KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF ENGINEERING

DEPARTMENT OF ELECTRICAL/ELECTRONIC ENGINEERING

Satisfying End-to-End Quality of Service Requirements in Mobile Packet Networks

Submitted for fulfilment of the degree of M.Sc. Telecommunications Engineering

By

PATRICK FIATI

(PG2652908)

Supervisor:

K.O.BOATENG (PhD)

Abstract

Internet service providers face a daunting challenge in provisioning network resources, due to the rapid growth of the Internet and wide fluctuations in the underlying traffic patterns. The ability of dynamic routing to circumvent congested links and improve application performance makes it a valuable traffic engineering tool. However, deployment of load-sensitive routing is hampered by the overheads imposed by link-state update propagation, path selection, and signaling. Under reasonable protocol and computational overheads, traditional approaches to load-sensitive routing of IP traffic are ineffective, and can introduce significant route flapping, since paths are selected based on out-of-date link-state information. Although stability is improved by performing load-sensitive routing at the flow level, flapping still occurs, because most IP flows have a short duration relative to the desired frequency of link-state updates. To address the efficiency and stability challenges of load-sensitive routing, we introduce a new hybrid approach that performs dynamic routing of long-lived flows, while forwarding shortlived flows on static preprovisioned paths. By relating the detection of long-lived flows to the timescale of link-state update messages in the routing protocol, route stability is considerably improved.

Index Terms: OSPF, IS-IS, RIP, MPLS, UMTS

DECLARATION

I hereby declare that, this submission is my own work except for specific references which have been duly acknowledged, this work is the result of my own field research and it has not been submitted either in part or whole for any other degree in Kwame Nkrumah University of Science and Technology or any other educational institution elsewhere.

Signature……………………………… Date...

FIATI PATRICK

(Candidate)

Signature………………………………... Date...

Dr. K.O. Boateng

(Supervisor)

Signature……………………………….. Date ………………………….

Dr. P. Y Okyere

(Head, Department of Electrical / Electronic Engineering)

DEDICATION

This dissertation is dedicated to ALMIGHTY GOD and all the members of FIATI family.

ACKNOWLEDGEMENTS

I would like to acknowledge my intellectual debt to Dr. Boateng, my supervisor. Your suggestions, advice and direction have made this project possible.

I also appreciate the assistance of my friends and colleagues who gave me guidance especially Mr. Mazen Mroue of MTN, Daniel Kuyoli and my mother.

Finally, I should be held responsible for misinterpretation, misrepresentation, errors and all other possible flaws in this study.

LIST OF ABBREVIATIONS AND ACRONYMS

3GPP 3rd Generation partnership project (produces WCDMA standard

ACM Association of Computing Machines

AMPS Advanced Mobile Phone Service

ARP Allocation and retention priority

ASIC application-specific integrated circuits

ATM asynchronous transfer mode

AToM Any Transport over MPLS

Border Gateway Protocol

CBS Cell broadcast service

CDMA Code division multiple access

CoS class of service

D-AMPS digital AMPS

EDGE Enhanced Data Rates for Global Evolution

EIGRP Enhanced Interior Gateway Routing Protocol

ETSI European Telecommunications Standards Institute

GPRS General Packet Radio Services

GSM Global system for mobile communications

HLDLC High Level Data Link Control

HSCSD high speed circuit-switched data

HTTP Hypertext transfer protocol

IEEE Institute of Electrical and Electronic Engineering

IGP Internal Gateway Protocol

IMS IP multimedia sub-system

IP Internet protocol

IS-IS Intermediate System to Intermediate System

ISP Internet service provider

LDP Label Distribution Protocol

LFIB label forwarding information base

LSC label switch controller

LSP label switched path

LSR label switching router

MBMS Multimedia broadcast multicast service

MMS Multimedia message

MPLS Multiprotocol Label Switching

NMT Nordic Mobile Telephone

OAM Operations and Maintenance

OMA Open Mobile Alliance

OSPF Open Shortest Path First

PDC personal digital cellular

PoC Push-to-talk over cellular

QoS quality-of-service

RIP Routing Information Protocol

RSVP Resource Reservation Protocol

SIP Session initiation protocol

SMG Special Mobile Group

TACS Total Access Communications System

TCP Transport control protocol

TDP Tag Distribution Protocol

TE traffic engineering

TFIB tag forwarding information base

TSC tag switch controller

TSP tag switched path

TSR tag switching router

UDP User datagram protocol

UMTS Universal mobile telecommunication services

VCI/VPI virtual circuit/path identifier

VLSM Variable Length Subnet Masks

VOIP Voice over IP

WAP Wireless application protocol

WCDMA Wideband CDMA, Code division multiple access

WML Wireless markup language

XHTML Extensible hypertext markup language

Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

1.0 INTRODUCTION

Traffic engineering of large IP backbone networks has become a critical issue in recent years, due to the unparalleled growth of the Internet and the increasing demand for predictable communication performance [1]. Ideally, an Internet Service Provider (ISP) optimizes the utilization of network resources by provisioning of backbone routes based on the load between the edge routers. However, the volume of traffic between particular points in the network can fluctuate widely over time, due to variations in user demand and changes in the network configuration, including failures or reconfigurations in the networks of other service providers. Currently, network providers must resort to coarse timescale measurements to detect network performance problems, or may even depend on complaints from their customers to realize that the network requires reconfiguration [2]. Detection may be followed by a lengthy diagnosis process to discover what caused the shift in traffic. Finally, providers must manually adjust the network configuration, typically redirecting traffic by altering the underlying routes. These traffic engineering challenges have spurred renewed interest in dynamic routing as a network-management tool, rather than as a method for providing quality-of-service (QoS) guarantees. By selecting paths that circumvent congested links, dynamic routing can balance network load and improve application performance. Despite these potential benefits, however, most backbone networks still employ static routing (e.g., based on routing protocols such as OSPF and IS-IS) because techniques for load-sensitive routing often lead to route flapping and excessive control traffic overheads. Early attempts in the ARPANET to route based on dynamic link metrics resulted in dramatic fluctuations in link load over time. Routing packets based on out-of-date link-state information caused flapping, where a large amount of traffic would travel to seemingly under-utilized links. These links would become overloaded, causing future packets to route to a different set of links, which would then become overloaded. Improvements in the definition of the link metrics reduced the likelihood of oscillations, but designing stable schemes for load-sensitive routing is fundamentally difficult in packet-based networks like the Internet. With the evolution toward integrated services in IP networks, recent research focuses on load-sensitive routing of flows or connections, instead of individual packets. For example, a flow could correspond to a single TCP or UDP session, all IP traffic between a particular source-destination pair, or even coarser levels of aggregation. In particular, several QoS routing schemes have been proposed to select paths based on network load, as well as application traffic characteristics and performance requirements.

Dynamic routing of flows should be more stable than selecting paths at the packet level, since the load on each link should fluctuate more slowly, relative to the time between updates of link-state information. Also defining network load in terms of reserved bandwidth and buffer space, rather than measured utilization, should enhance stability.

However, QoS-routing protocols impose a significant bandwidth and processing load on the network, since each router must maintain its own view of the available link resources, distribute link-state information to other routers, and compute and establish routes for new flows. The protocol and computational overheads can be significant in large backbone networks. Since most TCP/UDP transfers consist of just a handful of packets, load-sensitive routing of all flows would require frequent propagation of link-state metrics and recomputation of routes to avoid the same instability problems that arise in dynamic routing at the packet level. We address this problem by proposing and evaluating a hybrid routing scheme that exploits the variability of IP flow durations to avoid the undesirable effects of traditional approaches to dynamic routing.

While most Internet flows are short-lived, the majority of the packets and bytes belong to long-lived flows, and this property persists across several levels of aggregation. Although this inherent variability of Internet traffic sometimes complicates the provisioning of network bandwidth and buffer resources, heavy-tailed flow-size distributions can be exploited to reduce the overheads of certain control mechanisms. Most notably in the networking context, variability in flow duration has been the basis of several techniques that reduce router forwarding overheads by establishing hardware switching paths for long-lived flows. These schemes classify arriving packets into flows and apply a trigger (e.g., arrival of some number of packets within a certain time interval) to detect long-lived flows. Then, the router dynamically establishes a shortcut connection that carries the remaining packets of the flow. The shortcut terminates if no packets arrive during a predetermined timeout period (e.g., 60 seconds). Several measurement-based studies have demonstrated that it is possible to limit the setup rate and the number of simultaneous shortcut connections, while forwarding a large fraction of packets on shortcuts. We focus on dynamic routing as a traffic engineering technique that reacts to fluctuations in network load, rather than as a way to provide explicit performance guarantees.

1.1 Stability Challenges in Load-Sensitive Routing

Depending on the network topology and the path-selection algorithm, static routing often cannot select good paths for all source-destination pairs.[3, 4] For example, protocols such as OSPF and IS-IS always forward packets on shortest paths, based on static link weights. As such, they cannot exploit non-minimal routes, and typically have limited control of how traffic is distributed when a source-destination pair has multiple shortest-path routes. [5] Proposed extensions to RIP, OSPF and lS-IS support more flexible tie-breaking based on link load, without addressing the other limitations of static shortest paths. [6] With newer routing protocols such as MPLS, network administrators can preconfigure explicit tagged routes between specific source-destination pairs, providing greater control and flexibility in balancing network load for particular traffic patterns. Moving one step further, dynamic routing can circumvent network congestion and balance link load on a smaller time scale by reacting to current, traffic demands.

1.2 BACKGROUND STUDY

1.2.0 EVOLUTION OF GSM

1.2.1 First Generation

The first generation of mobile cellular telecommunications system appeared in the 1980s. The first generation was not the beginning of mobile communications, as there were several mobile radio networks in existence before then, but there were no cellular systems either [7]. The capacity of these early networks was much lower than that of cellular networks, and the support for mobility was weaker. In mobile cellular networks the coverage area is divided into small cells, and thus the same frequencies can be used several times in the network without disruptive interference. This increases the system capacity. The first generation used analog transmission techniques for traffic, which was almost entirely voice. There was no dominant standard but several competing ones. The most successful standards were Nordic Mobile Telephone (NMT), Total Access Communications System (TACS), and Advanced Mobile Phone Service (AMPS).

1.2.2 Second Generation

The second generation (2G) mobile cellular systems use digital radio transmission for traffic. Thus the boundary line between first and second generation systems is obvious [8]. It is the analog/digital split. The 2G networks have much higher capacity than the first generation systems. One frequency channel is simultaneously divided among several users (either by code or time division). Hierarchical cell structures- in which the service area is covered by macrocells, microcells, and picocells- enhance the system capacity further. There are four main standards for 2G systems: Global system for mobile communications (GSM) and its derivatives; digital AMPS (D-AMPS); Code division multiple access (CDMA) IS-95; and personal digital cellular (PDC). GSM is by far the most successful and widely used 2G system.

1.2.3 Generation 2.5.

“Generation 2.5” is a designation that broadly includes all advanced upgrades for the 2G networks. These upgrades may in fact sometimes provide almost the same capabilities as the planned 3G systems [9]. The boundary line between 2G and 2.5G is a hazy one. It is difficult to say when a 2G becomes a 2.5G system in a technical sense. Generally, a 2.5G GSM system includes at least one of the following technologies: high-speed circuit-switched data (HSCSD), General Packet Radio Services (GPRS), and Enhanced Data Rates for Global Evolution (EDGE). The biggest problem with plain GSM is its low air interface data rates. The basic GSM could originally provide only a 9.6-Kbps user data rate. Later, 14.4-Kbps data rate was specified, although it is not commonly used. Anyone who has tried to Web surf with these rates knows that it can be a rather desperate task. HSCSD is the easiest way to speed things up. This means that instead of one time slot, a mobile station can use several time slots for a data connection. In current commercial implementations, the maximum is usually four time slots. One time slot can use either 9.6-Kbps or 14.4-Kbps speeds. The total rate is simply the number of time slots times the data rate of one slot. This is a relatively inexpensive way to upgrade the data capabilities, as it requires only software upgrades to the network (plus, of course, new HSCSD-capable phones), but it has drawbacks.

1.2.4 Overview of 3G/3.5G

The rapid development of mobile telecommunications was one of the most notable success stories of the 1990s. The 2G networks began their operation at the beginning of the decade (the first GSM network was opened in 1991 in Finland), and since then they have been expanding and evolving continuously. In September 2002 there were 460 GSM networks on air worldwide, together serving 747.5 million subscribers. In the same year that GSM was commercially launched, ETSI had already started the standardization work for the next generation mobile telecommunication network. This new system was called the Universal Mobile Telecommunications System (UMTS). This work was done in ETSI's technical committee Special Mobile Group (SMG).

1.3 OSPF

The Open Shortest Path First (OSPF) protocol is an Interior Gateway Protocol used to distribute routing information within a single Autonomous System.

OSPF protocol was developed due to a need in the internet community to introduce a high functionality non-proprietary Internal Gateway Protocol (IGP) for the TCP/IP protocol family.

1.4 IS-IS

Intermediate System to Intermediate System

□An “IS” is ISO terminology for a router

□IS-IS was originally designed for use as a dynamic routing protocol for ISO CLNP, defined in the ISO 10589 standard

□Later adapted to carry IP prefixes in addition to CLNP (known as Integrated or Dual IS-IS) as described in RFC 1195

□Predominantly used in ISP environment

1.5 MPLS

Multi Protocol Label Switching

The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of IP switching.

1.6 PROBLEM STATEMENT

3.5G networks provide voice, data and video. The internet which is data is a global system of interconnected computer networks that interchange data by packet switching using the standardized Internet Protocol Suite (TCP/IP). The internet carries various information resources and services, such as electronic mail, online chat, file transfer and file sharing, online gaming, and inter-linked hypertext document and other resources of the World Wide Web.

Most networks require the use of a very effective IP protocol routing selection. This gives the reason why various routing protocols such as RIP, OSPF, IS-IS and MPLS were looked at to select the best routing protocol that will satisfy the end-to-end quality of service requirement for mobile packet networks. This thesis is relevant for most 3.5G Telecommunication industries or ISPs who wish to deploy any of the routing protocols listed above.

1.7 OBJECTIVE OF STUDY

The general objective is that since 3.5G networks consist of voice, video and data much emphasis is put on the internet.

The specific objective is

1. To critically study the various routing protocols.
2. To seek the opinion of industrial leaders as to which protocol they deemed suitable in satisfying end-to-end quality of service requirements in 3.5G mobile packet networks.
3. To recommend the best routing protocol for mobile packet networks such as 3.5G networks and elaborate on how it works.

1.8 JUSTIFICATION

3.5G networks is the current technology deployed by most telecommunication companies across the world. NTT DoCoMo of Japan has used this latest technology in the Japan. Also one of the telecom giant of Africa, MTN used 3.5G technology on mobile phones to telecast the South Africa 2010 World Cup to individuals in their homes and offices.

1.9 SCOPE OF STUDY

This research gives a background on the evolution of GSM (Global System for Mobile Communication). It further illustrates the various routing protocols that will satisfy the end-to-end quality of service requirements in mobile packet networks such as 3.5G.

A survey was conducted to determine the best routing protocol. IEEE and ACM documents were looked at.

1.10 LIMITATION

A number of challenges were met and these are

1. The number of people who are willing to answer the survey.

   Most telecom experts are not willing to answer the survey and are afraid of giving information because of competition among the various telecom companies.

2. The design of the survey whether to make it web based or on paper.

   Whether the web based or on paper will be easy to compile and interpret.

3. Time constraints.

   The time it will take the respondents to answer the survey and analyse the results.

1.11 ORGANISATION OF THESIS

This chapter gives an overview of the GSM technology and the routing protocols which are RIP, OSPF, IS-IS and MPLS. It also shows the mechanisms in producing this research.

Chapter 2, titled “Literature Review” describes the various terminologies in 3.5G technology and also describes the routing protocols listed above.

Chapter 3, titled “Methodology” describes how the survey was designed.

Chapter 4 is the Results, Discussion and Analysis. It analyses the results produced in the survey.

Chapter 5 is some literature on MPLS.

The thesis is concluded in chapter 6.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Person-to-Person Packet Switched Services - 3.5G

2.1.1 Images and Multimedia

It is already common today to send pictures via MMS (multimedia messaging), which, from a user perspective, is perceived almost as an enhanced SMS service. For MMS to be successful it is important that the messages are delivered with a high reliability, while the delivery time is short enough as long as it is roughly below one minute. Since the delivery time is not crucial, it is possible to use a less stringent 3GPP quality of service class for MMS. Another important requirement from an end user point of view is that it should be possible and easy to send MMS messages at the same time as, for example, making a circuit switched call. This requires that both the mobile station and the network are able to handle multiple radio access bearers in parallel.

Although a parallel circuit switched call and MMS transmission is possible, the interactivity and picture information flow of the MMS service is limited. Another imaging service more powerful than MMS is real time video sharing [14]; see **Figure 2.1** for an illustration of this service. From a user point of view real time video sharing is about

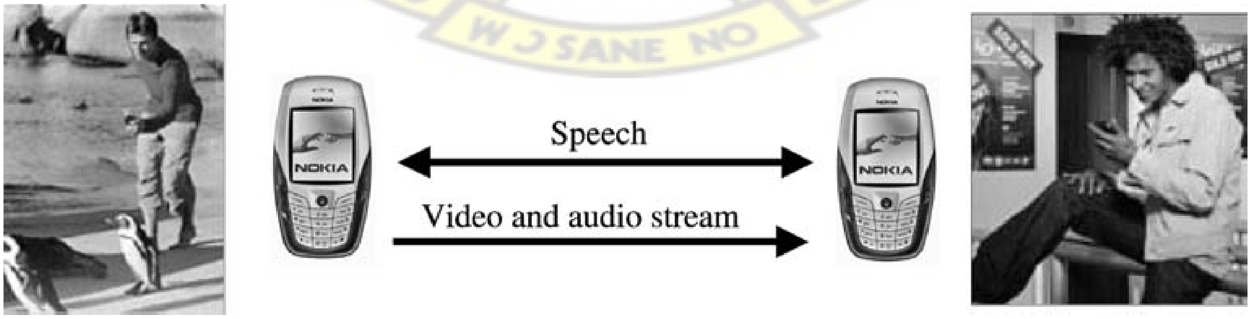


Figure 2.1: Real time video sharing

Showing to the other end what is going on in your side of the phone connection. A typical usage scenario is that the communication starts out with a normal speech connection and then, when one of the parties has something interesting to show; the one-way video stream is set up. That is, the video stream is only set up when both users feel a clear need to enhance the voice connection with a one-way video connection. This differentiates the one-way video sharing service from full two-way video phone services. The real time video sharing has both professional and private use cases: sharing vacation experiences, showing real estate property for real estate brokers, and explaining what the situation is when there is a need to repair equipment.

