DESIGN OF IP NETWORK USING GPRS/UMTS/HSDPA+ TECHNOLOGY

BY

DANIEL ADJEI ODAI

(BSc. Computer Engineering)

A Thesis submitted to the Institute Of Distance Learning, Kwame Nkrumah University of Science and Technology in partial fulfilment of the requirements for the degree of

MASTERS OF INFORMATION TECHNOLOGY

OCTOBER, 2016

DECLARATION

I hereby declare that this submission is my own work and that, to the best of my knowledge and beliefs, it contains neither material previously published by another person nor material which has been accepted for the award of any other degree of the university or any other University, except where due acknowledgement had been in the thesis.

Daniel Adjei Odai …… ……..

PG8309612 Signature Date

Certified By

Dr. M. Asante …… ……..

Supervisor Signature Date

Certified By

Dr. J. B. Hayfron-Acquah …… ……..

Head of Department Signature Date

ABSTRACT

The design and implementation of internet protocol (IP) networks is not new. Researches in the past have focused on the design and implementation of IP networks with Fixed Broadband (FBB) technologies. This study researches into how Mobile Broadband (MBB) technologies, such as General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS), could be used as an alternative to FBB technologies in the design and implementation of IP networks for businesses. The study made use of the User Equipment-toUser Equipment (UE-to-UE) communication solely within the GPRS and UMTS Radio Access Network (RAN); MBB over layers two and three of the Open Systems Interconnection (OSI) model, promulgated by the International Organization for Standardization (ISO/IEC 7498-1, 1994), and Internet Protocol Security (IPsec) as methods in the design of the MBB IP networks for businesses. Data for both FBB and MBB were obtained from experiments and compared to support the objective of the research. The analysis of both technologies based on the experiments performed showed, they are basically at par in performance with each having its strengths and weaknesses. The research showed MBB has low latency where radio service is adequate but suffers attenuation where people are crowded. The experiments and analyses showed MBB is suitable for use in the design and implementation of IP networks for businesses.

DEDICATION

I dedicate this work to my dear mother, Margaret Larley Adjei, who took care of all my needs until l started working. Also to my wife Helen Odai, for her encouragement.

ACKNOWLEDGEMENT

I would like to take this opportunity to thank a number of people who contributed to making this dissertation a success.

I am very grateful to my supervisor Dr. Michael Asante for his rich advice and comments.

I would like to thank Dr. James Benjamin Hayfron-Acquah for his valuable critique and guidance.

I would also like to thank my wife Helen Odai and my family for their encouragements.

Finally, I would like to thank my friends in the telecom industry for their assistance.

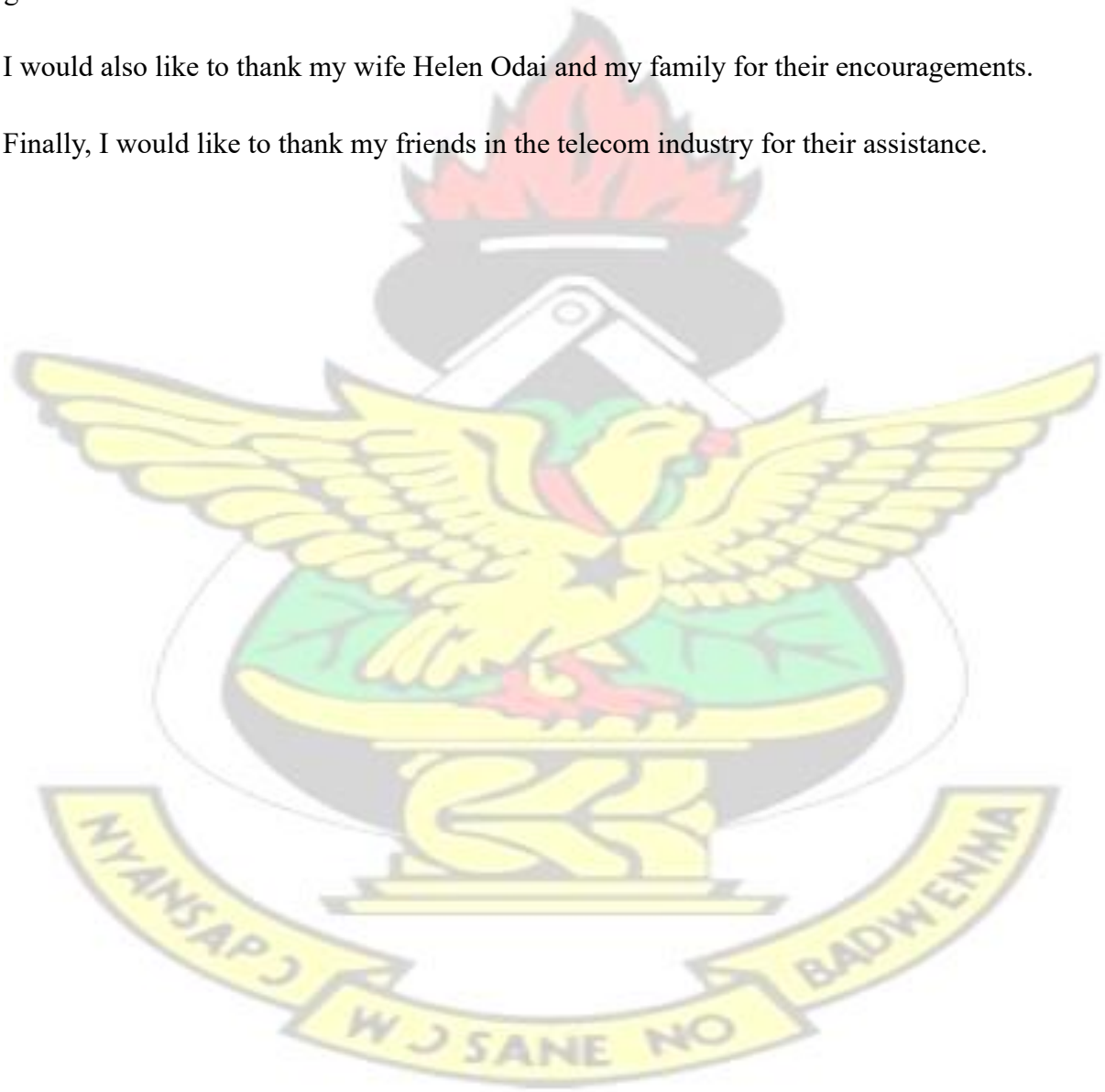


TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

3DES	Triple Data Encryption Algorithm
3GPP	Third Generation Partnership Project
AES	Advanced Encryption Standard
APN	Access Point Name
AuC	Authentication Centre
BSC	Base Station Controller
BSSGP	Base Station Subsystem GPRS Protocol
CG	Charging Gateway
EDGE	Enhanced Data rates for GSM Evolution
FBB	Fixed Broadband
Ga	Standard Interface Between GGSN and CG
GGSN	Gateway GPRS Support Node
Gi	Standard Interface Between GGSN and PLMN
Gn	Standard Interface Between SGSN and GGSN
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTP-C	GPRS Tunnelling Protocol - Control Part
GTP-U	GPRS Tunnelling Protocol - User Part
Gy	Standard Interface Between GGSN and OCS
HLR	Home Location Register
HSPA	High Speed Packet Access
HSPA+	Evolved HSPA
IP	Internet Protocol
LLC	Logical Link Control

MAC	Media Access Control
MBB	Mobile Broadband
MD5	Message Digest 5
MPLS	Multi-Protocol Label Switching
MS	Mobile Station
NAT	Network Address Translation
PAT	Port Address Translation
PDP	Packet Data Network
PLMN	Public Land Mobile Network
PSCN	Packet Switch Core Network
RAN	Radio Access Network
RANAP	Radio Access Network Application Part
RLC	Radio Link Control
RNC	Radio Network Controller
RTSP	Real Time Streaming Protocol
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SNDCP	Sub-Network Dependent Convergence Protocol
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
WAN	Wide Area Network

CHAPTER 1. INTRODUCTION

1.1. Background to the Study

Data communications in general had evolved globally and Ghana is not an exception.

The evolution could not have been possible without a favourable legal and regulatory environment. Ghana could not have reached thus far in data communication without the following acts: National Communications Act, 2008, Act 769, Electronic Communications Act, 2008, Act 775, the Electronic Transactions Act, 2008, Act 772, and the National Information Technology Agency Act, 2008, Act 771. The essence of these acts are meant to support the heightened convergence within the Ghanaian communications space.

Data service providers have made available the most recent technologies needed for effective data communication. From fixed broadband (Copper and fibre) to mobile broadband (GPRS, UMTS and LTE).

Data from service providers revealed that, the use of these technologies for setting up local area networks and wide area networks are skewed towards the fixed broadband capabilities.

Documented approach to using the other available technologies to setting up local and wide area networks for businesses could help balance the usage of these available data communication technologies to help businesses grow to improve the Ghanaian economy. This study is aimed at documenting the approach needed to using the mobile broadband to set up IP networks.

1.2. Problem Statement

"Ghana's creators and entrepreneurs are inspired by what they can do online, but today, their ability to participate fully on the Web can be hindered by the availability, quality and cost of Internet access. We aim to change that," said Estelle Akofio-Sowah, Google Ghana Country Manager (Ghana News Agency, 06/10/2015, Launch of Google's Project Link).

Businesses in Ghana are really inspired to offering online service but are at the same time frustrated by the lack of fixed broadband service penetration as expressed by the Google's country manager. To support this claim, the National Communication Authority's March 2016 report on fixed and mobile broadband subscriptions are as follows: 258,536 for FBB and 18,813,686 for MBB. (NCA, 2016). Though MBB has higher subscription, businesses are unable to fall on that to doing business online because, the focus had always been on using FBB to design and implement IP networks for businesses. The high MBB subscription are mainly for personal use on handheld mobile terminals and dongles and could not have been for the setup of IP network for businesses. The solution to the lack of FBB service to where businesses need it to doing business online could be addressed by the use of mobile broadband as alternative to fixed broadband in setting up IP networks to help entrepreneurs do business online.

1.3. Objectives of the Study

The research is being carried out with the general objective of internet protocol network design for businesses intended for use with mobile broadband technologies like, GPRS and UMTS.

The study has four specific areas it's focussing on. These are:

i. To examine how mobile broadband could be used to design and implement internet protocol network for businesses.

ii. To determine whether mobile broadband's quality of service is adequate for internet protocol network.

iii. To determine whether mobile broadband speed is good enough for data transmission.

iv. To compare mobile broadband technology properties for data transfer to that of fixed broadband.

1.4. Research Questions

Though the source of raw data for the study were gotten from experiments, i.e. drive tests, live traces and simulations, the following questions were set out to address the need for the study:

i. How viable is mobile broadband as alternative to fixed broadband in the design and implementation of IP network.

ii. From end-to-end, what is the level of the quality of service of mobile broadband?

iii. How good is the speed of mobile broadband for data transmission within acceptable time frame?

iv. As of now fixed broadband is the preferred technology in the design and implementation of IP networks. Could mobile broadband data transmission properties match that of fixed broadband's?

1.5. Significance of the Study

Mobile broadband in Ghana is wide spread in terms of coverage and quite affordable, efficient and convenient as captured in questionnaire response in CHAPTER 4 page 97108.

The contribution of this study is to help Ghanaian businesses offer better, more efficient and affordable service, by being visible and easily accessible, to grow the economy thereby reducing poverty. Once businesses are networked, various resources could be shared, both hardware and software; this would obviously reduce capital and operational expenditures and in effect making businesses gain competitive advantage and compete effectively within the global market.

1.6. Scope of the Study

The study would focus on using IP network design for use with the GPRS and UMTS technologies. As of the inception of this study, Long Term Evolution (LTE), which is also a mobile broadband technology was not commercial in Ghana hence not considered.

The study would focus on IP network design for areas where fixed broadband is totally nonexistent. This could be achieved with the User Equipment to User Equipment approach solely within the radio access network for mobile broadband.

The study would also look at providing IP network design for businesses that intend to expanding their existing fixed broadband IP networks to areas where hitherto, it would be impossible because of non-existent FBB service. In other words, the mobile broadband could be used to extend the fixed broadband. This could be achieved with layers two or three virtual private network and internet protocol security virtual private network tunnel between the FBB and MBB technologies.

CHAPTER 2. LITERATURE REVIEW

2.1. Introduction

The internet was once considered as an obstacle to attention. It has now become part of our daily activities. We are always occupied with checking for information from our mails and other social media outlets. We look out for information that is not readily available by using data to search the internet. “Googling” had become our default search engine for fishing out information. At work, we communicate remotely by using virtual conferencing either by videoconferencing or voice conferencing. Human resource management systems are used at the work place to now provide self-service to internal customers and online Customer Relationship Management (CRM) tools used to provide service to external customers with the use of corporate local area networks. At home, it's all about Whatsapp, YouTube, updating our Facebook page, etc.

The ideal way to access all of these tools and resources are with a broadband (high-speed) Internet connection, something we've come to expect at home and at the office.

GSM (Global System for Mobile communications) is quite limited as a data communication technology. It is mainly used for voice communication and termed as a circuit switched network.

The standard for GSM was designed to evolve. In the initial stages when need for data usage demand soared within the MBB space General Packet Radio Service (GPRS) was developed and added to GSM which kick started the delivery of the Internet on mobile handsets.

Mobile data technology had really evolved. Commercially, it all started with General Packet Radio Systems (GPRS) through to Enhanced Data rates for GSM Evolution (EDGE). The evolution continued to better speeds and quality of service starting with Universal Mobile Telephony System (UMTS), High-Speed Downlink Packet Access (HSDPA), Evolved High

Speed Packet Access (HSPA+) and now Long-Term Evolution (LTE). From GPRS through to HSPA+, the logical architecture of the core network remained same until LTE. Higher speeds could have been obtained after HSPA+ with the same architecture but, economically there is no need to thread that path since LTE is offering same and higher speeds with better economic prospects. (Punz, 2010).

These evolutions with better coding schemes had brought about amazing downlink speeds from initial GPRS of 114 kbps through to 300 Mbps for LTE (theoretical speed). LTE is not part of this study.

The delivery of internet on the mobile handset is great, but literatures are quite scanty and seem virtually non-existent on its deployment, usage and benefits as main IP backhaul for businesses.

The focus had always been limited to internet or mobile data services on mobile handset with this excellent technology.

This project seeks to bring to the fore how this excellent mobile internet technology could be deployed as alternative to known traditional fixed broadband IP network deployment for businesses in Ghana. Home use would not be left out, but the main focus is on business use.

A few IP network designs, that seek to summarise the vast possible deployment varieties of this mobile technology to businesses in Ghana, would be looked at.

An attempt would be made to provide sample implementations guidelines within the IP space to these designs using virtual lab.

The implementation would be simulated within an IP virtual lab space.

The benefits of this mobile internet technology would be weighed against the traditionally known fixed internet technology.

This project would limit itself to earlier and widely used data technologies under GSM and UMTS but not LTE.

2.2. Evolution of Mobile Broadband Technologies

The evolution of mobile Telecommunication Networks is strongly influenced by the evolution of Computer Networks, particularly the Internet: Mobile Telecommunication Networks are increasingly based on IP, the protocol used by Computer Networks. And just as Computer Networks, they offer whatever service is possible over IP: telephony, web-surfing, videodownloading etc. (Kappler, 2009).

Beginning with the first single cell mobile telephone services in the 1940s and continuing through the first and second generations of mobile telephone services, the primary function of the mobile device was to enable speech calls to be set up between the mobile user and a fixed network of base stations (BTS) and telephone exchanges.(Sanders et al., 2003).

In the previous years, the essence of acquiring a mobile phone was primarily for making voice calls. This trend had now shifted to data calls. The earlier seemingly data component that fascinated users was the short massage services (SMS). Then came the wireless application part protocol (WAP), which enabled users to text and send pictures. These technological advancements heightened the perception that, mobile phones are meant not just for voice services but could be used as a means of data transmission. This acceptance let to the demand for better service and higher data rates.

With the increase in usage of mobile data services, as a result of our insatiable quest for data and information on the go, the mobile handheld, tablets and other compatible mobile data service terminals had become indispensable in our daily lives. This makes the deployment of IP network over these mobile data technology for businesses imperative ever than before.
The General Packet Radio system (GPRS) was introduced to meet the needs of data services under GSM technology.

GPRS evolved to Enhanced Data rate for Global System for Mobile communication (GSM) Evolution. This evolution was necessitated by demand for higher data rates

2.3. GSM

The developers of Global System for Mobile communication (GSM) had improvement in mind. It is a circuit-switched network. Pandey (2009) explained that, though GSM started as a tool for making voice calls, it had improved to providing data service as well. In response to higher data rates as a result of the limited rates offered by GSM, coupled with it popularity, the developers introduced the General Packet Radio Service (GPRS). It was an added functionality to the existing GSM core network. This achievement brought about real data service within the GSM space.

GPRS

With the second-generation (2G) digital mobile communications came also the opportunity to provide data services over the mobile-communication networks.

This evolution was necessitated by demand for higher data rates over the Global System for Mobile communication (GSM). GSM was by then just ideal for circuit-switched network i.e. voice services. GSM had great deal of limitations for sending data. Thankfully the standard for GSM was designed with its evolution in sight. General Packet Radio Service (GPR) was given birth to add packet switching (mobile data) functionality to the GSM. This addition brought about internet access via mobile handhelds with its economic gains to handheld vendors. That was the beginning of what we are witnessing today with our smart mobile data compatible terminals.

Within the framework of the continuing development of GSM, packet-oriented service concept for the transfer of data was developed. Standardization of the new service General Packet Radio Service (GPRS) was completed in 1998.

The introduction of High-Speed Circuit-Switched Data (HSCSD) technology brought into existence GPRS with net bit rates of, up to 117 kbit/s from 9.6Kbps offered by GSM.

The main intention of integrating the GPRS into the GSM is to increase the number of connections per bearer. Packet-switching means that GPRS radio resources are used only when users are actually sending or receiving data. For better resource management, radio channels are not dedicated for users for specific length of time but rather the channels are shared amongst several users. The application being used determine the real number of users that could be supported and the volume of data that could be transferred.

Numerous defined logical connections are multiplexed to a single or more GSM physical channels. GPRS attains a flexible use of channel capacity for applications with variable bit rates.

As stated earlier, GPRS did not replace the existing GSM infrastructure but rather added some core elements, SGSN and GGSN, to the existing infrastructure to achieve higher data rates.

EDGE

With the continuing quest for higher data rates, GPRS evolved to EDGE (Enhanced Data rates for GSM Evolution also known as Enhanced GPRS), also, a second generation mobile technology. The theoretical maximum download speed for EDGE is 473.6 Kbit/s. Obviously this was considered a vast improvement over GPRS; about three times better download speed achievement over GPRS maximum speed if 114Kbps. The algorithm used for the modulation i.e. Phase-shift keying (PSK) brought about this transformation. PSK is a digital modulation scheme based on changing, or modulating, the initial phase of a carrier signal. PSK is used to represent digital information, such as binary digits zero (0) and one (1).PSK is typically applied in wireless local area networks (WLAN), Bluetooth technology and radio frequency identification (RFID) standards used in biometric passport and contactless payment systems.

2.3.1. GPRS and EDGE Protocol Stack

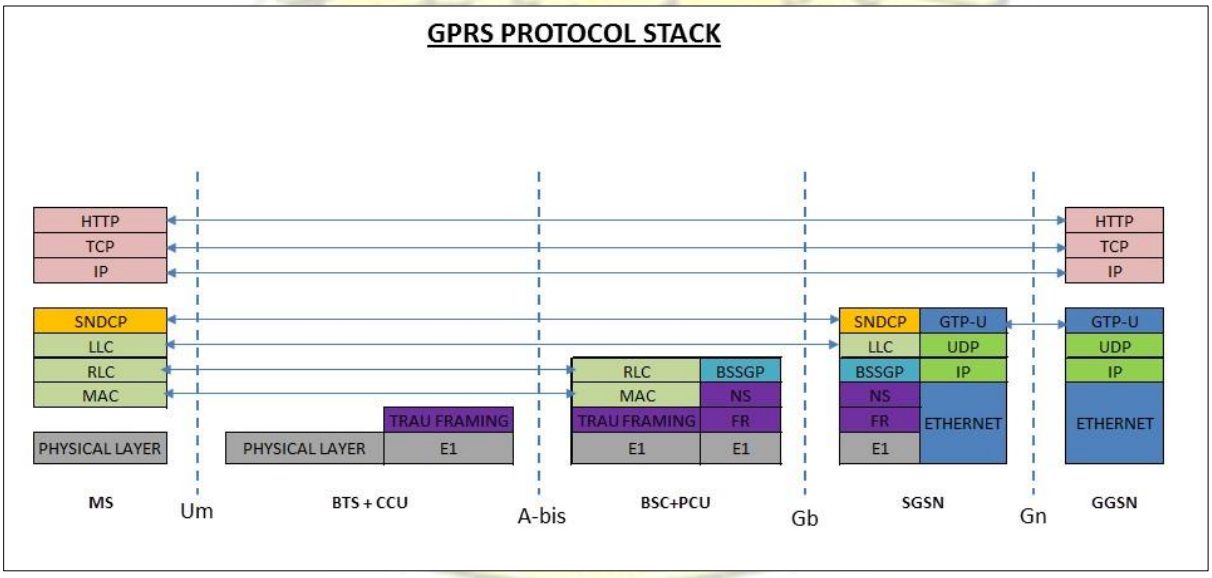


Figure 2.1: GPRS and EDGE Protocol Stack

Behind the user layer that we enjoy and are aware of, there exist other layers of communication of the GPRS protocol. GSM represents the initial digital cellular system developed in the early part of the eighties. GSM is a purely circuit switched technology.

GSM offers circuit switched data (CSD) at rates 2400 /4800 / 14400 bps. CSD emulates the behaviour of dial-up modems on public switched telephone network (PSTN).

Then came High Speed CSD (HSCSD) that bundles up to four GSM time-slots to achieve 38.4/57.6kbps data speeds. This implies one data session occupies four to eight times voice call bandwidth. Quite expensive to users and providers. Users have to pay more, about four to eight times what a voice call would cost. The quest for higher speeds by data consumers motivated researchers to meet that need which led to the birth of the General Packet Radio Service (GPRS). GPRS is purely a packet switched technology unlike GSM that is circuit switched with low data speed capabilities and quite expensive.

McGuiggan (2004) gave an insight to the description of the core nodes: with GPRS, a separate core network that leverage's on the GSM channelling, modulation and time-slot structure was introduced. The main nodes for this separate core network are the serving GPRS service node (SGSN) and the gateway GPRS service node. Then SGSN is the node that interfaces the GSM and the GGSN is the node that interfaces other public data networks. The logical interface to the GSM is known as Gb and that to the other public data networks is known as the. The logical interface between the SGSN and the GGSN is known as the Gn. These interfaces names do not represent any special acronym according to the cellular standardization body, the Third Generation Partnership Project technical report. (3GPP TR 25.848, 2003).

From the GPRS and EDGE protocol stack in Figure 2.1 , assuming a mobile station makes a HTTP request, this request would traverse the TCP/IP layers then to the sub-network dependent convergence protocol (SNDC). This protocol interfaces the IP protocol. The data request are now transparently forwarded via the protocols under the SNDC to the GGSN. The GGSN is

the only purely IP node in the GPRS protocol stack. This is the main node serving the purpose of this study.

The Um is the logical interface between the mobile station (MS) and the radio access network. A-bis is the air interface between the base station controller and the cell sites. Gb is the logical interface between the SGSN and the radio network. Gn is the logical interface between the GGSN and the SGSN. (Welte, 2011).

Seurre et al. (2003) affirm that, the GPRS framework must give method for data transmission in the user plane between the MS and other data networks, according to the QoS related to a PDP context and the interface constraints of the PLMN. This method of data transmission is known as the GPRS tunnel protocol. Regardless of the various logical interfaces associated with the GPRS network, an end-to-end data transmission path must be guaranteed.

2.4. UMTS

2.4.1. Introduction

Universal Mobile Telecommunication System (UMTS) is a third generation mobile network technology that evolved from the second generation mobile systems DGE and the flagship technology GSM.

Developed and maintained by the 3GPP (3rd Generation Partnership Project).

UMTS uses wideband code division multiple access W-CDMA radio access technology to provide greater spectral efficiency and bandwidth to mobile networks.

The UMTS Terrestrial Radio Access Network (UTRAN) consists of Node Bs (the 3G term for BTS) and Radio Network Controllers (RNCs). The RNCs play the management role as BSCs in the previous Radio Access Networks for GSM and EDGE

Unlike the BSCs in GSM that do not connect to each other, the RNCs in UMTS connect to one another. For the purpose and scope of this thesis, the interest is RNC connection to the Packet Switched Core Network. The driving force for the evolution of UMTS that started with 3G, HSPA and HSPA+ had been a response to high data speed demands.

UMTS 3G

3G refers to the third generation of mobile telephony technology by the International Telecommunications Union. The third generation, as the name suggests, follows two earlier generations, i.e. GPRS and EDGE. 3G comes with enhancements over previous wireless technologies, like high-speed transmission, advanced multimedia access and global roaming.

The following are the maximum speeds that could be obtained for the 3G mobile technology

HSPA

HSPA, which stands for High Speed Packet data Access, is a third generation partnership project (3GPP) protocol. HSPA is an upgrade to Wide Band Code Division Multiple Access (WCDMA) to improve data access speeds. HSPA was introduced in the 3GPP Release 5 to improve downlink access rates. It was further upgraded in 3GPP release 6 to improve uplink data rates. The combination of HSDPA and Enhanced UL is referred to as HSPA.

With the introduction of UMTS, the need for improved support for Download data services has increased. Higher bit rates and lower delays were strong driving forces for the introduction of HSDPA. HSPA technology offers a maximum of 14.4 Mbps of throughput per cell.

HSPA+

HSPA+ is the first phase of HSPA evolution. The second phase is the latest mobile data technology known as Long Term Evolution (LTE). LTE is outside the scope of this study.

Figure 2.2 shows the 3GPP maximum speeds targets for the HSPA+ technology.

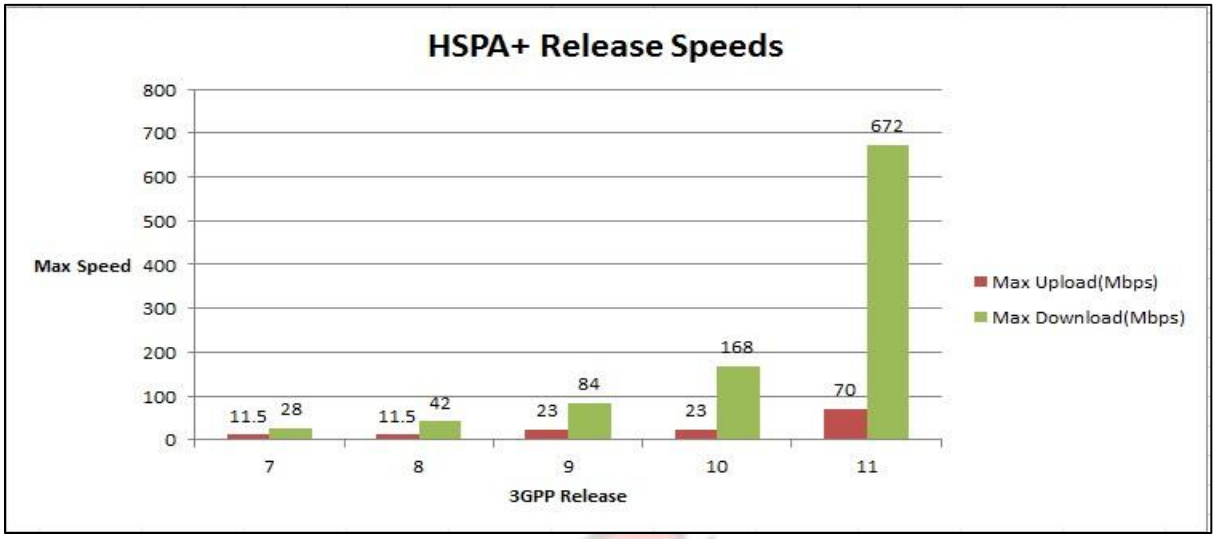


Figure 2.2: HSPS+ Release Speeds

Almost all telecommunication service providers in Ghana operate within 3GPP release 8 of HSPA+.

Ouyang & Fallah (2012) pointed out that, above UMTS release 8, LTE is preferred because HSPA+ above release 8 makes is not worth investing into due to the amount involved. Experiments for the thesis was solely done within HSPA+ release 7 and 8 speeds i.e. 42Mbps.

