more important processing tasks. Additionally, with DiffServ it is tough to predict end-to-end behavior.

DiffServ techniques were designed to integrate in orthogonal manner with traffic engineering mechanisms. While DiffServ techniques are concerned about traffic class's differentiation, traffic engineering needs to ensure QoS provision within class of service.

### 2.2.3 Router Operational Planes

A router operates in two operational planes: control and data plane. (Evans & Filsfils, 2007):

#### 2.2.3.1 Data Plane

Data plane includes processing intensive functions, packet forwarding lookups and packet filtering functions applied at network nodes and mostly implemented using hardware in high performance routers. QoS mechanisms of data plane can be classified according to the primitive behavior characteristics as follows:

- Classification (class of service)
- Marking: Setting up the QoS related traffic fields of IP or MPLS to identify the traffic easily.
- Policing and shaping: used for maximum rate enforcement.
- Prioritization: used for setting up traffic priority to provide it with estimated delay and jitter.
- Minimum rate assurance: Minimum bandwidth assurance for different traffic classes can be achieved by implementing scheduling techniques such as Deficit Round Robin (DRR) and Weighted Fair Queuing (WFQ).

#### 2.2.3.2 Control Plane

Its function includes signaling plane or controlling the data plane. It deals with admission control, routing protocols and resource reservation mechanisms, and it is typically implemented using software. For example RSVP is used for control plane or QoS signaling in the context of integrated services architecture for flow resource reservation & admission control. It is also used to setup MPLS traffic engineering LSPs.

## 2.3 IP Protocols for Internet

IPv4 header contain twelve fields plus option field which yields a size between 20-60 octets compared to eight fields used by IPv6 with a size of 40 octets (Figure 2.3). The option fields in IPv4 headers induce transmission complexities due to the use of variable length headers compared to the fixed header lengths in IPv6. Typically 5-tuple (source address, destination address, protocol, source port, destination port) is used as the IPv4 flow signature. The minimum value of the Internet Header Length (IHL) field of IPv4 is 5 (20 bytes) and the maximum value is 15 (60 bytes), thus at most 40 bytes are found in the option headers. The leftmost 6 bits of the Differentiated services field represent Classes of Service and Priority of Services, for more details refer to (RFC2475, 1998).

<table>
<tr><td>Ver = 4<br>(4 bits)</td><td>IP Header Length<br>(4 bits)</td><td>Type of Service<br>( 8 bits)</td><td colspan="2">Total Length<br>(16 bits)</td></tr>
<tr><td colspan="3">Identification<br>(16 bits)</td><td>Flags<br>(3 bits)</td><td>Fragment Offset<br>(13 bits)</td></tr>
<tr><td colspan="2">Time To Live<br>(8 bits)</td><td>Protocol<br>(Value = **41** for 6-in-4)<br>(8 bits)</td><td colspan="2">Header Checksum<br>(16 bits)</td></tr>
<tr><td colspan="5">Source IP address<br>(32 bits)</td></tr>
<tr><td colspan="5">Destination IP address<br>(32 bits)</td></tr>
<tr><td colspan="5">Options (if any)<br>(variable)</td></tr>
</table>

Figure 2.3: IPv4 Header Format

IPv6 header fields are shown in Figure 2.4; these fields occupy 40 octets (bytes) as a fixed length header. Typically 3-tuple of the IPv6 header (IP source address, IP destination address and flow label) representing the IPv6 flow signature.

Traffic class field is equivalent to the Differentiated services field of IPv4 header; it is used for QoS requirements.

<table>
<tr><td>Ver = 6<br>(4 bits)</td><td>Traffic class<br>(8 bits)</td><td colspan="3">Flow label<br>(20 bits)</td></tr>
<tr><td colspan="3">Payload Length<br>(16 bits)</td><td>Next Header<br>(8 bits)</td><td>Hop Limit<br>(8 bits)</td></tr>
<tr><td colspan="5">Source IP address<br>(128 bits)</td></tr>
<tr><td colspan="5">Destination IP address<br>(128 bits)</td></tr>
</table>

Figure 2.4: IPv6 Header Format

Since there is no unique usage for flow label field of IPv6, it is optional and could be deployed for various approaches. In terms of supporting QoS requirements, flow label is used by packet classifiers in order to identify packet's flow. (RFC3697, 2004) declared the specifications and requirements of IPv6 Flow Label values. It specifies that at least 120 seconds (time slot) should exist in order to split the reuse of the same value of flow label for a specific pair of source and destination addresses of IP. It also specifies that Flow label value be set to 0 values by source node for packets that do not belong to any flow.

## 2.4 Multiprotocol Label Switched (MPLS) Technology

MPLS is a routing and forwarding protocol standardized by IETF in 2001. MPLS domain (cloud) is "a contiguous set of nodes which operate MPLS routing and forwarding and which are also in one Routing or Administrative Domain" (RFC3031, 2001).

MPLS facilities in MPLS/VPN, MPLS/QoS, MPLS/TE, ATM + IP and fast rerouting motivated the Internet Service Providers (ISP) to deploy MPLS technology in their IPv4 backbone. These MPLS facilities contributing to minimizing the distortions of streams by setting up multiple LSPs (tunnels) between source and destination to ensure the logical separation between streams (Shekhar Srivastava, Liefvoort, & Medhi, 2009). In terms of failure detection, MPLS supports two levels of failure detection mechanisms, data plane failure detection and control plane failure detection (RFC5884, 2010). This will overcome the condition if only one of the operational planes is working in certain LSP. For example, if the control plane fails but the data plane is working, it will detect it and reroute the traffic to an alternative LSP. The same goes for the case in which the data plane fails.