The end user performance requirements for the real time video sharing service are that:

- Image quality and update rates should be high enough to enable 'scanning' the environment with the camera.
- Delay between taking a picture and showing it to the other side is low enough to enable true interactivity.
- It is easy and fast to set up the one-way video stream once the voice connection is available.

Note that real time video sharing has different requirements than content-to-person streaming, because in content-to-person streaming there is no or little interactivity and hence no requirements for low delays. For real time video sharing low delays are, on the other hand, crucial. A tolerable delay between taking a picture and showing it to the peer end could be in the order of some seconds (<5 s). When it comes to bit rate requirements it is very much dependent on mobile station display sizes. Based on initial results from video streaming in current networks, a lower bit rate limit for a 3.5 cm times 4 cm mobile phone display is around 40 to 64 kbps. However, note that the required bit rate to use is a nonstraightforward function of the tolerable delay, the image update rates and the applied coding schemes. From a network point of view, the one-way video streaming service has one obvious property that is different from many other proposed services: it requires a fairly high uplink bit rate. The UMTS network must be able to deliver a high and reasonably constant bit rate in order to support the low delay streaming connection as well as the voice connection if the voice connection is mapped over the packet switched domain. These bit rate and delay requirements may be met in a cost efficient way by utilising the QoS differentiation features that are available in UMTS. From a technical perspective, the peer-to-peer connections are in the packet switched domain set up by using the IMS system and by utilising the session initiation protocol (SIP). From a network and end user perspective this sets requirements on the SIP signalling, that it is fast enough not to disturb the user when setting up the additional video stream connection. Fast SIP signalling may be obtained by supporting one of multiple compression algorithms for SIP.

2.1.2 Push-to-Talk over Cellular (PoC)

Push-to-talk over cellular (PoC) service is instant in the sense that the voice connection is established by simply pushing a single button and the receiving user hears the speech without even having to answer the call. While ordinary voice is bi-directional, the PoC service is a one directional service. The basic PoC application may hence be described as a walkie-talkie application over the packet switched domain of the cellular network. In addition to the basic voice communication functionality, the PoC application provides the end user with complementary features like, for example:

- Ad hoc and predefined communication groups;
- Access control so that a user may define who is allowed to make calls to him/her;

- ‘Do-not-disturb’ in case immediate reception of audio is not desirable.

With ordinary voice calls a bi-directional communication channel is reserved between the end users throughout the duration of the call. In PoC, the channel is only set up to transfer a short speech burst from one to possibly multiple users. Once this speech burst has been transferred, the packet switched communication channel can be released.

The speech packets in the PoC solution are carried from the sending mobile station to the server by the OPRS/UMTS network. The server then forwards the packets to the receiving mobile stations. In the case of a one-to-many connection, the server multiplies the packets to all the receiving mobile stations. This is illustrated in Figure 2.2 The PoC service is independent of the underlying radio access network.

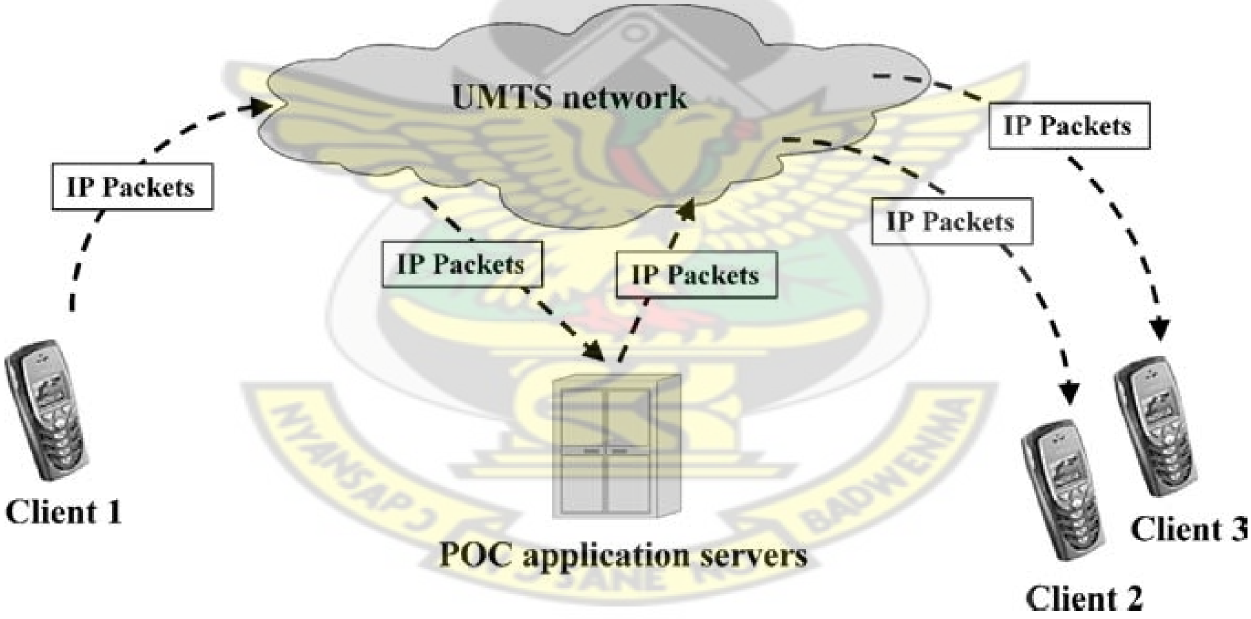


Figure 2.2: Push to talk solution architecture

In order for the PoC service to be well perceived by the end users it must meet multiple requirements. Some examples of end user requirements are:

- Simple user interface, for example, a dedicated push-to-talk button;

- High voice quality and enough sound pressure in the speaker to work also in noisy environments;
- Low delay from pressing the push-to-talk button until it is possible to start talking, called ‘start-to-talk time’;
- Low delay for the voice packets to receive the peer end, called voice through delay.

The end user is expected to be satisfied with the interactivity of the PoC service if the start-to-talk delay is around or below two seconds, while the speech round trip time should be kept lower than 1.5 seconds.

2.1.3 Voice over IP (VoIP)

The driver for Voice-over-IP, VoIP, in fixed networks has been access to low cost long distance and international voice calls. The driver for VoIP in cellular networks is rather to enable rich calls. A rich call can be defined as a real time communication session between two or more persons which consists of one or more media types. VoIP connection can be complemented with 2-way video, streaming video, images, content sharing, gaming etc., see Figure 2.3 VoIP and rich calls can be carried over WCDMA as the end-to-end network delay is low enough to meet the conversational service requirements. The QoS differentiation and IP header compression are important to make an efficient VoIP service in WCDMA.

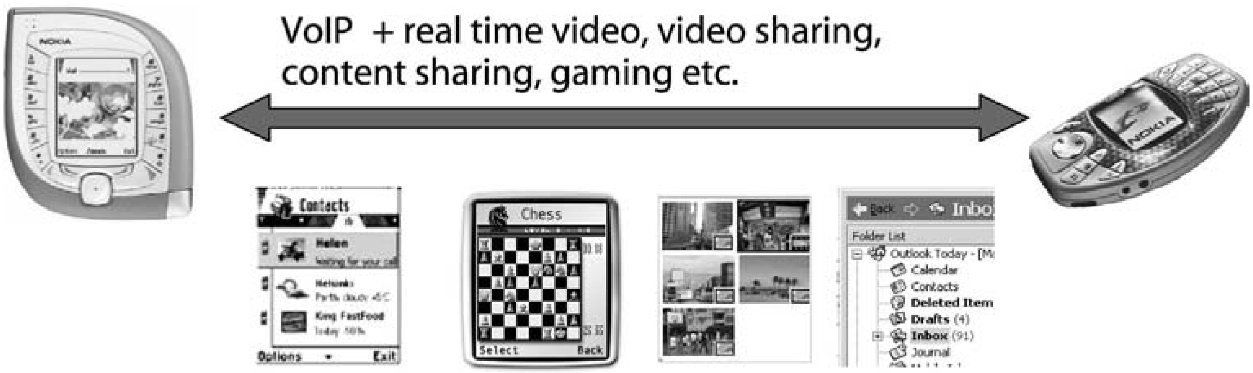


Figure 2.3: VoIP as a building block for rich calls

2.1.4 Multiplayer Games

We first group the existing multiplayer games into key categories based on their end user requirements. Three reasonable categories are, according to the study in [11, 12], real time action games, real time strategy games and turn based strategy games. Note that these requirements have been derived from studies using a fixed network connection and not a cellular network connection. Although cellular networks behave somewhat differently than fixed networks, and although mobile station displays are much smaller than computer displays, the results give indications for what the maximum delay may be in order to generate a nice gaming experience for the end user.

It can be noted that for experienced players it is an advantage to have significantly lower end-to-end network delays than what is given by the requirement in Table 2.1; end-to-end network delays down to as low as 70 to 80 ms are needed to satisfy the most demanding users. The end-to-end network delay is particularly noticeable for the users if some users have low delays, like 70 ms, while others have higher delays, like 200 ms. Bearing in mind that today's WCDMA networks provide round trip times of 150–200 ms it is possible to provide real time strategy and turn based strategy games, and even real time action games over WCDMA.

The real time action games are constantly transmitting and receiving packets with typical bit rates of 10–20 kbps. Such bit rates can be easily delivered over cellular networks. However, these packets must be delivered with a very low delay which sets high requirements for the network performance. For real time strategy and turn based strategy games both the requirements on the bit rate and the end-to-end network delays are looser and there is more freedom on how to map these services to radio channels.

2.2 Content-to-person Services

2.2.1 Browsing

During the early launch and development of WAP for mobile browsing, there were huge expectations that browsing via the mobile station would take off rapidly. Because of several reasons the take off did not happen as fast as expected. However, with better mobile station displays – resolution and colour – and with higher bit rates and increased content, the browsing experience on mobile station devices is increasing rapidly and service usage is going up. There have been several releases of the WAP protocol stack, of which the most important releases are WAP1.1 and WAP2.0 [15]; see further Figure 2.12. The WAP version denoted WAP1.1 was approved in June 1999 and the first products based on this version were launched later in the same year. The WAP2.0 version was released in July 2001 by the WAP forum, which is currently part of the Open Mobile Alliance (OMA). The most important difference between WAP1.1 and WAP2.0 is that WAP2.0 is based on the standard Internet transport protocols

(TCP/IP, HTTP/XHTML), while the WAP1.1 release utilizes WAP1.1 specific transport protocols. From an end user point of view, the TCP/IP protocols provide faster download of large content size. The focus in WAP1.1 development was to make browsing perform well in systems with large packet round trip times and with limited bit rates. That is, WAP1.1 enables the

Table 2.1: Evolution of the WAP protocol stacks

WAP 1.1	**WAP 2.0**
WML	WML + XHTML
UDP	TCP
IP	IP

Transmitter to send the packets almost at once, without waiting for connection establishment between the communication peers. This makes WAP1.1 fast for small packets over unreliable links. The weakness is that the link will usually not be fully utilised if the file to transfer is large. The decreased link utilisation lowers the end user bit rate for large files if the air interface bit rate is high.

WAP2.0 introduces standard Internet protocols to the WAP protocol stacks. Because the TCP/IP protocols have well developed link and congestion management algorithms, this makes WAP2.0 more efficient when transferring large files over radio links with high bit rates. To make TCP even more efficient for mobile systems, a particular flavour called wireless TCP (wTCP) has been defined. The wTCP protocol is based on standard TCP features, but in wTCP the support of certain features is mandatory and recommendations for parameter values have been aligned to cope with the higher packet round trip time in wireless networks. The difference between WAP1.1 and WAP2.0 download times is quite small for small page sizes because of the low round trip time in WCDMA. A low round trip time helps standard Internet protocols perform satisfactorily over WCDMA without special optimisation.

From a user perspective it is crucial that browsing is easily accessible and fast. Rough performance requirements for browsing are that the first page download time is lower than 10 s and for the second page download, lower than 4 to 7 s is preferred . However, bear in mind that end user service requirements are different from market to market and also in different market segments within the same market. Another user requirement is that it should be possible to use browsing smoothly when travelling by car, train or bus. This requires efficient handling of cell reselections in order to prevent connection breaks. Because WCDMA utilises handover for packet switched data, there are no breaks at cell reselection.

From a network perspective the first page download is different from the second page download. The reason is that the first page download time may include GPRS attach, security procedures, PDP context activation and radio bearer set-up times depending on how the network and the mobile station have been configured. For the second and consecutive pages the download time will be lower because the initial set-up messages have already been sent. The second page download time is mainly limited by the basic packet round trip time, the radio channel bit rate, TCP/IP efficiency, HTTP versions and possibly also the radio bearer set-up time depending on the idle period from the last page download.

2.2.2 Audio and Video Streaming

Multimedia streaming is a technique for transferring data such that it can be processed as a steady and continuous stream. Streaming technologies are becoming increasingly important with the growth of the Internet because most users do not have fast enough access to download large multimedia files quickly. Mobile station memory may also limit the size of t
he downloads. With streaming, the client browser or plug-in can start displaying the data before the entire file has been transmitted.

For streaming to work, the client side receiving the data must be able to collect the data and send it as a steady stream to the application that is processing the data and converting it to sound or pictures. Streaming applications are very asymmetric and therefore typically withstand more delay than more symmetric conversational services. This also means that they tolerate more jitter in transmission. Jitter can be easily smoothed out by buffering. Internet video products and the accompanying media industry as a whole are clearly divided into two different target areas: (1) Web broadcast and (2) video streaming on demand.

Web broadcast providers usually target very large audiences that connect to a highly performance-optimised media server (or choose from a multitude of servers) via the actual Internet. The on-demand services are more often used by big corporations that wish to store video clips or lectures to a server connected to a higher bandwidth local intranet – these on-demand lectures are seldom used simultaneously by more than hundreds of people.

Both application types use basically similar core video compression technology, but the coding bandwidths, level of tuning within network protocol use, and robustness of server technology needed for broadcast servers differ from the technology used in on-demand, smaller-scale systems. This has led to a situation where the few major companies developing and marketing video streaming products have specialised their end user products to meet the needs of these two target groups. Basically, they have optimised their core products differently: those directed to the ‘28.8 kbps market’ for bandwidth variation-sensitive streaming over the Internet and those for the 100–7300 kbps intranet market. At the receiver the streaming data or video clip is played by a suitable independent media player application or a browser plug-in. Plug-ins can be downloaded from the Web, usually free of charge, or may be readily bundled to a browser. This depends largely on the browser and its version in use – new browsers tend to have integrated plug-ins for the most popular streaming video players.

In conclusion, a client player implementation in a mobile system seems to lead to an application-level module that could handle video streams independently (with independent connection and playback activation) or in parallel with the browser application when the service is activated from the browser. The module would interface directly to the socket interface of applied packet network protocol layers, here most likely UDP/IP or TCP/IP.

2.2.3 Content Download

Content download examples are shown in Figure 2.15: application downloads, ringing tone downloads, video clips and MP3 music. The content size can vary largely from a few kB ringing tones to several MB music files. The download times should preferably be low, which puts high requirements on the radio bit rate, especially for the large downloads with several 100 kB.

2.2.4 Multimedia Broadcast Multicast Service, (MBMS)

A new service introduced in 3GPP Release 6 specifications is Multimedia Broadcast Multicast Service (MBMS). There are two high level modes of operation in MBMS, as given in

1. Broadcast mode, which allows sending audio and video. The already existing Cell

Broadcast Service (CBS) is intended for messaging only. The broadcast mode is expected to be a service without charging and there are no specific activation requirements for this mode.

2. Multicast mode allows sending multimedia data for the end users that are part of a multicast subscription group. End users need to monitor service announcements regarding service availability, and then they can join the currently active service. From the network point of view, the same content can be provided in a point-to-point fashion if there are not enough users to justify the high power transmission. A typical example in

3GPP has been the sport results service where, for example, ice hockey results would be available as well as video clips of the key events in different games of the day. Charging is expected to be applied for the multicast mode.

From the radio point of view, MBMS is considered an application independent way to deliver the MBMS User Services, which are intended to deliver to multiple users

simultaneously.The MBMS User Services can be classified into three groups as follows:

1. Streaming services, where a basic example is audio and video stream;

2. File downloads services;

3. Carousel service, which can be considered as a combination of streaming and file download. In this kind of service, an end user may have an application which is provided data repetitively and updates are then broadcast when there are changes in the content. For MBMS User Services, an operator controls the distribution of the data. Unlike CBS, the end user needs first to join the

service and only users that have joined the service can see the content. The charging can then be based on the subscription or based on the keys which enable an end user to access the data. The MBMS content can be created by the operator itself or by a third party and, as such, all the details of what an MBMS service should look like will not be specified by 3GPP, but left for operators and service providers. One possible MBMS high level architecture is shown in Figure 2.4, where the IP multicast network refers here to any server providing MBMS content over the Internet. The example data rates in range from the 10 kbps text-based information to the 384 kbps video distribution on MBMS. The codecs are expected to be the current ones – such as AMR for voice – to ensure a large interoperability base for different terminals for the services being provided.