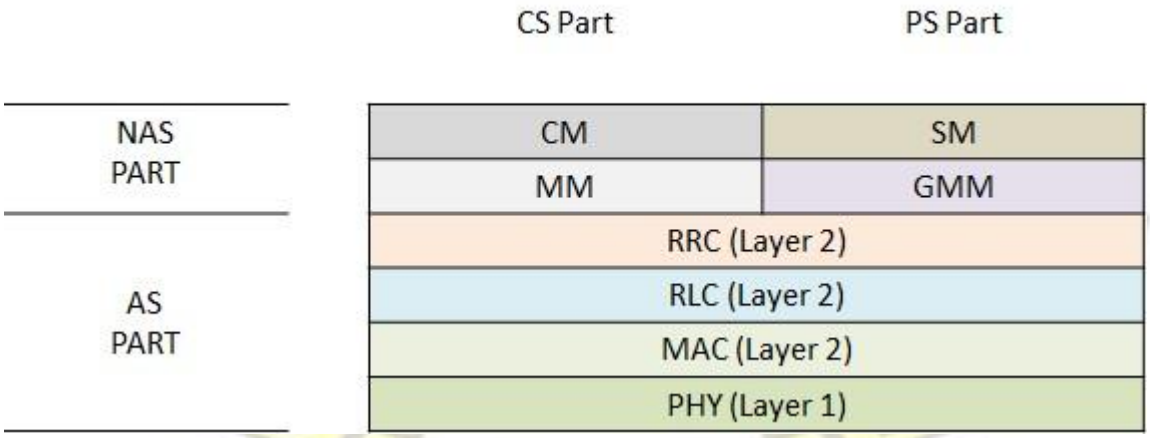


Figure 2.3: UMTS Protocol Stack

UMTS protocol stack, as depicted in Figure 2.3, consists of Access Stratum (AS) and Non Access Stratum (NAS).

Access Stratum supports OSI-layer 1 to 3. It consists of:

- Physical Layer (layer 1)
- Media Access Control and Radio Link Controller(layer 2) and
- Radio Resource Control (layer 3).

NAS or core network part is divided based on Circuit Switched (CS) or Packet Switched (PS) functionalities.

For CS functions it consists of Connection Management (CM) and Mobility Management (MM) layers.

CM layer takes care of Call Control (CC), Supplementary Services(SM) and Short Message Service (SMS). This is for UMTS CS control plane stack.

For UMTS CS user plane stack, NAS part do not include connection management and Mobility Management layers but it includes application data layer protocol end to end (between UENodeB-RNC-MSC-Remote users).

For Packet Switch functions, which are the focus of this thesis, it consists of Session Management(SM) and GPRS Mobility Management (GMM) layers. This is for UMTS Packet Switch control plane stack.

For Packet Switch user plane stack, the Access Stratum part incorporates Packet Data Convergence and NAS part incorporates packet protocol data (e.g. IP, PPP, etc.) and packet data applications (example FTP, HTTP etc.).

The Packet Data Convergence does compression of IP headers. It is an optional feature in the UMTS protocol stack. (Anandalingam and Raghavan, 2003).

2.5. TCP/IP Suite

The TCP/IP suite is a software. According to Odom (2008, p. 17)), the meaning of networking model or networking architecture is actually a set of documents where the documents describe the function of network requirements. Parts of the documents may describe a protocol and

others the physical requirements for networking. The TCP/IP model falls under this description and it is named after the two most important protocols in the suite:

- The Transmission Control Protocol (TCP) and
- The Internet Protocol (IP).

The IP protocol has two major versions, i.e. IP version 4 (IPV4) and version 6 (IPV6).

IPV4 is this thesis would rely on. Most systems within our environment are yet to migrate to the new IPV6.

As explained by Douglas Comer, the TCP/IP protocol suite, like the OSI reference model, is defined as a set of layers.

The layers closer to user activities are known as the upper layers. These upper layers rely on the lower layers to transform the upper layers data to formats compatible with the lower layers for transmission over the physical medium that occupies the lowest of the layers. Out of the TCP/IP suite was the OSI model formulated as a standard for data transmission over IP networks. As such, it does not directly map to the 7-layer OSI reference model.

The TCP/IP protocol stack has only four layers:

Application Layer

The layers of the TCP/IP model conforms to the standards set by the Open Systems Interconnect (OSI). The TCP/IP model is made up of four layers as against seven layer of the OSI standard. The TCP/IP application layer is equivalent to the Application, Presentation, and Session layers of OSI standard.

Some well-known examples of application level entities within the TCP/IP domain are:

- FTP/Telnet/SSH
- HTTP/Secure HTTP (SHTTP)
- POP3/SMTP
- SNMP

Transport Layer

The application layer of the TCP/IP model is comparatively composed of quite a number of protocols. Example is the hypertext transfer protocol (HTTP). The main protocols of this layer are:

i. TCP and ii. User Datagram Protocol (UDP)

The TCP protocol ensures large file sizes are segmented into packets of maximum size 1500 bytes before transmission. TCP also ensures error correction of packet transmission. TCP is connection oriented.

UDP is connectionless and does not guarantee error correction and detection.

Internet Layer

The Internet Protocol (IP) defines the TCP/IP internet layer. It ensures each host within a network has a unique IP address, it handles packet routing from one host to another based on the source and destination IPs.

Network Access Layer

The Network Layer involves the most reduced layer of the TCP/IP suite convention stack. The network access layer is made out of two sub-layers; the media access control (MAC) and the physical sub-layers. The MAC sub-layer adjusts nearly to the data link layer of the OSI display, and is some of the time alluded to by that name. The physical sub-layer adjusts to the physical layer of the OSI model. According to Comer (2014), some of the technologies that run on the network access layer are:

- Ethernet

- Wireless Fidelity (Wi-FI)/WiMAX
- PPP, PPP over Ethernet (PPPoE)
- ATM/Frame Relay

2.6. The OSI Model

The International Standard Organization defined a model for systems communications known as the Open Systems Interconnection Reference Model.

The OSI model's top three layers - Application, Presentation and Session - deal with functions that aid applications in communicating with other applications.

The OSI model has 7 layers defined for network communications. Below are the layers:

Application Layer

The application layer is the uppermost layer of the OSI model. It makes available to users, the ability to access information of a network application. The primary interface for users to interact with applications is made possible via the application layer. The capability of the application layer is not limited to just user to computer or application access within a local area network but from network to network. The internet is an example of what the application could do. It allows us to legally access applications at wherever it is located.

Presentation Layer

The presentation layer is a translator that deduces its name from its function. Data in its raw state cannot be transmitted without adapting it to a standard form. The adaptation is done before it is successfully transmitted. Computers or embedded systems have been manufactured to receive such adapted data format and convert it back to readable format. Data compression, decompression, encryption and decryption are the main task of this layer.

Session Layer

The role of the session layer is like that of a moderator or a referee. Its main function is to dialogue control between devices or nodes. It serves to organize their communication by

offering three modes Simplex (Monologue communication. One transmitting and the other receiving), Half Duplex (Nodes take turn in transmitting and receiving), Full Duplex (Both communicating end could transmit and receive at the same time) - by splitting up a communication session into three different phases. The phases are connection establishment, data transfer and connection release.

Transport Layer

Services located here segment and reassemble data from upper-layer applications and unite it onto the same data stream. They provide end to end data transport services and establish a logical connection between the sending host and destination host on an internetwork. Data integrity is ensured at this layer by maintaining flow control, and also by allowing users the option of requesting reliable data transport between systems. Flow control prevents the problem of a sending host of one side of the connection overflowing the buffer in the receiving host - an event which could result in loss of data.

Network Layer

The network layer's interface is to networks. It is employed by the transport layer to provide the best end-to end packet delivery services for it. The job of sending packet from the source network to the destination network is the Network Layer's primary function.

In life there are various routes leading to destinations. The same applies to the clouds of IP networks we have today. The appropriate paths to these destinations is determine by protocols inherent in the third layer of the OSI model, i.e. the Network Layer. Path determination makes it possible for a router to appraise all available paths to a given destination and decide on the best one. Routers use network topology information when orienting themselves to the network and evaluating the different possible paths through it.

Data Link Layer

The Data Link Layer provides the services of ensuring that messages are delivered to the appropriate devices and translates messages from up above into bits for the physical layer to transmit. It formats the messages into data frames and adds to it a customised header containing the hardware destination and source address.

Physical Layer

The Physical Layer is the tangible part of the OSI model and focuses on two responsibilities: It sends bits and receives bits. Bits only come in values of 1 or 0.

Its task is transporting various bits from one node to the other. Its task also covers the following: Physical characteristics of interfaces and media, representation of bits, data rate, synchronization of bits, line configuration, physical topology, transmission mode etc.

(Behrouz and Forouzan, 2010).

2.7. The IP Protocol

2.7.1. Introduction

The United States Department of Defence is the architect of the Transmission Control Protocol (TCP). The purpose was for this protocol to meet the demands of both Network and the Transport layers. This approach proved incapable of meeting the purpose for which the protocol was developed. The solution was to set apart the Internet Protocol aimed at providing Network Layer services and the Transmission Control Protocol to providing Transport Layer services.

The Internet Protocol (IP) is considered the most critical part of the TCP/IP protocol suite. TCP, UDP, ICMP, and IGMP data are transmitted as IP datagrams. IP is known to be unreliable and connectionless datagram delivery service, i.e. it is not full proof that an IP datagram successfully arrives at its destination.

The service that IP provides is of the best effort type. In case of any mishap, for example, a router momentarily running out of buffers, IP has an inherent error handling mechanism in the form of algorithm to handling such issues - IP dismisses the datagram and make an effort to

send an Internet Control Message Protocol (ICMP) message back to the source about the problem. Any required reliability is provided by the Transmission Control Protocol of upper layer.

Internet Protocol mode of operation is connectionless. This means, successive packets do not maintain any form of information about the other. That is why IP datagrams delivery could be out of order. For example, an IP source node transmits consecutive datagrams to a destination. The arrival of the consecutive datagrams is not based on which packet was sent first but rather the route traversed in reaching the destination. The destination node which also has the TCP/IP suite software would rearrange the packets in the right order. This arrangement is possible because each packet is assigned a unique number that follows the preceding packet.

(Stevens, 2009).

2.7.2. The IP Header

Affix to an IP version packet is the IP header. It contains data about the packet such as IP version, source IP, destination IP, time-to-live, etc. As stated earlier, the version of IP that this thesis is considering is the IP version four.

As shown in Figure 2.4, the normal size of the IP header is twenty bytes.

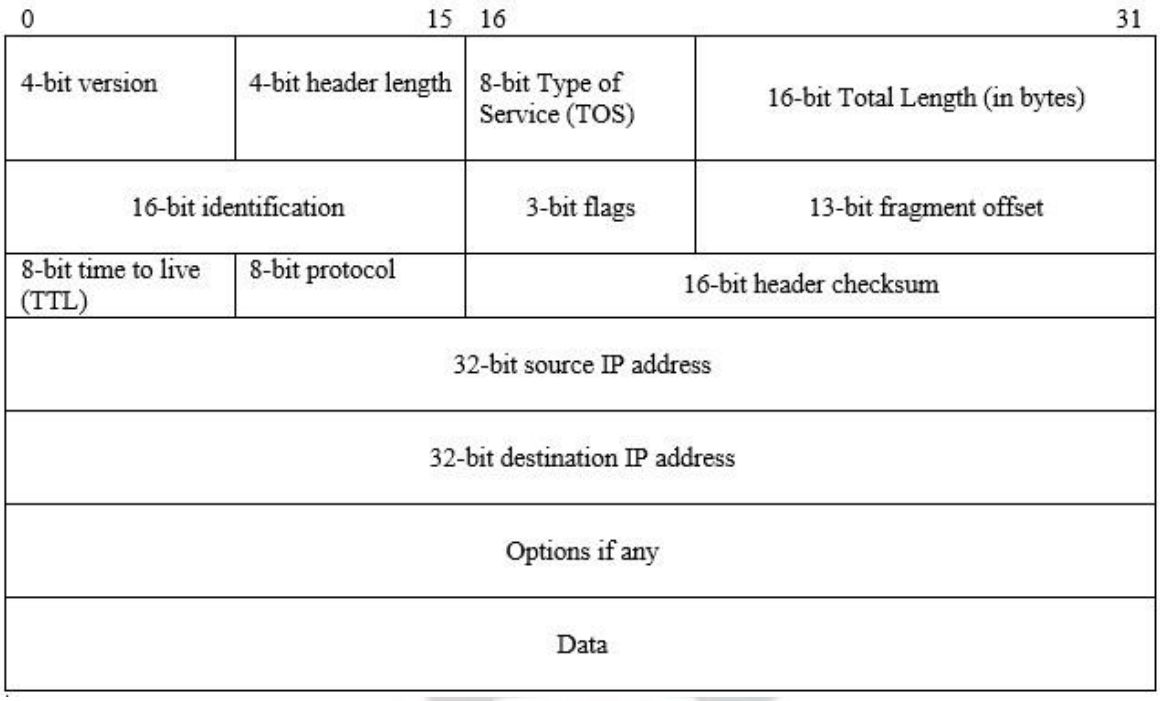


Figure 2.4: IP Header

Figure 2.4 is a summary description of the IP header.

The required number of fields of an IPV4 is twelve with one optional field. The lower limit for the header length is 160 bits, an equivalence of twenty bytes. Table 2.1 is a summary description of the IP header fields.

Table 2.1: Summary IPV4 Header

Field	Length	Description
Version	4 bits	Version of IP (in this case IPV4
Internet Header Length	4 bits	Specifies the length of the IP header (minimum 160 bits)
DSCP	8 bits	Classifies traffic for QoS
Total Length	16 bits	Specifies the length of both the header and data payload
Identification	16 bits	Uniquely identifies fragments of a packet
Flags	3 bits	Flags for fragmentation
Fragment Offset	13 bits	Identifies the fragment relative to the start of the packet
Time to Live	8 bits	Decremented by each router traversed

Protocol	8 bits	Specifies the next upper layer protocol
Header Checksum	16 bits	Checksum for error checking
Source Address	32 bits	Source IPv4 address
Destination Address	32 bits	Destination IPv4 address
Options	Variable	Optional field for various parameters

2.7.3. IP Addressing

The Internet Assigned Numbers Authority (IANA) is a standard body responsible for the allocation of IP addresses. They have grouped IP addresses in class based on the network size. The IPV4 is made up of two parts the network and the host parts. The network part is determine the mask, i.e. number of binary bits one "1". The host part is determined by the number of binary bits zero "0". The default IP version 4, which is used by this thesis, ranges and classes have been summarised in Table 2.2 below:

Table 2.2: Default IPV4 Ranges

Classful IPV4 Address Ranges			
Class	First Network ID	Mask	Slash Notation
A	1 - 126	255.0.0.0	/8
B	128 - 191	255.255.0.0	/16
C	192 - 223	255.255.255.0	/24

By default, class A has a default network size of 2^8 = 256 and 2^{24} - 2 = 167,77,216 hosts per network. The slash notation column is the network mask that determines the network of an IP address. The general formula for determining the network and hosts are 2^n for network and 2^n – 2 for the hosts. The first and last IPs for the host part are not assignable to host, hence the minus two in the formula.

IP addresses are not free. For private use, IANA has given out ranges of IP addresses within each class to be used. These IP address range are not usable in the internet. They are only meant for private network usage. The summary of the free IP address ranges is as shown in Table 2.3. (Hunt, 2002).

Table 2.3: Free IPV4 Default Ranges

Private IPV4 Address Ranges			
Class	Range	Mask	Slash Notation
A	10.0.0.0	255.0.0.0	/8
B	172.16.0.0 - 172.31.0.0	255.255.0.0	/16
C	192.168.0.0	255.255.255.0	/16

The thesis used mainly the class "A" free range in the design of the IP networks.

2.7.4. IP Routing

The Internet Protocol (IP) of the TCP/IP protocol suite is responsible for packet transmission from one node to the other. This is termed as IP routing.

The Transmission Control Protocol is responsible for the right size of packet transmission; It slices the packets into sizes of not more than 1500 bytes for onward routing by the IP. The routing could be done statically or dynamically. For static routing, the gateway for the packet is by default specified. For dynamic routing, the default gateway of the source node sending the packet is configured to dynamically learn the appropriate and efficient route to send the packet. This thesis used both the static and dynamic routing protocols. The dynamic routing choice was the Open Shortest Path First (OSPF). (Doyle and Carroll. 2006).

2.8. Port/Network Address Translation

Network Address Translation (NAT) concept was born because of the shortage of public IPv4 addresses. Many organizations moved to deploy private addresses using the IPv4 private addressing space to contain the shortage.

Below is the private IP range that are permissible to be used

- 10.0.0.0–10.255.255.255 (10.0.0.0/8 prefix)
- 172.16.0.0–172.31.255.255 (172.16.0.0/12 prefix) and
- 192.168.0.0–192.168.255.255 (192.168.0.0/16 prefix)

NAT was primarily deployed to translate private addresses to public addresses, but NAT could also translate from any address to any other address, including public to public and private to private addresses. For NAT, the translation is one private IP to either one public IP or multiple public IPs.

This mapping was improved by the introduction of Port Address Translation.

For PAT, one public IP could be used by as many as 65,536 users or applications. The first 1,024 ports that translates to known protocols is reserved. The remaining 64,512 ports is available for any user or application. (Tomsho, 2011).

2.9. MBB Core Elements

Basically, Mobile Broadband had had the same core elements from its inception - GPRS to HSPA+. This span of technologies covers the scope of this thesis. The major architectural change comes with the introduction of Long Term Evolution (LTE) technology which is outside the scope of this thesis.

The variations or changes to the architecture from GPRS to HSPA+, herein referred to as GPRS for the sake of brevity or established convention, had been the peripheral devices. These peripheral devices may be mentioned in this document for reference sake but not dwelt on in detail as part of the core components of the GPRS architecture in study.

The core components of the GPRS architecture are the:

- “Serving GPRS Support Node (SGSN)” and
- “Gateway GPRS Support Node (GGSN)”

The SGSN is the contact node to the already discussed radio access technologies i.e. GSM and UMTS.

The GGSN is the gateway to the already discussed packet data networks technologies i.e. TCP/IP protocol suite and the OSI model. (Assad, 2007).

2.9.1. The SGSN

Within the GPRS core network, the Serving GPRS Support Node (SGSN) acts as the exit and entering point to and from the radio access network. The SGSN is responsible for authenticating MS/UE before they attach to the GPRS core network. The SGSN authenticates the MS/UE by querying defined subscriber identity module (SIM) profile in the home location register (HLR). In case no record is found in the HLR database about the SIM, the SGN reject the MS/UE attach request otherwise it accepts the request. The SGSN also manages MS/UE mobility and session activities. (Fitzek and Charaf, 2009).

The SGSN also collects charging data (call data records) for each mobile subscriber, such as the actual use of the radio network and GPRS network resources, this call data record is known as the SCDR (SGSN Call Data Records).

2.9.2. The GGSN

One of the main nodes of the GPRS network is the Gateway GPRS Support Node. The GGSN is the gateway to other packet data networks for the MS/UE. The logical interface it provides to other packet data networks is known as the Gi. The IP address used by either UE or MS for accessing other packet data networks is provided by the GGSN. When a MS/UE session is active, the GGSN records detail of the session known as call data records (CDR). The CDR is used for offline charging. The GGSN communicates with an online charging system known as

the Intelligent Network to deduct credit from the MS/UE SIM based on the volume of packet data uploads or downloads.

2.9.3. PDP Context

After a MS/UE is powered on and attached to a GPRS network, the MS/UE initiates a session to acquire IP address to enable it communicate with other IP nodes. The acquired IP address is known as packet data protocol (PDP) address and the process to acquiring the IP address is known as PDP context activation.

The PDP context established is composed of various attributes like the quality of service, the PDP address type (either IPv4 or IPv6), the GGSN public IP address and the others.

2.9.3.1 PDP Context Activation Procedures

The complete format of APN that identifies a GPRS network is apn.mnc.mcc.gprs. The main purpose of a mobile station (MS) or User Equipment (UE) is to acquire an IP address to enable it communicate with other IP nodes. The attempt at establishing a session request by a MS/UE is known as the packet data protocol (PDP) activation.

The MS/UE uses the allocated IP address to accessing other public or private data networks.

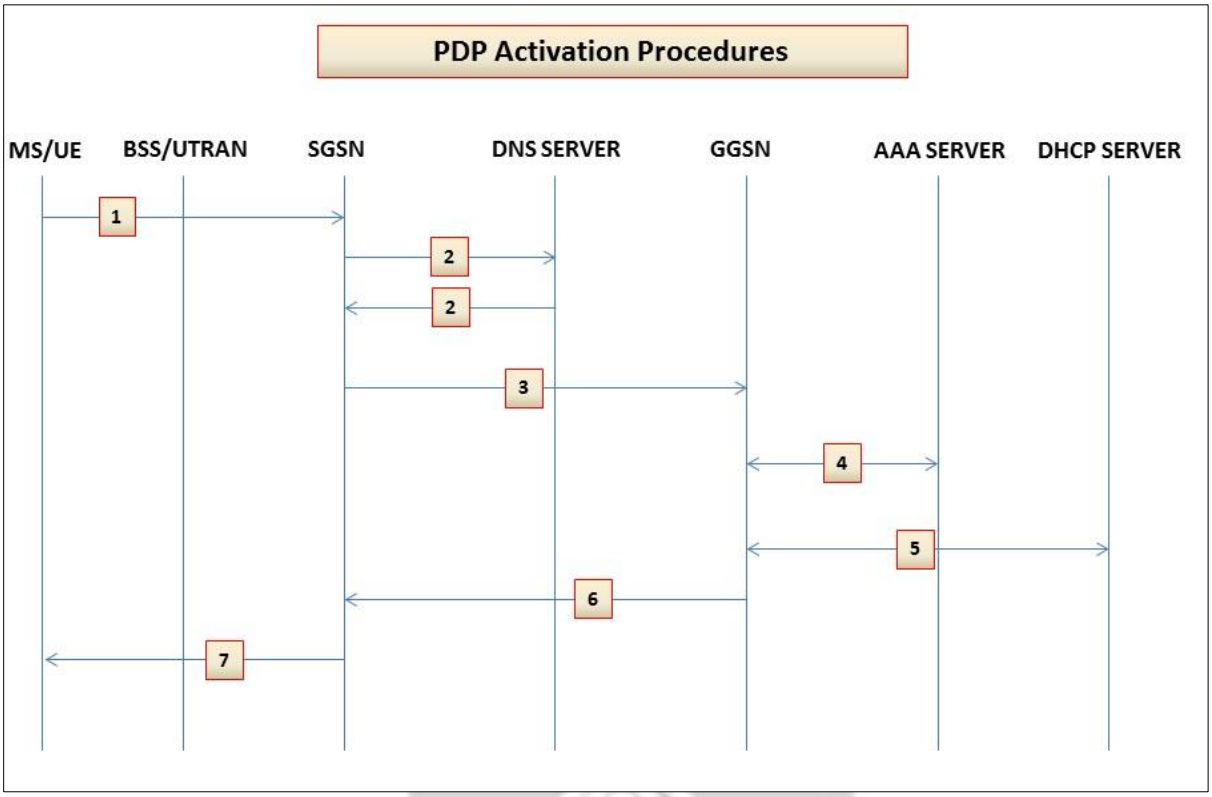


Figure 2.5: PDP Activation Procedures

Description of packet data activation procedures as captured in Figure 2.5.

i. The MS/UE would need an IP address to enable it communicate with other IP nodes therefore, a PDP activation request is made to the SGSN by the MS or UE.

ii. The request by the MS/UE in step one contains a network identifier called APN. The SGSN upon receiving the request make a DNS query to locate the GGSN identified by the APN. The DNS responds with the IP address of the desired GGSN. This DNS is not for resolving URLs to IP addresses for browsing but rather locates GGSNs based on PDP request.

iii. The SGSN now forwards the request made by the MS/UE it had received to the GGSN in a form of a PDP context.

iv. The MS/UE authentication at this stage is optional but the GGSN performs that if needed.

v. IP allocation to MS/UE could be dynamic or static. Should the MS/UE needs to be allocated an IP dynamically, the GGSN would allocate one using its embedded DHCP service.

vi. The GGSN communicates the assigned IP address to the MS/UE to the SGSN in the form of PDP context response using the GPRS tunnel protocol. vii. The SGSN finally communicates the IP address assigned by the GGSN to the MS/UE in the form of PDP context accept using the GPRS tunnel protocol.

After stage vii, a GPRS tunnel protocol tunnel is created between the MS/UE. This enables the MS/UE to now communicate with other IP nodes.

2.9.4. APN

The access point name identifies a GPRS network. By definition of the standards that governs GPRS, the APN definition is done in the GGSN. An example of an APN definition could bear the name, MIT.com.

To configure an APN, the service operator configures three elements on the GSN node:

Access point: A definition that helps in APN creation and also spells out APN's access characteristics for the sake of security. Authentication, accounting or authorisation could be used to achieve the desired security prescriptions with Remote Authentication Dial-In User Service (RADIUS). For dynamic IP allocation, the dynamic host configuration protocol (DHCP) is used and for domain named service (DNS), the DNS IP address of a service provider is used.

Access point list: Defines a logical interface that is associated with the virtual template

Access group: A definition that determines access between the mobile station and the packet data network.

A sample APN by name MIT.com with a /24 class-C private IP block of 192.168.100.0 255.255.255.0 would be used for all design implementations.

A virtual sample office, MIT-Office, with a /24 class-B IP block of 172.16.100.0 255.255.255.0 would be used for all design implementations.

A /32 class-A public IP of 1.2.3.4 255.255.255.255 would be used for the implementation. This IP may have been used by an entity in a live network. Its usage in this project is just for academic purpose.

An open source complex networks simulator, GNS3, would be used to demonstrate the designs implementation.

2.10. MBB Standard Architecture

The MBB has quite a number of standard logical interfaces with a few optional ones not shown in Figure 2.6 diagram. It is composed of two main core nodes group, the Radio Access Network (RAN) and the Packet Switched Core Network (PSCN).

The Radio Access Network (RAN) houses the following nodes:

- The Mobile Station (MS)which is known as the handset
- The Base Transceiver Station known as radio cell sites for 2G (GPRS)
- The Node-B which are also cell radio sites for 3G (UMTS)
- The Base Station Controller (BSC) which manages the 2G cell sites within a specified area.
- The Radio Network Controller that manages all the Node-Bs within a specified area.

These nodes, e.g. Mobile Station Controller (MSC), Equipment Identity Register (EIR), Foreign SGSN for roaming and Border Gateway etc., are not of importance to this study hence omitted.

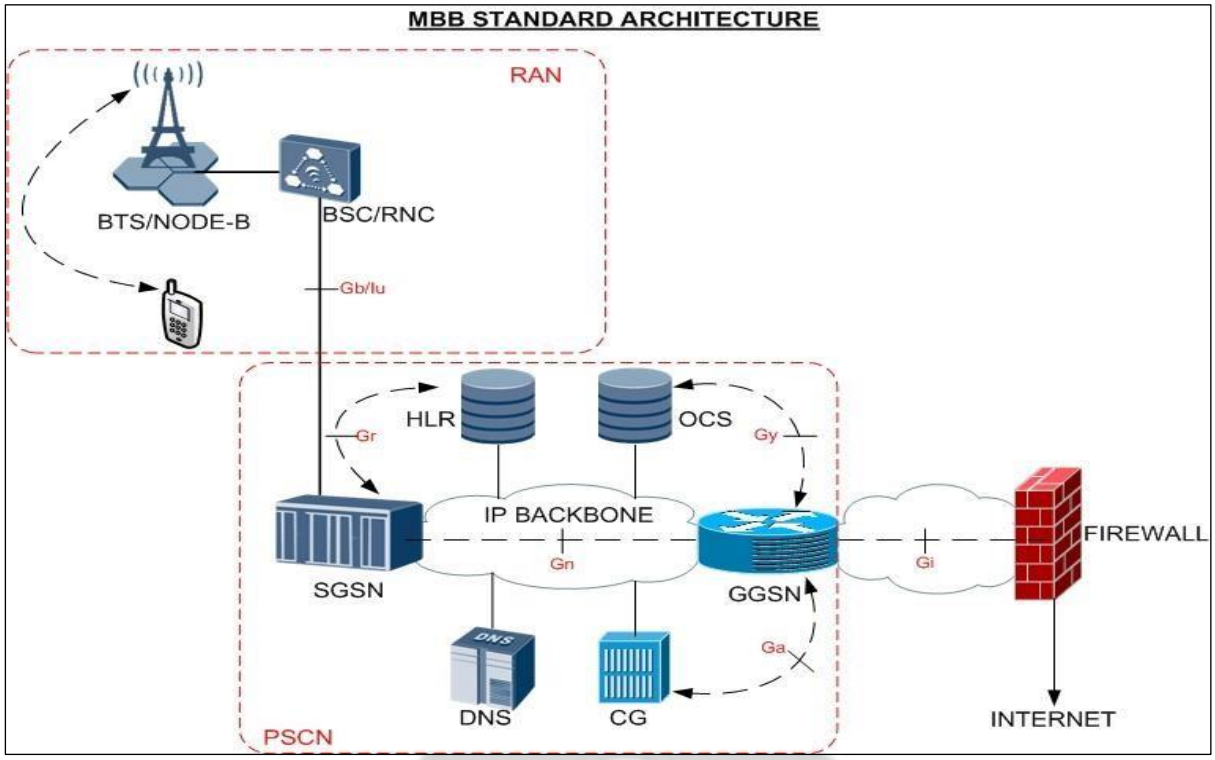


Figure 2.6: MBB Standard Architecture

Based on the scope of this study, which primarily focuses on using MBB to designing IP networks for businesses, the following nodes have been omitted in the MBB standard architecture diagram in Figure 2.6. Some of the omitted nodes are, the Policy and Charging Rule Function (PCRF); Value added nodes like the Wireless Application Protocol (WAP). The WAP render pages to very old browsers and phones that does not support graphics. Also omitted is the Multimedia Messaging Services (MMS) that provides messaging platform for phones with lower operating systems. Example, Palm OS. 2002, Ericsson R380, and the others.