MPLS networks have the capability of minimizing distortions of streams by setting up multiple label switched paths (LSPs), or tunnels, between source and destination to ensure the logical separation between streams (S. Srivastava, van de Liefvoort, & Medhi, 2009). The success of MPLS technology in providing QoS for real time IP applications makes it one of the favorite choices for ISPs when merged to IPv6 in Internet backbone networks. Therefore several IPv6 scenarios over MPLS have been identified in the literatures as a part of IPv6 deployments (Table 2.2) (Griviaud, 2008).

TABLE 2.2: IPV6 OVER MPLS DEPLOYMENT SCENARIO (GRIVIAUD, 2008)

| Scenario | Impact on |
|---|---|
| **IPv6 Tunnels configured on CE** | No Impact on MPLS |
| **IPv6 over Circuit_over_MPLS** | No Impact on IPv6 |
| **IPv6 Provider Edge Router (6PE) over MPLS** | No Impact on MPLS core |
| **Native IPv6 MPLS** | Require full network upgrade |

In terms of VPN over MPLS domain, the similarities in scope and policies simplify the coexistence of IPv6 VPN with IPv4 VPN in MPLS domain. In (RFC4659, 2006), Cisco authored for IPv6 VPN (6VPE) over MPLS/IPv4 infrastructure.

### 2.4.1 MPLS Domain

Ingress and Egress of MPLS domain are two Label Edge Routers (LERs) or Provider Edge routers (PE) representing the input and output doors of the MPLS cloud (Figure 2.5).

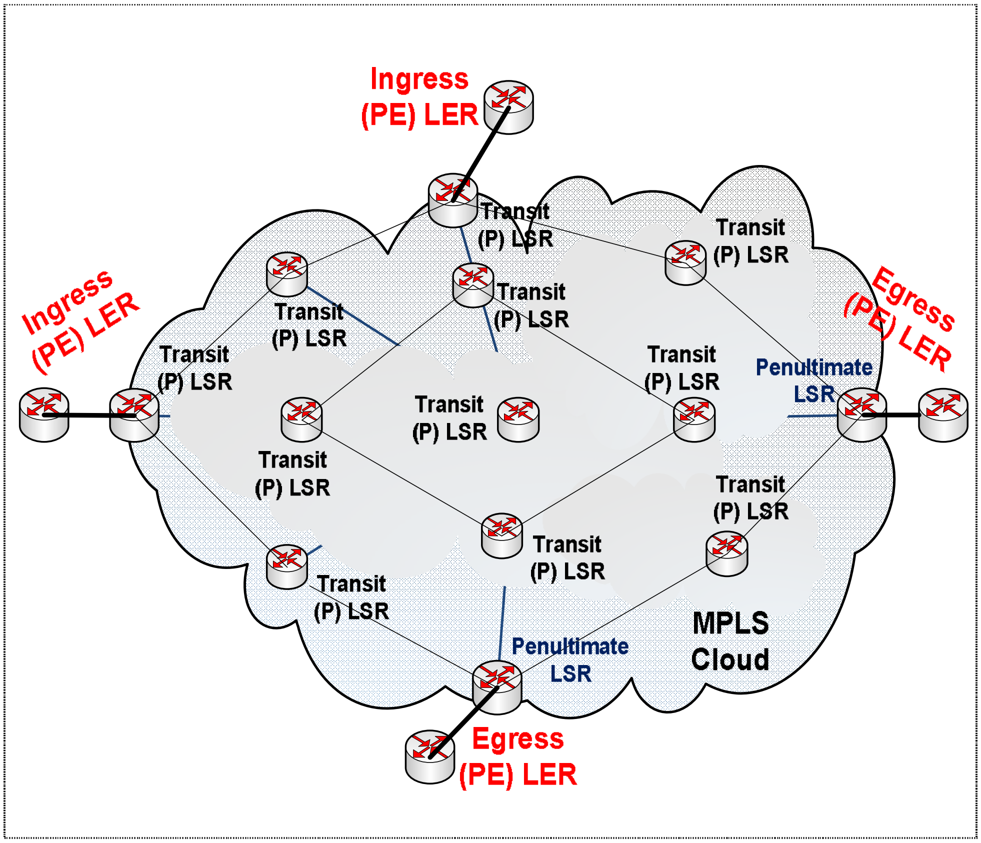

Figure 2.5: MPLS Domain

The MPLS core routers are known as Label Switch Routers (LSRs) or Transit routers or Provider (P) routers. The ingresses and egresses of MPLS cloud are connected via mesh of unidirectional tunnels (paths) namely Label Switched Paths (LSPs).

### 2.4.2 MPLS Packet Processing and Forwarding Mechanism

Four main processes are known for dealing with entering packets into MPLS cloud. The first process is the classification process, in which packets entering ingress will be classified and assigned to forwarding equivalent classes (FEC) according to the required treatment similarity, so that the same MPLS label would be provided to all packets belonging to the same FEC. The second is the label push (or encapsulation) process, in which the MPLS label is pushed by ingress to prefix the packet header (Figure 2.6). The third process, forwarding, guides the encapsulated packet through an LSP using a label switching mechanism assisted by the label information base (LIB) table. The fourth is the final label pop (or decapsulation) process, which is maintained by egress (or penultimate) LSR, and followed by a return to normal layer 3 routing (Ghein, 2006; Mine & Lucek, 2008).

The Label Switching Router (LSR) located one hop before the Egress is called **Penultimate**. The Penultimate pops the label instead of Egress, when this facility is activated. Core LSRs forwards the labeled packets without considering their layer 3 IP headers, behaving as Transit routers.