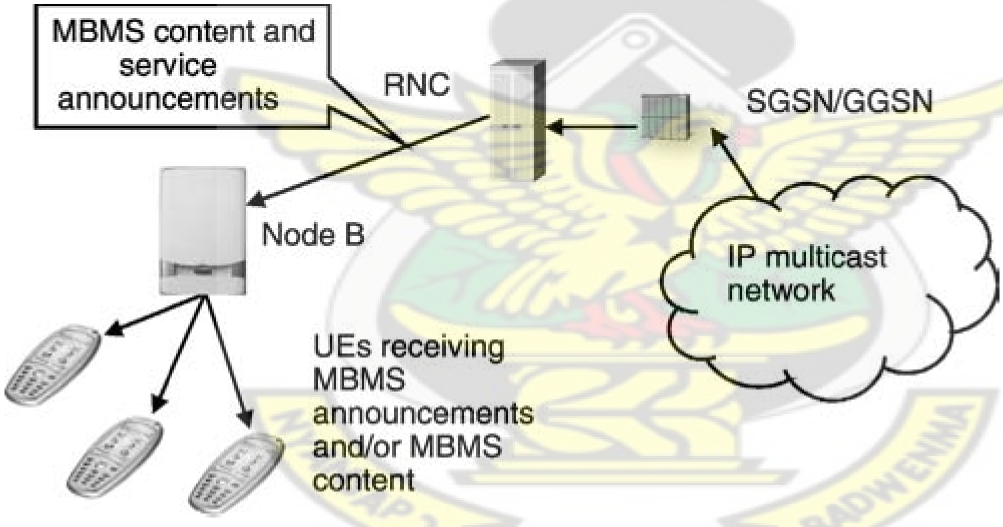

MBMS content and service announcements
RNC
SGSN/GGSN
Node B
IP multicast network
UEs receiving MBMS announcements and/or MBMS content

Figure 2.4: Example MBMS high level architecture

3.3 Business Connectivity

Business connectivity considers access to corporate intranet or to Internet services using laptops. We consider shortly two aspects of business connectivity: end-to-end security and the effect of radio latency to the application performance. End-to-end security can be obtained using Virtual

Private Networks, VPN, for the encryption of the data. One option is to have a VPN client located on the laptop and the VPN gateway in the corporate premises. Such an approach is often used by large corporates that are able to obtain and maintain required equipment for the remote access service. Another approach uses a VPN connection between the mobile operator core site and the company intranet. The mobile network uses standard UMTS security procedures. In this case the company only needs to subscribe to the operator's VPN service and obtain a VPN gateway. These two approaches are illustrated in **Figure 2.5**

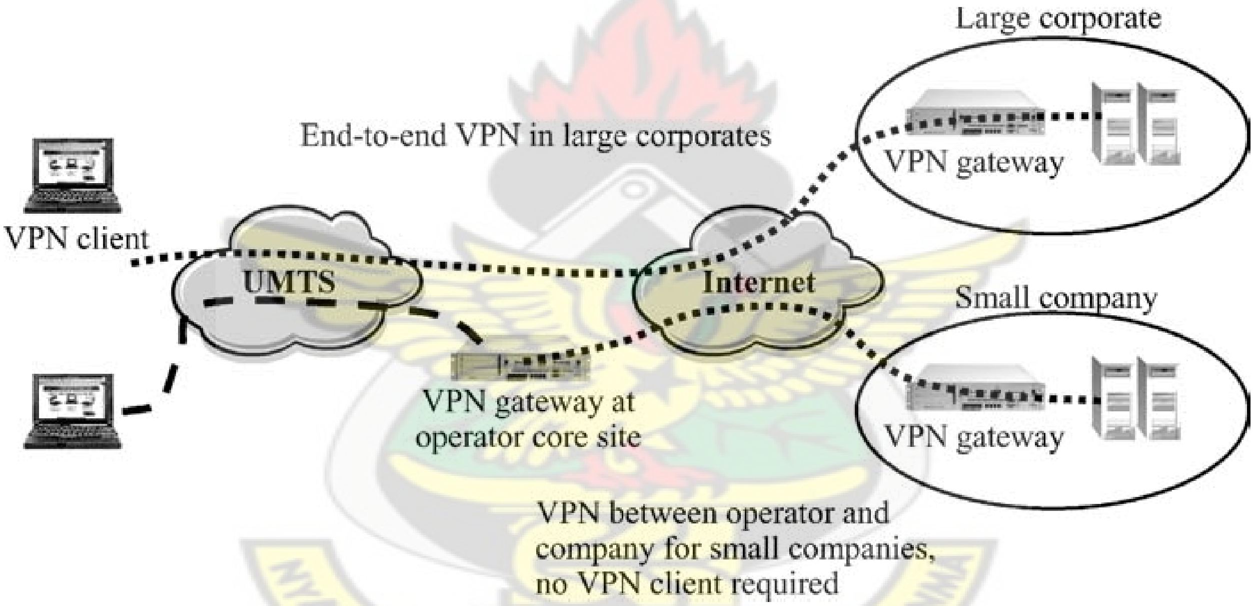


Figure 2.5: Virtual private network architectures

The business connectivity applications can be, for example, web browsing, email access or file download. The application performance should preferably be similar to the performance of DSL or WLAN. The application performance depends on the available bit rate but also on the network latency. The network latency is here measured as the round trip time. The round trip time is the delay of a small IP packet to travel from the mobile to a server and back. The end user experienced bit rate is defined here as the download file size divided by the total time. This figure assumes that a dedicated channel with 384 kbps already exists and no channel allocation is required. The curves show that a low round trip time is beneficial, especially for small file sizes, due to TCP slow start. Low round trip time will be more relevant if we need to download several small files using separate TCP sessions. The application performance is also affected by the application protocol, e.g. HTTP 1.1 vs HTTP 1.0 in web browsing. A web page typically consists of several objects: text and a number of pictures. In the case of HTTP 1.0 each object is downloaded in a separate TCP session, while for HTTP 1.1 all objects from the same server can be downloaded in one TCP connection. It is beneficial to use HTTP 1.1 to minimise the effect of TCP slow start on the application performance.

2.4 IP Multimedia Sub-system (IMS)

IP Multimedia Sub-system, IMS, allows operators to provide their subscribers with multimedia services that are built on Internet applications and protocols .IMS enables IP connectivity between users using the same control and charging mechanisms. The basic session initiation capabilities provided by SIP protocol are utilised to establish peer-to-peer sessions [16]. The IMS concept is shown in **Figure 2.6**

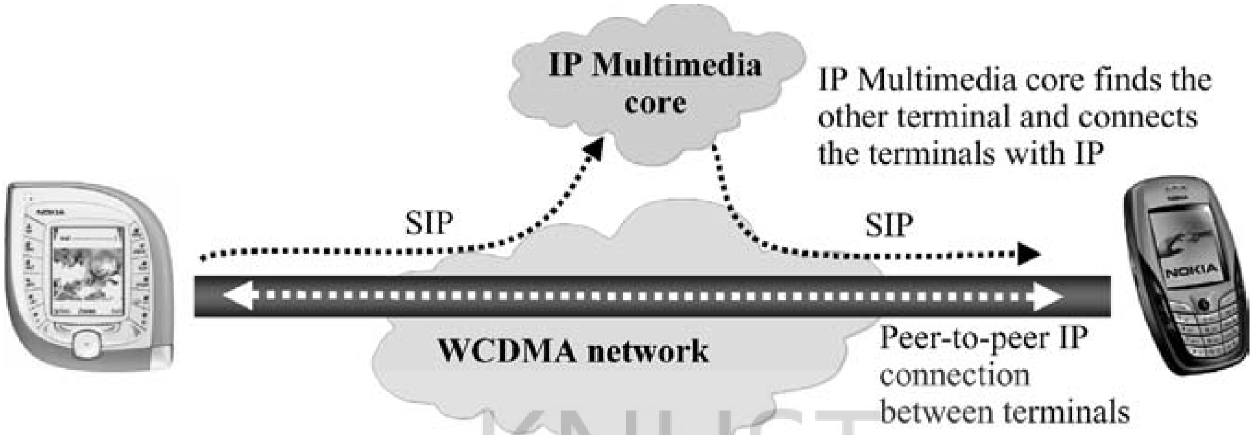

IP Multimedia core
IP Multimedia core finds the other terminal and connects the terminals with IP
SIP
SIP
WCDMA network
Peer-to-peer IP connection between terminals
NOKIA

Figure 2.6: Basic principles of the IP Multimedia Sub-system

IMS provides the means for network operators to maintain their role in the value chain by providing new multimedia services and predictable end user performance. The same platform can be used in both real time services, like VoIP, and non-real time services, like content sharing.

2.5 Quality of Service Differentiation

When the system load gets higher, it becomes important to prioritise the different services according to their requirements. This prioritisation is called QoS differentiation. 3GPP QoS architecture is designed to provide this differentiation [17].

The terminology is shown in **Figure 2.7**

The main distinguishing factor between the four traffic classes is how delay-sensitive the traffic

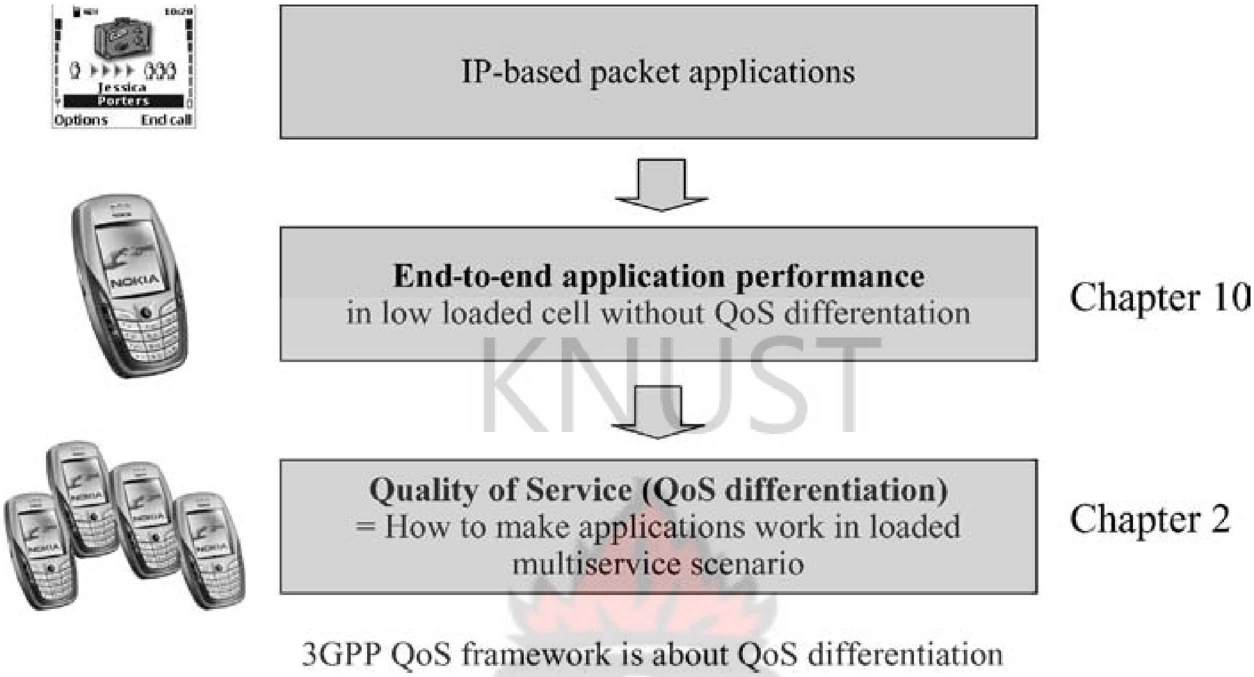

IP-based packet applications
End-to-end application performance
in low loaded cell without QoS differentation
Chapter 10
Quality of Service (QoS differentiation)
= How to make applications work in loaded
multiservice scenario
Chapter 2
3GPP QoS framework is about QoS differentiation

Figure 2.7: Definition of quality of service differentiation

Is: the conversational class is meant for very delay-sensitive traffic, while the background class is the most delay-insensitive. There are, further, three different priority categories, called allocation/retention priority categories, within each QoS class. Interactive has also three traffic handling priorities. Conversational and streaming class parameters also include the guaranteed bit rate and the transfer delay parameters. The guaranteed bit rate defines the minimum bearer bit rate that UTRAN must provide and it can be used in admission control and in resource allocations. The transfer delay defines the required 95th percentile of the delay. It can be used to define the RLC operation mode (acknowledged, non-acknowledged mode) and the number of retransmissions. The conversational class is characterised by low end-to-end delay and symmetric or nearly symmetric traffic between uplink and downlink in person-to-person communications. The maximum end-to-end delay is given by the human perception of video and audio conversation: subjective evaluations have shown that the end-to-end delay has to be less than 400 ms. The streaming class requires bandwidth to be maintained like conversational class but streaming class tolerates some delay variations that are hidden by dejitter buffer in the receiver. The interactive class is characterised by the request response pattern of the end user. At the message destination there is an entity expecting the message (response) within a certain time. The background class assumes that the destination is not expecting the data within a certain time. UMTS QoS classes are not mandatory for the introduction of any low delay service. It is possible to support streaming video or conversational Voice over IP from an end-to-end performance point of view by using just background QoS class. QoS differentiation becomes useful for the network efficiency during high load when there are services with different delay requirements. If the radio network has knowledge about the delay requirements of the different services, it will be able to prioritise the services accordingly and improve the efficiency of the network utilisation. Considerable efficiency gains can be obtained in Step 2 just by introducing a few prioritisation classes within interactive or background class by using allocation and retention parameters, ARP. The pure prioritisation in packet scheduling is not alone enough to provide full QoS differentiation gains. Users within the same QoS and ARP class will share the available capacity. If the number of users is simply too high, they will all suffer from bad quality. In that case it would be better to block a few users to guarantee the quality of the existing connections, like streaming videos. The radio network can estimate the available radio capacity and block an incoming user if there is no room to provide the required bandwidth without sacrificing the quality of the existing connections. Finally Step 4 allows further differentiation between guaranteed bit rate services with different delay requirements. If the delay requirements are known, the WCDMA RAN can allocate suitable radio parameters – like retransmission parameters – for the new bearer.

2.6 OSPF, IS-IS, RIP

The rapid growth and expansion of today's networks has pushed RIP to its limits. RIP has certain limitations that could cause problems in large networks.RIP has a limit of 15 hops. A RIP network that spans more than 15 hops (15 routers) is considered unreachable.

RIP cannot handle Variable Length Subnet Masks (VLSM). Given the shortage of IP addresses and the flexibility VLSM gives in the efficient assignment of IP addresses, this is considered a major flaw.

Periodic broadcasts of the full routing table will consume a large amount of bandwidth.

2.7 Shortest Path Algorithm

The shortest path is calculated using the Dijkstra algorithm. The algorithm places each router at the root of a tree and calculates the shortest path to each destination based on the cumulative cost required to reach that destination. Each router will have its own view of the topology even though all the routers will build a shortest path tree using the same link-state database.

The cost (also called metric) of an interface in OSPF is an indication of the overhead required to send packets across a certain interface. The cost of an interface is inversely proportional to the bandwidth of that interface. A higher bandwidth indicates a lower cost.

IS-IS/ OSPF are Interior Gateway Protocols (IGP). They distribute routing information between routers belonging to a single Autonomous System (AS).

Both OSPF and ISIS use Dijkstra SPF algorithm. Each exhibit same convergence properties

ISIS is less widely implemented on router platforms. ISIS runs on data link layer, OSPF runs on IP layer. Biggest ISPs tend to use ISIS. Main ISIS implementations are more tuneable than equivalent OSPF implementations.

2.8 MPLS

MPLS is an advanced forwarding scheme. It extends routing with respect to packet forwarding and path controlling.

Each MPLS packet has a header. In a non-asynchronous transfer mode(ATM) environment, the header contains a 20 bit label, a 3-bit experimental field (formerly known as class of service, or CoS, field), a 1-bit label stack indicator, and an 8-bit time-to-live (TTL) field. In an ATM environment, the header contains only a label encoded in the virtual circuit/path identifier (VCI/VPI) field. An MPLS-capable router, termed a label switching router(LSR) examines the label and possibly the experimental field in forwarding the packet.

At ingress the LSRs of an MPLS-capable domain’s IP packets are classified and routed based on a combination of the information carried in the IP header of the packets and the local routing information maintained by the LSRs. An MPLS header is then inserted for each packet. Within an MPLS-capable domain, an LSR will use the label as the index to look up the forwarding routing table of the LSR. The packet is processed as specified by the forwarding table entry. The incoming label is replaced by the outgoing label, and the packet is switched to the next LSR. This label-switching process is very similar to ATM’s VCI/VPI processing. Before a packet leaves an MPLS domain, its MPLS header is removed. The paths between the ingress LSRs and egress LSRs are called label-switched paths (LSPs). MPLS uses some signaling protocol such as Resource Reservation Protocol (RSVP) or Label Distribution Protocol (LDP) to set up LSPs.

CHAPTER THREE

3.0 METHODOLOGY

3.1 Overview

Surveys are to be conducted in order to collect primary and secondary data, analyse them and determine the best routing protocol to satisfy the end to end quality of service requirement in mobile packet networks such as 3 / 3.5G networks. Secondary data will focus on the advantages and disadvantages as well as the reliability of possible candidate routing protocols. Primary data are to be collected by surveying views of Senior Managers of telecommunication operators in line with this topic. Specifically, a total of 50 respondents are to be randomly selected from MTN to make up the sample. The survey questionnaire is to be structured in the Likert format. Data gathered from this research instrument is then to be analysed and interpreted. Along with primary data, secondary data are to be gathered in the form of published articles and literatures from the Institute of Electrical and Electronic Engineering (IEEE) journals and Association of Computing Machines (ACM) website to support the survey results.

3.2 Research Design

The descriptive method of research is used for this study. To define the descriptive type of research, Creswell [18] stated that the descriptive method of research is to gather information about the present existing condition. The emphasis is on describing rather than on judging or interpreting. The aim of descriptive research is to verify formulated hypotheses that refer to the present situation in order to elucidate it. The descriptive approach is quick and practical in terms of the financial aspect. Moreover, this method allows a flexible approach, thus, when important new issues and questions arise during the duration of the study, further investigation may be conducted.

Descriptive research on the other hand is a type of research that is mainly concerned with describing the nature or condition and the degree in detail of the present situation. This method is used to describe the nature of a situation, as it exists at the time of the study and to explore the cause/s of a particular phenomenon. The aim of descriptive research is to obtain an accurate profile of the people, events or situations. With this research type, it is essential that the researcher already has a clear view or picture of the phenomena being investigated before the data collection procedure is carried out. This kind of research is used to obtain first hand data from the respondents so as to formulate rational and sound conclusions and recommendations for the study. The descriptive approach is quick and practical in terms of the financial aspect.

In this study, the descriptive research method is employed so as to identify the role and significance of the best routing protocol during the time of research. It is opted to use this research method considering the objective to obtain first hand data from the respondents. The descriptive method is advantageous due to its flexibility; this method can use either qualitative or quantitative data or both, giving the greater options in selecting the instrument for data-gathering. The aim of the survey is to solicit views on what is the best routing protocol to satisfy the end to end quality of service requirements in mobile packet networks such as 3 / 3.5G networks; the descriptive method is then appropriate for this research since this method is used for gathering prevailing conditions. The survey is done using Senior Managers of telecommunication operators as respondents in order to gather relevant data; the descriptive method is then appropriate as this can allow the identification of the similarities and differences of the respondents' answers. For this research, two types of data are to be gathered. These include the primary and secondary data types. The primary data are derived from the answers the participants give during the survey process. The secondary data on the other hand, are obtained from published documents and literatures that are relevant to the questionnaire. With the use of the survey questionnaire and published literatures, this study took on the combined quantitative and qualitative approach of research. By means of employing this combined approach, the researcher is able to obtain the advantages of both quantitative and qualitative approaches and overcome their limitations.

Quantitative data collection methods are centred on the quantification of relationships between variables. Quantitative data-gathering instruments establish relationship between measured variables. When these methods are used, the researcher is usually detached from the study and the final output is context free. Measurement, numerical data and statistics are the main substance of quantitative instruments. With these instruments, an explicit description of data collection and analysis of procedures are necessary. An approach that is primarily deductive reasoning, it prefers the least complicated explanation and gives a statement of statistical probability. The quantitative approach is more on the detailed description of a phenomenon. It basically gives a generalization of the gathered data with tentative synthesized interpretations.