According to Kasera & Narang (2004), the Packet Switched Core Network houses the following nodes:

- Serving General Packet Radio Service (SGSN) node. It is the node that interfaces the RAN and primarily responsible for user equipment mobility and session management.

- Gateway General Packet Radio Service (GGSN) node. It is responsible for acting as gateway to other IP networks. It assigns IP address to user equipment and takes part in service usage charging.
- Online Charging System: This is the node that actually does charging of MBB service usage. The charging is done either by volume of data downloaded/uploaded or by time of service usage.
- Charging Gateway: It is an offline charging system. It collects data call detail records for future billing.
- Home Location Register: It is the database of all users' profile. It is also used for user authentication between the SGSN and itself. Before MBB service is accessed, SGSN would contact HLR to confirm user existence before service is rendered.
- Domain Name Server (DNS): Unlike other domain name servers used for locating web sites IP addresses, this DNS is used for locating only GGSN for SGSN during packet data protocol requests from user equipment via the SGSN.
- Firewall: It is used to ensure only legitimate packets either leaves or enter the PSCN to RAN then the user equipment. It is also used to protect the MBB core network.

CHAPTER 3. METHODOLOGY

3.1. Introduction

The general aim of this study is the analysis of benefits of the design and implementation of IP networks with Mobile Broadband (MBB) technology as against the use of traditional Fixed Broadband (FBB) technology.

A pragmatic research approach was used in gathering data for this thesis.

Three main areas of the study are:

- MBB IP Networks Design Types

- MBB IP Networks implementation and
- Speed, security, quality of service and throughput analysis

To the ordinary user of data, service should always be available, secured and pretty fast.

The measurements and determination of speed/throughput. quality of service and security were done by capturing IP packets whiles data services were accessed from source to destination.

The IP network design were segmented into three:

- The MBB User Equipment to User Equipment (SIM-To-SIM) design: The term user equipment is a standard name for any UMTS compatible data device. That's any device that could support either 3G, HSPA, HSPA+ or LTE. For EDGE and GPRS, any compatible device is known as Mobile Station (MS)
- The Layers two and three virtual private networks design: These design would seek to expand these layers of FBB IP networks to where fixed broadband could not reach but mobile data coverage is present.
- The Internet Protocol Security (IPsec) design: This design seek to take SIM-To-SIM out of its confines to any part of the world.

3.2. Tools Used for the Design

The following are the various tools used for the exercise.

- Laptops: Lenovo ThinkPad T540p – Core i7 and Dell Vostro 1540 – Core i3 all with FBB and MBB data services from Vodafone.
- Uncapped FBB service from Vodafone (Huawei ADSL Modem)
- Uncapped MBB service from Vodafone (Huawei HSPA+ compatible Modem. Model K4201)
- Destination URLs for acquiring log traces for protocol and quality of service analysis:

- ftp://ftp1.optonline.net/pub/ for FTP, UDP,
- http://radiotest.eu/HTTP_DL01/ for HTTP and TCP
- https://www.youtube.com/ for RTSP

- Packet Capture: Wireshark Network Packet Capturing and Analyser. It is an open source software for TCP/IP packet capture and analyser that could be obtained from: https://www.wireshark.org/download.htm
- Packet Analysis: Wireshark and Capsa (Free edition: www.colasoft.com/capsa/) Packet Analysers.
- Drawing Tools: Microsft Visio, Powerpoint and LibreOffice Draw
- Network Design Icons: In addition to Visio, Powerpoint and LibreOffice's default network icons, additional ones were downloaded from Huawei (www.huawei.com) and Cisco (www.cisco.com) for the IP networks design.
- Virtual Lab: GNS3, a graphical network simulator, is used as virtual lab for the implementation, testing and analysis for the IP networks implementation.
- An Access Point Name (MIT.com) provided by Vodafone to support the study.
- Apache Web Server. An open source software that could be obtained from (www.apachefriends.org).
- Filezilla. It is a open source software that provides file transfer (FTP) protocol server services to FTP clients.

3.3. Protocols

The destination URLs were carefully chosen to provide the needed protocols for this study.

The protocols of interest for the study are as follows:

- HTTP
- UDP
- TCP and

- RTSP

A summary of protocols used for the design implementations are but not limited to the following:

- Frame Relay
- ICMP
- Telnet
- SSH
- OSPF and
- Static Routing protocols

3.4. MBB Preliminary Test

For near perfect and unbiased exercise, Vodafone (chosen service operator for the thesis) was contacted to make sure there exist no capacity constraints about both MBB and FBB.

Vodafone advised the test be conducted at very low traffic period for both technologies, i.e. between 02:00 – 07:00 GMT to have a fair playing field to testing download speeds for both technologies.

To independently confirm there were no bottlenecks on the packets trajectory from source to destination, trace routes were performed from source using both technologies to IP of one of the chosen destinations i.e.; http://radiotest.eu/HTTP_DL01/.

3.5. IP: radiotest.eu

Ping test to the URL radiotest.eu was done with Windows Disk Operating System application to obtain the IP address of the URL as shown in Figure 3.1

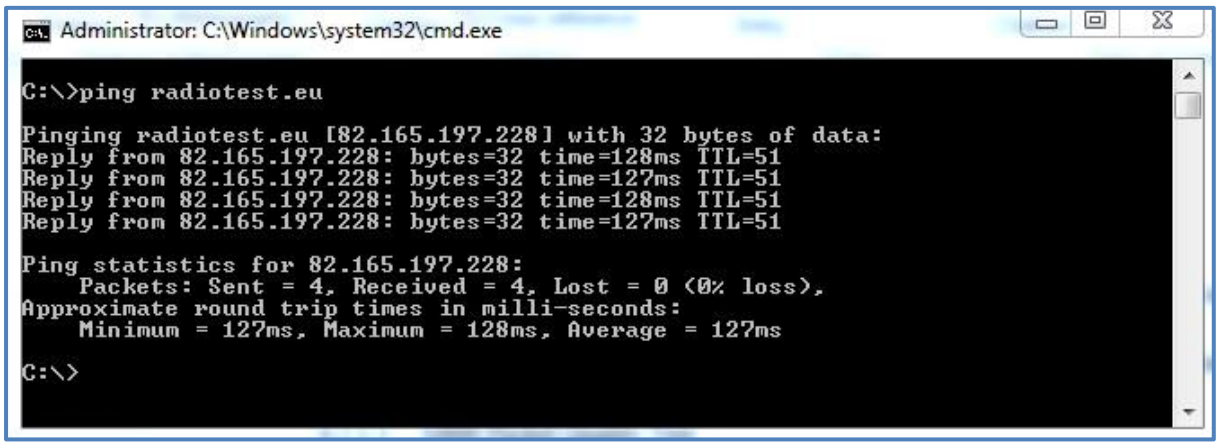


Figure 3.1: Ping To Radio Test Site

The objective is to independently confirm whether there exist no bottlenecks within the service provider's network to the test destination.

The open source application WinMTR (it combines the functionality of ping and traceroute in a single network diagnosis) was used to perform the trace route to the destination IP 82.165.197.228 obtained from [http://radiotest.eu].

Also, the obtained IP of radiotest.eu was used to confirm or otherwise a trouble free FBB service. WinMTR was used to perform the test. The test performed is captured in Figure 3.37.

The obtained IP address was entered into the host field and the start button activated for the commencement of the trace route.

The Hostname column shows unresolved IP addresses of various hops along the path to the radio test site. The unresolved feature could be configured under the options button. The IP address 192.168.1.1 is the default gateway of the source node used for the test, i.e. the laptop.

The Nr column lists the nodes on the pathway by numbers. The loss% column indicates the number of packets lost at each specified node. The sent and received columns measures the number of packets sent and received. The other parameters are of no essence to the test. The IP address 80.87.78.69 is the gateway IP of the service provider.

3.6. The Mobile Broadband (MBB) IP Designs

Traceroute To radiotest.eu

The obtained IP of radiotest.eu was used to confirm or otherwise a trouble free MBB service.

WinMTR, an open license application in Figure 3.2 was used to perform the test.

The obtained IP address was entered into the host field and the start button activated for the commencement of the trace route.

The Hostname column shows unresolved IP addresses of various hops along the path to the radiotest site. The unresolved feature could be configured under the options button. The IP address 192.168.0.1 is the default gateway of the source node used for the test, i.e. the laptop.

The "No response from host" obtained is a hidden node from the public. It is a security measure put in place by the operator.

The Nr column list the nodes on the pathway by numbers. The loss% column indicates the number of packets lost at each specified node. The sent and received columns measures the number of packets sent and received. The other parameters are of no essence to the test. The IP address 85.205.18.121 is the internet gateway IP of the service provider.

This traceroute test was carried out to establish the degree of latency along the IP packet path.

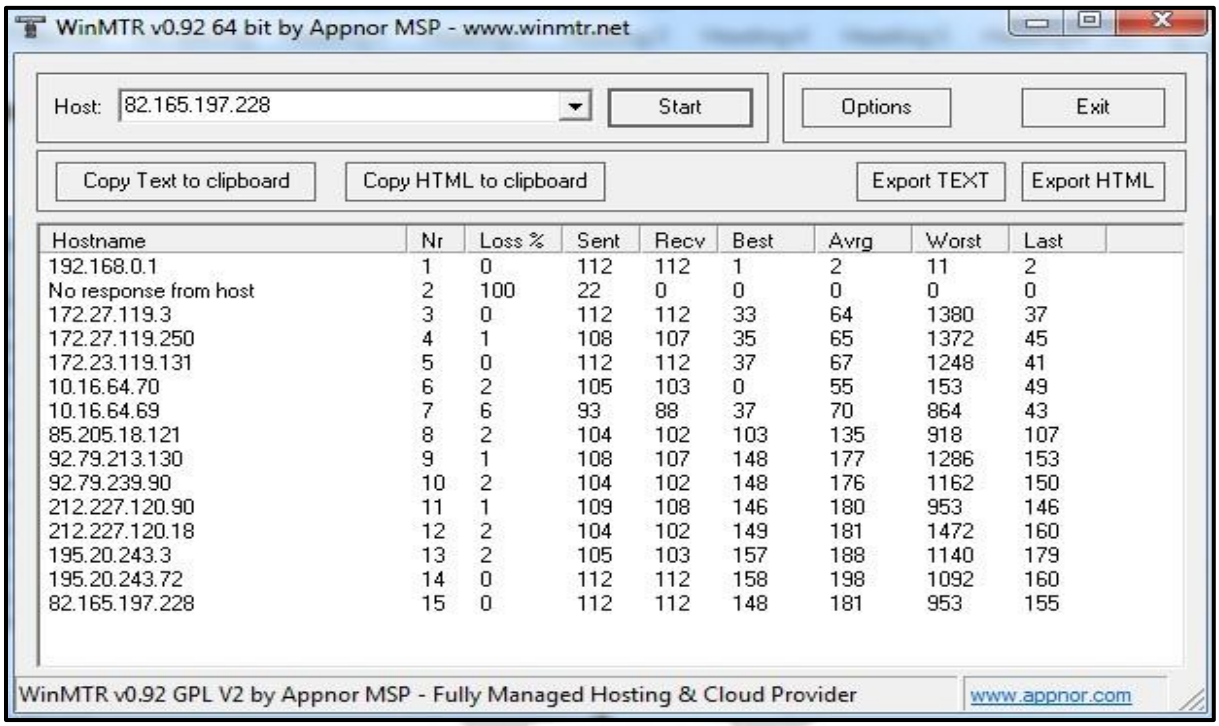


Figure 3.2: MBB Tracroute To radiotest.eu

3.6.1. Traceroute Packet Capture with Wireshark

Figure 3.3 is a sample Wireshark trace capture that was made possible with a MBB handheld device with hotspot facility to a PC. The source IP 192.168.0.2 in the trace, is that of the PC used in capturing the trace. The destination IP 82,165,197,228 is that of the resolved site http://radiotest.eu .

The protocol used in exchanging packets between the two destinations is the Internet Control Message Protocol (ICMP).

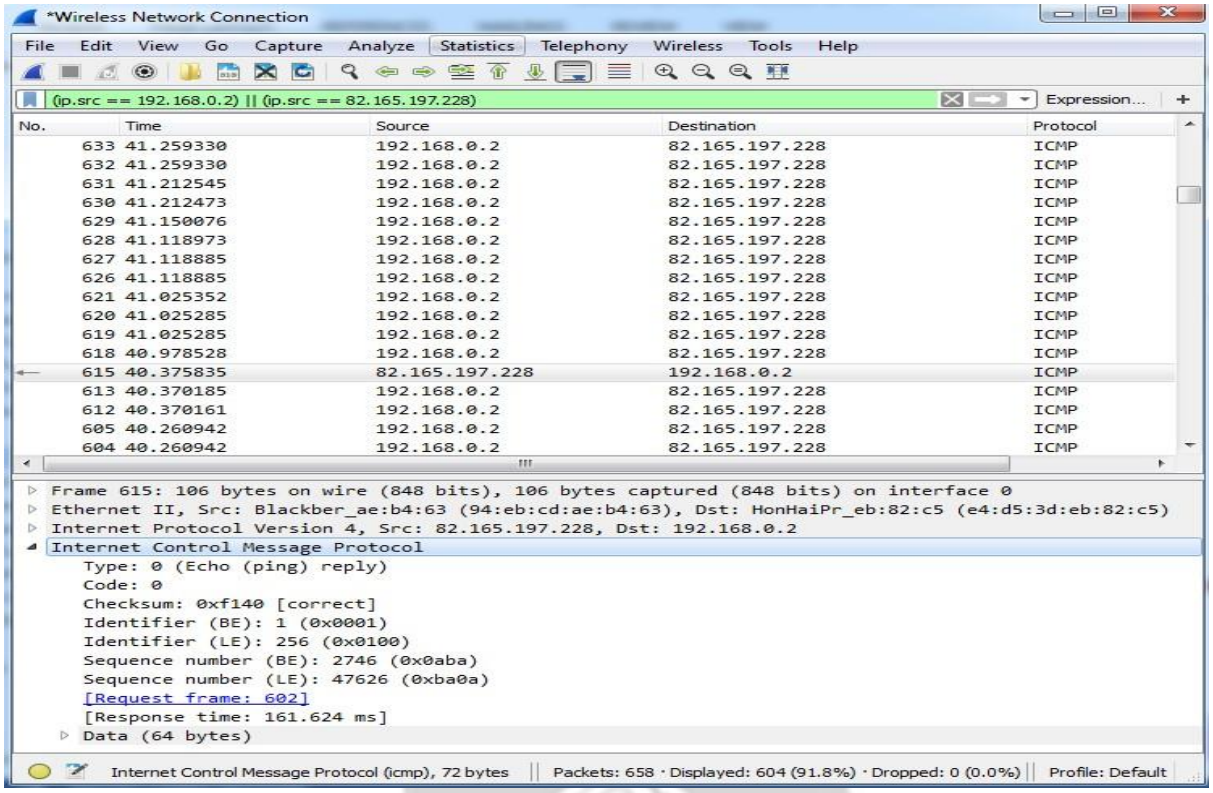


Figure 3.3: MBB Packet Capture

3.6.2. MBB HTTP Download Setup

The objective of this test is to ascertain the download speed offered by the MBB technology.

The test was performed using the following 3G setup.

- A Hotspot was setup on the 3G Mobile device terminal.
- A Laptop with Wi-Fi capability was connected to the 3G mobile device.
- Packet traces were captured on the laptop with Wireshark whiles downloads were being performed.

Figure 14 is a detailed diagram depicting the data call flow of the hotspot setup for the HTTP download test in Figure 13.

An HSPA+ compatible phone and a laptop were used to set up the experiment for the speed test. The laptop is also equipped with wireless capability. The term hotspot is used to indicate

wireless network availability as transport to accessing data resource. The phone is used in setting up the hotspot for the laptop to gain access to wireless connectivity.

The setup was used to download 10 megabytes (10MB) of data from Radio Test site http://radiotest.eu/HTTP_DL01/ . Other sizes of data could downloaded for analysing the HTTP download test but 10MB was chosen as being ideal.

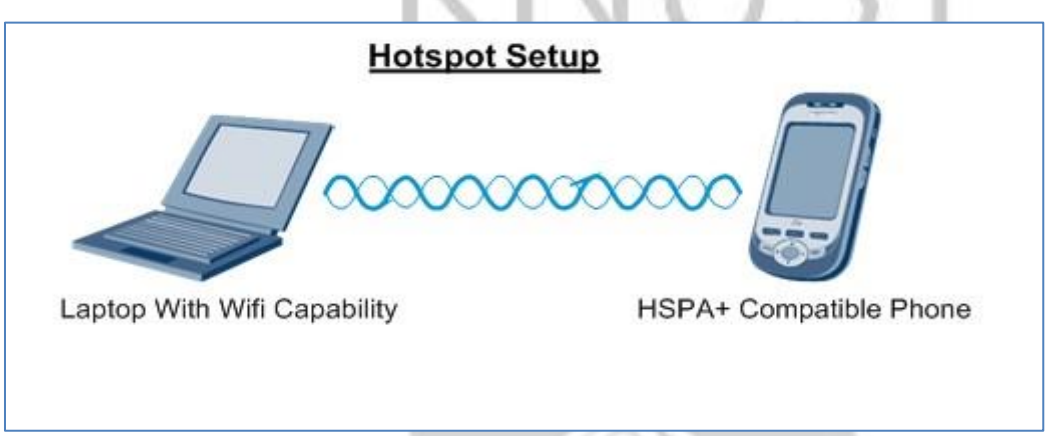


Figure 3.4: MBB Speed Test- Hotspot Setup

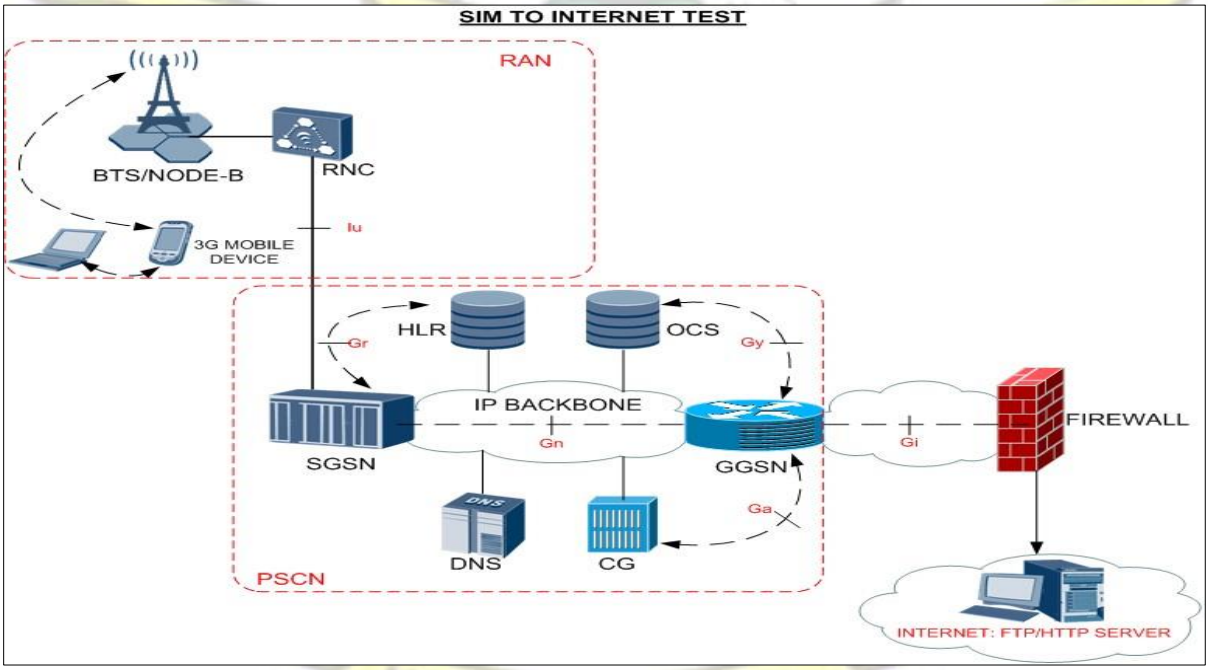


Figure 3.5: SIM To Internet Test

There are various factors that may cause IP packet in transition to get lost before reaching its destination. Some of the causes are bad physical Ethernet interface card, loose cable, bad link (congestion) and others. (RFC 3819, 2004).

IP packets for MBB and FBB were examined to determine download quality i.e. inherent packet loss.

The parameters considered were:

- TCP Retransmissions and
- TCP Duplicate Acknowledgements

TCP retransmission is the resending of packets which have either been damaged or lost.

TCP duplicate acknowledgements arise out of fast transmit and fast recovery of packets.

3.6.3. MBB Packet Quality Test

Mobile broadband networks provide an opportunity for operators to offer new services to potential and existing subscribers. The negotiated or contracted quality of service needs to be sustained without overprovisioning network resources. (Soldani et al., 2006).

Figure 3.6 is a Wireshark trace simultaneously taken during the MBB HTTP download test.

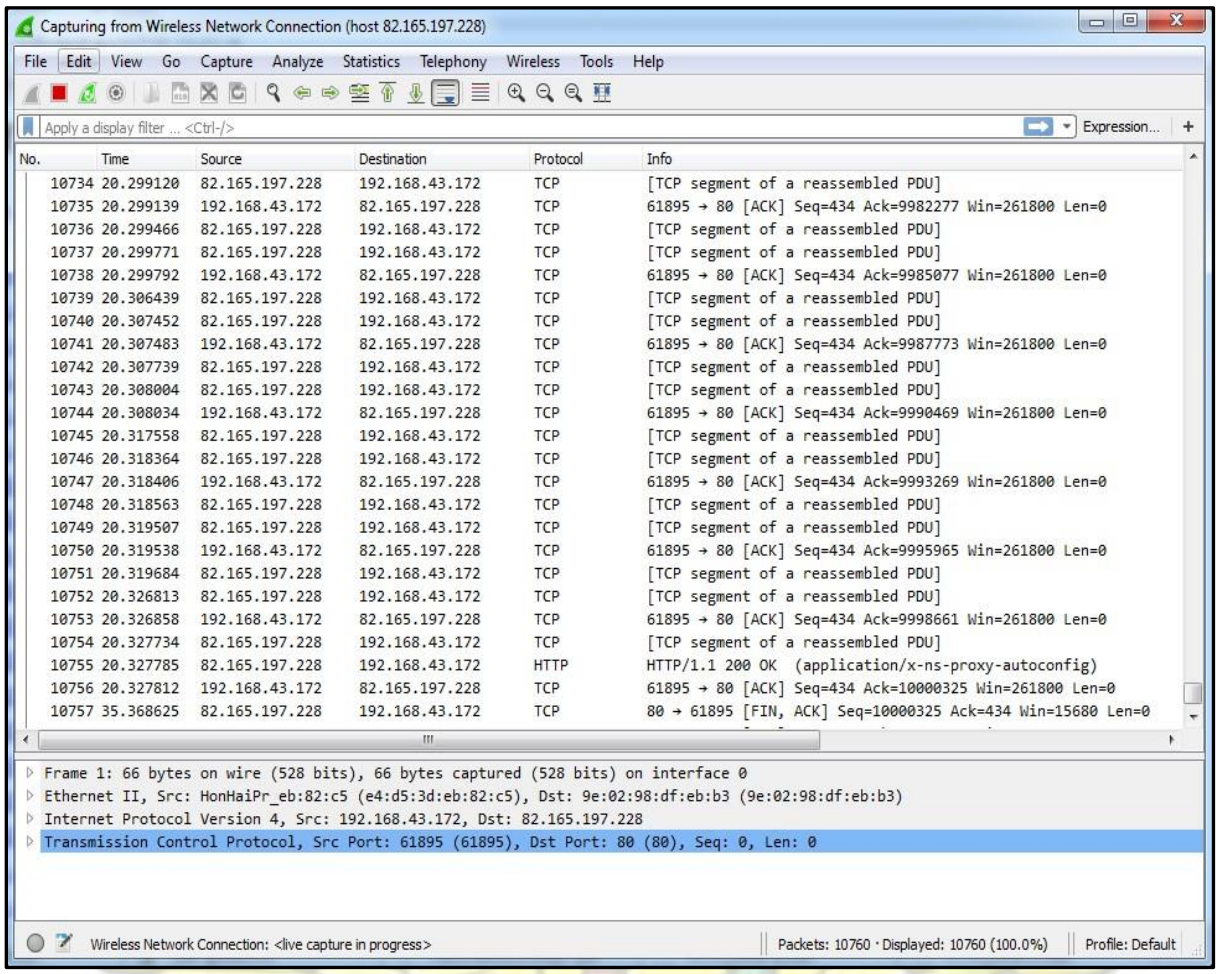


Figure 3.6: HTTP Download Test - Trace Capture

HTTP is a layer protocol application defined in the TCP/IP protocol suite. Its transmission protocol port number is 80 and its representative protocols, HTTP and TCP, have been displayed under the protocol column of the captured trace as highlighted in Figure 3.6.

Detail of HTTP download site is shown in Figure 3.7

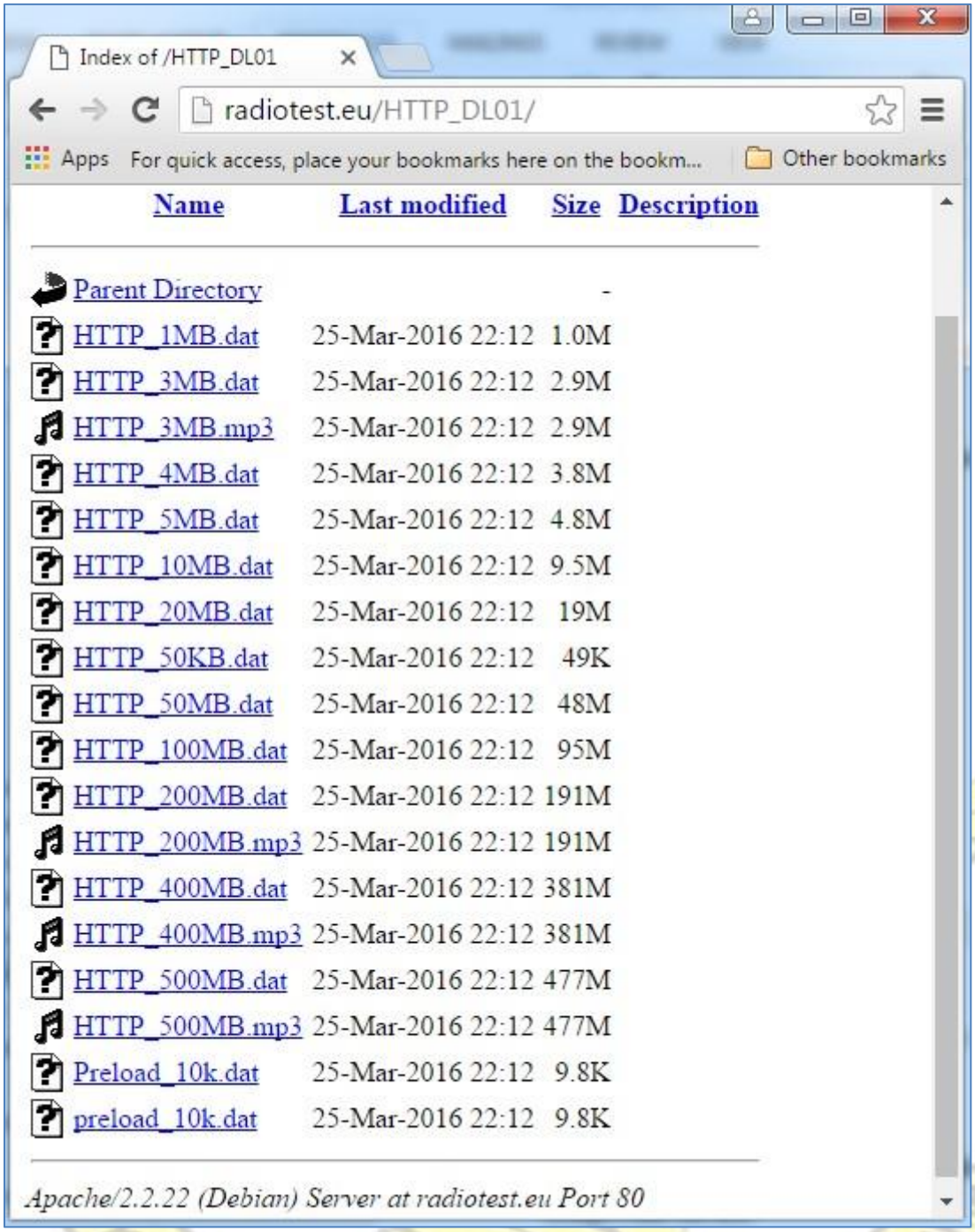


Figure 3.7: HTTP Download Site

The HTTP download site, in Figure 3.7, hosts various data sizes meant for testing HTTP download over mobile broadband service. The data sizes are industry standard for testing mobile data service.

3.6.4. MBB Speed/Throughput Obtained

Speeds obtained for MBB and FBB are highlighted in Table 3.1 and Table 3.2 download statistics summary tables.

Sample MBB Summary Result.

Table 3.1: MBB Download Summary

TIME	CAPTURE	STATISTICS
First packet: 2014-10-07 23:48:50 Last packet: 2014-10-07 23:49:21 Elapsed: 00:00:31	Dropped packets: unknown Capture filter: unknown Link type: Ethernet Packet size limit 262144 bytes	Packets: 11029 Between first & last packet:31.194 sec Avg. packets/sec: 353.562 Avg packet size: 972.910 bytes Bytes: 10730223 Avg bytes/sec: 343984.293 Avg Mbit/sec: 2.752

Table 3.1 is a summary result of the HTTP download test performed over the MBB. 3MB of data download was chosen for the experiment. The data download was completed within 31 seconds. Average packet download per second was 353.563 bytes. Average speed was 2.752Mbps.

Overall Speed Summary Result

Table 3.2: Summary of Overall Speed

Test Type	Location	Protocol	Speed/Mbps
MBB	Near Cell Site	HSPA+	7.22
MBB	Away from Cell site	HSPA+	4.41
MBB	Near Cell Site	3G	3.7
MBB	Away from Cell Site	3G	3.1
MBB	Near Cell Site	EDGE	0.203
MBB	Away from cell site	EDGE	0.172

FBB	Home	IP	3.1

The HTTP download experiments were performed over the various MBB technologies such as HSPA+, 3G and EDGE. The tests were conducted at various positions to the cell site. The positions considered for the test were, considerable distance away from the cell site were signal levels were low and from positions were signal levels were quite strong. The HTTP download test was also performed over the FBB technology meant for comparison to the MBB download speed values. For the FBB, choosing a position for the test was not considered since it is a fixed service. The results obtained are captured in Table 3.2 above.

3.6.5. MBB Design Options

Numerous design options are available but the chosen ones for the study are considered as enough to cater for the rest.

3.6.6. Home/Office Access To Internet

A Mobile Broadband User Equipment (UE) could be used as an Access Point (AP) for providing internet connectivity to WiFi capability nodes.

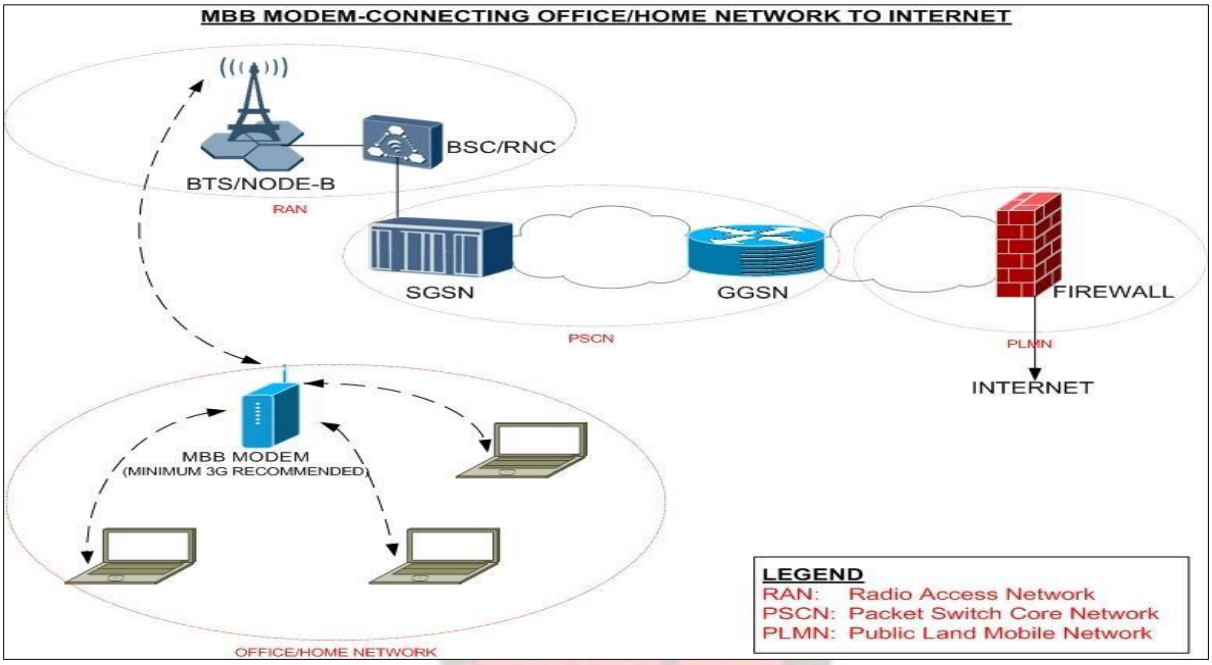


Figure 3.8: MBB Modem To Internet

3.6.7. Design Description

The MBB Modem initiates and establishes a PDP context with the SGSN.

MBB Modem is assigned a private IP by GGSN.

A GTP tunnel to internet is setup for MBB Modem

MBB Modem shares hotspot with nodes accessing internet.

Firewall translates ingress private IP to egress public IP by Port Address Translation (PAT)

3.6.8. SIM-TO-SIM Setup: No Internet

This designed involves connectivity between RAN and PSCN only, no traffic gets to the internet.

This type of design is referred to as SIM –To-SIM communication Assumptions:

- N-multiple office sites with MBB IP nodes, e.g. servers.
- SIMs are provisioned with static private IPs to prevent servers IP from changing. No DHCP.

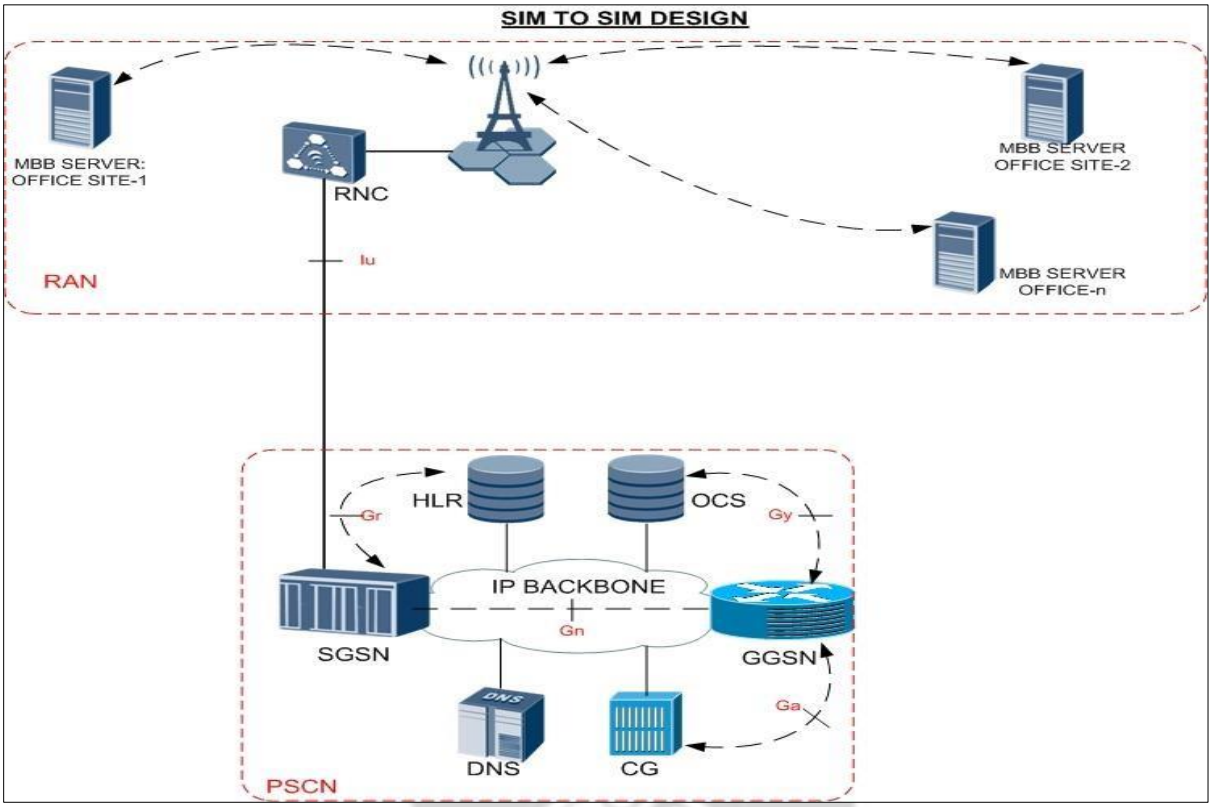


Figure 3.9: SIM To SIM

Design Description

The servers communicate with each other as follows:

A MBB compatible server initiates a session by first establishing a PDP context with the GGSN in the PSCN.

- The GGSN accepts the PDP context request and creates a tunnel for the session.
- Packets move from one site to the other from Server (source)->RNC->SGSN->GGSN->SGSN->RNC->Server(destination). Same applies for reverse traffic

3.6.9. MBB Local Sites To WAN By IPsec

This design depicts Local branches of an office networked by MBB technology.

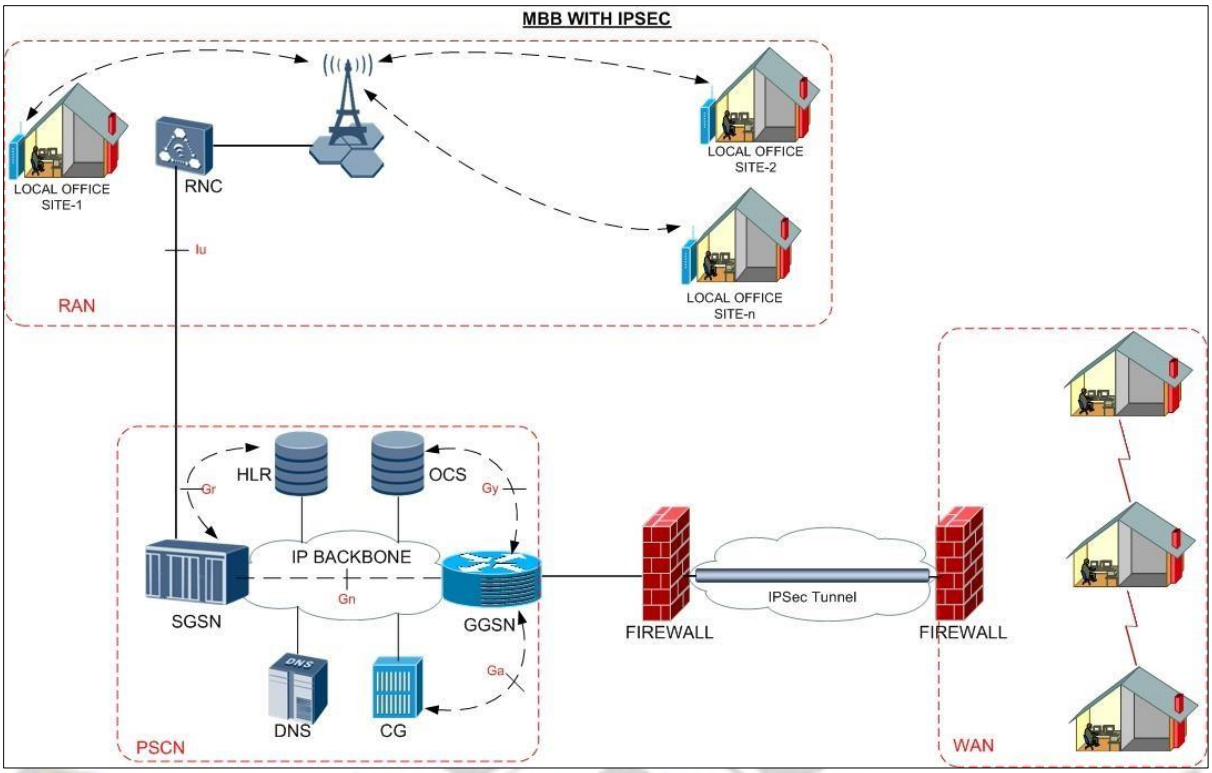


Figure 3.10:MBB With IPSec

Description

- The APN defines a MBB network for the local sites.
- The remote sites are networked by a WAN technology e.g. MPLS.
- Private IP subnets from Class A, B or C with appropriate network mask, depending on the number of nodes, are recommended for both local and remote sites.
- The local and remote networks are networked by the IPsec technology.
- At the remote sites, to cut down cost for the business entity, the firewall could be replaced with a node that supports:
    - Routing
    - IPsec
    - and Access Control

For the IPsec tunnel to be active, at least the following basic proposals must be agreed on between the business entity and the MBB service provider:

- IKE Phase-1 Parameters to exchange ○ Encryption Algorithm [AES or 3DES] ○ Hash Algorithm [SHA or MD5] ○ Diffie Hellman Group [1 or 2 or 3] ○ Key Lifetime
- IKE Phase-2 Parameters to exchange ○ Encryption Algorithm [AES or 3DES] ○ Hash Algorithm [SHA or MD5] ○ Diffie Hellman Group [1 or 2 or 3] ○ Key Lifetime
- Pre-Shared Key
- Gateway IPs

3.6.10. MBB with Layer Two VPN

Introduction

For the layer-2 VPN technology to work with the MPP service for remote office use, it is advisable to use a service provider that could provide the MBB and Layer-2 infrastructure at the same time. It would be almost impossible to have two different service providers for this design and implementation.

Setup Description

One of the famous technologies that could take advantage of this type of VPN is the MBB technology that this exercise is all about. The infrastructure to link remote sites is quite huge and is largely provided by telecommunication service providers. With this L2 technology, service providers just act as a physical wire linking the various remote sites.

The MPLS or Frame Relay network made available by the service provider would act as a normal physical link between the MBB networks by providing a Layer-2 service.

The Office remote site would be in the same virtual LAN.

Figure 3.11 is a high level design of a L2-VPN setup for MBB technology.

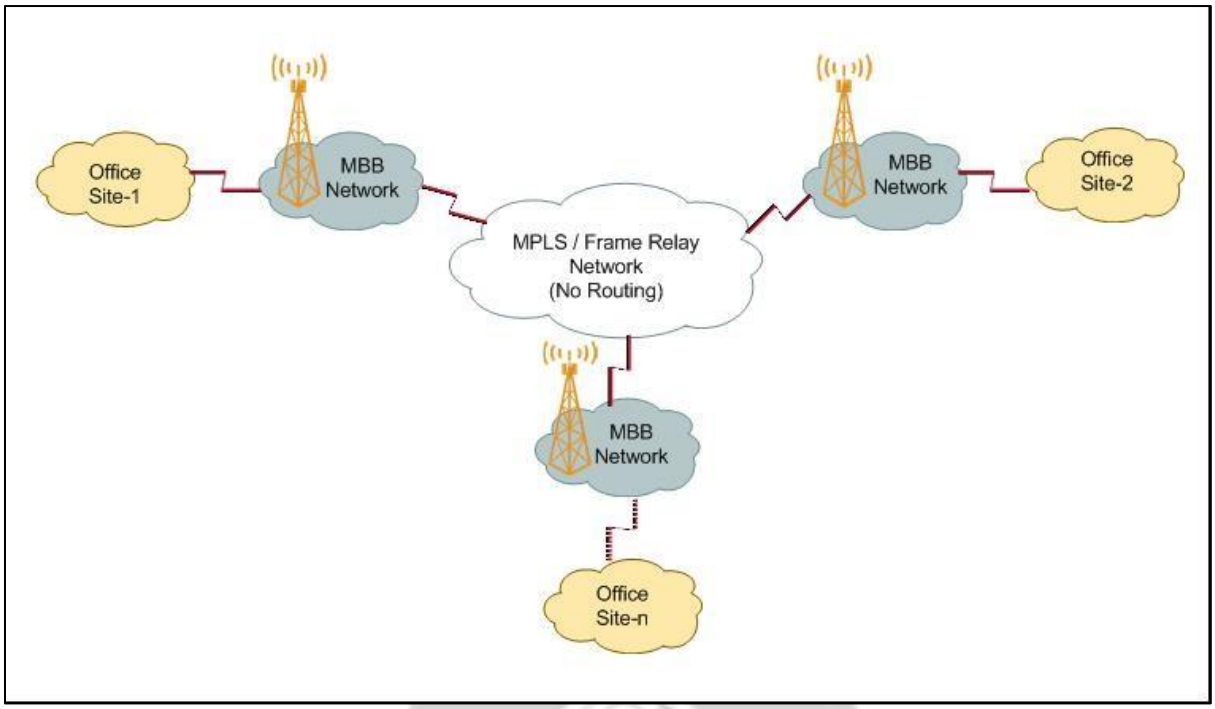


Figure 3.11: High Level Design of Layer-2VPN

3.6.11. MBB with Layer Three VPN

Introduction

For the layer-2 VPN technology to work with the MPP service for remote office use, it is advisable to use a service provider that could provide the MBB and Layer-2 infrastructure at the same time. It would be almost impossible to have two different service providers for this design and implementation.

Setup Description

The L3-VPN service provider would configure its Provider Edge (PE) devices, normally routers for MPLS networks, for each office site. The MBB traffic would be routed to the PE devices. The service provider would in turn route the MBB traffic from its PE routers via the MPLS infrastructure to the traffic destination. This is done for each site by the service provider. Figure 3.12 is a high level design of a L3-VPN setup for MBB technology.

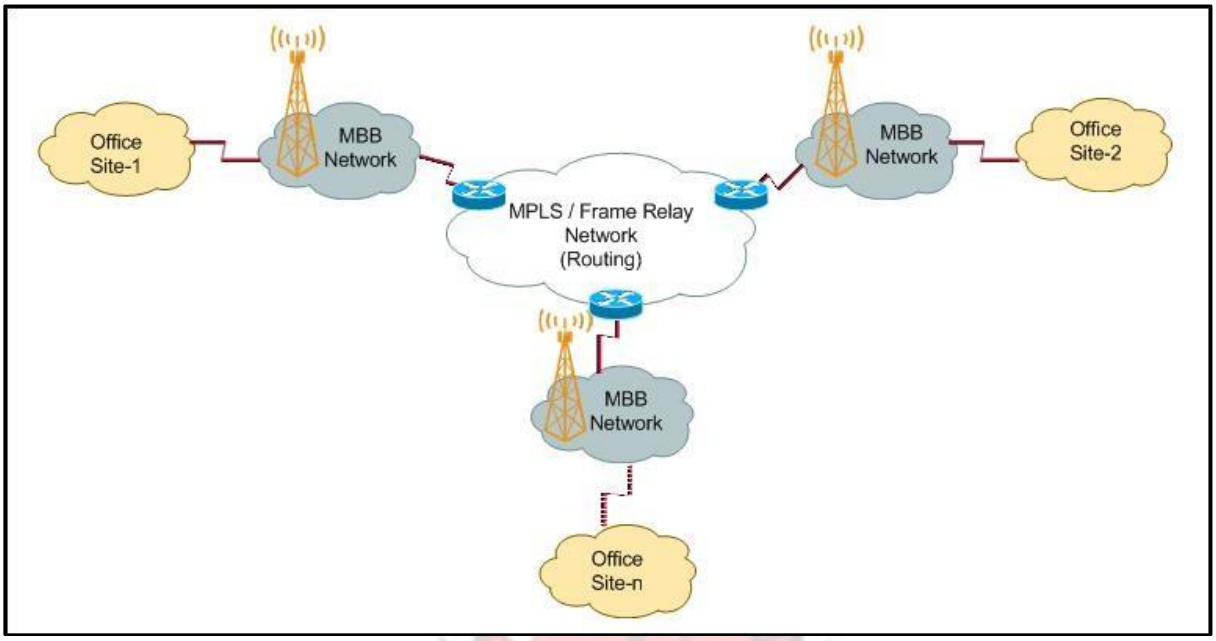


Figure 3.12: High Level Design Layer-3 VPN

3.7. MBB Design Options Implementation

Introduction

The sample implementations to be looked at are limited just to this study. There are quite a number of designs that could be looked at with their varied implementation options as well but this thesis would focus on the four areas already discussed.

The focus of the study had been to the Gi interface. This is where the proposed implementations would be concentrated. This study does not have the resource to take into consideration the Gn interface implementation of the designs proposed. These are taken care of by the service providers. The implementation experiments for the design options were done in a virtual space using GNS3 network emulator.

3.7.1. SIM-To-SIM Phase-1

Introduction

Fixed broadband internet services coverage is less than 50% in Ghana. Businesses are spread all over the country in locations where the FBB service is completely absent.

Quite a number of businesses; in an attempt to getting their offices networked opt for expensive networking technologies like VSAT (Very Small Aperture Terminal), etc.

Businesses could network their offices using the best available mobile broadband technologies.

Objective

The objective of this experiment is to show that, businesses could link their offices spread apart via MBB using SIM-To-SIM communication mode of data transfer.

Setup and Configuration

As pointed out in the SIM-To-SIM design presentation in page 47, no internet connectivity is required.

The required nodes are MBB compatible routers, interlinked to form a LAN or WAN (depending on how far apart are the offices) to complete the setup for inter data transmission.

For the SIM-To-SIM setup, we would experimentally implement two scenarios.

The first setup, as shown below, the MBB service provider would link all offices via its GPRS architecture. No internet is needed. The responsibility of the offices is to ensure, all nodes hooked to this setup must support MBB,

Figure 3.13 is a screenshot of the GNS3 Virtual Lab, logically depicting how the first SIM-To-SIM setup could be accomplished.

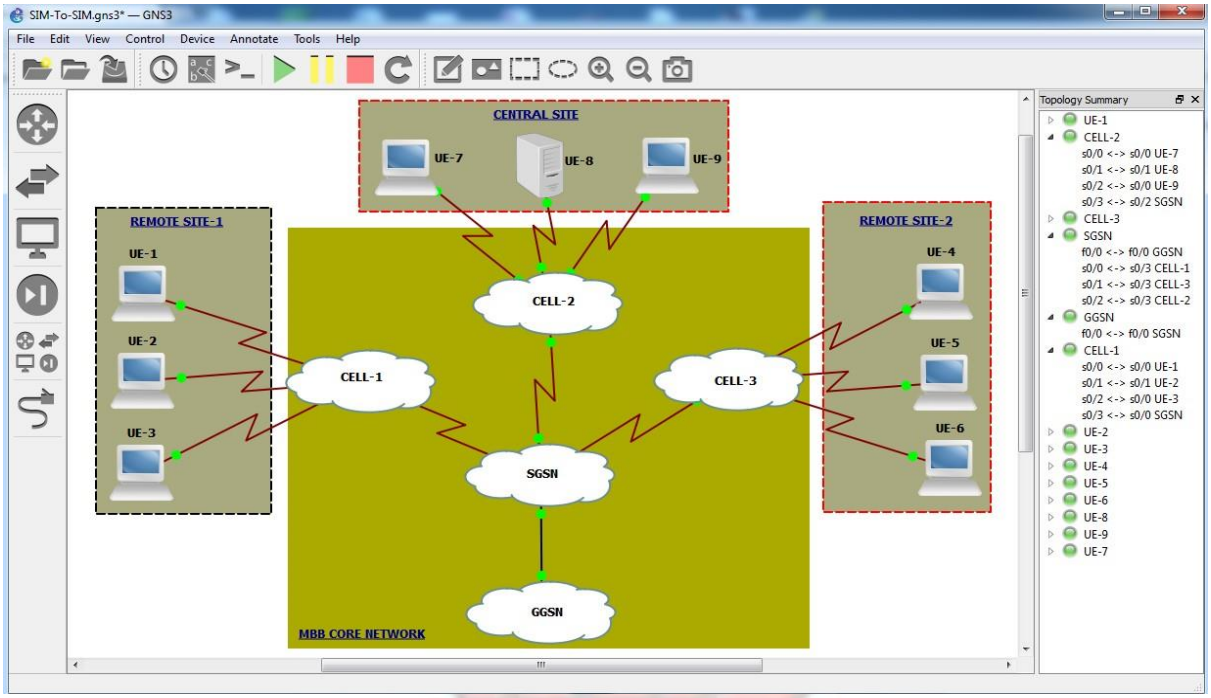


Figure 3.13: SIM To SIM No Internet

Configuration Detail

As explained earlier, with this kind of setup, no configuration is required by the office. All necessary configurations would be handled by the service provider.

The APN IP Pool used is 192.168.100.0/24

SIM cards to be used by business offices have been assigned static IPs within the above IP Pool by the service provider.

The MBB compatible nodes within the various office sites automatically acquired the static IPs of the configured SIM cards from the APN address pool 192.168.100.0/24.

The MBB nodes and SERVER are logically in the same LAN. These nodes and SERVER(s) could be physically located anywhere the service provider Radio Access Network is present.

Observation

IP connectivity tests were carried out between the three offices of the experimental setup to ensure smooth data transfer without any packet loss

Figure 3.14 is a screenshot showing successful IP connectivity between the MBB compatible nodes, depicted as PC and the server. Protocol used for the test is ICMP.

From Remote Site-1 To SERVER in Central Site

Test was conducted by sending packets from remote site one to central server to confirm connectivity and the ability to send data.

Figure 3.14: SIM-ToSIM MBB-PCI To Server

From Remote Site-2 To SERVER in Central Site

Figure 3.15: SIM-ToSIM MBB-PC2 To Server

Conclusion

SIM-To-SIM communication as shown in the design and setup scenarios, is considered the most secure and less capital intensive for businesses to adopt as means of linking various offices.

3.7.2. SIM-To-SIM Phase-2

Introduction

SIM-To-SIM communication could be of immense benefit to businesses to use as means of IP backhaul and WAN technology to use to network their various branches as depicted in page 54. Offices could further take advantage of this mode of communication by adding value to what the service provider offers.

Objective

The objective of this experiment is to investigate how businesses could further take advantage of the SIM-To-SIM communication mode by adding value to what the MBB service providers offer.

Setup Description and Configuration

This experiment makes use MBB technology to link a central office and two remote sites. In this experiment, it is assumed the business has a MBB compatible routers as various sites to form a virtual LAN made available by the service provider.

Each MBB compatible router would then have its own private LAN at its other side, i.e. its local office LAN. The MBB router would then act as gateway for the local LAN.

IP Planning

- APN IP Pool for SIM cards: 192.168.10.0/24
- Central Office LAN IP: 172.24.20.0/24
- Office Site-1 LAN IP: 172.24.10.0/24
- Office Site-2 LAN IP: 172.24.300.0/24

Figure 3.16 is a screenshot of the experimental setup with the aid of GNS3 virtual network emulator.