Quantitative approach is useful as it helps the researcher to prevent bias in gathering and presenting research data. Quantitative data collection procedures create epistemological postulations that reality is objective and unitary, which can only be realized by means of transcending individual perspective. This phenomenon in turn should be discussed or explained by means of data analysis gathered through objective forms of measurement. The quantitative data gathering methods are useful especially when a study needs to measure the cause and effect relationships evident between pre-selected and discrete variables. The purpose of the quantitative approach is to avoid subjectivity by means of collecting and exploring information which describes the experience being studied.

Quantitative methods establish very specific research problem and terms. The controlled observations, mass surveys, laboratory experiments and other means of research manipulation in qualitative method makes gathered data more reliable. In other words, subjectivity of judgment, which is not needed in a thesis discussion, can be avoided through quantitative methods. Thus, conclusions, discussions and experimentations involved in the process are more objective. Variables, both dependent and independent, that are needed in the study are clearly and precisely specified in a quantitative study. In addition, quantitative method enables longitudinal measures of subsequent performance of the respondents. Fryer [19] noted that qualitative researchers aim to decode, describe, analyze and interpret accurately the meaning of a certain phenomena happening in their customary social contexts. The focus of the researchers utilizing the framework of the interpretative paradigm is on the investigation of authenticity, complexity, contextualization, mutual subjectivity of the researcher and the respondent as well as the reduction of illusion.

Contrary to the quantitative method, qualitative approach generates verbal information rather than numerical values [20]. Instead of using statistical analysis, the qualitative approach utilizes content or holistic analysis; to explain and comprehend the research findings, inductive and not deductive reasoning is used. The main point of the quantitative research method is that measurement is valid, reliable and can be generalized with its clear anticipation of cause and effect [21]. Being particularistic and deductive in nature, quantitative method is dependent on the formulation of a research hypothesis and confirming them empirically using a specific data set. The scientific hypothesis of a quantitative method holds no value. This means that the researcher's personal thoughts, subjective preferences and biases are not applicable to this type of research method.

The survey opts to integrate the qualitative approach in this study due to its significant advantages. The use of qualitative data gathering method is advantageous as they are more open to changes and refinement of research ideas as the study progresses; this implies that qualitative data gathering tools are highly flexible. Moreover, no manipulation of the research setting is necessary with this method; rather than employ various research controls such as in experimental approaches, the qualitative data gathering methods are only centred on understanding the occurring phenomena in their naturally occurring states. Aside from these advantages, researchers use qualitative data-gathering tools as some previous researchers believe that qualitative data are particularly attractive as they provide rich and well-grounded descriptions and explanations as well as unforeseen findings for new theory construction. One of the notable strengths of the qualitative instruments is that they evoke a more realistic feeling of the research setting which cannot be obtained from statistical analysis and numerical data utilized through quantitative means. These data collection methods allow flexibility in conducting data gathering, research analysis and interpretation of gathered information. In addition, qualitative method allows the presentation of the phenomenon being investigated in a more holistic view.

3.3 Participants

In order to determine whether a web-based survey questionnaire does play an important role in choosing the best routing protocol, a total of 50 respondents are asked to participate. To achieve pertinent information, certain inclusion criteria are imposed. The participants qualified for sample selection must be staff or employees of their respective companies' technical/ engineering department. This qualification ensured that the participants understand the nature of the questionnaire and its use for 3/ 3.5G networks, making the survey items easy to answer. The respondents were selected from MTN, thus, a total of 50 Senior Managers were selected from the company; as the study also aimed to determine the best routing protocol for 3G/ 3.5G networks, it considered only companies operating 3/ 3.5G networks. Simple random sampling is done for the sample selection. This sampling method is conducted where each member of a population has an equal opportunity to become part of the sample. As all members of the population have an equal chance of becoming a research participant, this is said to be the most efficient sampling procedure. In order to conduct this sampling strategy, the researcher defined the population first, listed down all the members of the population and then selected members to make the sample. For this procedure, the lottery sampling or the fish bowl technique is employed. This method involves the selection of the sample at random from the sampling frame through the use of random number tables. Numbers are assigned for each employee in the master list. These numbers were written on pieces of paper and drawn from a box; the process is repeated until the sample size was reached.

3.4 Instruments

The survey questionnaire is used as the main data-gathering instrument for this study (See Appendix A). The questionnaire was divided into two main sections: a profile and the survey proper. The profile contains socio-demographic characteristics of the respondents such as the number of years they had served the company as well as their assigned job position. The questions were structure using the Likert format. In this survey type, three choices are provided for every question or statement. The choices represent the degree of agreement each respondent has on the given question.

The Likert survey is the selected questionnaire type as this enabled the respondents to answer the survey easily. In addition, this research instrument allowed the research to carry out the quantitative approach effectively with the use of statistics for data interpretation. In order to test the validity of the questionnaire used for the study, the researcher tested the questionnaire to five respondents. These respondents as well as their answers were not part of the actual study process and were only used for testing purposes. After the questions have been answered, the researcher asked the respondents for any suggestions or any necessary corrections to ensure further improvement and validity of the instrument. The researcher revised the survey questionnaire based on the suggestion of the respondents. The researcher then excluded irrelevant questions and changed vague or difficult terminologies into simpler ones in order to ensure comprehension.

3.5 Data Processing and Analysis

After gathering all the completed questionnaires from the respondents, total responses for each item were obtained and tabulated. In order to use the Likert-scale for interpretation, weighted mean to represent each question was computed. Weighted mean is the average wherein every quantity to be averaged has a corresponding weight. These weights represent the significance of each quantity to the average. A pie chart was used to represent the various weights.

3.6 Ethical Considerations

As this study required the participation of human respondents, specifically engineering professionals, certain ethical issues were addressed. The consideration of these ethical issues was necessary for the purpose of ensuring the privacy as well as the safety of the participants. Among the significant ethical issues that were considered in the research process include consent and confidentiality. In order to secure the consent of the selected participants, the researcher relayed all important details of the study, including its aim and purpose. By explaining these important details, the respondents were able to understand the importance of their role in the completion of the research. The respondents were also advised that they could withdraw from the study even during the process. With this, the participants were not forced to participate in the survey. The confidentiality of the participants is also ensured by not disclosing their names or personal information in the survey. Only relevant details that helped in answering the research questions are included.

CHAPTER FOUR

4.0 RESULTS, DISCUSSION AND ANALYSIS

The questionnaire was designed to provide to two analytical approaches. Firstly descriptive statistics were used to analyse data from closed questions which consisted predominantly of nominal level codes. Ordinal level data was obtained from technical managers comments regarding routing protocols, indicating a rank order without quantifiable increments. These were categorised without inferring a quantitative meaning [22]. Charts and tables where appropriate illustrate these data, and descriptive statistics were judged to be the most appropriate for this research due to its size – generalising to a target population through inferential statistics was not appropriate.

Secondly, the qualitative free text was analysed for thematic content and used to evaluate open ended questions, which involves looking for commonalities among participants and assessing relationships within data. Therefore common reasons for selecting the best routing protocol in data network were extracted and compared.

Each response on the questionnaire was coded (where possible) and entered into Microsoft Excel. When the computerised data set was complete, each question was examined separately and frequency of responses displayed in a table. Appropriate information was presented in graph form and cross-tabulated to aid understanding and interpretation [23]. The open ended (qualitative) responses were categorised and responses entered into a spreadsheet in an attempt to categorise responses. Contingency tables (cross tabulation of two ordinal or nominal level variables) were used to identify potential relationships between answers.

4.1 Presentation of Results and Discussion

Figure 4.1 shows that 40 technical managers chose MPLS as the best routing protocol in data packet networks such as 3.5G, 5 technical managers chose OSPF, 3 chose IS-IS and 2 chose RIP.

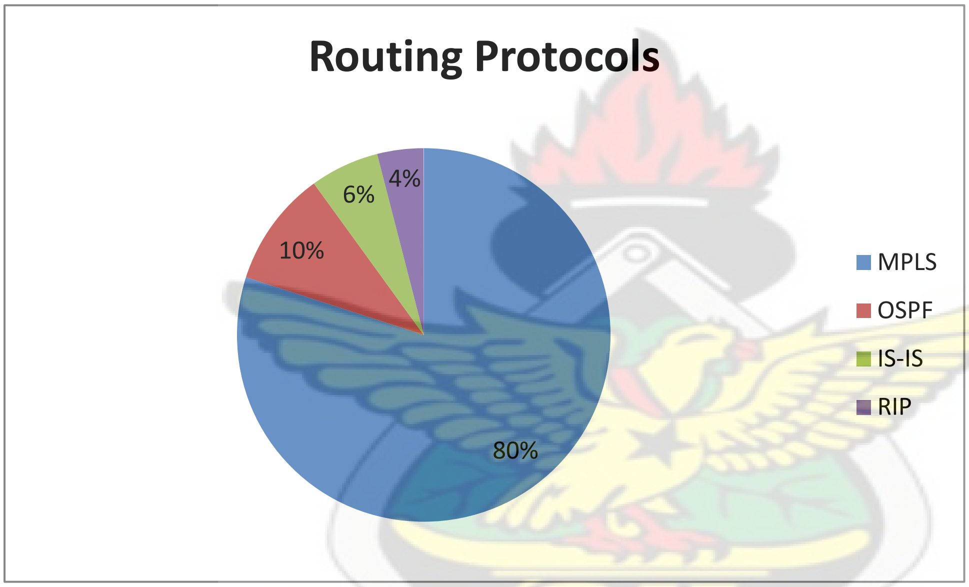


Figure 4.1 (Q1): The best routing protocol used in data networks such as 3.5G

Figure 4.2 shows the respondents answering whether their answer in (Q1) is the most deployed in modern ISPs and 3.5G networks. Majority of the technical managers answered YES then followed by I don't know and very few answered NO.

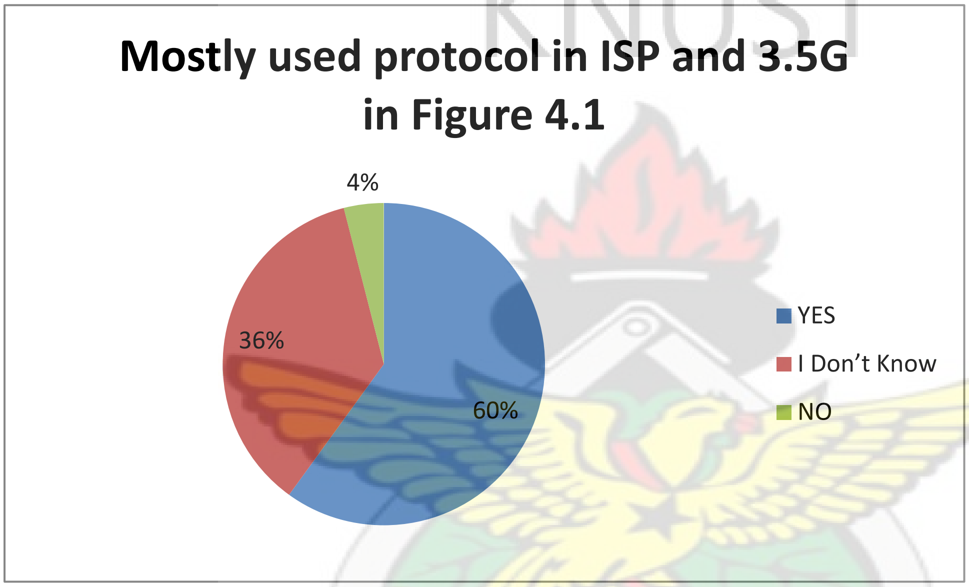


Figure 4.2 (Q2): Your choice (Q1) is mostly deployed in modern ISPs and 3.5G networks.

Figure 4.3 shows whether the answered chosen in (Q1) has matured a lot and it is a stable technology. Majority of the respondents (70%) or 35 out of 50 believe their answer to best protocol used in data packet network has really matured and has been tested for several times and it is a stable technology that can be relied on. 28% answered NO indicating the answer to Q1 is not matured and it not a stable technology. 2% answered I don't know indicating they either don’t know or they are not very sure whether their answer to Q1 has matured and it’s a stable technology.

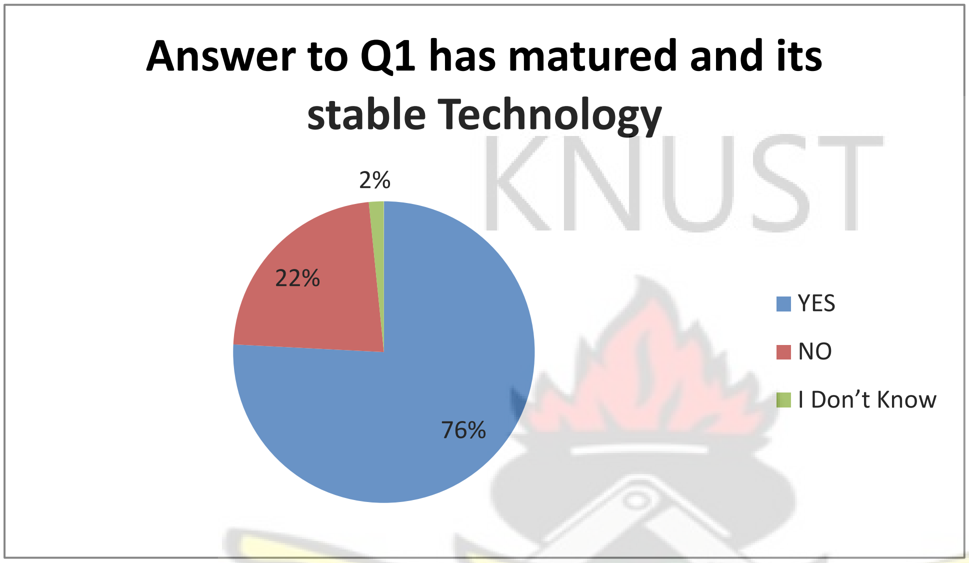


Figure 4.3 (Q3): Your choice in (Q1) has matured a lot and it’s a stable technology.

Figure 4.4 shows whether the answer chosen in (Q1) is based on Internet Protocol (IP). 47 out of 50 respondents answered YES representing 94%, those who chose I don’t know were 3 out of 50 representing 6%, Non of the respondents chose NO indicating 0%.

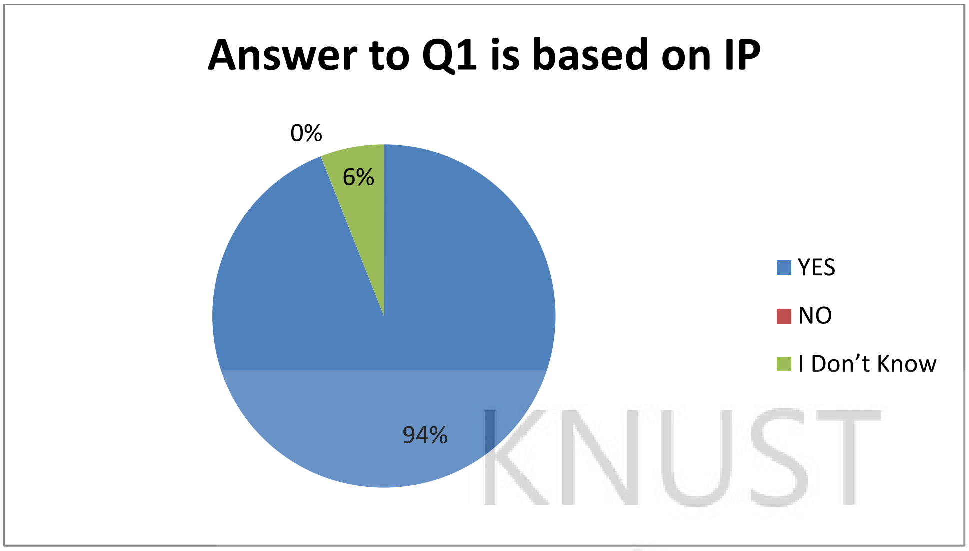


Figure 4.4 (Q4): Your choice (Q1) is based on IP and the internet is based on IP.

Figure 4.5 shows whether the future of the answer to Q1 is ensured for quite a while to come. This was to investigate the respondents view for the future of their answer in Q1, whether they believe will become a well acceptable protocol in the future ahead of the rest. Majority answered YES representing 86% (43 out of 50 respondents) indicating they are sure their of the best routing protocol for data packet network will dominate in the future. 12% answered I don't know and 2% answered NO meaning their answer to Q1 is not future guaranteed.

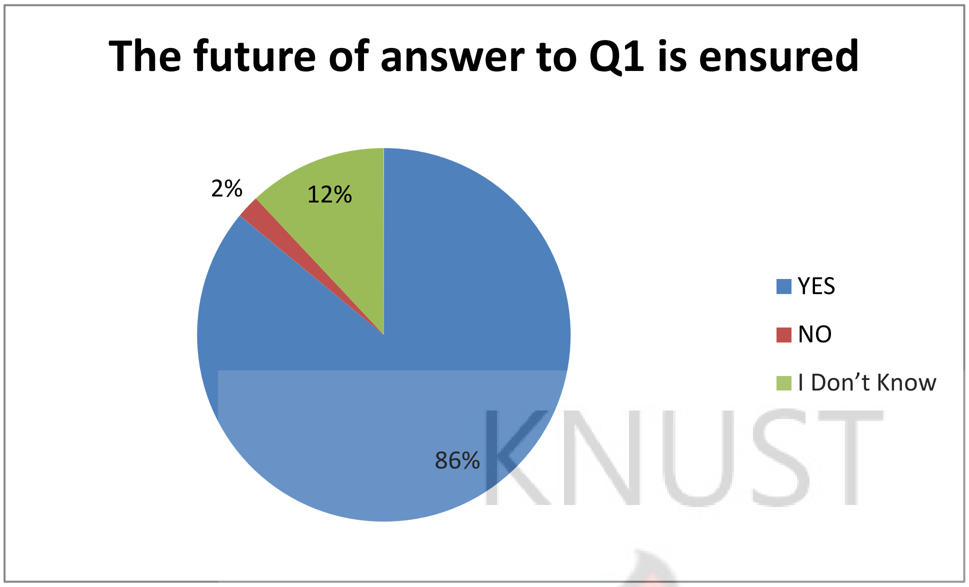


Figure 4.5 (Q5): The future of your choice in (Q1) is ensured for quite a while to come and it is reliable.

Figure 4.6 Illustrates whether the answer to (Q1) can avoid or circumvent route flapping and network congestion. Majority of the respondents chose YES representing 98% (49 out of 50 respondents) indicating most of the respondents believe that their choice of routing protocol can avoid route flapping and network congestion. 2% answered I don’t know while 0% answered NO.

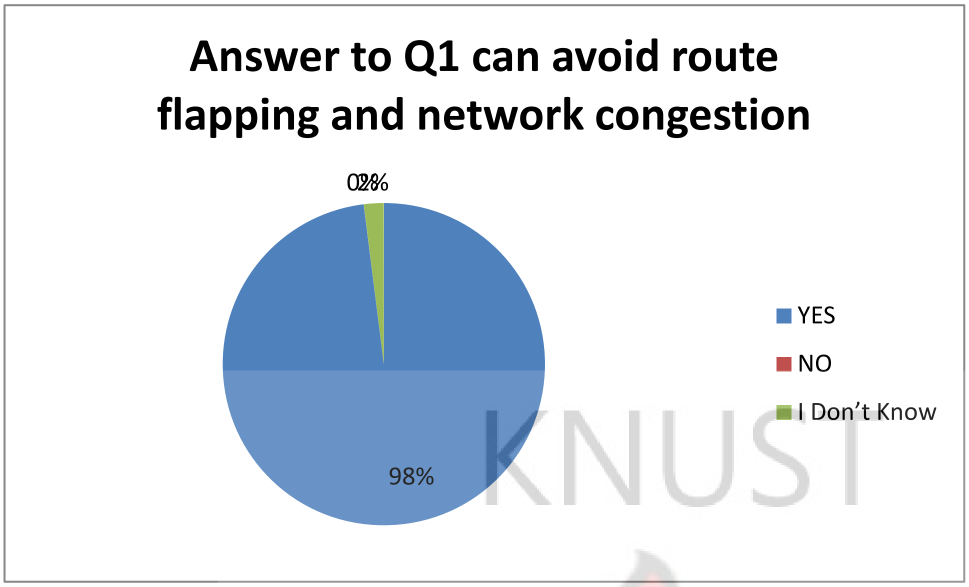


Figure 4.6 (Q6): Your choice in (Q1) can circumvent route flapping and network congestion.

Figure 4.7 show whether the choice in Q1 can transport IPv4, IPv6, Ethernet, High Level Data Link Control (HLDLC) and other layer 2 technologies. 44 out of 50 answered YES (88%) their choice of the best routing protocol in data packet network can transport IPv4, IPv6, Ethernet, HLDLC and other layer 2 technologies. 4 out 50 respondents (8%) answered I don't know whiles 2 out of 50 respondents answered NO which represents (4%).

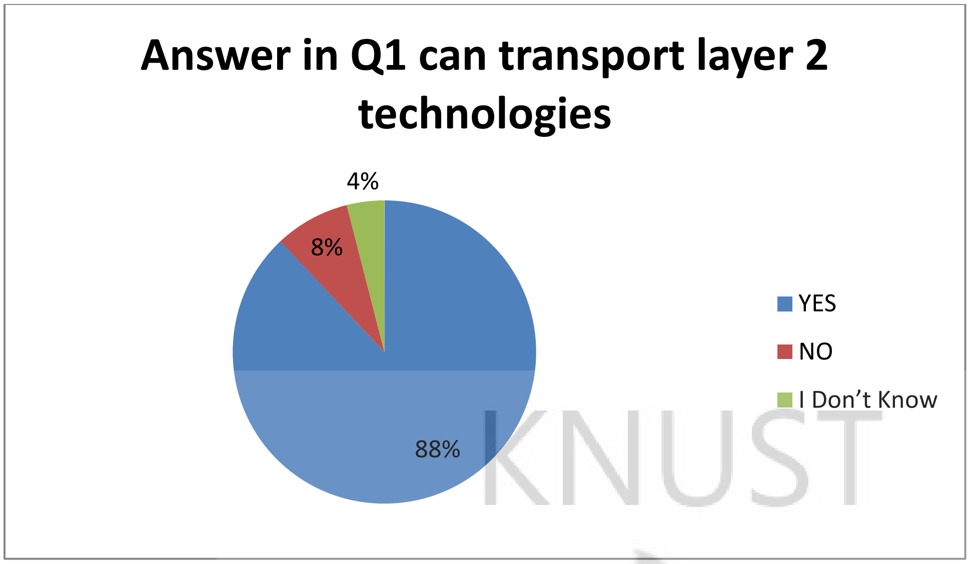


Figure 4.7 (Q7): Your choice in (Q1) can transport IPv4, IPv6, Ethernet, High Level Data Link Control (HDLC) and other Layer 2 technologies.

Figure 4.8 demonstrates the choice of answer in Q1 outperforms traditional static and dynamic algorithms. 50 out 50 respondents answered YES representing a 100% total agreement. Nobody answered for both NO and I don't know which represents 0% each.

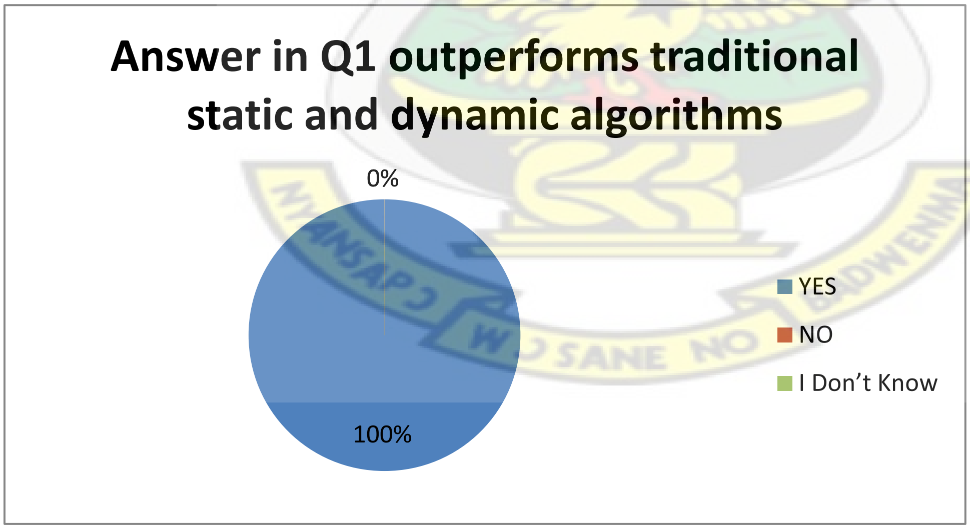


Figure 4.8 (Q8): Your choice in (Q1) outperforms traditional static and dynamic algorithms

Figure 4.9 shows whether when there are multiple paths in routing, deploying your choice in (Q1) is the best option in selecting the shortest path. 70% representing 35 out 50 respondents answered YES followed by 24% (12 out of 50 respondents) answered NO and then 6% (3 out of 50) also answered I don't know.

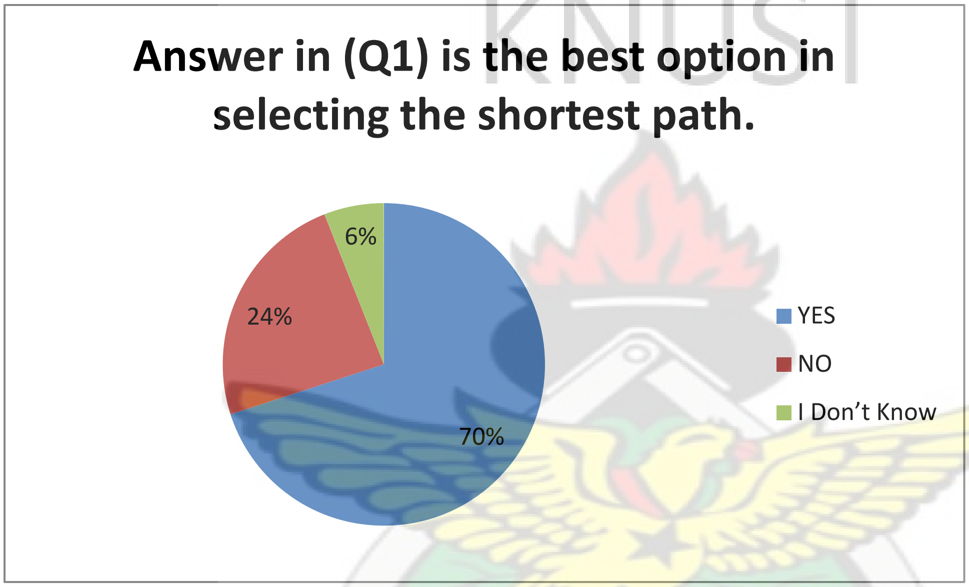


Figure 4.9 (Q9): When there are multiple paths in routing, deploying your choice in (Q1) is the best option in selecting the shortest path.

4.2 Result Analysis

Results from the respondents indicated that MPLS as their preferred protocol. Many researchers have done a lot of works in the areas of MPLS routing protocols where they came with results that corresponds with that of the respondents in this study. Some studies done by S. Jha and M. Hassan in 2002 [24] showed that MPLS is a label-forwarding scheme which provides a better solution to address the problems faced by present-day networks-speed, scalability, quality-of-service (QoS) management, and traffic engineering. They also showed that, MPLS has emerged as an elegant solution to meet the bandwidth-management and service requirements for next generation IP-based backbone networks. Fabino M. *et al.* [25] in their studies gave the advantages of using MPLS which makes them to dominate in mobile, wireless communication networks.

The purpose of traffic engineering (TE) is to enhance network utilization and to improve the architecture of a network in a systematic way, so that the network becomes robust, adaptive and easy to operate. MPLS has extended routing capabilities that efficiently controls the network traffic by removing congestion and spreading the load over different links. Different route selection algorithm based on MPLS frame work is provided in [26-28]. This corresponds to the results from the respondents where they were asked whether their choice of protocol can circumvent route flapping and network congestion. Majority of them (98%) answered YES. The results also indicated that, majority of the respondents (88%) agreed that their choice of protocol can transport IPv4, IPv6, Ethernet, High Level Data Link Control (HDLC) and other Layer 2 technologies. Some research have also been done to show interoperability and performance evaluation between IPv4 and IPv6 with MPLS. Yunos R. *et al.*[29] conducted research on performance evaluation between IPv4 and IPv6 with Linux MPLS tunnel. MPLS Linux tunneling is used to transport IPv6 data stream over IPv4 network for interoperable IPv4 and IPv6 deployment. The performance metrics such as jitter, datagram/packet loss and bandwidth were measured in both TCP and UPD traffic flow. The experiment test-bed was constructed using virtual machine tool for simulating the IPv4, IPv6, and the MPLS tunneling mechanism. Their study revealed that IPv6 offered better performance than IPv4 in almost all of the testing except in TCP transfer. In addition, MPLS tunnel improved performance in packet transfer for TCP transfer, UDP transfer and bandwidth testing. MPLS which combines the flexibility of Layer3 routing with Layer2 switching is being widely developed. Unfortunately, existing MPLS specifications can only support unicast well, but lack of supporting multicast. The main difficulty in MPLS supporting multicast is how to bind labels to multicast FEC. Zhongshang Zhang et al.[30] in their studies presented a new mechanism for MPLS supporting IP multicast routing protocol. In their proposed mechanism, label distribution is triggered by traffic and not by control messages. This mechanism makes the network's scalability and dynamic property better than the mechanism whose label distribution is triggered by control messages.

Tran Cong et al. [31] also focused their study on interoperability between mobile IPv4 and mobile IPv6. For better QoS services and how their proposal can be applied for large network on Internet, they developed their solution on an MPLS network that is now used for QoS and high-speed core network. In the case of protocol reliability, maturity and stability, 76% answered YES whiles 22% answered NO and 2% answered I don’t know for their choice of protocol maturity and stability. For reliability, 86% answered YES 12% answered NO and 2% answered I don’t know.

Chen and Oh in 1999 [32] performed some research to examine the reliability of multiprotocol label switching (MPLS) .MPLS is a convergence of various implementations of IP switching using ATM-like “label swapping” to speed up packet forwarding without changes to existing IP routing protocols. An important practical issue is the capability to recover quickly from faults. In their work, they examined distributed methods for fast fault recovery using modified label distribution protocol messages. To maintain and verify service continuity, methods are proposed for traffic and performance monitoring. All these studies showed some level of agreement with our studies.

CHAPTER FIVE

5.0 MULTIPROTOCOL LABEL SWITCHING

5.1.0 Introduction

The success of MPLS is undoubtedly a result of the fact that it enables the network to carry all kinds of traffic, ranging from IP traffic to Voice over IP (VoIP) traffic to Layer 2 traffic. MPLS is the means for an IP network to consolidate many networks into one. MPLS can consolidate the ATM, Frame Relay, Voice, and IP networks into one unified network infrastructure, thereby generating a huge cost advantage.

MPLS has matured a lot and is a stable technology, seeing many new deployments and new features. Given the fact that MPLS is based on IP, and the Internet is based on IP technology, it seems that the future of MPLS is ensured for quite a while to come [33].

5.1.1 The Evolution of MPLS

Multiprotocol Label Switching (MPLS) has been around for several years. It is a popular networking technology that uses labels attached to packets to forward them through the network.

5.1.2 Definition of MPLS

The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of by IP switching.

The label switching technique is not new. Frame Relay and ATM use it to move frames or cells throughout a network. In Frame Relay, the frame can be any length, whereas in ATM, a fixedlength cell consists of a header of 5 bytes and a payload of 48 bytes. The header of the ATM cell and the Frame Relay frame refer to the virtual circuit that the cell or frame resides on. The similarity between Frame Relay and ATM is that at each hop throughout the network, the "label" value in the header is changed. This is different from the forwarding of IP packets. When a router forwards an IP packet, it does not change a value that pertains to the destination of the packet; that is, it does not change the destination IP address of the packet. The fact that the MPLS labels are used to forward the packets and no longer the destination IP address have led to the popularity of MPLS.

5.1.3 Pre-MPLS Protocols

Before MPLS, the most popular WAN protocols were ATM and Frame Relay. Cost-effective WAN networks were built to carry various protocols. With the popularity of the Internet, IP became the most popular protocol. IP was everywhere. VPNs were created over these WAN protocols. Customers leased ATM links and Frame Relay links or used leased lines and built their own private network over it. Because the routers of the provider supplied a Layer 2 service toward the Layer 3 customer routers, the separation and isolation between different customer networks were guaranteed. These kinds of networks are referred to as overlay networks.

Overlay networks are still used today, but many customers are now using the MPLS VPN service.

5.1.4 Benefits of MPLS

These benefits include the following:

■ The use of one unified network infrastructure

■ Better IP over ATM integration

■ Border Gateway Protocol (BGP)-free core

■ The peer-to-peer model for MPLS VPN

■ Optimal traffic flow

■ Traffic engineering

Consider first a bogus reason to run MPLS. This is a reason that might look reasonable initially, but it is not a good reason to deploy MPLS.

5.1.5 Bogus Benefit

One of the early reasons for a label-swapping protocol was the need for speed. Switching IP packets on a CPU was considered to be slower than switching labeled packets by looking up just the label on top of a packet. A router forwards an IP packet by looking up the destination IP address in the IP header and finding the best match in the routing table. This lookup depends on the implementation of the specific vendor of that router. However, because IP addresses can be unicast or multicast and have four octets, the lookup can be complex. A complex lookup means that a forwarding decision for an IP packet can take some time. Although some people thought that looking up a simple label value in a table rather than looking up the IP address would be a faster way of switching packets, the progress made in switching IP packets in hardware made this argument a moot one. These days, the links on routers can have a bandwidth up to 40 Gbps.

A router that has several high-speed links would not be able to switch all the IP packets just by using the CPU to make the forwarding decision. The CPU exists mainly

to handle the control plane. The control plane is the set of protocols that helps to set up the data or forwarding plane. The main components of the control plane are the routing protocols, the routing table, and other control or signaling protocols used to provision the data plane. The data plane is the packet forwarding path through a router or switch. The switching of the packets—or the forwarding plane—these days is done on specifically built hardware, or application-specific integrated circuits (ASIC). The use of ASICs in the forwarding plane of a router has led to IP packets being switched as fast as labeled packets. Therefore, if your sole reason for implementing MPLS in your network is to pursue the faster switching of packets through the network, it is a bogus reason.

5.1.6 The Use of One Unified Network Infrastructure

With MPLS, the idea is to label ingress packets based on their destination address or other preconfigured criteria and switch all the traffic over a common infrastructure. This is the great advantage of MPLS. One of the reasons that IP became the only protocol to dominate the networking world is because many technologies can be transported over it. Not only is data transported over IP, but also telephony. By using MPLS with IP, you can extend the possibilities of what you can transport. Adding labels to the packet enables you to carry other protocols than just IP over an MPLS-enabled Layer 3 IP backbone, similarly to what was previously possible only with Frame Relay or ATM Layer 2 networks. MPLS can transport IPv4, IPv6, Ethernet, High-Level Data Link Control (HDLC), PPP, and other Layer 2 technologies.

The feature whereby any Layer 2 frame is carried across the MPLS backbone is called *Any* Transport over MPLS (AToM). The routers that are switching the AToM traffic do not need to be aware of the MPLS payload; they just need to be able to switch the labeled traffic by looking at the label on top of it. In essence, MPLS label switching is a simple method of switching multiple protocols in one network. You need to have a forwarding table consisting of incoming labels to be swapped by outgoing labels and a next hop.

In short, AToM enables the service provider to provide the same Layer 2 service toward the customers as with any specific non-MPLS network. At the same time, the service provider needs only one unified network infrastructure to carry all kinds of customer traffic.

5.1.7 Better IP over ATM Integration

In the previous decade, IP won the battle over all other networking Layer 3 protocols, such as AppleTalk, Internetwork Packet Exchange (IPX), and DECnet. IP is relatively simple and omnipresent. A much-hyped Layer 2 protocol at the time was ATM. Although ATM as an end-to end protocol—or desktop-to-desktop protocol—as some predicted, never happened, ATM did have plenty of success, but the success was limited to its use as a WAN protocol in the core of service provider networks. Many of these service providers also deployed IP backbones. The integration of IP over ATM was not trivial. To better integrate IP over ATM, the networking community came up with a few solutions. One solution was to implement IP over ATM according to the well-known RFC 1483, “Multiprotocol Encapsulation over ATM Adaptation Layer 5,” which specifies how to encapsulate multiple routed and bridged protocols over ATM adaptation Layer (AAL) 5. In this solution, all ATM circuits had to be manually established, and all mappings between IP next hops and ATM endpoints had to be manually configured on every ATM-attached router in the network. Another method was to implement LAN Emulation (LANE). Ethernet had become a popular Layer 2 technology at the edge of the network, but it never achieved the scalability or reliability requirements of large service provider networks. LANE basically makes your network look like an emulated Ethernet network. This means that several Ethernet segments were bridged together as if the ATM WAN network in the middle were an Ethernet switch.