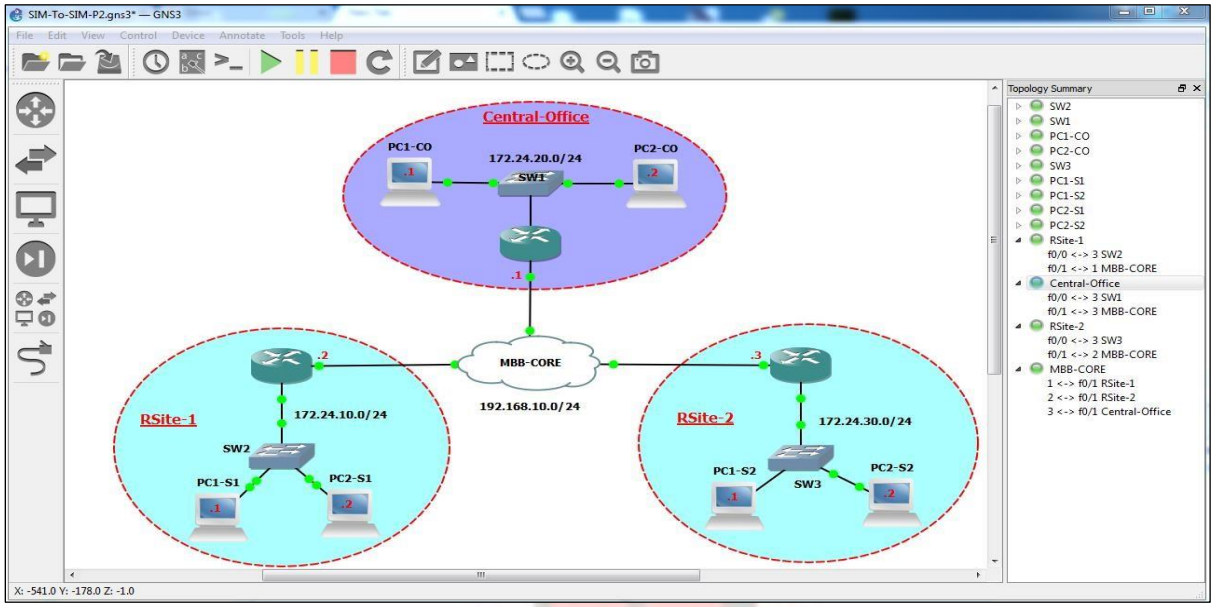


Figure 3.16: SIM-To-SIM Setup 2

Configuration Detail

Open Shortest Path First routing protocol was used for the entire setup.

Figure 3.17 is a sample detailing main parts of the setup configuration:

```
Central-Office
Central-Office#show ip ospf
 Routing Process "ospf 1" with ID 192.168.10.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm last executed 00:01:03.732 ago
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x0198A2
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

Central-Office#
```

Figure 3.17: SIM-To-SIM Sample Detail Configuration

Observation

It was observed that, IP packets could be transmitted from remote sites to main office LAN and vice versa.

From Site-1 To Main Office

Figure 3.18 is a screenshot of packets sent from Site-1 to Main Office. It shows on the surface successful pings to the main office site as expected. The ping count was 20 and none of the packets was lost.

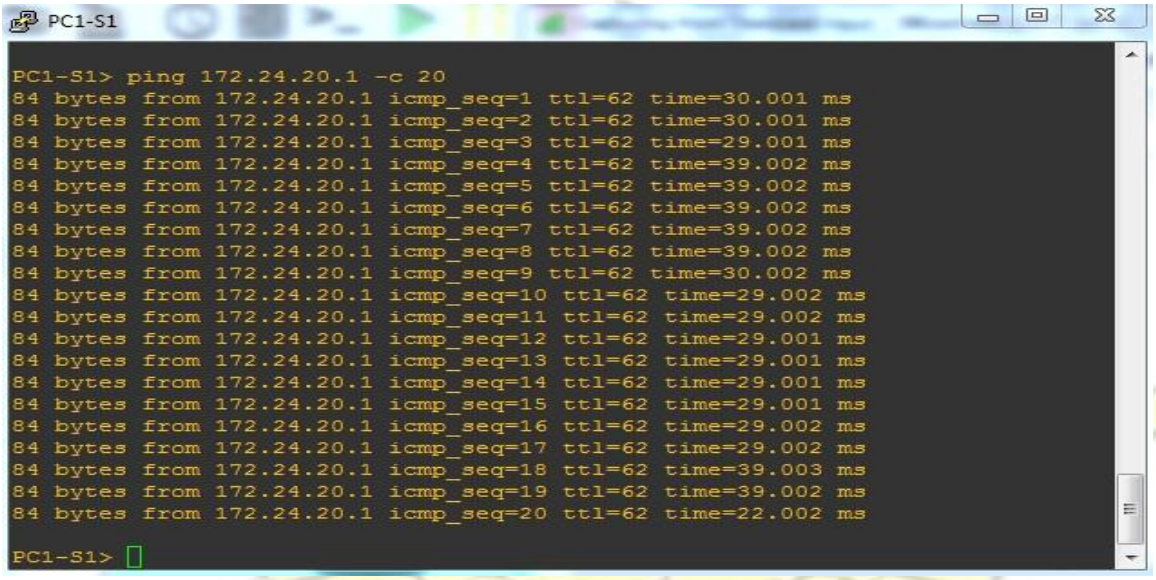


Figure 3.18: SIM-To-SIM Phase Two Ping Test

Figure 3.19 is a display of live packet capture with Wireshark during the test. The fields of interest are the source (i,e source IP), destination (i.e destination IP) and protocol used to send the packets from source to destination IP. The source IP is 172.24.20.1 and the destination IP is 172.24.10.1. The source and destination IPs belong to different LANs ICMP protocol was used to transmit packets from the source to the destination. There were echo ping replies from the destination as expected.

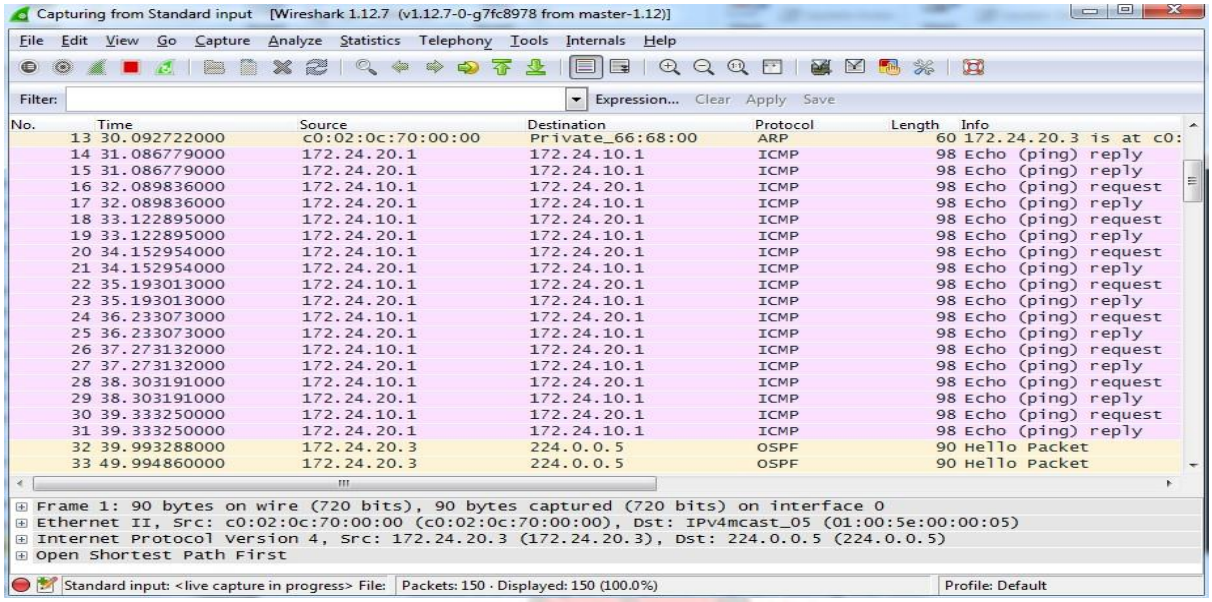


Figure 3.19: Live Packet Capture - Site-1 To Main Office

Frome Site-2 To Main Office

The virtual PC with IP 172.24.30.1 was used to send ICMP packets to the destination 172.24.20.1 to test network reachability between the two sites. Responses were obtained as expected. A total of twenty packets were sent with none lost.

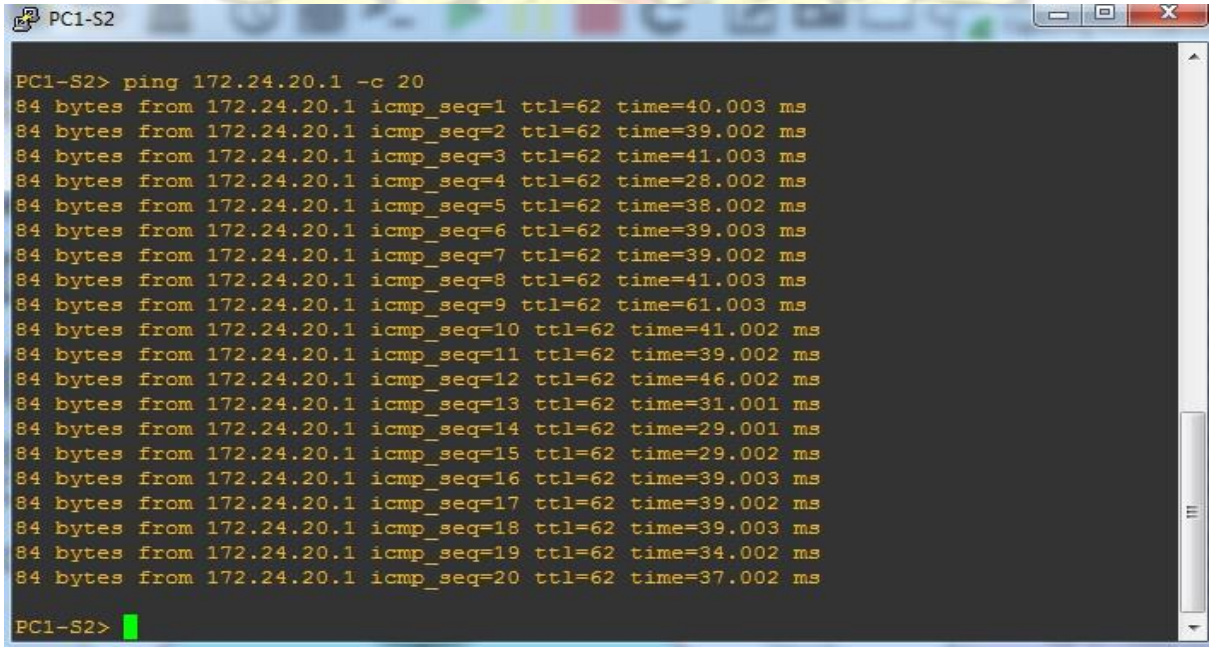


Figure 3.20: Connectivity Test Site-2 To Main Office

Figure 3.21 is a display of live packet capture with Wireshark during the test. The source IP is 172.24.30.1 and the destination IP is 172.24.20.1. The source and destination IPs belong to different LANs corresponding to the two different sites. ICMP protocol was used to transmit packets from the source to the destination. There were echo ping replies from the destination as expected.

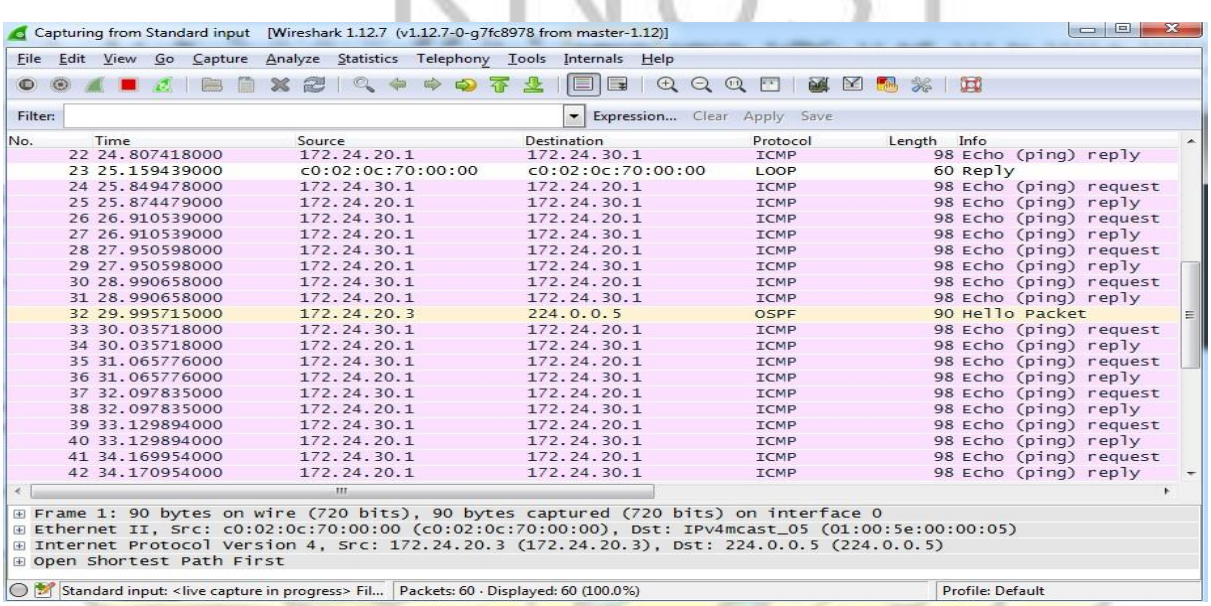


Figure 3.21: Live Packet Capture - Site-2 To Main Office

From Site-1 To Site-2

The test was aimed at confirming connectivity between the various sites. A ping test was performed from one office remote site to the other, the results obtained i.e. the successful Internet Control Message Protocol (ICMP) response from the remote site.

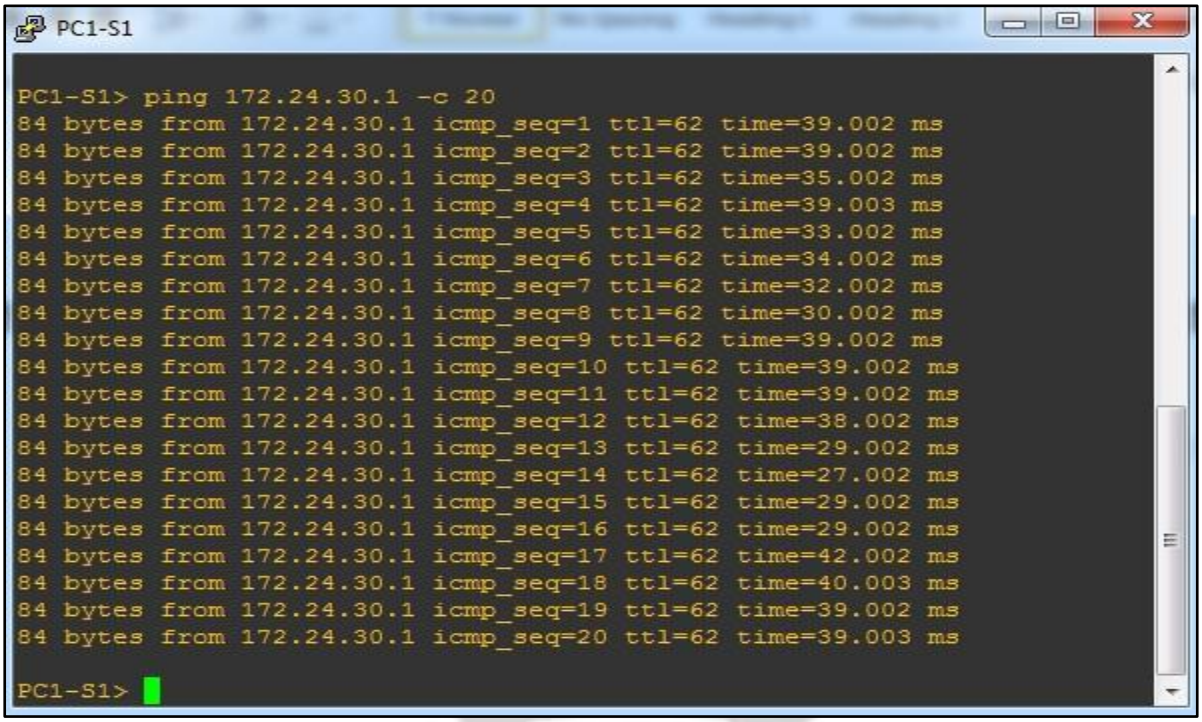


Figure 3.22: Connectivity Test Site-1 To Site-2

Figure 3.23 is a display of live packet capture with Wireshark during the test. The source IP is 172.24.10.1 and the destination IP is 172.24.30.1. The source and destination IPs belong to different LANs corresponding to the two different sites. ICMP protocol was used to transmit packets from the source to the destination. There were echo ping replies from the destination as expected.

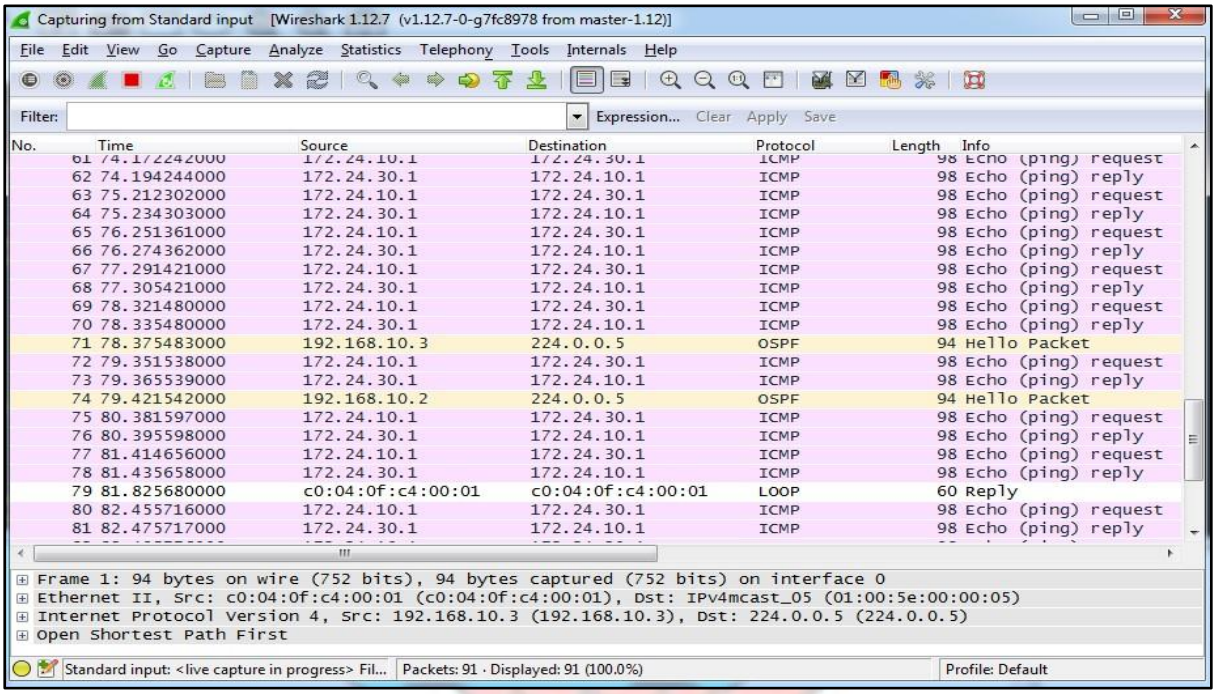


Figure 3.23: Live Packet Capture - Site-1 To Site-2

Conclusion

SIM to SIM communication is the most secure, less expensive and less effort to implement. Businesses could take advantage of this technology to link remote offices without an internet service provider services.

Security of packets in transit is much assured as compared to traffic using the internet medium. It is very difficult but not impossible to eavesdrop packets within the GSM and UTMS space thereby making the SIM to SIM ideal option for sensitive packets if security measures are not put in place. The GPRS protocol has various levels of encryption, i.e. GPRS encryption levels 1-3 known as GPRS Encryption Algorithm levels 1-3 (GEA1, GEA2 and GEA3). For no encryption, it is GEA0. According to Perez & Pico (2011), users and service provider's networks could be attacked when service is rendered with GEA0. An attacker could use a rogue BTS to convince the victim mobile station to send and receive all information that is unencrypted.

3.7.3. MBB Layer Two VPN

Introduction

It allows businesses to extend Ethernet services such as virtual LANs (VLANs) across L3 MPLS network.

The Internet Service Provider (ISP) supporting this service is seen as a virtual Layer two Switch.

Layer two VPN could be Point-To-Point or Point-To-Multipoint

The Layer Two VPN implementation detail at the internet service provider domain is outside the scope of this thesis since the thesis interest lies in its utilization by the MBB technology, i.e. MBB over L2 VPN service.

The design shown in Figure 3.23 depicts a Virtual Private LAN Service at various locations of a business i.e. MBB with an APN that is linked by a L2VPN.

Objective

The aim of this experiment is to interconnect various sites of a virtual office LAN with MBB 3G technology over a layer two virtual private network.

Setup and Configuration

Setup Description

Four remote sites of an office with MBB compatible nodes as gateways. The sites are interconnected by a Layer-2 VPN service by an ISP.

IP Plan

Table 3.3: Layer-2 VPN LANs

LANs		
Network Name	IP	MAC Address
MBB	192.168.50.0	255.255.255.0

Site-1	10.10.10.0	255.255.255.0
Site-2	10.10.20.0	255.255.255.0
Site-3	10.10.30.0	255.255.255.0
HQ	10.10.40.0	255.255.255.0

Table 3.3 portrays the various network IP used for the design of the MBB over the layer-2 VPN. These network IPs fall within the range of the standard class A IP version 4 address range. The default mask, which determined the network, is 255.0.0.0. To avoid IP waste, the network IP ranges chosen have been sub netted with the mask 255.255.255.0.

Table 3.4: Layer-2 VPN Nodes

NODES			
Node	IP	MAC Address	Comment
S1-GW	192.168.50.1	255.255.255.0	MBB LAN
S1-GW	10.10.10.1	255.255.255.0	Site-1 LAN
S2-GW	192.168.50.2	255.255.255.0	MBB LAN
S2-GW	10.10.20.1	255.255.255.0	Site-2 LAN
S3-GW	192.168.50.3	255.255.255.0	MBB LAN
S3-GW	10.10.30.1	255.255.255.0	Site-3 LAN
HQ-GW	192.168.50.4	255.255.255.0	MBB LAN
HQ-GW	10.10.40.1	255.255.255.0	Head Office LAN
Host 1	10.10.20.2	255.255.255.0	
Host 2	10.10.20.3	255.255.255.0	

Host 3	10.10.10.2	255.255.255.0	
Host 4	10.10.10.3	255.255.255.0	
Host 5	10.10.30.2	255.255.255.0	
Host 6	10.10.30.3	255.255.255.0	
SERVER-1	10.10.40.2	255.255.255.0	
SERVER-2	10.10.40.3	255.255.255.0	

Table 3.4 is a record of how IP addresses were assigned to various nodes for the design. Each

IP nodes is contained within its network by applying the defined networks in Table 3.3.

Network Setup

The IP network was setup using the virtual network emulator, GNS3.

Routing protocol used is OSPF.

Figure 3.24 is the network setup for the experiment

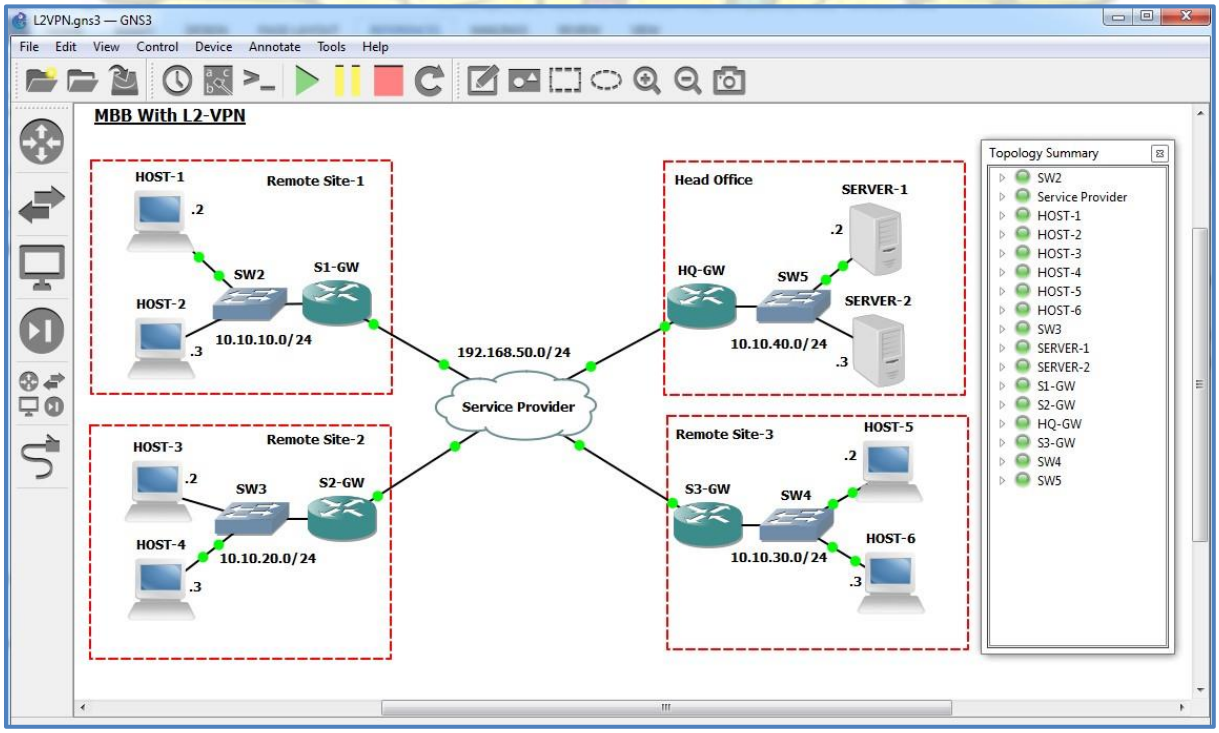


Figure 3.24: MBB Over Layer -2 VPN

IP Network Simulation

The network is made to run and ping tests were conducted to verify whether IP packets transmission among various sites were successful.

Figure 3.25 , Figure 3.26 and Figure 3.27 are tests results obtained from the MBB over L2-VPN experiment.

Ping Test: From S1-GW to HQ-GW

Pint test was performed from site one gateway router to head office gateway router to confirm successful connectivity between the two nodes. The ping test performed was successful.

```
S1-GW#ping 10.10.40.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.40.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/29/32 ms
S1-GW#
S1-GW#ping 192.168.50.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.50.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/33/44 ms
S1-GW#
```

Figure 3.25: Ping Test S1-GW To Head Office

Ping Test: From S1-GW to Head Office SERVER-1

```
S1-GW#ping 10.10.40.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.40.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/52/72 ms
S1-GW#
```

Figure 3.26: Ping Test S 1-GW To HQ -GW

Ping Test: SERVER-1 to HOST-1

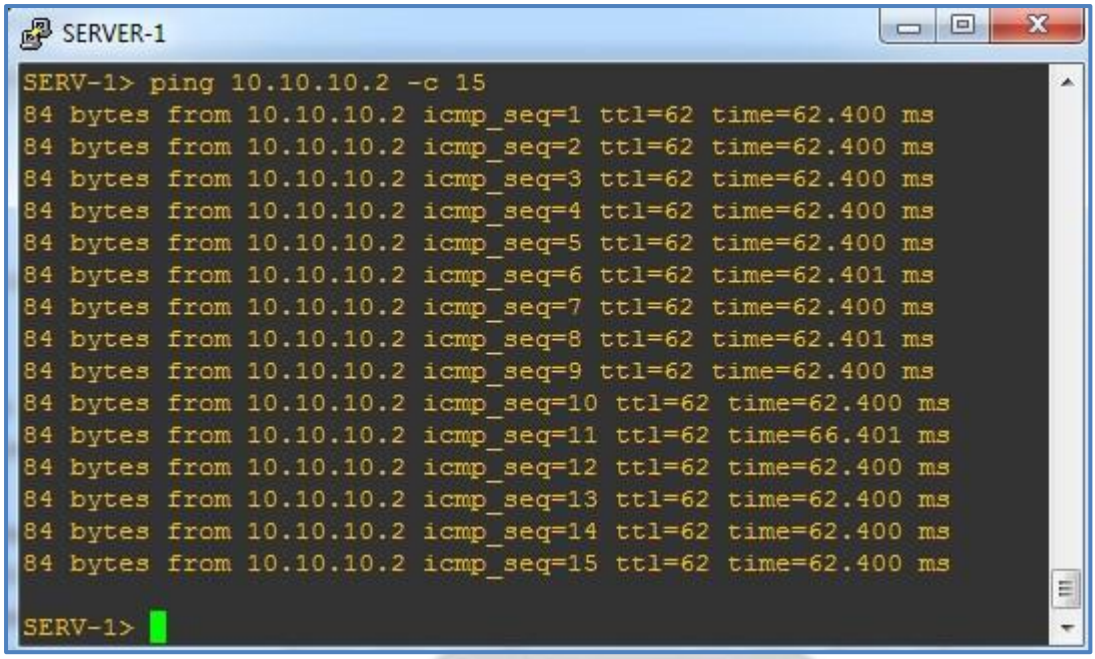


Figure 3.27: Ping of Test Server-1 To Host-1

3.7.4. MBB Layer Three VPN

Setup Description and Configuration

Figure 3.28 is screenshot of the implementation setup with GNS3 network Simulator.