Finally, Multiprotocol over ATM (MPOA), which is a specification by the ATM Forum, gives you the tightest integration of IP over ATM but also the most complex solution.

All these methods were cumbersome to implement and troubleshoot. A better solution for integrating IP over ATM was one of the driving reasons for the invention of MPLS. The prerequisites for MPLS on ATM switches were that the ATM switches had to become more intelligent. The ATM switches had to run an IP routing protocol and implement a label distribution protocol.

5.1.8 BGP-Free Core

When the IP network of a service provider must forward traffic, each router must look up the destination IP address of the packet. If the packets are sent to destinations that are external to the service provider network, those external IP prefixes must be present in the routing table of each router. BGP carries external prefixes, such as the customer prefixes or the Internet prefixes. This means that all routers in the service provider network must run BGP. MPLS, however, enables the forwarding of packets based on a label lookup rather than a lookup of the IP addresses.

MPLS enables a label to be associated with an egress router rather than with the destination IP address of the packet. The label is the information attached to the packet that tells every intermediate router to which egress edge router it must be forwarded. The core routers no longer need to have the information to forward the packets based on the destination IP address. Thus, the core routers in the service provider network no longer need to run BGP. The router at the edge of the MPLS network still needs to look at the destination IP address of the packet and hence still needs to run BGP. Each BGP prefix on the ingress MPLS routers has a BGP next-hop IP address associated with it. This BGP next-hop IP address is an IP address of an egress MPLS router. The label that is associated with an IP packet is the label that is associated with this BGP next-hop IP address. Because every core router forwards a packet based on the attached MPLS label that is associated with the BGP next-hop IP address, each BGP next-hop IP address of an egress MPLS router must be known to all core routers. Any interior gateway routing protocol, such as OSPF or ISIS, can accomplish this task.

Figure 5.1 shows the MPLS network with BGP on the edge routers only.

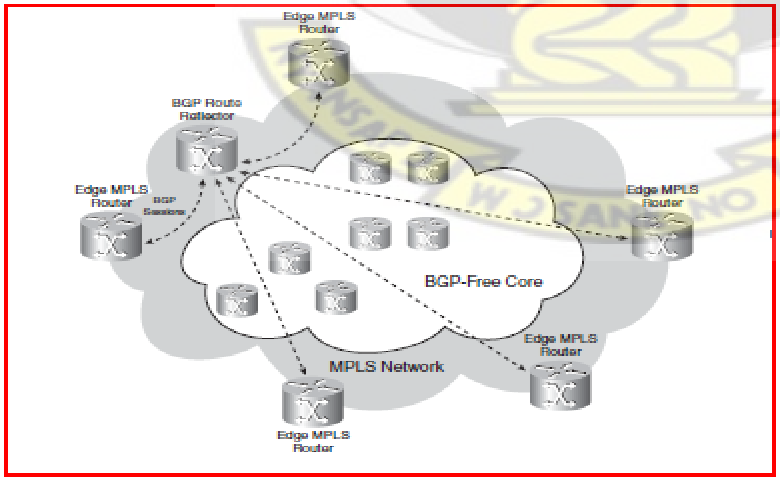


Figure 5.1: BGP-Free MPLS Network

An Internet service provider (ISP) that has 200 routers in its core network needs to have BGP running on all 200 routers. If MPLS is implemented on the network, only the edge routers—which might be 50 or so routers—need to run BGP.

All routers in the core of the network are now forwarding labeled packets, without doing an IP lookup, so they are now relieved from the burden of running BGP. Because the full Internet routing table is well above 150,000 routes, not having to run BGP on all routers is a serious consideration. Routers without the full Internet routing table need a lot less memory. You can run the core routers without the complexity of having to run BGP on them.

5.1.9 Peer-to-Peer VPN Model versus Overlay VPN Model

A VPN is a network that emulates a private network over a common infrastructure. The private network requires all customer sites to be able to interconnect and be completely separate from other VPNs. The VPN usually belongs to one company and has several sites interconnected across the common service provider infrastructure [34].

Service providers can deploy two major VPN models to provide VPN services to their customers:

■ Overlay VPN model

■ Peer-to-peer VPN model

5.1.10 Overlay VPN Model

In the overlay model, the service provider supplies a service of point-to-point links or virtual circuits across his network between the routers of the customer. The customer routers form routing peering between them directly across the links or virtual circuits from the service provider. The routers or switches from the service provider carry the customer data across the service provider network, but no routing peering occurs between a customer and a service provider router. The result of this is that the service provider routers never see the customer routes.

These point-to-point services could be of Layer 1, 2, or even 3. Examples of Layer 1 are timedivision multiplexing (TDM), E1, E3, SONET, and SDH links. Examples of Layer 2 are virtual circuits created by X.25, ATM, or Frame Relay.

Figure 5.2 shows an example of an overlay network build on Frame Relay. In the service provider network are Frame Relay switches that set up the virtual circuits between the customer routers on the edge of the Frame Relay network.

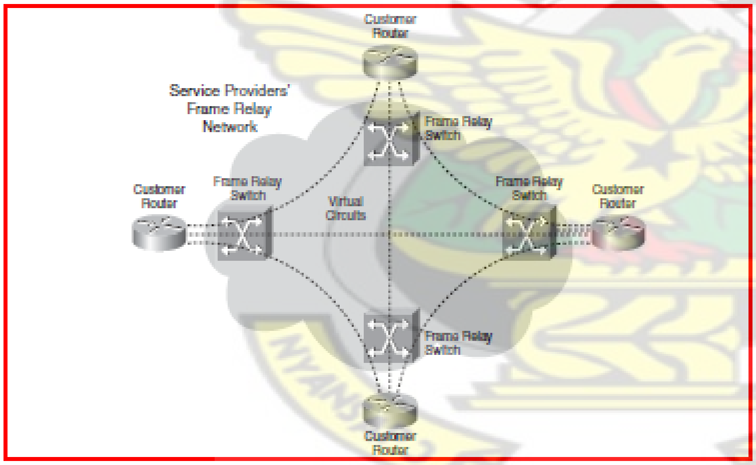


Figure 5.2: Overlay Network on Frame Relay

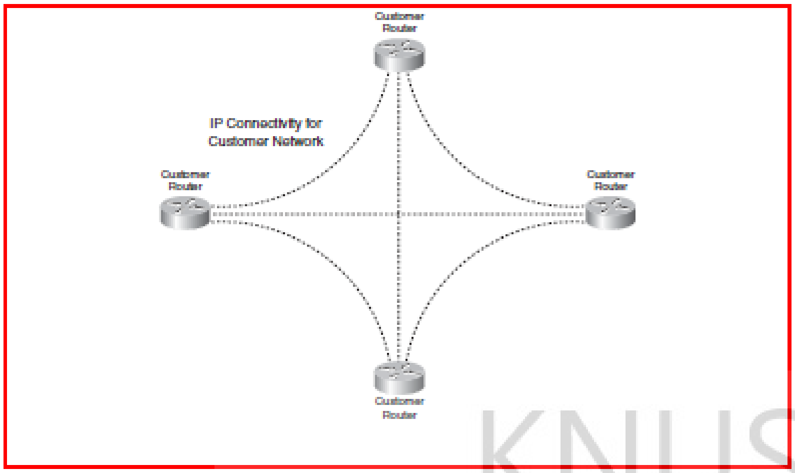
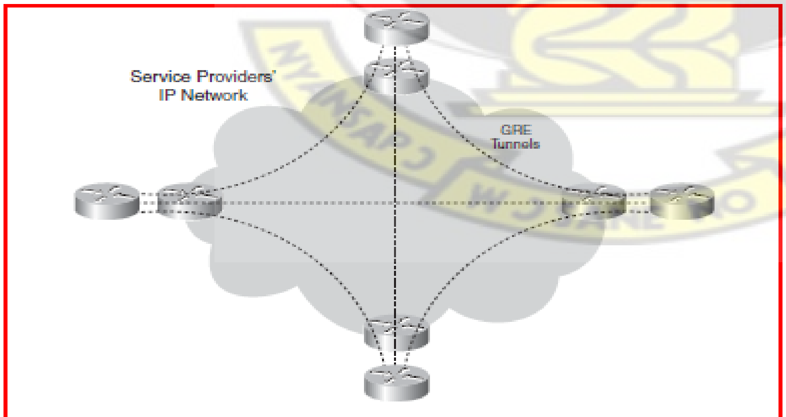


Figure 5.3: Overlay Network: Customer Routing Peering

The overlay service can also be provided over the IP Layer 3 protocol. Most commonly used tunnels to build the overlay network on IP are generic routing encapsulation (GRE) tunnels. These tunnels encapsulate the traffic with a GRE header and an IP header. The GRE header, among other things, indicates what the transported protocol is. The IP header is used to route the packet through the service provider network. **Figure 5.4** shows an example of an overlay network with GRE tunnels. One advantage of GRE tunnels is that they can route traffic other than IP traffic.



It is possible to use IPsec on the GRE tunnels and thus provide security as the data is encrypted.

Figure 5.4: Overlay Network on GRE Tunnels

5.1.11 Peer-to-Peer VPN Model

In the peer-to-peer VPN model, the service provider routers carry the customer data across the network, but they also participate in the customer routing. In other words, the service provider routers peer directly with the customer routers at Layer 3. The result is that one routing protocol neighborship or adjacency exists between the customer and the service provider router. **Figure 5.5** shows the concept of the peer-to-peer VPN model [35].

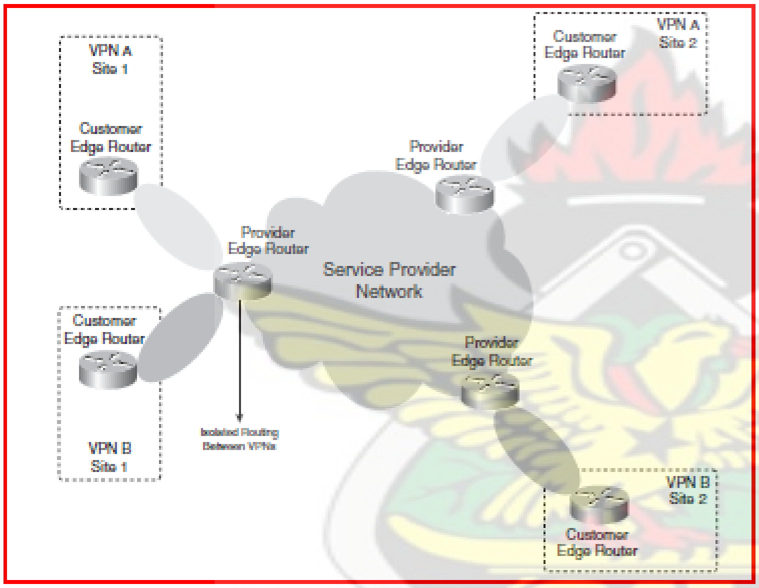


Figure 5.5: Peer-to-Peer VPN Model

Before MPLS existed, the peer-to-peer VPN model could be achieved by creating the IP routing peering between the customer and service provider routers. The VPN model also requires privateness or isolation between the different customers. You can achieve this by configuring packet filters (access lists) to control the data to and from the customer routers. Another way to achieve a form of privateness is to configure route filters to advertise routes or stop routes from being advertised to the customer routes. Or, you can deploy both methods at the same time.

Before MPLS came into being, the overlay VPN model was deployed much more commonly than the peer-to-peer VPN model. The peer-to-peer VPN model demanded a lot from provisioning because adding one customer site demanded many configuration changes at many sites. MPLS VPN is one application of MPLS that made the peer-to-peer VPN model much easier to implement. Adding or removing a customer site is now easier to configure and thus demands much less time and effort. With MPLS VPN, one customer router, called the customer edge (CE) router, peers at the IP Layer with at least one service provider router, called the provider edge (PE) router.

The privateness in MPLS VPN networks is achieved by using the concept of virtual routing/ forwarding (VRF) and the fact that the data is forwarded in the backbone as labeled packets. The VRFs ensure that the routing information from the different customers is kept separate, and the MPLS in the backbone ensures that the packets are forwarding based on the label information and not the information in the IP header. **Figure 5.6** shows the concept of VRFs and forwarding labeled packets in the backbone of a network that is running MPLS VPN.

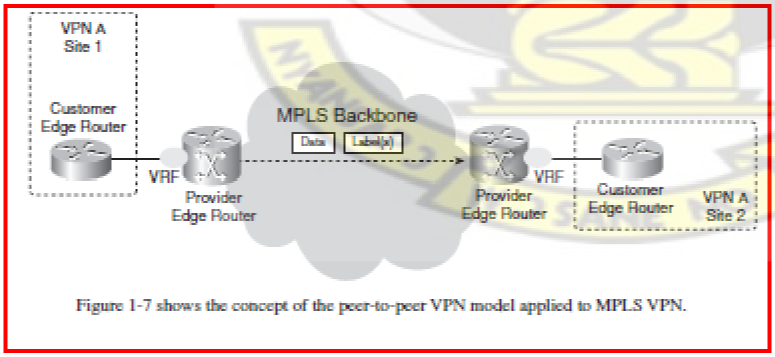


Figure 1-7 shows the concept of the peer-to-peer VPN model applied to MPLS VPN.

Figure 5.6: MPLS VPN with VRF

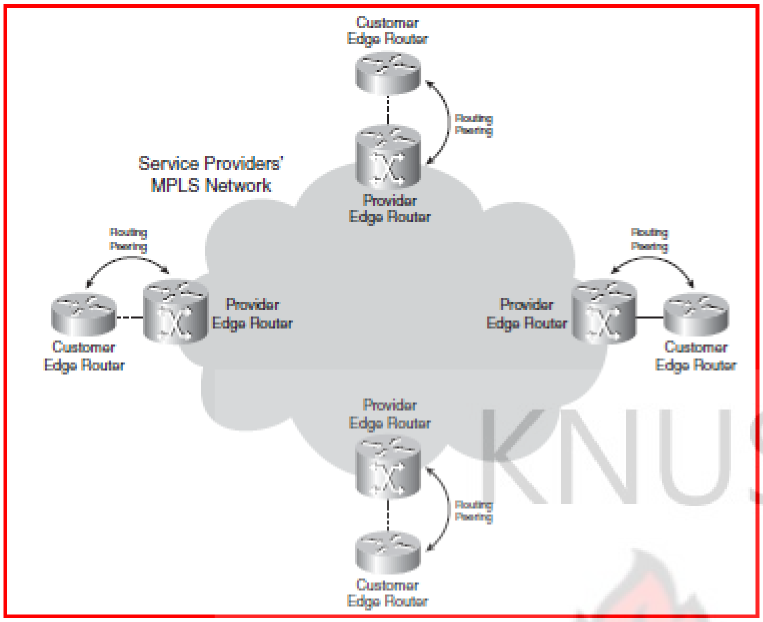


Figure 5.7: Peer-to-Peer MPLS VPN Model

Adding one customer site means that on the PE router, only the peering with the CE router must be added. You do not have to hassle with creating many virtual circuits as with the overlay model or with configuring packet filters or route filters with the peer-to-peer VPN model over an IP network. This is the benefit of MPLS VPN for the service provider. Most service provider customers have a hub-and-spoke network, whereas some have a fully meshed network around the service provider backbone. Others have something in between. The benefit of MPLS VPN for the customer is at its greatest when the customer has a fully meshed network. Refer to Figure 5-2 to see a fully meshed customer network around a Frame Relay network, and compare that to the same customer network with MPLS VPN in **Figure 5-7**. In **Figure 5-2**, each customer edge router peers with *n*–1 other customer edge routers—where *n* is the total number of customer edge routers. In **Figure 5-7**, each customer edge router peers with only one service provider edge router.

Another benefit for the service provider is that it only needs to provision the link between the PE and CE routers. With the overlay model, the service provider needs to provision the links or virtual circuits between the sites. It is much easier to predict the traffic and thus the bandwidth requirement of one site than to predict the complete traffic model between all the customer sites.

It is only fair to list the disadvantages of the peer-to-peer VPN model compared to the overlay VPN model:

■ The customer must share the routing responsibility with the service provider.

■ The edge devices of the service provider have an added burden.

The first disadvantage is that the customer must have a routing peer with the service provider. The customer does not control its network end to end anymore on Layer 3 and regarding the IP routing, as with the overlay model. The second disadvantage is for the service provider. The burden for the service provider is the added task of the edge device—the PE router. The service provider is responsible for the scalability and routing convergence of the customer networks because the PE routers must be able to carry all the routes of the many customers while providing timely routing convergence.

5.1.12 Optimal Traffic Flow

Because the ATM or Frame Relay switches are purely Layer 2 devices, the routers interconnect through them by means of virtual circuits created between them. For any router to send traffic directly to any other router at the edge, a virtual circuit must be created between them directly. Creating the virtual circuits manually is tedious. In any case, if the requirement is the any-to-any connection between sites, it is necessary to have a full mesh of virtual circuits between the sites, which are cumbersome and costly. If the sites are only interconnected as in **Figure 5.8**, the traffic

from CE1 to CE3 must first go through CE2.

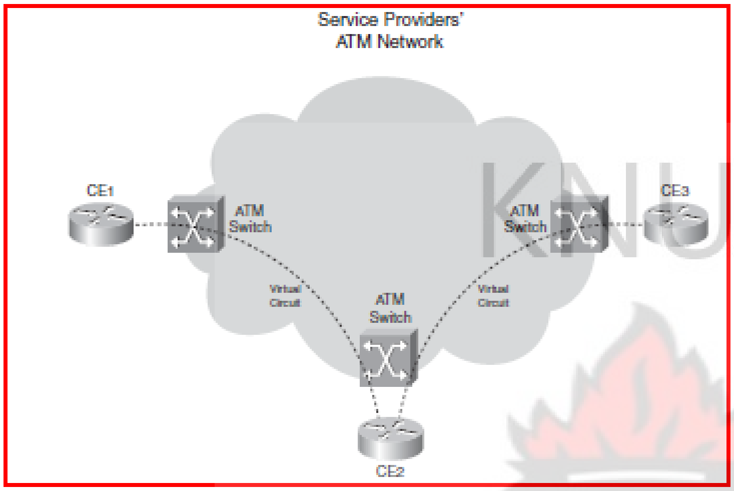


Figure 5.8: Non-Fully Meshed Overlay ATM Network

The result is that the traffic crosses the ATM backbone twice and takes a detour through the router CE2.

5.1.13 Traffic Engineering

The basic idea behind traffic engineering is to optimally use the network infrastructure, including links that are underutilized, because they do not lie on the preferred path. This means that traffic engineering must provide the possibility to steer traffic through the network on paths different from the preferred path, which is the least-cost. path .provided by IP routing. The least-cost path is the shortest path as computed by the dynamic routing protocol. With traffic engineering implemented in the MPLS network, you could have the traffic that is destined for a particular prefix or with a particular quality of service flow from point A to point B along a path that is different from the least-cost path. The result is that the traffic can be spread more evenly over the available links in the network and make more use of underutilized links in the network. **Figure 5.9** shows an example of this.

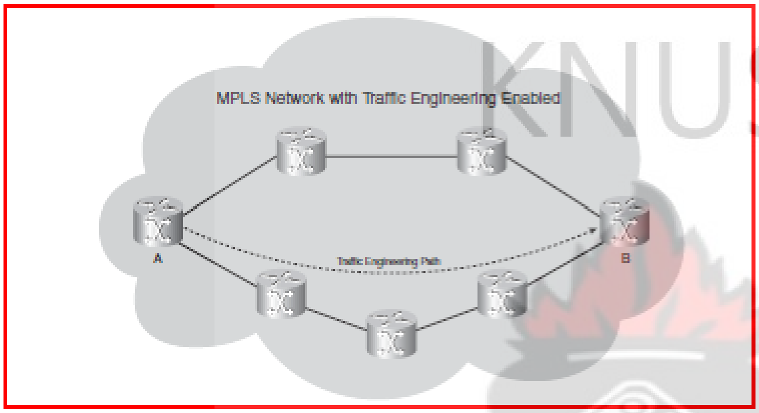


Figure 5.9: Traffic Engineering Example

As the operator of the MPLS-with-traffic-engineering-enabled network, you can steer the traffic from A to B over the bottom path, which is not the shortest path between A and B (four hops versus three hops on the top path). As such, you can send the traffic over links that might otherwise not be used much. You can guide the traffic in this network onto the bottom path by changing the routing protocols metrics. Examine **Figure 5.10.**

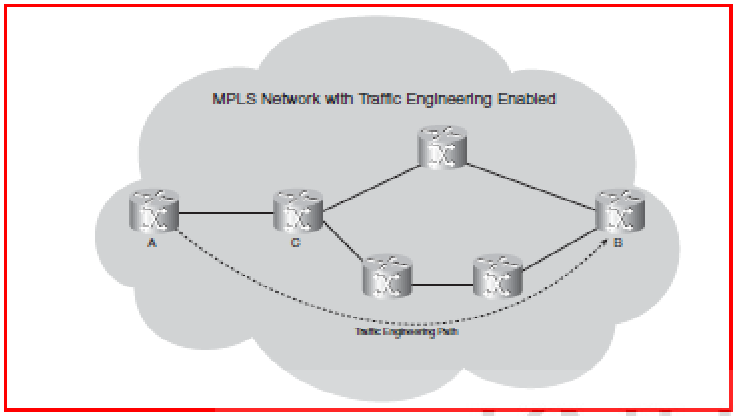


Figure 5.10: Traffic Engineering Example 2

If this network is an IP-only network, you cannot have router C send the traffic along the bottom path by configuring something on router A. The router C decision to send traffic on the top or bottom path is solely its own decision. If you enable MPLS traffic engineering in this network, you can have router A send the traffic toward router B along the bottom path. The MPLS traffic engineering forces router C to forward the traffic A-B onto the bottom path. This can be done in MPLS because of the label forwarding mechanism. The head end router of a traffic-engineered path—here router A—is the router that specifies the complete path that the traffic will take through the MPLS network. Because it is the head end router that specifies the path, traffic engineering is also referred to as a form of source-based routing. The label that is attached to the packet by the head end router makes the packet flow along the path as specified by the head end router. No intermediate router forwards the packet onto another path.

An extra advantage of running MPLS traffic engineering is the possibility of Fast ReRouting (FRR). FRR allows you to reroute labeled traffic around a link or router that has become unavailable. The rerouting of traffic happens in less than 50 ms, which is fast even for standards of today.

5.2 MPLS Architecture

MPLS stands for Multiprotocol Label Switching. The multiprotocol aspect of MPLS was fulfilled after the initial implementation of MPLS in Cisco IOS. Although at first only IPv4 was being label switched, later on more protocols followed. In Cisco IOS, you can now label IPv6 packets, to Transport over MPLS," describes how to label and transport Layer 2 frames over an MPLS backbone. Label switching indicates that the packets switched are no longer IPv4 packets, IPv6 packets, or even Layer 2 frames when switched, but they are labeled. The most important item to MPLS is the label [36].

5.2.1 Introducing MPLS Labels

One MPLS label is a field of 32 bits with a certain structure. **Figure 5.11** shows the syntax of one MPLS label.

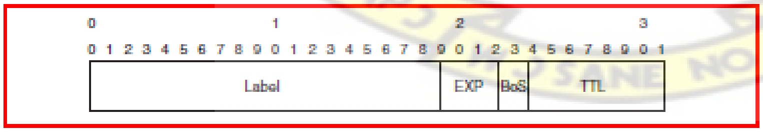


Figure 5.11: Syntax of One MPLS Label

The first 20 bits are the label value. This value can be between 0 and 2^{20}–1, or 1,048,575. However, the first 16 values are exempted from normal use; that is, they have a special meaning.

The bits 20 to 22 are the three experimental (EXP) bits. These bits are used solely for quality of service (QoS).

Bit 23 is the Bottom of Stack (BoS) bit. It is 0, unless this is the bottom label in the stack. If so, the BoS bit is set to 1. The stack is the collection of labels that are found on top of the packet. The stack can consist of just one label, or it might have more. The number of labels (that is, the 32-bit field) that you can be found in the stack is limitless, although you should seldom see a stack that consists of four or more labels.

Bits 24 to 31 are the eight bits used for Time To Live (TTL). This TTL has the same function as the TTL found in the IP header. It is simply decreased by 1 at each hop, and its main function is to avoid a packet being stuck in a routing loop. If a routing loop occurs and no TTL is present, the packet loops forever. If the TTL of the label reaches 0, the packet is discarded.

5.2.2 Label Stacking

MPLS-capable routers might need more than one label on top of the packet to route that packet through the MPLS network. This is done by packing the labels into a stack. The first label in the stack is called the top label, and the last label is called the bottom label. In between, you can have any number of labels. **Figure 5.12** shows you the structure of the label stack.

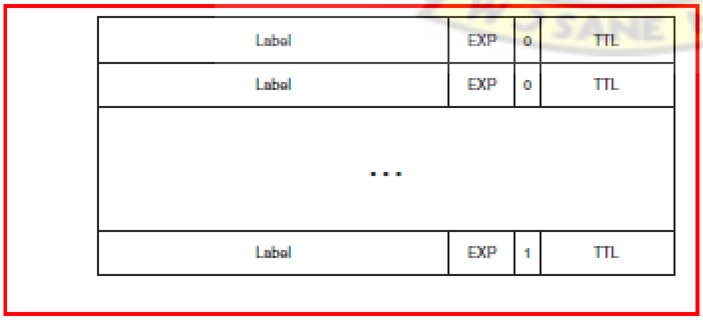


Figure 5.12: Label Stack

NOTE These bits are named “experimental” for historical reasons. At one time, nobody knew what they were going to be used for. Notice that the label stack in Figure 2-2 shows that the BoS bit is 0 for all the labels, except the bottom label. For the bottom label, the BoS bit is set to 1.

Some MPLS applications actually need more than one label in the label stack to forward the labeled packets. Two examples of such MPLS applications are MPLS VPN and AToM. Both MPLS VPN and AToM put two labels in the label stack.

3.2.3 Encoding of MPLS

Where does this label stack reside? The label stack sits in front of the Layer 3 packet—that is, before the header of the transported protocol, but after the Layer 2 header. Often, the MPLS label stack is called the shim header because of its placement.

Figure 5.13 shows you the placement of the label stack for labeled packets.

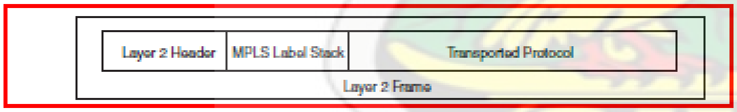
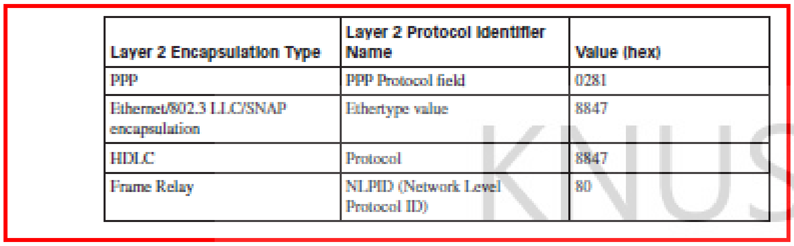


Figure 5.13: Encapsulation for Labeled Packet

The Layer 2 encapsulation of the link can be almost any encapsulation that Cisco IOS supports: PPP, High-Level Data Link Control (HDLC), Ethernet, and so on. Assuming that the transported protocol is IPv4, and the encapsulation of a link is PPP, the label stack is present after the PPP header but before the IPv4 header. Because the label stack in the Layer 2 frame is placed before the Layer 3 header or other transported protocol, you must have new values for the Data Link Layer Protocol field, indicating that what follows the Layer 2 header is an MPLS labeled packet. The Data Link Layer Protocol field is a value indicating what payload type the Layer 2 frame is carrying. Table 5-1 shows you what the names and values are for the Protocol Identifier field in the Layer 2 header for the different Layer 2 encapsulation types.

Table 5.1: MPLS Protocol Identifier Values for Layer 2 Encapsulation Types



Layer 2 Encapsulation Type	Layer 2 Protocol Identifier Name	Value (hex)
PPP	PPP Protocol field	0281
Ethernet/802.3 LLC/SNAP encapsulation	Ethertype value	8847
HDLC	Protocol	8847
Frame Relay	NLPID (Network Level Protocol ID)	80

ATM is absent from Table 5-1 because it uses a unique way of encapsulating the label. For Frame Relay, the NLPID is 0x80, indicating that an IEEE Subnetwork Access Protocol (SNAP) header is used. The SNAP header is used here in Frame Relay to tell the receiver what protocol Frame Relay carries. The SNAP header contains an Organizationally Unique Identifier (OUI) of 0x000000 and an Ethertype of 0x8847, indicating that the transported protocol is MPLS.

The transported protocol can theoretically be anything; Cisco IOS supports IPv4 and IPv6. In the case of AToM, the transported protocol can be any of the most popular Layer 2 protocols, such as Frame Relay, PPP, HDLC, ATM, and Ethernet.

5.2.4 MPLS and the OSI Reference Model

The OSI reference model consists of seven layers. Refer to **Figure 5.14** for the OSI reference model [37].

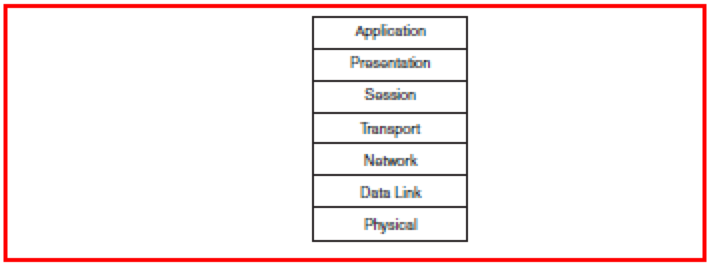


Figure 5.14: OSI Reference Model

The bottom layer is Layer 1, or the physical layer, and the top layer is Layer 7, or the application layer. Whereas the physical layer concerns the cabling, mechanical, and electrical characteristics, Layer 2, the data link layer, is concerned with the formatting of the frames. Examples of the data link layer are Ethernet, PPP, HDLC, and Frame Relay. The significance of the data link layer is only on one link between two machines, but not beyond. This means that the data link layer header is always replaced by the machine at the other end of the link. Layer 3, the network layer, is concerned with the formatting of packets end to end. It has significance beyond the data link. The most well-known example of a protocol operating at Layer 3 is IP.Where does MPLS fit in? MPLS is not a Layer 2 protocol because the Layer 2 encapsulation is still present with labeled packets. MPLS also is not really a Layer 3 protocol because the Layer 3 protocol is still present, too. Therefore, MPLS does not fit in the OSI layering too well. Perhaps the easiest thing to do is to view MPLS as the 2.5 layer and be done with it.

5.2.5 Label Switch Router

A label switch router (LSR) is a router that supports MPLS. It is capable of understanding MPLS labels and of receiving and transmitting a labeled packet on a data link. Three kinds of LSRs exist in an MPLS network:

■ Ingress LSRs—Ingress LSRs receive a packet that is not labeled yet, insert a label (stack) in front of the packet, and send it on a data link.

■ Egress LSRs—Egress LSRs receive labeled packets, remove the label(s), and send them on a data link. Ingress and egress LSRs are edge LSRs.

■ Intermediate LSRs—Intermediate LSRs receive an incoming labeled packet, perform an operation on it, switch the packet, and send the packet on the correct data link. An LSR can do the three operations: pop, push, or swap. It must be able to pop one or more labels (remove one or more labels from the top of the label stack) before switching the packet out. An LSR must also be able to push one or more labels onto the received packet. If the received packet is already labeled, the LSR pushes one or more labels onto the label stack and switches out the packet. If the packet is not labeled yet, the LSR creates a label stack and pushes it onto the packet. An LSR must also be able to swap a label. This simply means that when a labeled packet is received, the top label of the label stack is swapped with a new label and the packet is switched on the outgoing data link. An LSR that pushes labels onto a packet that was not labeled yet is called an imposing LSR because it is the first LSR to impose labels onto the packet. One that is doing imposition is an ingress LSR. An LSR that removes all labels from the labeled packet before switching out the packet is a disposing LSR. One that does disposition is an egress LSR. In the case of MPLS VPN , the ingress and egress LSRs are referred to as provider edge (PE) routers. Intermediate LSRs are referred to as provider (P) routers. The terms PE and P routers have become so popular that they are also used when the MPLS network does not run MPLS VPN.

5.2.6 Label Switched Path

A label switched path (LSP) is a sequence of LSRs that switch a labeled packet through an MPLS network or part of an MPLS network. Basically, the LSP is the path through the MPLS network or a part of it that packets take. The first LSR of an LSP is the ingress LSR for that LSP, whereas the last LSR of the LSP is the egress LSR. All the LSRs in between the ingress and egress LSRs are the intermediate LSRs.

In **Figure 5.15**, the arrow at the top indicates the direction, because an LSP is unidirectional. The flow of labeled packets in the other direction—right to left—between the same edge LSRs would be another LSP.

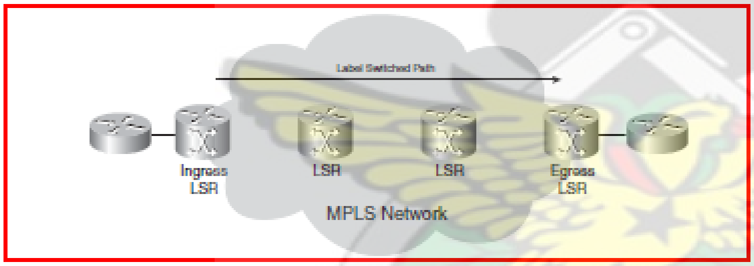


Figure 5.15: An LSP Through an MPLS Network

The ingress LSR of an LSP is not necessarily the first router to label the packet. The packet might have already been labeled by a preceding LSR. Such a case would be a nested LSP—that is, an LSP inside another LSP. In **Figure 5.16**, you can see an LSP spanning the whole width of the MPLS network. Another LSP starts at the third LSR and ends on the next-to-last LSR. Therefore, when the packet enters the second LSP on its ingress LSR (this means the third LSR), it is already labeled. This ingress LSR of the nested LSP then pushes a second label onto the packet. The label stack of the packet on the second LSP has two labels now. The top label belongs to the nested LSP,and the bottom label belongs to the LSP that spans the entire MPLS network. A backup traffic engineering (TE) tunnel is an example of such a nested LSP.

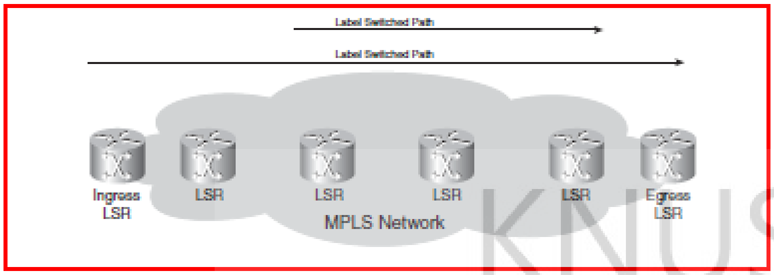


Figure 5.16: Nested LSP

5.2.7 Forwarding Equivalence Class

A Forwarding Equivalence Class (FEC) is a group or flow of packets that are forwarded along the same path and are treated the same with regard to the forwarding treatment. All packets belonging to the same FEC have the same label. However, not all packets that have the same label belong to the same FEC, because their EXP values might differ; the forwarding treatment could be different, and they could belong to a different FEC. The router that decides which packets belong to which FEC is the ingress LSR. This is logical because the ingress LSR classifies and labels the packets.

Following are some examples of FECs:

- Packets with Layer 3 destination IP addresses matching a certain prefix
- Multicast packets belonging to a certain group
- Packets with the same forwarding treatment, based on the precedence or IP DiffServ Code Point (DSCP) field

■ Layer 2 frames carried across an MPLS network received on one VC or (sub) interface on the ingress LSR and transmitted on one VC or (sub) interface on the egress LSR

■ Packets with Layer 3 destination IP addresses that belong to a set of Border Gateway Protocol (BGP) prefixes, all with the same BGP next hop.

This last example of a FEC is a particularly interesting one. All packets on the ingress LSR for which the destination IP address points to a set of BGP routes in the routing table—all with the same BGP next-hop address—belong to one FEC. It means that all packets that enter the MPLS network get a label depending on what the BGP next hop is. **Figure 5.17** shows an MPLS network in which all the edge LSRs run internal BGP (iBGP).