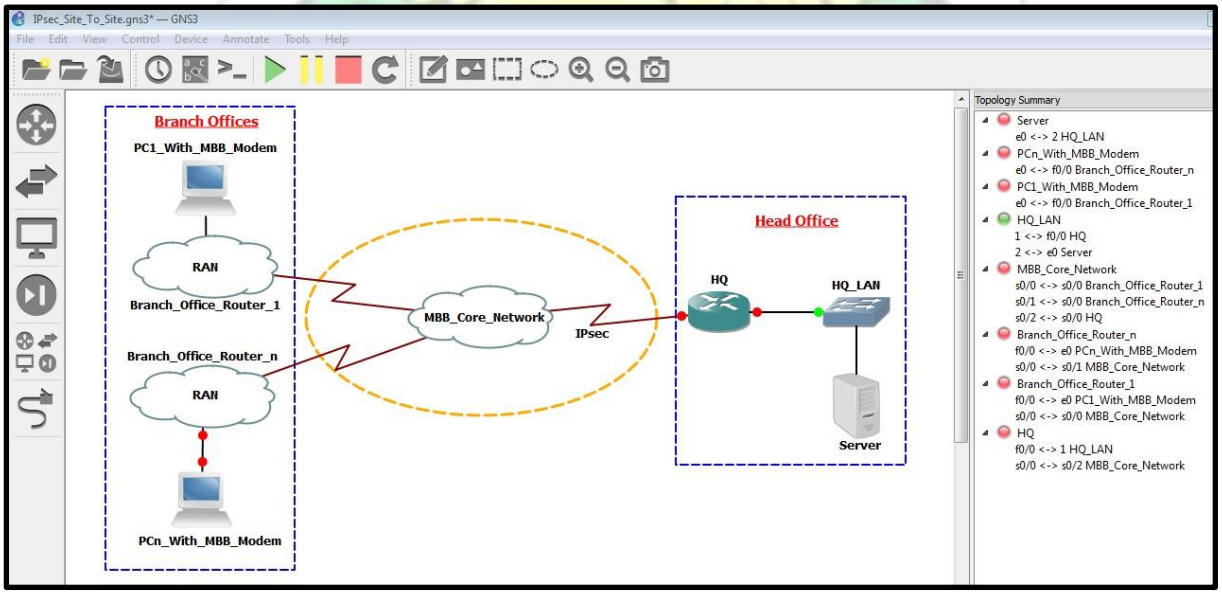


Figure 3.28: MBB IPsec Tunnel

- PC1, PC2 and Server are Virtual PC terminals embedded in GNS3 simulator.

- The clouds, RAN and MBB core are a type of known GNS3 Qwemu. Quemu is a generic and open source machine emulator and virtualizer capable of running various Internetworking Operating Systems. For the purpose of thie project, Cisco "IOS (tm) 2600 Software (C2691-ADVENTERPRISEK9-M), Version 12.3(17a), RELEASE SOFTWARE (fc2)" was ran on them to meet the objective of the experiment.
- HQ, a router, is also a GNS3 Quemu on which the above Cisco IOS was run on to meet the objective of the experiment.
- OSPF dynamic protocol was deployed on each interface that links the various nodes in the virtual network.
- The WAN (representing a public network for this experiment) transport protocol used between the RAN and MBB core network; MBB and HQ is Frame Relay
- A dynamic routing protocol, OSPF, was used for the setup
- The IPsec VPN was setup between the MBB core network and the Head Office edge node, HQ
- The MBB PCs automatically acquired static IPs (Dynamic IPs could be used depending intended usage) from APN MIT.com address pool 192.168.100.0/24.
- A point-to-point WAN (internet could be used) was setup between the MIT office and service provider firewalls with IP block 10.10.10.0/30. 10.10.10.1/30 for service provider Firewall and 10.10.10.2/30 for MIT Office Firewall.
- IP block used for MIT Office LAN is 172.16.100.0/24. The servers were assigned static IPs from this IP block.

PC1 with MBB Modem

The following are configuration details of unique nodes within the experimental setup
PC1, PC2 and Server VPC terminals have similar configurations with the exception of their IPs and MAC addresses. In this regard only PC1 configuration is shown to avoid repetition.

Table 3.5: VPC Terminals

VPCS>
NAME : VPCS[1]
IP/MASK : 192.168.1.2/24
GATEWAY : 192.168.1.1
DNS :
MAC : 00:50:79:66:68:01
LPORT : 10003
RHOST:PORT : 127.0.0.1:10002
MTU: : 1500
VPCS>

Table 3.5 shows detail parameters used for the virtual PC with name VPCS in the design.

Observation

The implemented IPsec network was simulated and the following were observed as shown Figure 3.29.

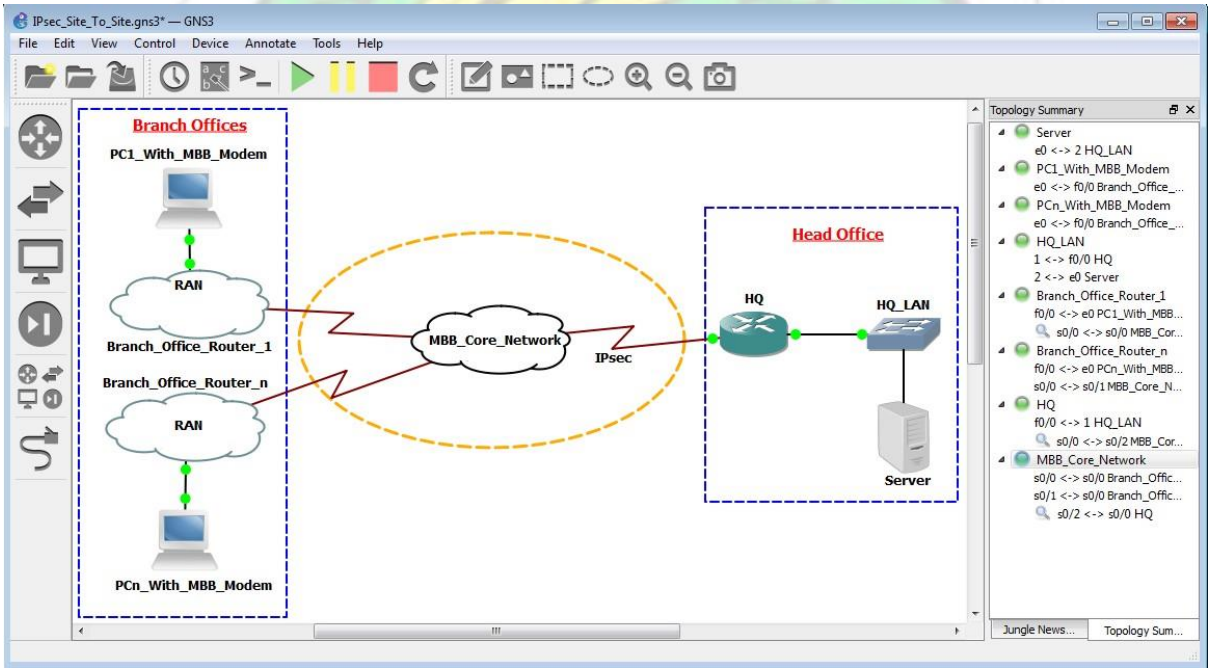


Figure 3.29: Simulated IPSec Network

During network simulation mode, Wireshark traces were setup on the following interfaces.

- Branch_Office_Router_1 to MBB_Core_Network. Frame Relay link
- MBB_Core_Network to HQ. IPsec segment.

The following were observed for MBB _Core_Network to HQ

Packets were able to be transported from the Branch Office to the Head Office over the IPsec VPN tunnel. Figure 3.30 is a screen shot of twenty ICMP packet transmitted as test of the setup. The packets successfully reached the destination.

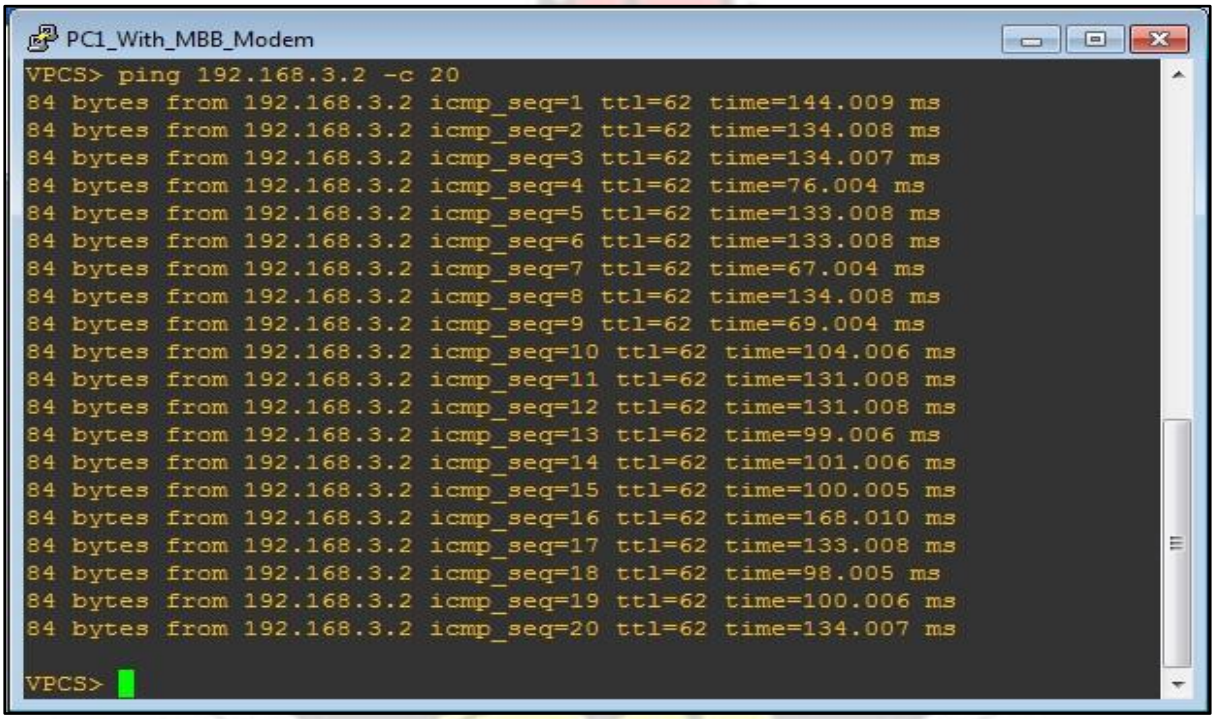


Figure 3.30: IPSec Ping Test

Whiles the packets were in transit, with the help of Wireshark protocol capture and analyser, trace was setup on MBB_Core_Network to HQ segment of the network to verify the packets encapsulation over the IPsec VPN tunnel. Figure 3.31 screenshot, the protocol field, confirmed packets were really encapsulated by a member of the IPsec protocol suite, i.e. the Encapsulation Security Payload (ESP) .

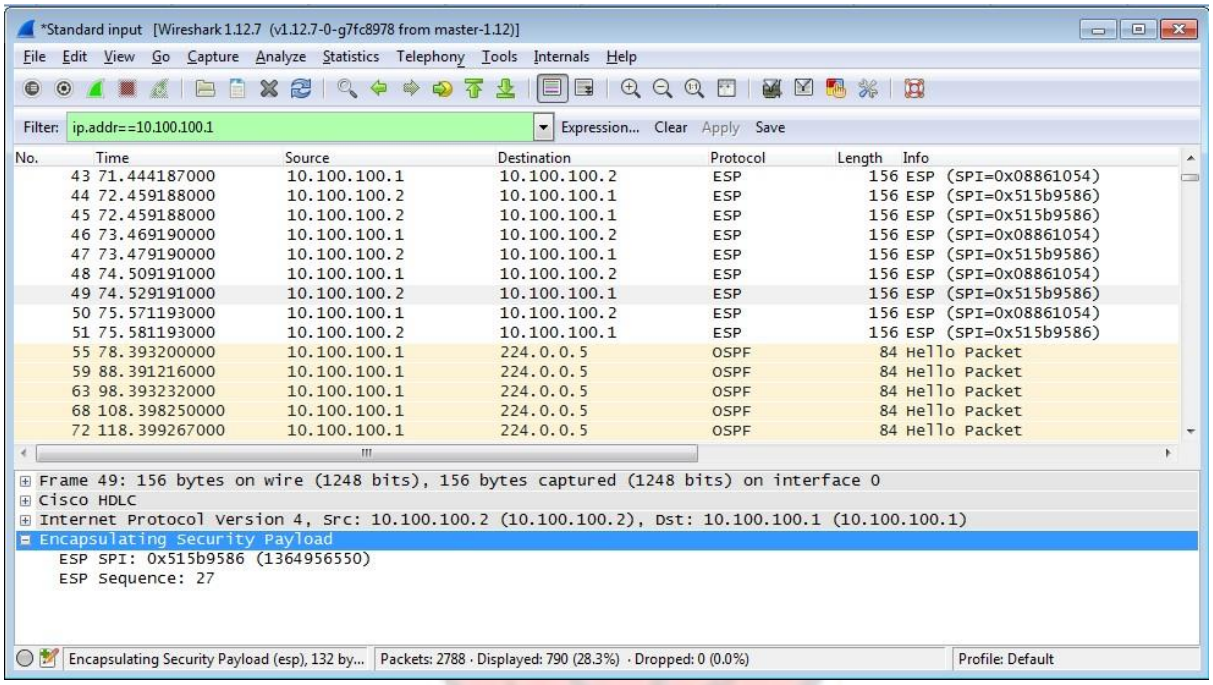


Figure 3.31: IPSec Encapsulation Payload

IPsec packets are protected. The part of the IPsec protocol suite that provides packet protection is the encapsulating security payload.

The dynamic routing protocol, OSPF was at hand to making sure packets locate their path to the right destination.

In addition to the packets verification in relation to the right protocols, a debug trace was set up on either nodes of the IPsec tunnel to further ensure packets are rightly being treated as they should. Figure 3.32 is a sample debug trace taken on MBB_Core_Network node:

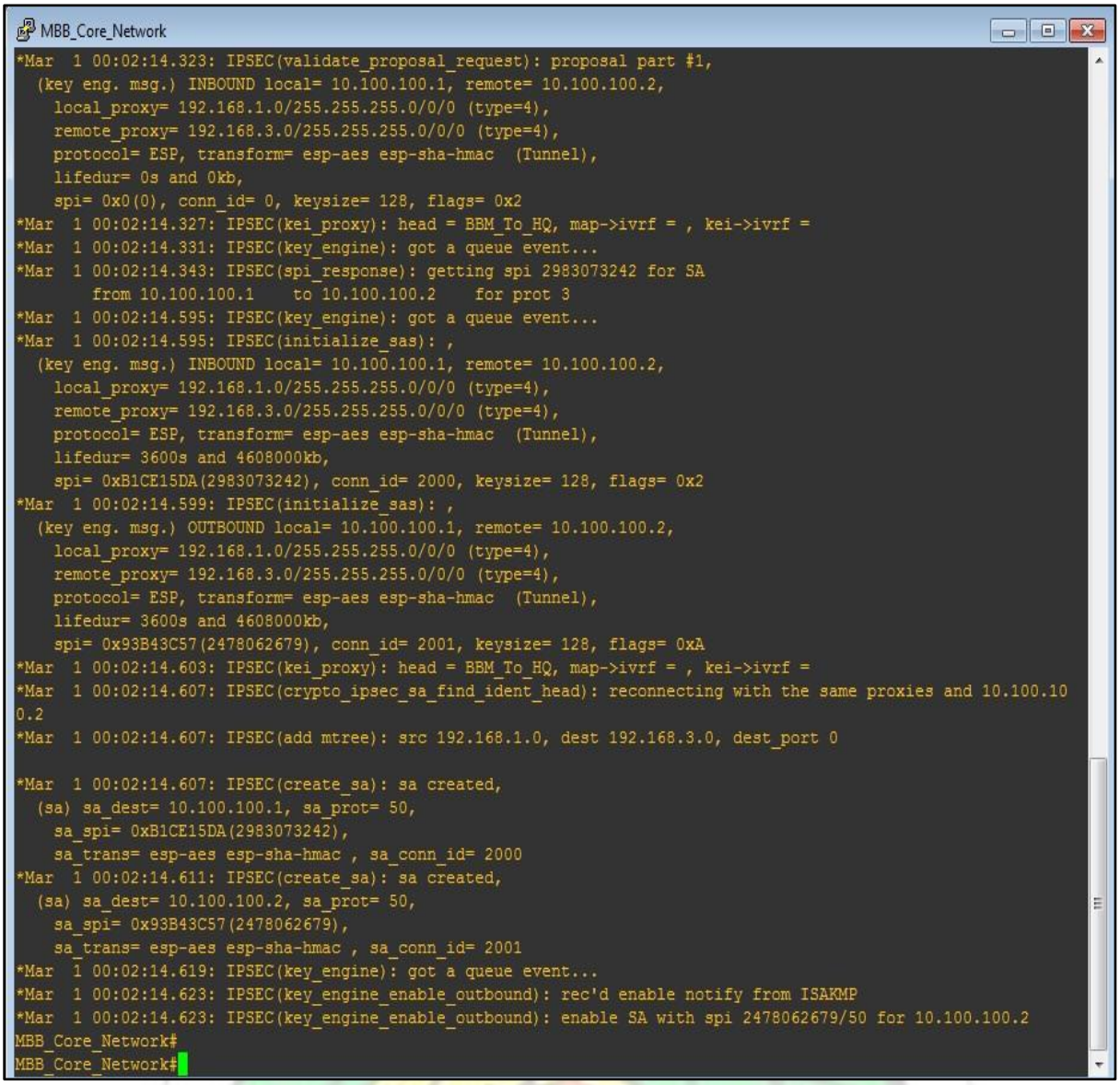


Figure 3.32: IPSec Debug Trace

Conclusion

MBB provides flexibility, especially for source of IP packet origination, to have data transmitted over IPsec tunnel from a source to a desired destination.

The experiment confirmed the ability to use IPsec VPN as a means of linking remote sites by using MBB protocols such as HSPA+, 3G etc to setup WAN IP networks

3.7.5. MBB IPsec VPN Tunnel

Introduction

Virtual Private Networks (VPN) act like a private leased line. VPNs use the public network, internet or wide area network, to securely transmit packets from one end to the other.

There are several ways in accomplishing the extension of networks over unsecure networks. This implementation would focus on IPsec VPN tunnel, a site-to-site VPN type, as means of extending a 3G IP network from say a corporate network to a branch office.

What make VPN private is the ability of this technology to hide communicating nodes over a public network, example wide area network.

Objective

The objective of this experiment is to securely link various office sites where ever they may be in this world once there is internet with MBB technology over IPsec technology.

Setup Description and Configuration

The general parameters and conditions to be met for setting up IPsec tunnel were spelt out under the design topic MBB Local Sites To WAN By IPsec in 48.

Figure 3.33 is the setup used for the experiment in running mode.

It is a screenshot of the virtual lab setup to investigate how the mobile broadband could be used to ride on IPsec technology as medium to link various remote sites. The PC with MBB modem was used to depict how an office with MBB compatible devices could connect to the Radio Access Network of the MBB wireless network and have it linked to another remote site using IPsec.

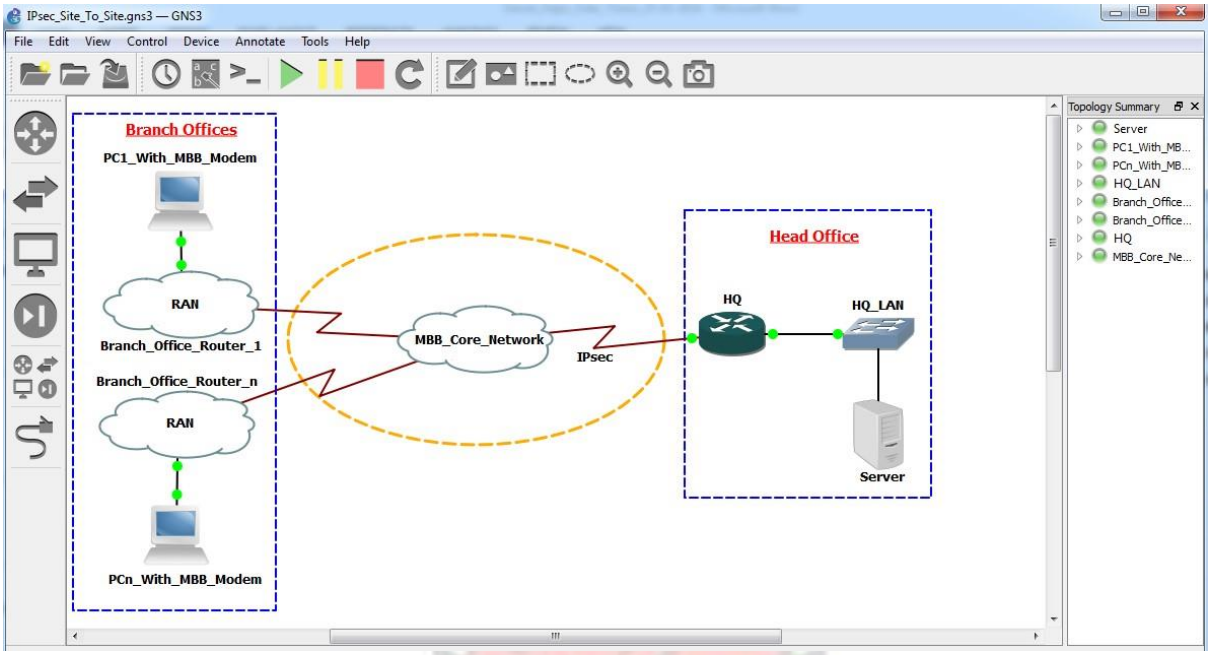


Figure 3.33: Setup - IPSec

For this experiment, the following specific parameters were used at both ends.

MBB Core

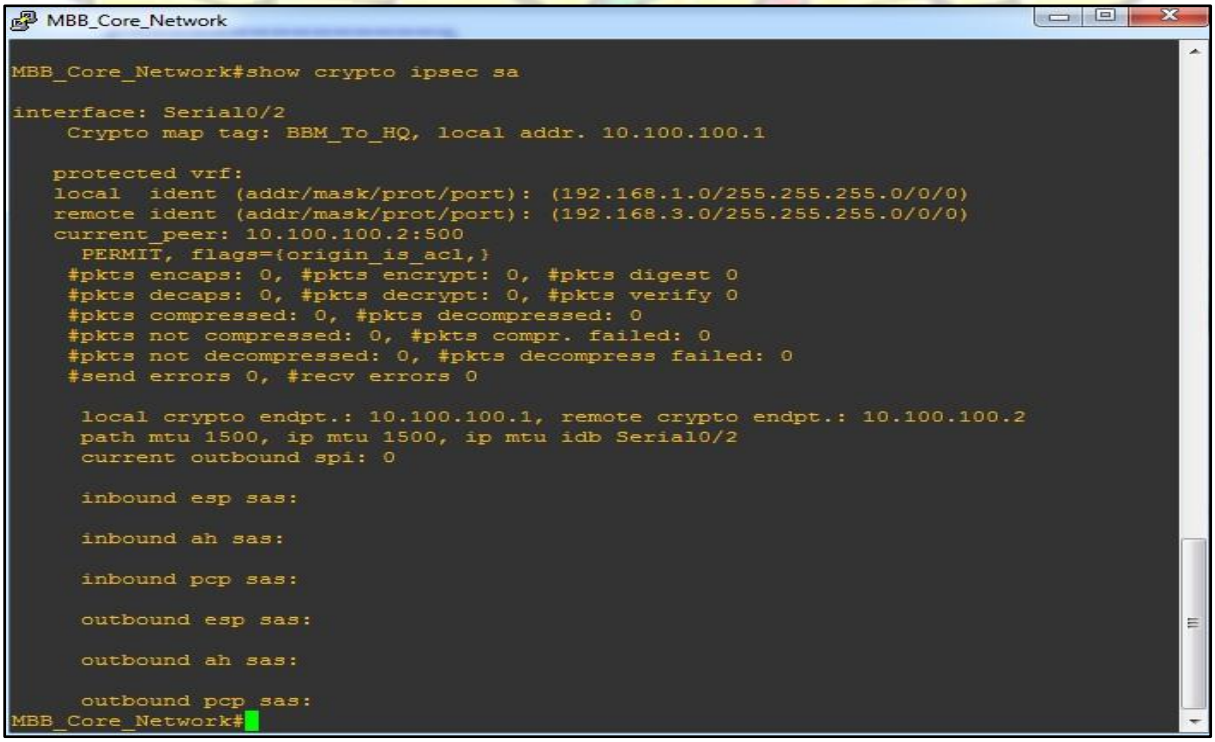


Figure 3.34: IPSec Parameters - MBB Core

Test: Branch Office to HQ

The following ping test was performed from the branch site to the head office over the IPsec VPN tunnel.

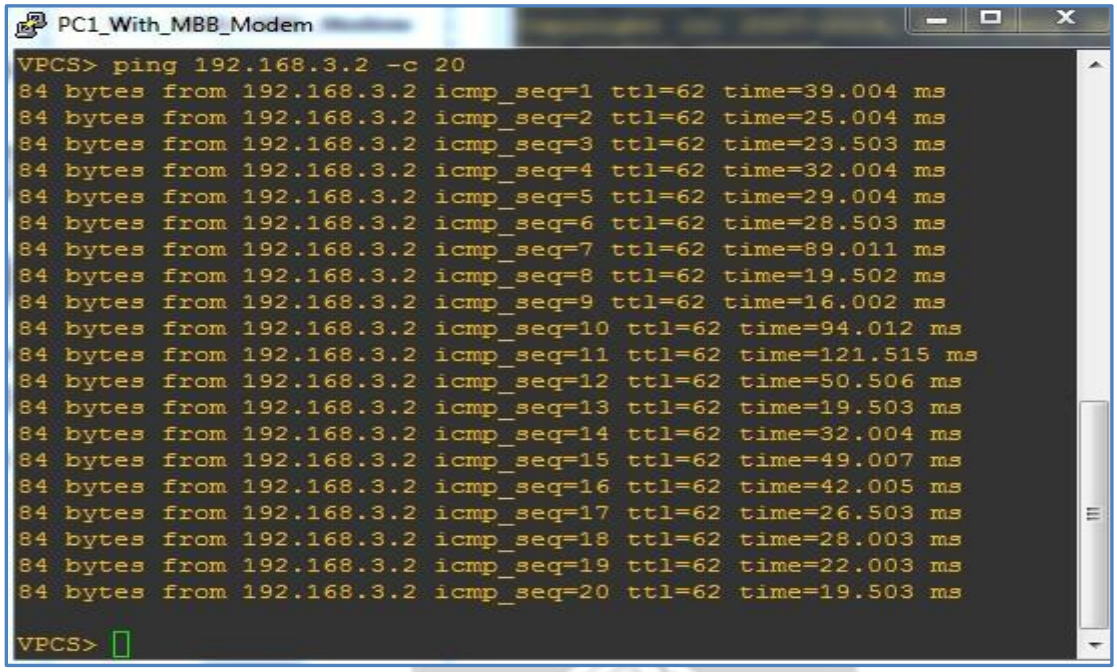


Figure 3.35: IPSec Test

HQ

Figure 3.36 is a screenshot of the parameters used to setting up the IPsec at the HQ remote site.