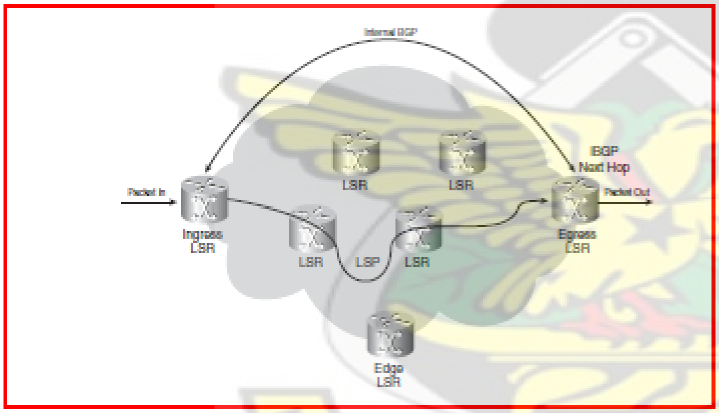


Figure 5.17: An MPLS Network Running iBGP

The destination IP address of all IP packets entering the ingress LSR will be looked up in the IP forwarding table. All these addresses belong to a set of prefixes that are known in the routing table as BGP prefixes. Many BGP prefixes in the routing table have the same BGP next-hop address, namely one egress LSR. All packets with a destination IP address for which the IP lookup in the routing table recurses to the same BGP next-hop address will be mapped to the same FEC. As already mentioned, all packets that belong to the same FEC get the same label imposed by the ingress LSR.

5.2.8 Label Distribution

The first label is imposed on the ingress LSR and the label belongs to one LSP. The path of the packet through the MPLS network is bound to that one LSP. All that changes is that the top label in the label stack is swapped at each hop. The ingress LSR imposes one or more labels on the packet. The intermediate LSRs swap the top label (the incoming label) of the received labeled packet with another label (the outgoing label) and transmit the packet on the outgoing link. The egress LSR of the LSP strips off the labels of this LSP and forwards the packet. Consider the example of plain IPv4-over-MPLS, which is the simplest example of an MPLS network. Plain IPv4-over-MPLS is a network that consists of LSRs that run an IPv4 Interior Gateway Protocol (IGP) (for example, Open Shortest Path First [OSPF], Intermediate System-to-Intermediate System [IS-IS], and Enhanced Interior Gateway Routing Protocol [EIGRP]). The

ingress LSR looks up the destination IPv4 address of the packet, imposes a label, and forwards the packet. The next LSR (and any other intermediate LSR) receives the labeled packet, swaps the incoming label with an outgoing label, and forwards the packet. The egress LSR pops the label and forwards the IPv4 packet without labels on the outgoing link. For this to work, adjacent LSRs must agree on which label to use for each IGP prefix. Therefore, each intermediate LSR must be able to figure out with which outgoing label the incoming label should be swapped. This means that you need a mechanism to tell the routers which labels to use when forwarding a packet. Labels are local to each pair of adjacent routers. Labels have no global meaning across the network. For adjacent routers to agree which label to use for which prefix, they need some form of communication between them; otherwise, the routers do not know which outgoing label needs to match which incoming label. A label distribution protocol is needed. You can distribute labels in two ways:

■ Piggyback the labels on an existing IP routing protocol

■ Have a separate protocol distribute labels

Piggyback the Labels on an Existing IP Routing Protocol

The first method has the advantage that a new protocol is not needed to run on the LSRs, but every existing IP routing protocol needs to be extended to carry the labels. This is not always an easy thing to do. The big advantage of having the routing protocol carry the labels is that the routing and label distribution are always in sync, which means that you cannot have a label if the prefix is missing or vice versa. It also eliminates the need of another protocol running on the LSR to do the label distribution. The implementation for distance vector routing protocols (such as EIGRP) is straightforward, because each router originates a prefix from its routing table. The router then just binds a label to that prefix. Link state routing protocols (such as IS-IS and OSPF) do not function in this way. Each router originates link state updates that are then forwarded unchanged by all routers inside one area. The problem is that for MPLS to work, each router needs to distribute a label for each IGP prefix— even the routers that are not originators of that prefix. Link state routing protocols need to be enhanced in an intrusive way to be able to do this. The fact that a router needs to advertise a label for a prefix it does not originate is counterintuitive to the way link state routing protocols work anyway. Therefore, for link state routing protocols, a separate protocol is preferred to distribute the labels.

None of the IGPs has been changed to deploy the first method. However, BGP is a routing protocol that can carry prefixes and distribute labels at the same time. However, BGP is not an IGP; it is used to carry external prefixes. BGP is used primarily for label distribution in MPLS VPN networks.

Running a Separate Protocol for Label Distribution

The second method—running a separate protocol for label distribution—has the advantage of being routing protocol independent. Whatever the IP routing protocol is, whether it is capable of distributing labels or not, a separate protocol distributes the labels and lets the routing protocol distribute the prefixes. The disadvantage of this method is that a new protocol is needed on the LSRs.

The choice of all router vendors was to have a new label distribution protocol distribute the labels for IGP prefixes. This is the Label Distribution Protocol (LDP). LDP, however, is not the only protocol that can distribute MPLS labels.

Several varieties of protocols distribute labels:

■ Tag Distribution Protocol (TDP)

■ Label Distribution Protocol (LDP)

■ Resource Reservation Protocol (RSVP)

TDP, which predates LDP, was the first protocol for label distribution developed and implemented by Cisco. However, TDP is proprietary to Cisco. The IETF later formalized LDP. LDP and TDP are similar in the way they operate, but LDP has more functionality than TDP.

With the widespread availability of LDP in general-deployment Cisco IOS releases, TDP was quickly replaced by LDP.

The result is that TDP is becoming obsolete.

5.2.9 Label Distribution with LDP

For every IGP IP prefix in its IP routing table, each LSR creates a local binding—that is, it binds a label to the IPv4 prefix. The LSR then distributes this binding to all its LDP neighbors. These received bindings become remote bindings. The neighbors then store these remote and local bindings in a special table, the label information base (LIB). Each LSR has only one local binding per prefix, at least when the label space is per platform. If the label space is per interface, one local label binding can exist per prefix per interface. Therefore, you can have one label per prefix or one label per prefix per interface, but the LSR gets more than one remote binding because it usually

has more than one adjacent LSR. Out of all the remote bindings for one prefix, the LSR needs to pick only one and use that one to determine the outgoing label for that IP prefix. The routing table (sometimes called the routing instance base, or RIB) determines what the next hop of the IPv4 prefix is. The LSR chooses the remote binding received from the downstream LSR, which is the next hop in the routing table for that prefix. It uses this information to set up its label forwarding information base (LFIB) where the label from the local binding serves as the incoming label and the label from the one remote binding chosen via the routing table serves as the outgoing label. Therefore, when an LSR receives a labeled packet, it is now capable of swapping the incoming label it assigned, with the outgoing label assigned by the adjacent next-hop LSR. **Figure 5.18** shows the advertisement by LDP of the bindings between the LSRs for the IPv4 prefix 10.0.0.0/8. Each LSR allocates one label per IPv4 prefix. The local binding is this one prefix and its associated label.

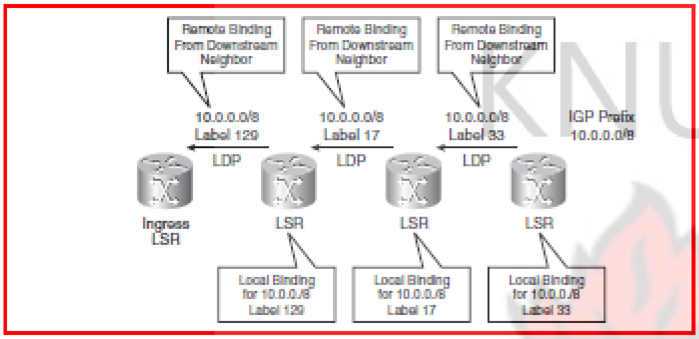

Remote Binding From Downstream Neighbor
Remote Binding From Downstream Neighbor
Remote Binding From Downstream Neighbor
10.0.0.0/8 Label 129
10.0.0.0/8 Label 17
10.0.0.0/8 Label 33
IGP Prefix 10.0.0.0/8
LDP
LDP
LDP
Ingress LSR
LSR
LSR
LSR
Local Binding for 10.0.0.0/8 Label 129
Local Binding for 10.0.0.0/8 Label 17
Local Binding for 10.0.0.0/8 Label 33

Figure 5.18: An IPv4-over-MPLS Network Running LDP

Figure 5.19 shows the IPv4 packet—destined for 10.0.0.0/8—entering the MPLS network on the ingress LSR, where it is imposed with the label 129 and switched toward the next LSR. The second LSR swaps the incoming label 129 with the outgoing label 17 and forwards the packet toward the third LSR. The third LSR swaps the incoming label 17 with the outgoing label 33 and forwards the packet to the next LSR and so on.

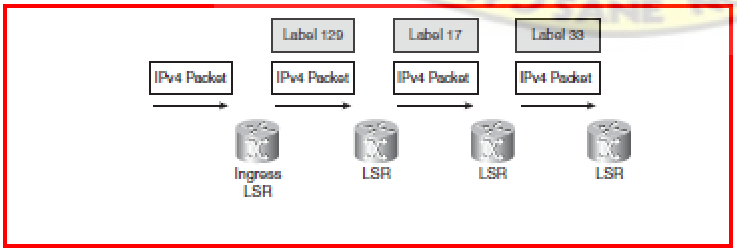


Figure 5.19: An IPv4-over-MPLS Network Running LDP: Packet Switching

5.2.10 Label Forwarding Instance Base

The LFIB is the table used to forward labeled packets. It is populated with the incoming and outgoing labels for the LSPs. The incoming label is the label from the local binding on the particular LSR. The outgoing label is the label from the remote binding chosen by the LSR from all possible remote bindings. All these remote bindings are found in the LIB. The LFIB chooses only one of the possible outgoing labels from all the possible remote bindings in the LIB and installs it in the LFIB. The remote label chosen depends on which path is the best path found in the routing table.

In the example of IPv4-over-MPLS, the label is bound to an IPv4 prefix. However, the LFIB can be populated with labels that LDP does not assign. In the case of MPLS traffic engineering, the labels are distributed by RSVP. In the case of MPLS VPN, the VPN label is distributed by BGP. In any case, the LFIB is always used to forward an incoming labeled packet.

CHAPTER SIX

6.0 CONCLUSION

Internet Service Providers or 3.5G networks face difficult challenges in engineering large backbone networks due to wide fluctuations in the underlying traffic and increasing user demands for predictable communication performance. Dynamic routing can play an important role in traffic engineering of ISP networks or 3.5G networks, if selecting routes based on load can be made both stable and efficient.

The purpose of traffic engineering (TE) is to enhance network utilization and to improve the architecture of a network in a systematic way, so that the network becomes robust, adaptive and easy to operate. The routing protocols OSPF, IS-IS, RIP and MPLS have been critically studied to determine the best for 3.5G networks.

In addition to this a survey was conducted to get the views of Senior Managers of telcos such as MTN. The results of this exercise suggest that MPLS is the protocol of the future. This is because it satisfies end-to-end QoS requirements in 3.5G mobile packet networks.

MPLS outperforms traditional static and dynamic routing algorithm such as OSPF, IS-IS and RIP. When there are multiple paths in routing, deploying MPLS is the best option in selecting the shortest path. MPLS can circumvent route flapping and network congestion. In addition, it shows that MPLS is robust to inaccuracies in network provisioning and shifts in the offered traffic. The MPLS labels are advertised between routers so that they can build a label-to-label mapping. These labels are attached to the IP packets, enabling the routers to forward the traffic by looking at the label and not the destination IP address. The packets are forwarded by label switching instead of by IP switching.

In conclusion, given the fact that MPLS is based on IP, and the internet is based on IP technology, it seems that the future of MPLS is ensured for quite a while to come. It is therefore recommended that MPLS is the best routing protocol for most 3.5G networks and it is suggested that its Operations and Maintenance as a routing protocol can be studied for future works.

6.1 FUTURE WORK

Currently there are no specific mechanisms proposed to address requirements for user and data plane Operations and Maintenance (OAM) for Multi-Protocol Label Switching (MPLS). The main goal is to identify commonly applicable set of requirements for MPLS OAM. Specifically, a set of requirements that apply to most common set of MPLS networks deployed by service providers. These requirements can then be used as a base for network management tool development and to guide the evolution of specified tools, as well as the specification of OAM functions that are intrinsic to protocols used in MPLS networks.

REFERENCES

[1] University of Michigan, Real-Time Computing Laboratory, Department of EECS; AT&T Labs- Research, Network Mathematics Research, Networking and Distributed System; Load-Sensitive Routing of Long-Lived IP flows.

[2] G. Rutka, Some Aspects of Traffic Analysis for internet Traffic Prediction, Faculty of Electronics and Telecommunication, Riga Technical University, Riga, Azenes str.12-317, LV-1048 phone:+371 29627600, email: gundega.rutka@rtu.lv ISSN 1392-1215 2009 No.5(93).

[3] IEEE. Issue date May 2002, vol.20, Issue 4; Optimizing OSPF/IS-IS weights in a changing world.

[4] IEEE. Issue Date 2000 page 519-528, vol.2 ; Internet traffic engineering by optimizing OSPF weights. IFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies Proceedings.

[5] Philip Smith pfs@cisco.com; IS-IS Tutorial, MENOG4 5th-9th April 2009, Bahrain.

[6] Xipeng Xiao, Alan Hannan, and Brook Bailey; Traffic Engineering with MPLS in the internet; Global Center Inc. Lionel M.Ni, Michigan State University.

[7] Juha Korhonen; Introduction to 3G Mobile Communication, second edition.

[8] K Tuulos; WCDMA for beginners, WCDMA System Training, 27-Sep-2000.

[9] www.iec.org, UMTS Web Proforum Tutorials. The International Engineering Consortium.

[10] Arthur D. Little; HSPA and Mobile Wimax for Mobile Broadband Wireless Access, 27th March 2007.

[11] www.iec.org, WCDMA Tutorial, Web Proforum Tutorials. The International Engineering Consortium.

[12] Savo G. Glisic, Professor of Telecommunications, University of Oulu, Finland; Adaptive WCDMA Theory and Practice, Copyright 2003 John Wiley & Sons, Ltd. ISBN: 0-470-84825-1.

[13] Keiji Tachikawa, NTT DoCoMo, Inc., Japan; WCDMA Mobile Communications System, Copyright 2002, John Wiley& Sons, Ltd. ISBN:0-470-84761-1.

[14] Harri Holma and Antti Toskala, Nokia, Finland; WCDMA for UMTS, Radio Access for Third Generation, Mobile Communications, Third Edition.

[15] Jyri Hamalainen, Cellular Network Planning and Optimization, Part VII:WCDMA RRM; Communications and Networking Department, TKK, 1.2.2008.

[16] Ericsson AB 2005, WCDMA RAN Advanced Troubleshooting and Tracing, Student Book , LZT 123 8229 R1A.

[17] Ericsson 2006, WCDMA RAN Operation, Student Book, LZT 123 7371 R4A.

[18] Creswell, J. W. (1994). Research Design: Qualitative and Quantitative Approaches. Thousand Oaks, CA: SAGE.

[19] Fryer, D. (*1991*). Qualitative methods in occupational psychology: Reflections upon why they are so useful but so little used.

[20] Polgar S. and Thomas S.A. (1995) *Introduction to Research in the Health Sciences*. London. Churchill Livingstone

[21] Cassell, C., & Symon, G. (1994). Qualitative research in work contexts. In C. Cassell, & G. Symon (Eds.), Qualitative methods in organizational research (pp. 1-13). Thousand Oaks, CA: Sage Publications

[22] Polit D. F. and Hungler B.P. (1995) "Nursing Research: Principles and Methods.

[23] Walsh M. (2001) *Research Made Real*. Cheltenham. Nelson Thornes Ltd.

[24] Jha S. and Hassan M. (2002) "Engineering Internet QoS", Artech House.

[25] Chiussi, F. M. Khotimsky, D. A. Krishnan, S. (sept. 2002) "Mobility Management in 3G All IP Networks", IEEE Communication Magazine, Lucent Technologies.

[26] Youngseek, L. Yongho, S. Yanghee C. Changhoon, K. (2002) "A Constrained Multipath Traffic Engineering Scheme for MPLS Networks", Proc. Of IEEE Inst. Conf. ICC New York.

[27] Vasu, J. Shahram, L. "An Overview of MPLS and Constraint Based Routing" www.unlv.edu.

[28] Shyam, S. Venkatessan M."Alternate Path Routing Algorithm Engineering", www.ee.edu.

[29] Yunos, R., Noor, N. M., Ahmad, S. A., (2010) “Performance Evaluation Between IPv4 and IPv6 on MPLS Linux Platform” Information Retrieval and Knowledge Management CAMP) pp. 204-208.

[30] Zhongshan, Z. Keping L., Wendong, W., Shiduan, C. (2000) “The New Mechanism for MPLS Supporting IP Multicast”, IEEE Circuits and Systems Asia-Pacific Conf. pp.247

[31] Tran, C. H., Nguyen, N. C., Nguyen D. T., Truong D. H. (2007), “ Interoperability between Mobile IPv4 and Mobile IPv6 based on MPLS Core Network”, IEEE Advanced Communication Technology, The 9th international conference vol. 2 pp. 1187.

[32] Chen, T. M., Oh, T. H. (1999), “Reliable Services in MPLS”, Communications Magazine, IEEE. Southern Methodist Univ. Dallas, TX pp. 58.

[33] Luc De Ghein, CCIE No. 1897, ciscopress.com; MPLS Fundamentals, A Comprehensive Introduction to MPLS Theory and Practice.

[34] Mazen Mroue; MTN MPLS-VPN Service, 1-Sept-2010.

[35] Huawei, www.huawei.com, HSPA VPN Solution.

[36] Stanley Freiman; MTN Group CTIO Conference 2008, MPLS Backbones.

[37] MTN 2008-2012 Objectives, Strategies and Measurement, Corporate Opportunites: MPLS - Trends and Outlook.

APPENDIX-A

Questionnaire

(Q1) In your opinion, which of the following do you think is the best routing protocol in data packet networks such as 3.5G networks.

(a) MPLS (b) OSPF (c) IS-IS (d) RIP

(Q2) Your choice in question (1) is mostly deployed in modern ISPs and 3.5G networks.

(a) YES (b) NO (c) I don't know

(Q3) Your choice in question (1) has matured a lot and it's a stable technology.

(a) YES (b) NO (c) I don't know

(Q4) Your choice in question (1) is based on IP and the internet is based on IP.

(a) YES (b) NO (c) I don't know

(Q5) The future of your choice in question (1) is ensured for quite a while to come.

(a) YES (b) NO (c) I don't know

(Q6) Your choice in question (1) can circumvent route flapping and network congestion.

(a) YES (b) NO (c) I don't know

(Q7) Your choice in question (1) can transport IPv4, IPv6, Ethernet, High Level Data Link Control (HDLC) and other Layer 2 technologies.

(a) YES (b) NO (c) I don't know

(Q8) Your choice in question (1) outperforms traditional static and dynamic algorithms.

(a) YES (b) NO (c) I don't know

(Q9) When there are multiple paths in routing, deploying your choice in question (1) is the best option in selecting the shortest path.

(a) YES (b) NO (c) I don't know

If No , give a reason

……………………………………………………………………………………………………