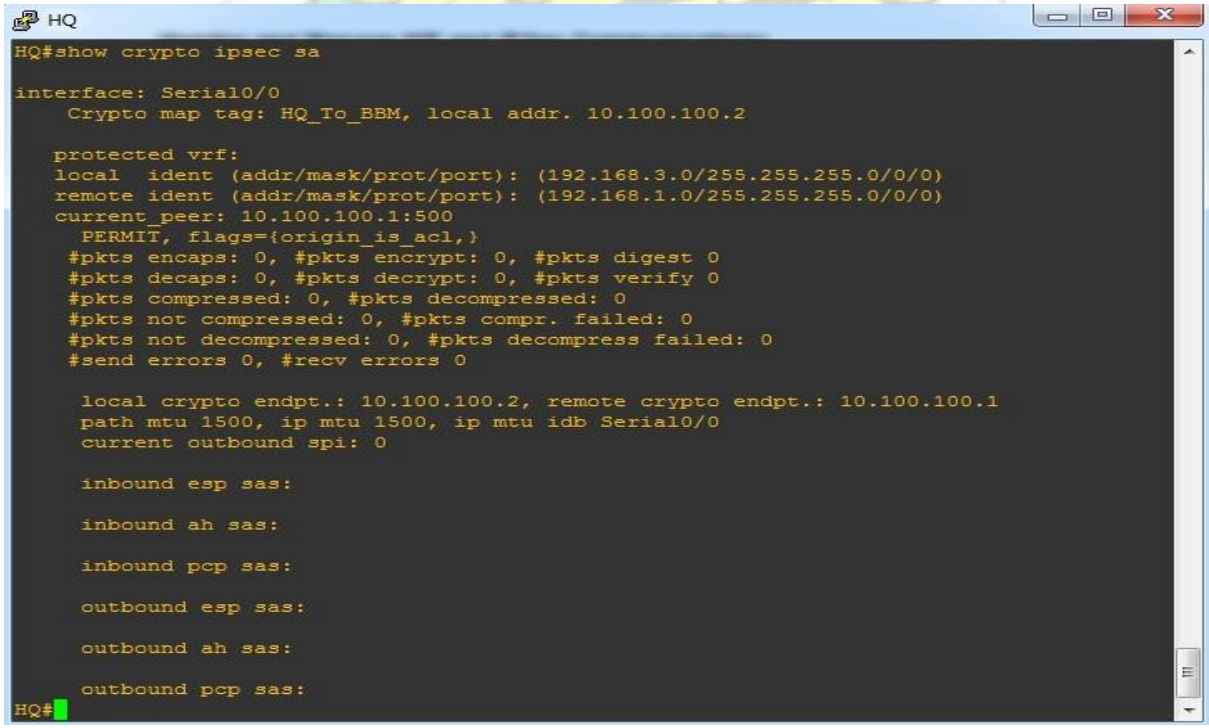


Figure 3.36: IPSecParameters - HQ

Observation

It was observed from the test conducted that, ICMP packets were transmitted successfully from the branch office to the head office.

3.8. The Fixed Broadband (FBB)

The main focus of the thesis is actually about MBB but certain important parameters about FBB which appeal to users were captured to serve as basis for comparison, when needed, for MBB. Figure 3.37 is a traceroute test performed with FBB.

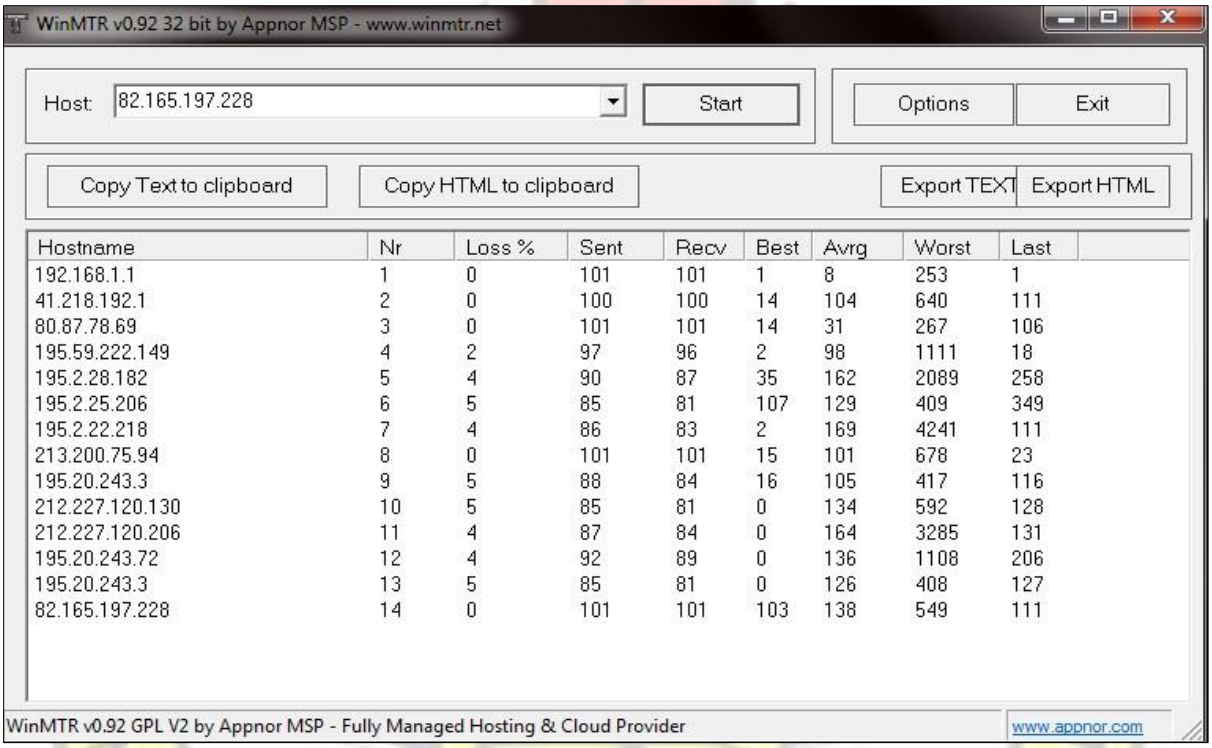


Figure 3.37: FBB Traceroute To radiotest.eu

3.8.1. Traceroute Packet Capture with Wireshark

The test was performed with a computer connected to wireless ADSL modem with internet facility.

Whiles the test was being performed, packets to and from the destination IP@82.165.197.228 were captured. Figure 3.38 is a screenshot of the captured packet.

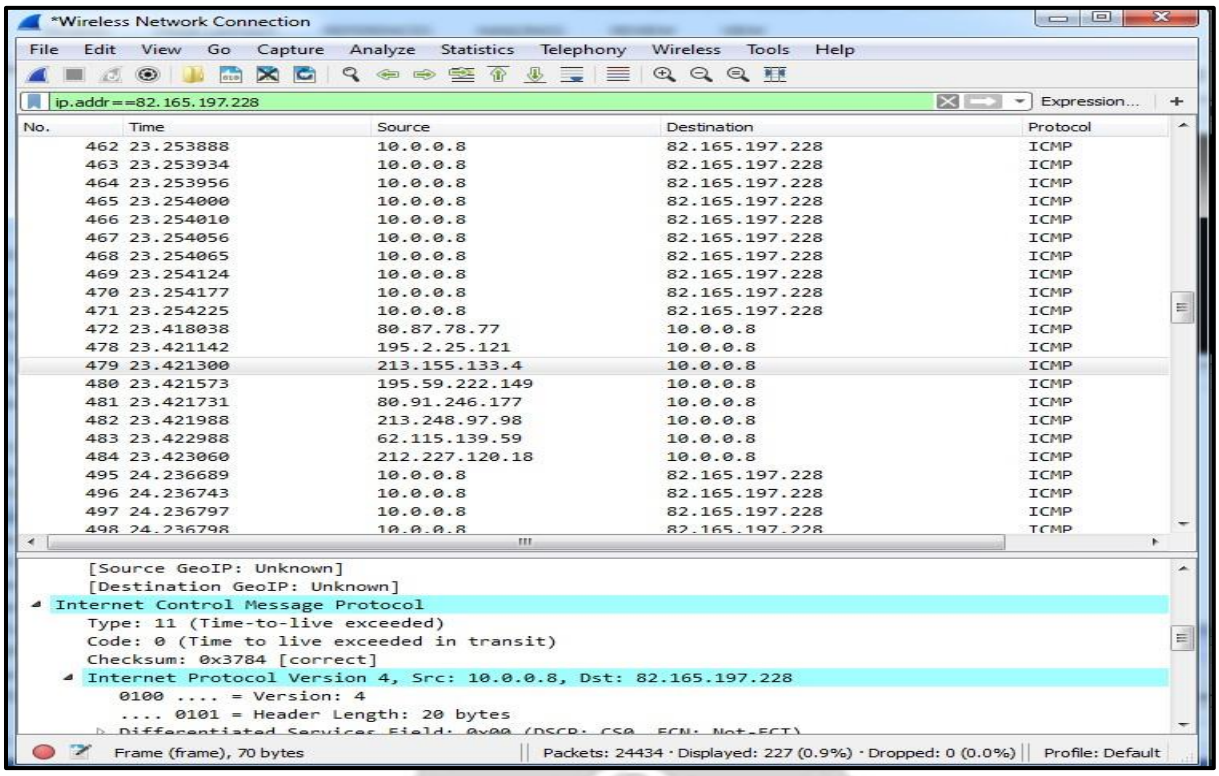


Figure 3.38: FBB Packet Capture

3.8.2. FBB Packet Quality Test

10MB of data was downloaded from Radio Test site http://radiotest.eu/HTTP_DL01/ using FBB service. Whiles the HTTP test was being performed, a Wireshark trace was simultaneously taken as shown in Figure 3.4

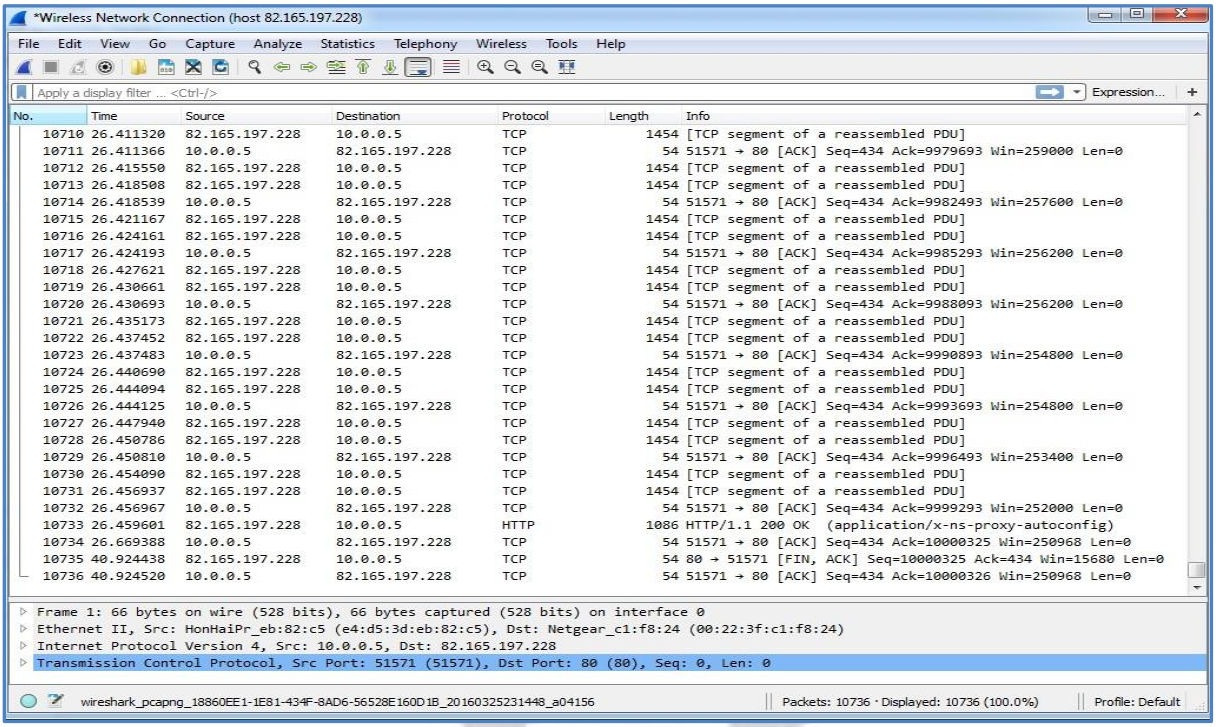


Figure 3.39: FBB Download Trace Capture

3.8.3. Sample FBB Summary Result

Table 3.6: FBB Download Summary

TIME	CAPTURE	STATISTICS
First packet: 2014-10-08 00:18:28 Last packet: 2014-10-08 00:18:58 Elapsed: 00:00:30	Dropped packets: unknown Capture filter: unknown Link type: Ethernet Packet size limit 262144 bytes	Packets: 11012 Between first & last packet:30.005 sec Avg. packets/sec: 367.009 Avg packet size: 974.286 bytes Bytes: 10728839 Avg bytes/sec: 357571.448 Avg Mbit/sec: 2.861

Table 3.6 is a summary result obtained for the HTTP download over the FBB service. The download elapsed for 30 seconds. There were no packet drops. The average packet size during the download test was 974.286 bytes per second. The everage download speed obtained was

2.861Mbps.

CHAPTER 4. ANALYSIS & INTERPRETATION

4.1. Introduction

The makeup of this chapter is the analysis and interpretation of the experimental findings of this thesis. This thesis is intended to research into how to design and implement IP networks with Mobile Broadband technology for businesses as alternative to Fixed Broadband technology which is very popular and widely embraced by businesses and individual users.

The objective of the study was to focus on the following broad areas which were considered as adequate to bring to the fore how businesses could link their various office locations with the MBB technology.

- SIM-To-SIM communication
- MBB with IPsec Virtual Private Networks
- MBB with Layer Two Virtual Private Networks and
- MBB with Layer Three Virtual Private Networks

The analysis of the methodology outcomes have been segmented into two:

- Speed, throughput and quality of service tests for both FBB and MBB carried on the service provider's live network.
- Network Protocols, Pings, quality of service test for implemented MBB designs carried with the aid of GNS3, the virtual environment for network design and simulation, The other aspect of the analysis focused on the responses obtained from the questionnaire prior to the start of this thesis.

Before the experiments were carried out, various preliminary tests were performed on the MMB chosen network to ensure no bottlenecks existed. Results obtained, as evidenced in chapters 3.8.1 and 3.8.2 showed no packet loss within the operator's network.

IP hops that belonged to the Operator's network, From "No response from host" to 194.112.78.177, where near zero packet loses as observed from the experiment carried out in Figure 3.2. The packet percentage loss observed were within acceptable limits. The "No response from host" is actually a live node whose IP is hidden from the public for security reasons as explained by the service provider. The test was successful and the result obtained was as expected.

4.2. Mobile Broadband (MBB) Analysis

4.2.1. MBB: Throughput and QOS

The sequence numbers is a representative of the number of received over time (in seconds) in one direction. The direction could either be upload or download. The graph in Figure 4.1 is a result of the HTTP download for MBB. The steeper the slope, the faster the download. 10MB of data was downloaded within 20 seconds.

As expected, there was an initial delay before the downloaded commenced. Unlike FBB, it is quite normal within the MBB space to have such little initial delay due to contention of resources by users. The results was further analysed to get further insight into the initial round trip delay as shown in Figure 4.1

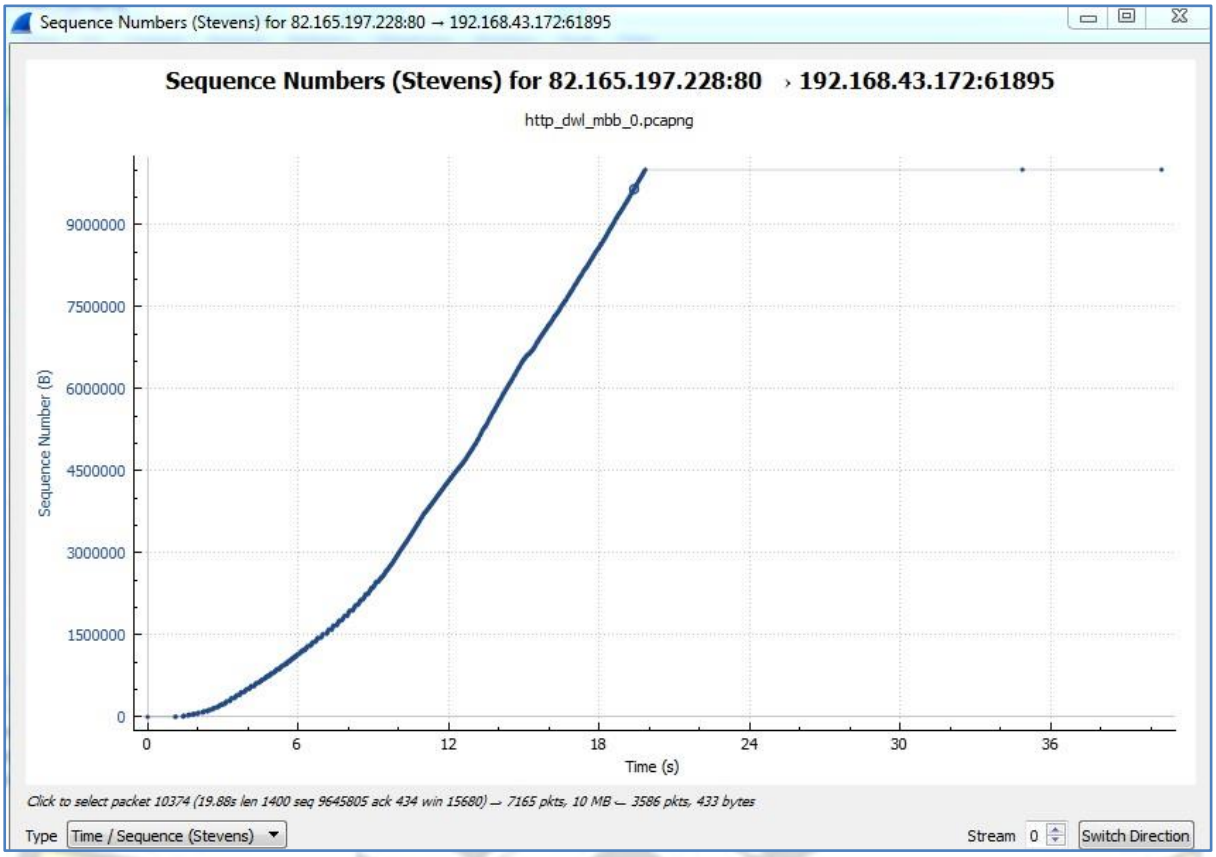


Figure 4.1: MBB Throughput and QoS

Wireshark's Steven's Time/Sequence graph tool was used to analysing above TCP download quality result. The steeper slope of the graph shows faster and steady TCP packet download as revealed by Chris. (Sanders, 2011). It is evident that the download time was shorter as compared to what was obtained for FBB. This result would certainly not be the same under all conditions. Where radio resource are scarce, certainly different result, which may not meet expectation, would be obtained.

The above result means, MBB under good radio resource condition could be used as an alternative to FBB. To further enforce the deductions made, the trace was further subjected to analysis to measure the speed of download within the shorter time obtained.

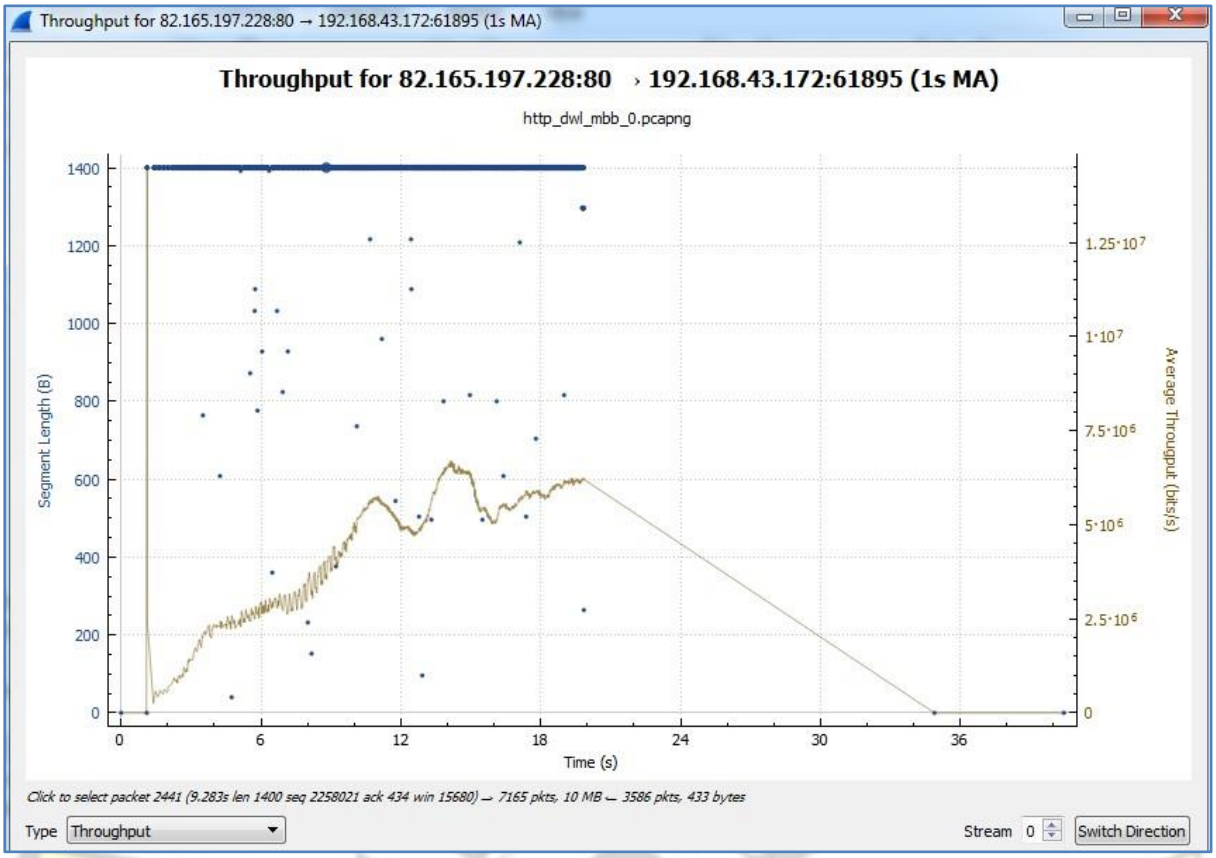


Figure 4.2: MBB Speed Analysis

There was an initial spike in throughput of about 13Mbps. This would not be factored in the analysis though worth mentioning to support earlier deductions made about MBB performing very well under good radio resource availability. Aside the spike, an impressive throughput of about 6Mbps was obtained.

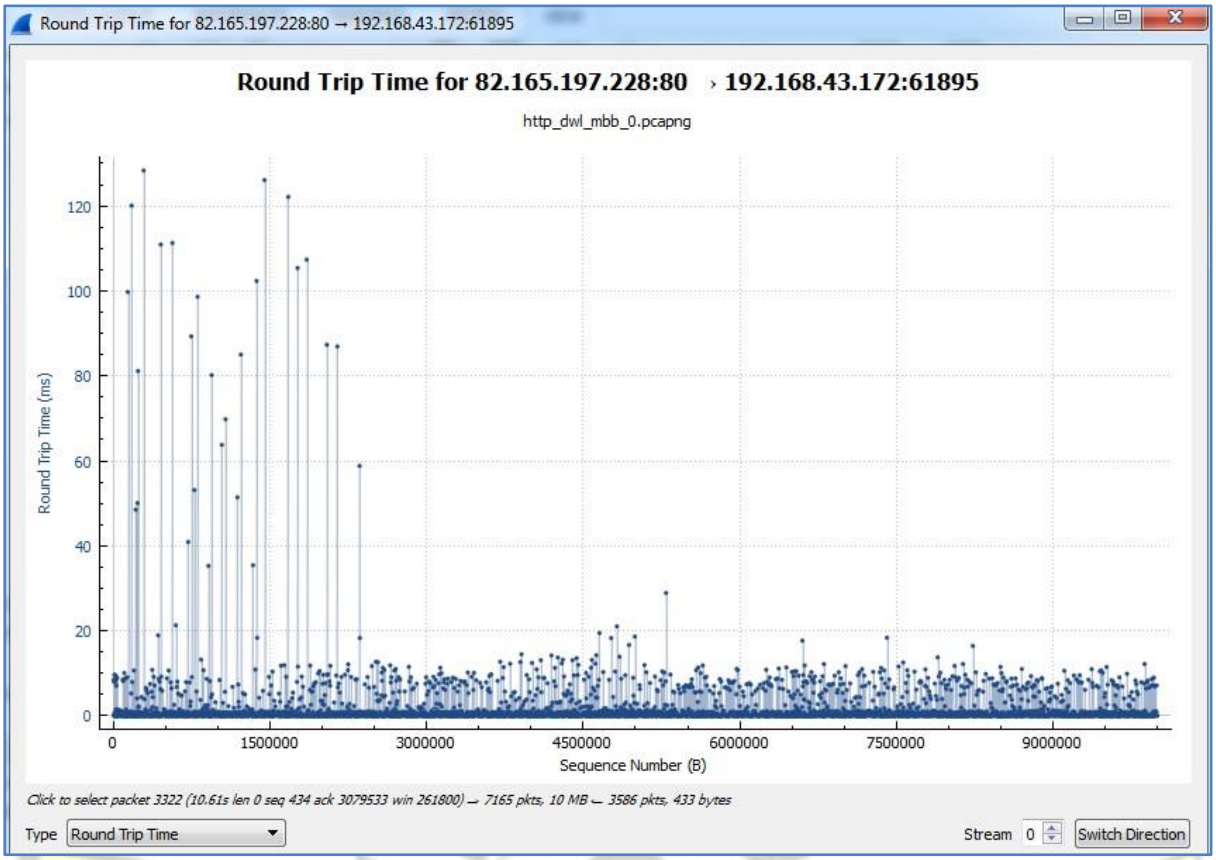


Figure 4.3: MBB Initial Round Trip Delay

Theoretically, HSPA+ could offer a maximum download speed of about 42Mbps.

The round trip time graph also revealed that, about two megabytes (2MB) of the downloaded data suffered maximum delay of about 120ms. The cause of the delay could be attributed to resource contention which is synonymous with mobile data.

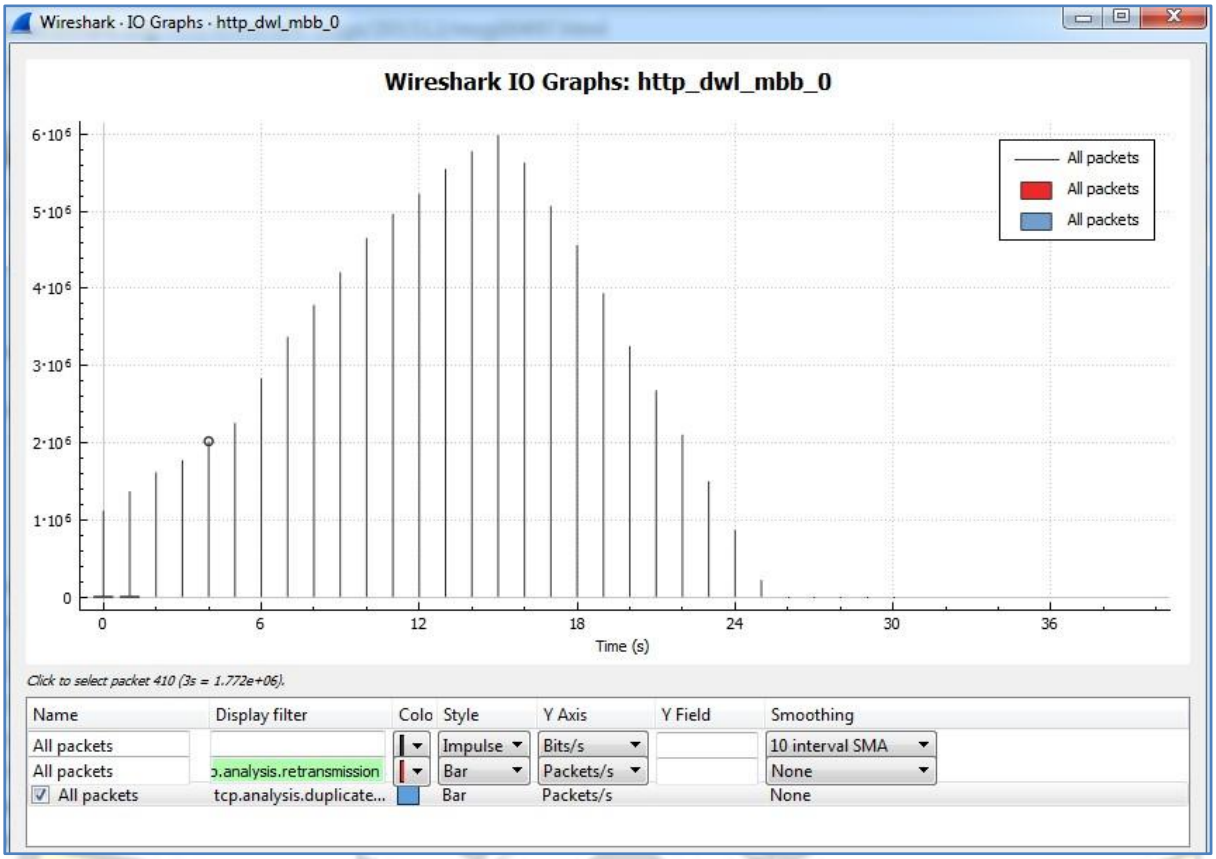


Figure 4.4: MBB QoS Analysis

Aside the initial expected results for MBB download throughput and delay roundtrip analyses, there was virtually no incidents of TCP retransmissions and duplicate acknowledgements during download as shown in Figure 4.4 quality of service input/output graph. This reinforces the explanation that, the delay could be initial radio resource contention. Once the resource was acquired, the download was completed within expected time.

4.2.2. Unfavourable Result

Analysis of tests conducted in crowded areas where radio resource is limited due to the number of users contending for the same resource showed packet loses as expected. Figure 4.5 shows unfavourable data download pattern. An indication of packet loss as expected from a crowded area.

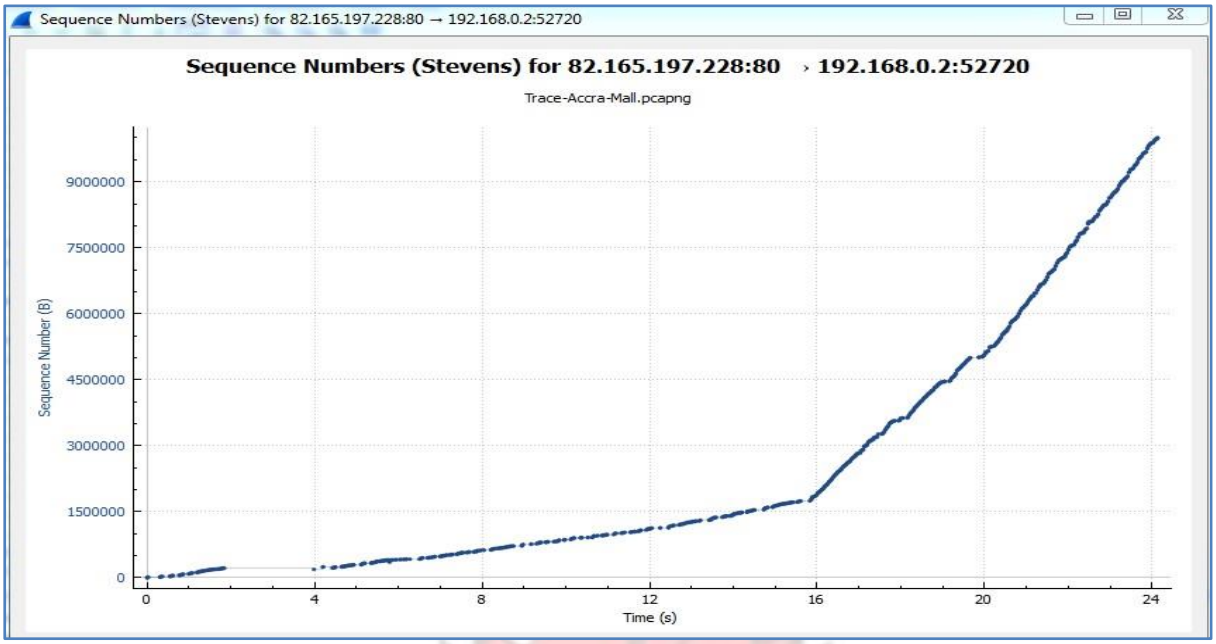


Figure 4.5: MBB Packet Loss

The download was really impacted. The breaks in the graph means packet losses. (Orebaugh et al., 2006). From the results obtained, it would not be advisable to use MBB in crowded areas for services within an IP network that demand greater speed and are critical without feasibility studies. This problem could be solved with more radio resource availability. The detail to this solution proposal is outside the scope of this study.

4.2.3. Analysis: MBB SIM-To-SIM Experiment

The objective of the experiments, i.e. SIM-to-SIM phase one and phase two were achieved. Each office site was able to communicate successfully with one another solely within the Radio Access Network space. The ping test performed were successful amongst the office sites. Analysis into the Internet Control Message Protocol (ICMP) packets sent from source to the other had successful response from the destination as expected.The objective was to be able to send packets from one user equipment as client to another where service if offered. The test was successful as expected. is a deeper look into one of the sample test performed from

IP@192.168.100.1 to IP@192.168.100.4 . This trace was taken simultaneously with the test in Figure 3.14 .

Figure 4.6: Ping Test UE-To-UE

The objective was to be able to send packets from one user equipment as client to another where service if offered. The test was successful as expected. Figure 4.7 gives an insight into ICMP packets requests from the source IP 192.168.100.1 to destination IP 192.168.100.4 with successful replies.

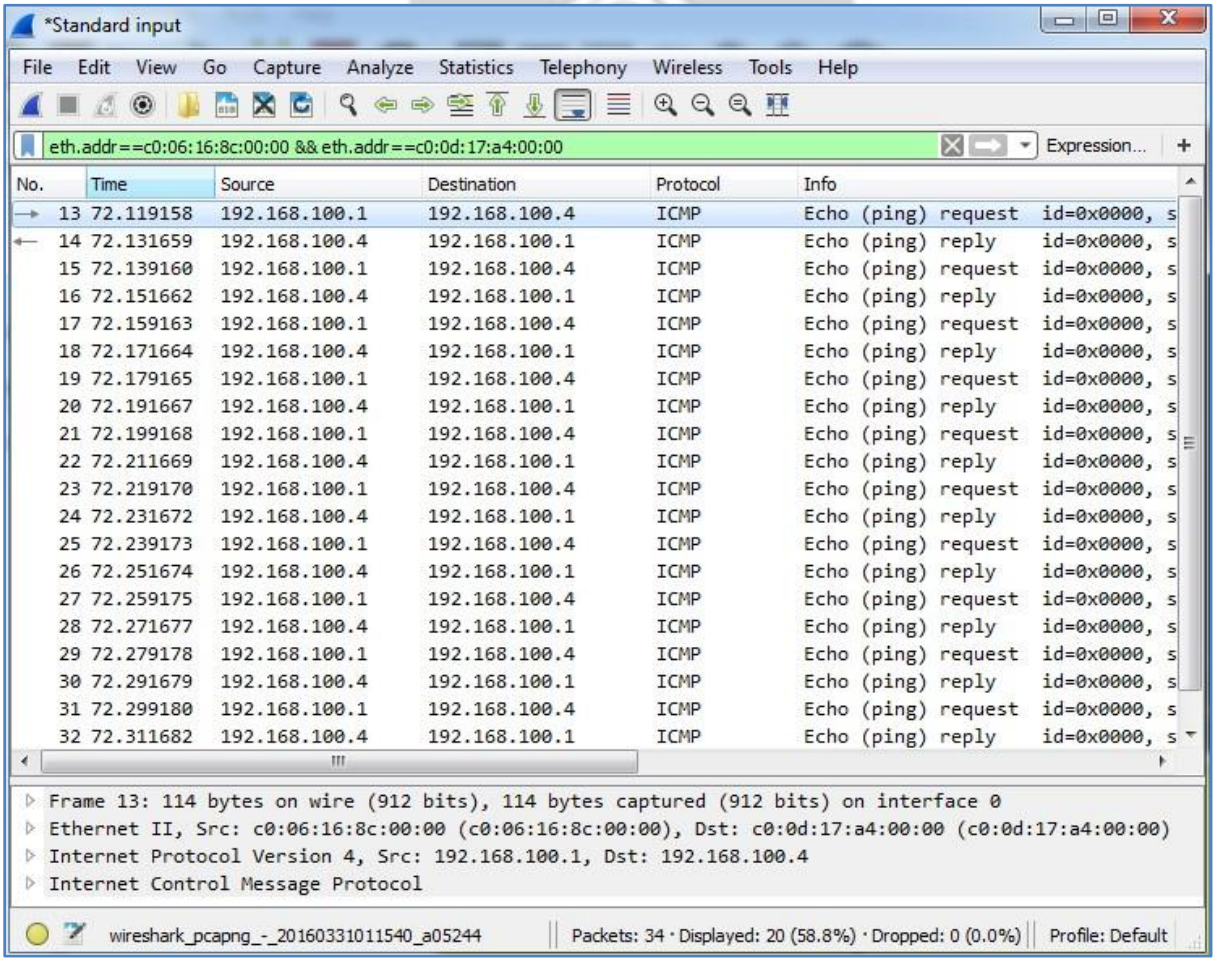


Figure 4.7: Analysis SIM -To -SIM

4.2.4. Analysis: MBB with IPsec Experiment

The objective of the test was realised, i.e. branch office and head office were able to communicate using MBB technology over the IPsec tunnel. This implies MBB traffic could be securely transmitted over IPsec tunnel.

Whiles the test was being performed, packets were captured for analysis to ensure the ICMP packets sent were encapsulated by the Encapsulation Payload (ESP) payload protocol of the IPsec protocol.

Figure 4.8 Shows detail of packets sent and their encapsulation.

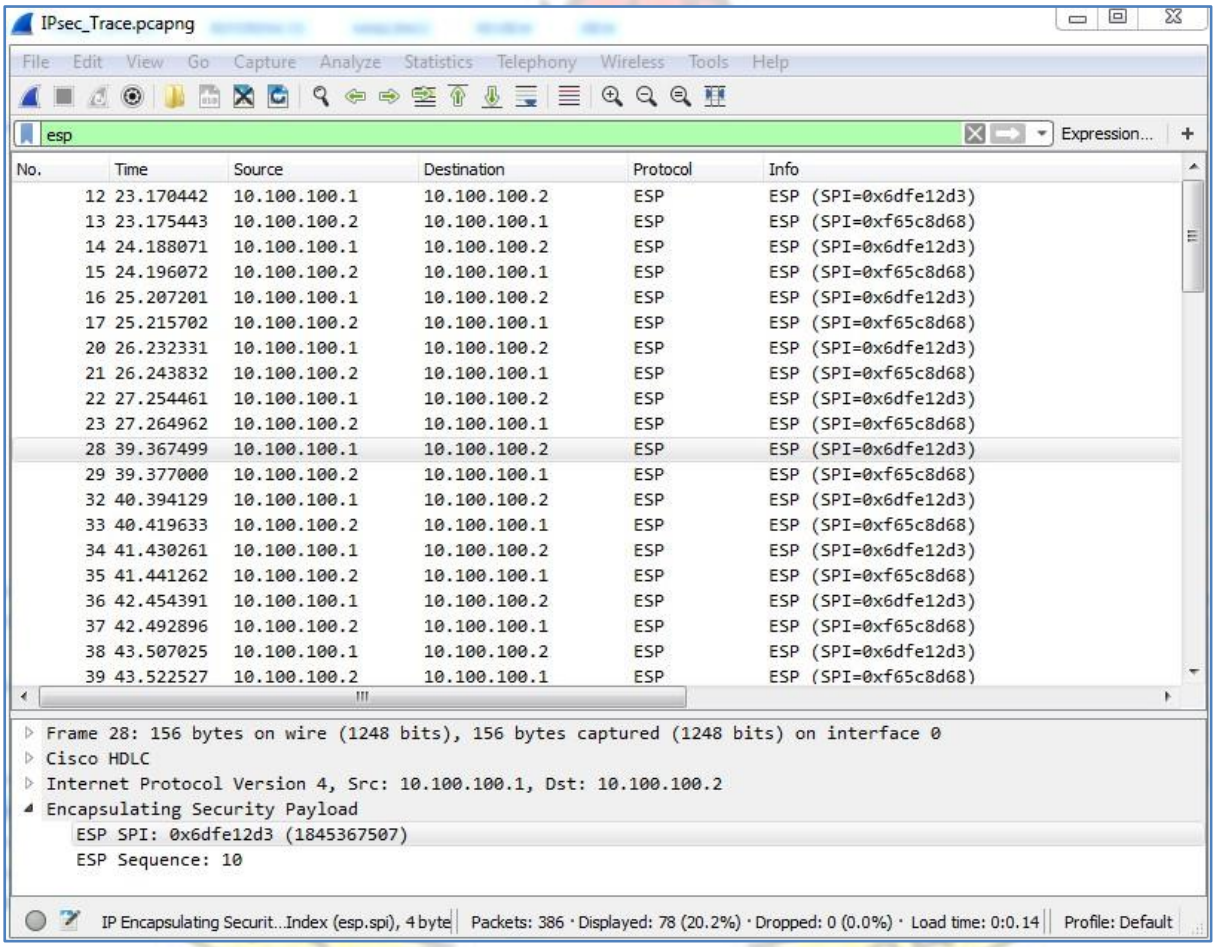
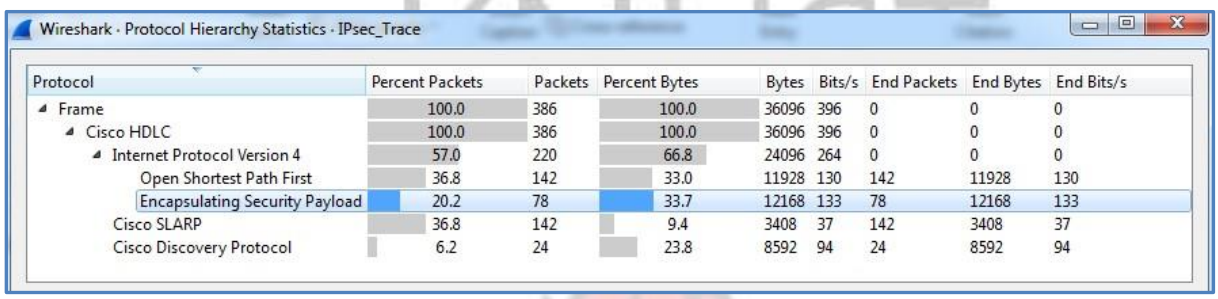


Figure 4.8: IPSec Encapsulation

Looking into the detail of packet number 28 with ESP sequence 10 in the detail panel, it could be observed that all packets have been enveloped. The protocol column is also not showing ICMP (real packets sent) but rather ESP.

To further ensure that the MBB packet were really encapsulated, the protocol hierarchy of the captured trace was scrutinised. Figure 4.9 shows the details of the protocols in the capture. No visible ICMP packets as expected.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	386	100.0	36096	396	0	0	0
Cisco HDLC	100.0	386	100.0	36096	396	0	0	0
Internet Protocol Version 4	57.0	220	66.8	24096	264	0	0	0
Open Shortest Path First	36.8	142	33.0	11928	130	142	11928	130
Encapsulating Security Payload	20.2	78	33.7	12168	133	78	12168	133
Cisco SLARP	36.8	142	9.4	3408	37	142	3408	37
Cisco Discovery Protocol	6.2	24	23.8	8592	94	24	8592	94

Figure 4.9: IPsec Protocol Hierarchy

4.2.5. Analysis: MBB Layer-2 VPN Experiment

Unlike the SIM-To-SIM experiment where the SGSN and the radio access network acted like a virtual LAN for the various remote office sites, the Layer-2 VPN has a MPLS network acting as virtual LAN for the remote office sites.

The sites were able to communicate with one another as expected.

4.2.6. Analysis: MBB Layer-3 VPN Experiment

The layer three setup is quite different from that of Layer-2 in terms of logic. Physically the implementations look quite similar. The difference as observed from the test is, the service provider has to implement IP routing within its network to enable the MBB traffic passage from one remote office site to the other. The tests conducted were successful as expected.

4.3. Fixed Broadband (FBB) Analysis

4.4. FBB Speed, Throughput and QoS Analysis

The purpose of the thesis is to design and implement IP networks with MBB technology as an alternative to FBB technology.

The throughput test was conducted to bring to the fore what MBB could offer as an alternative to FBB. Test detail: 3.6.4 MBB Speed/Throughput Obtained, Page 44

4.4.1. FBB: Throughput & QoS

The analysis was done with Wireshark inbuilt statistics tool.

The graph is plotted with packets sequence numbers against their arrival times. Theoretically the gradient represents the medium's bandwidth.

The graph in Figure 47 is a Time-Sequence graph that shows the tested data stream over time. Ten Mega Bytes of data was downloaded within 24 seconds as shown in the graph. The slope is quite steady that depicts favourable download condition within the FBB network as expected.

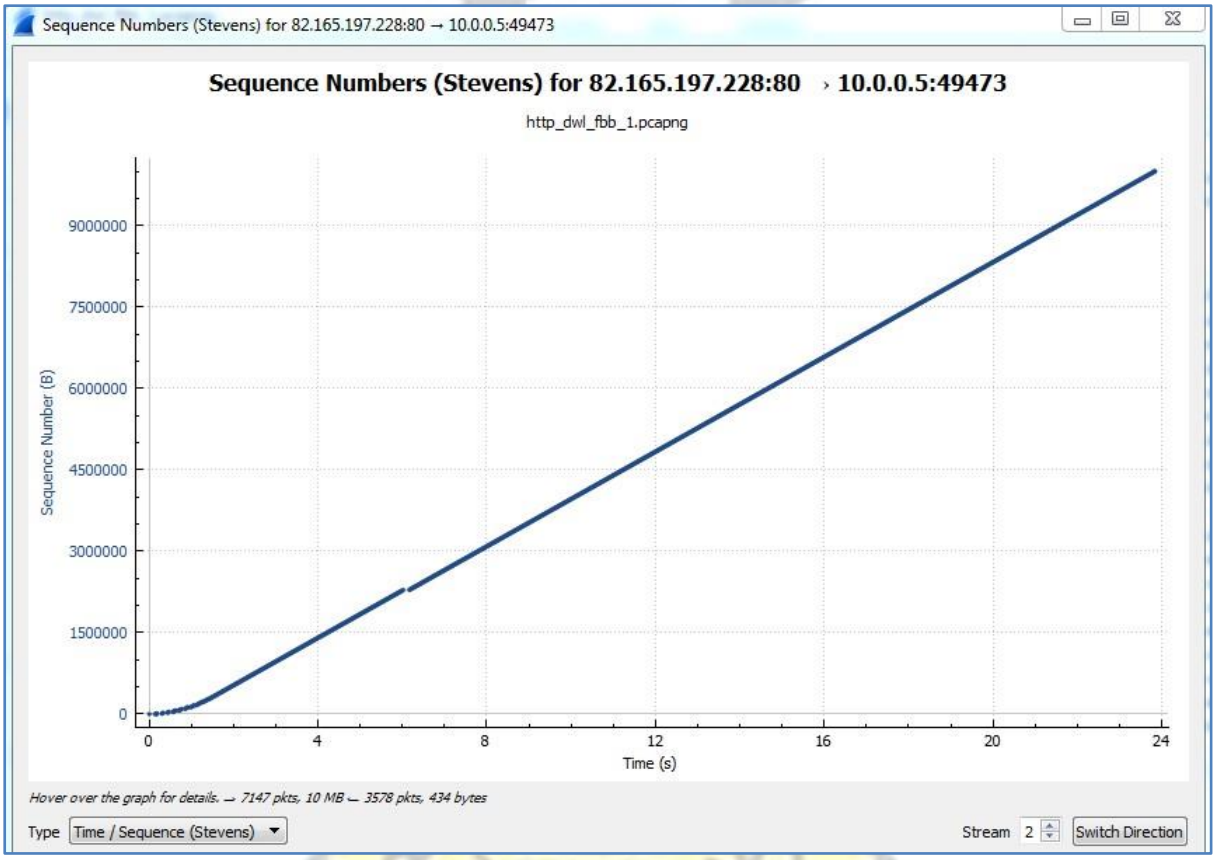


Figure 4.10: FBB Throughput and QoS

The input/output graph in Figure 4.10 shows the maximum sustained speed of approximately

3.6Mbps over the download period. 10MB of data was downloaded with twenty-four seconds. The download was smooth and steady as expected. There were no initial delays as observed for the MBB download but the duration of download was shorter than that of the FBB because of the throughput offered by the HSPA+.

The speed obtained is as expected.

The TCP download quality of service is analysed in Figure 4.11 to ensure no hidden problems existed though previous tests result showed expected results when analysed.

There are quite a number of TCP flags that could be used to analyse the quality of the test conducted but this thesis is restricting itself to “tcp.analysis.duplicate_ack” and “tcp.analysis.retransmission” flags, which are deemed enough to unearth any hidden problem.

The graph showed no visible hidden problems based on the TCP flags used. The result is as expected.

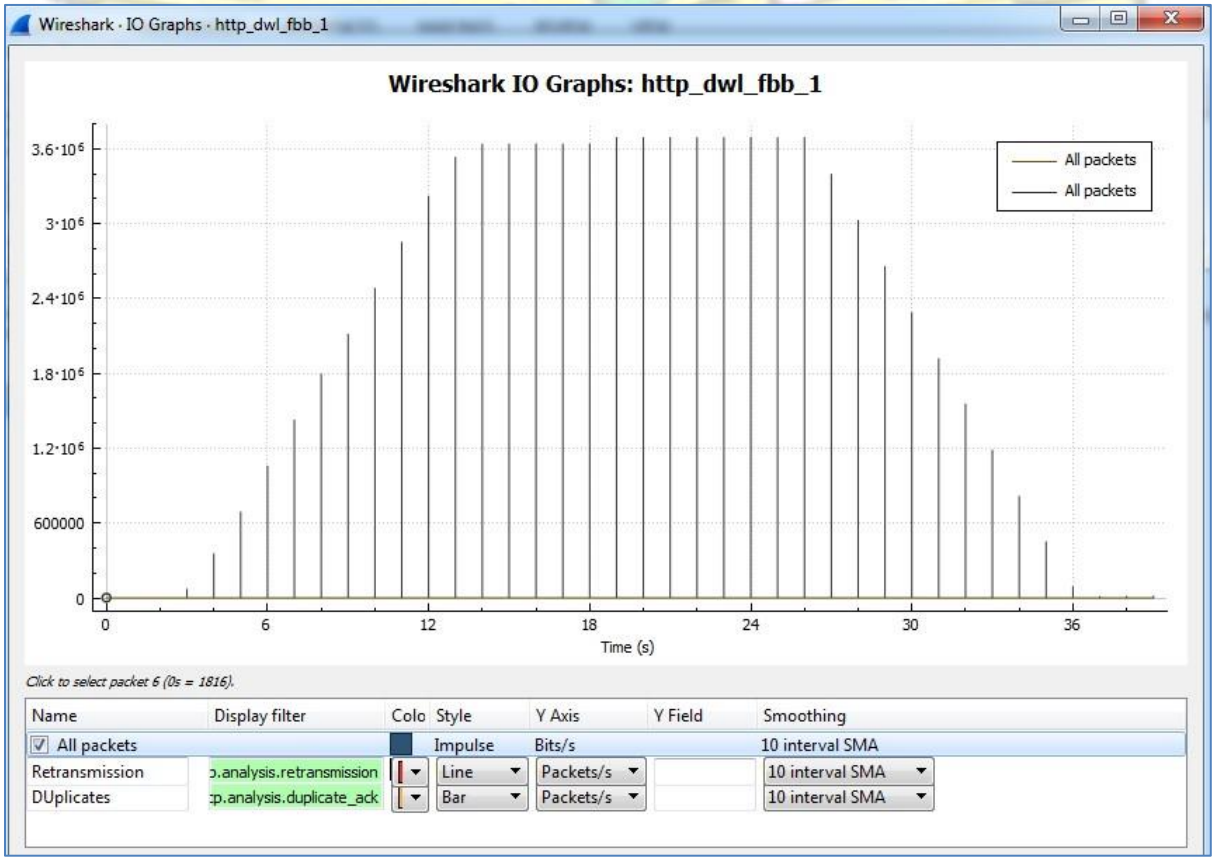


Figure 4.11 : FBB QoS Analysis

4.5. Analysis of Questionnaire Response.

The objective of the questionnaire was to measure the technical and non-technical awareness of mobile broadband amongst the Ghanaian populace. The data collected is not the source of raw data for the thesis. The raw data for the thesis was obtained primarily from experiments under METHODOLOGY, page 33. An online free tool for conducting survey, provided by Google was used to design and collect data from respondents. The detailed questions could be obtained in **Error! Reference source not found.**, page **Error! Bookmark not defined.**. It has two parts. For those who are not aware of the technical aspects of the mobile broadband, the questionnaire ended after question seven when "No" option is chosen. It continues to the end for those who chose the "Yes" option. The logical structure of the questionnaire is as shown in Figure 4.12 below.

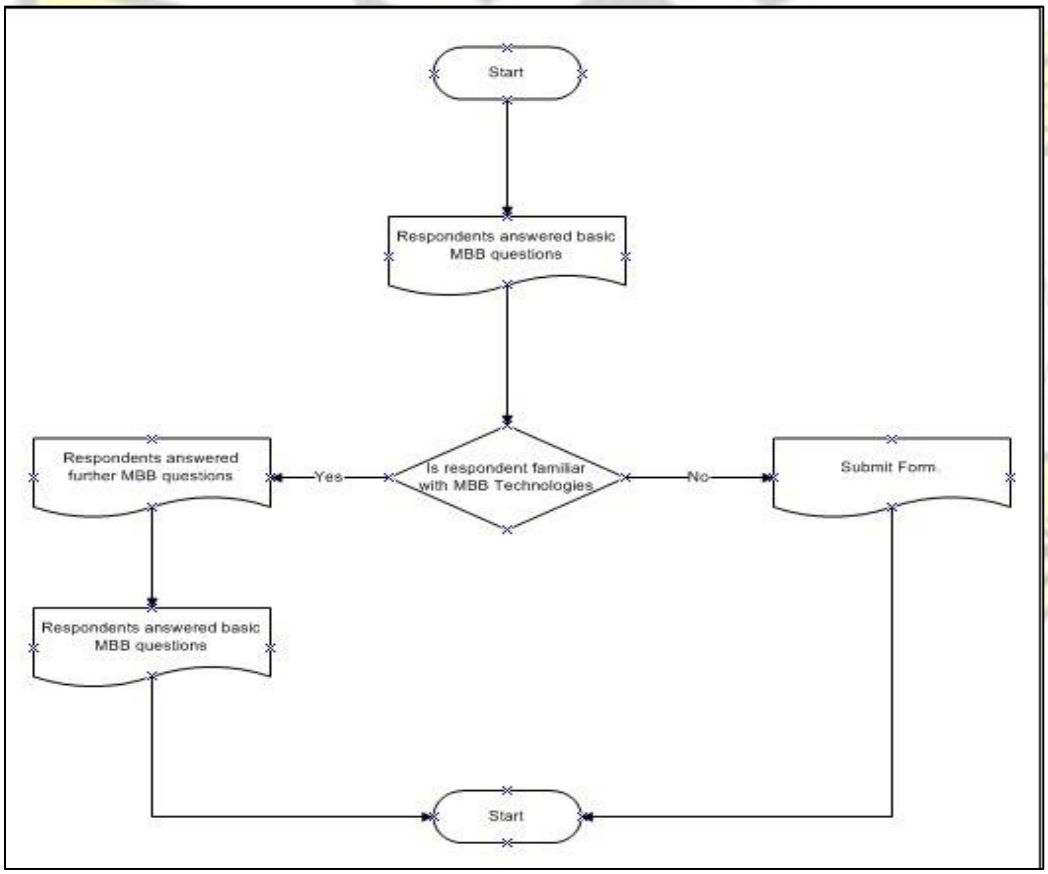


Figure 4.12: Questionnaire - Logical Structure

A portion of the overall responses that sought to measure the technical awareness of MBB amongst Ghanaians is show in Figure 4.13

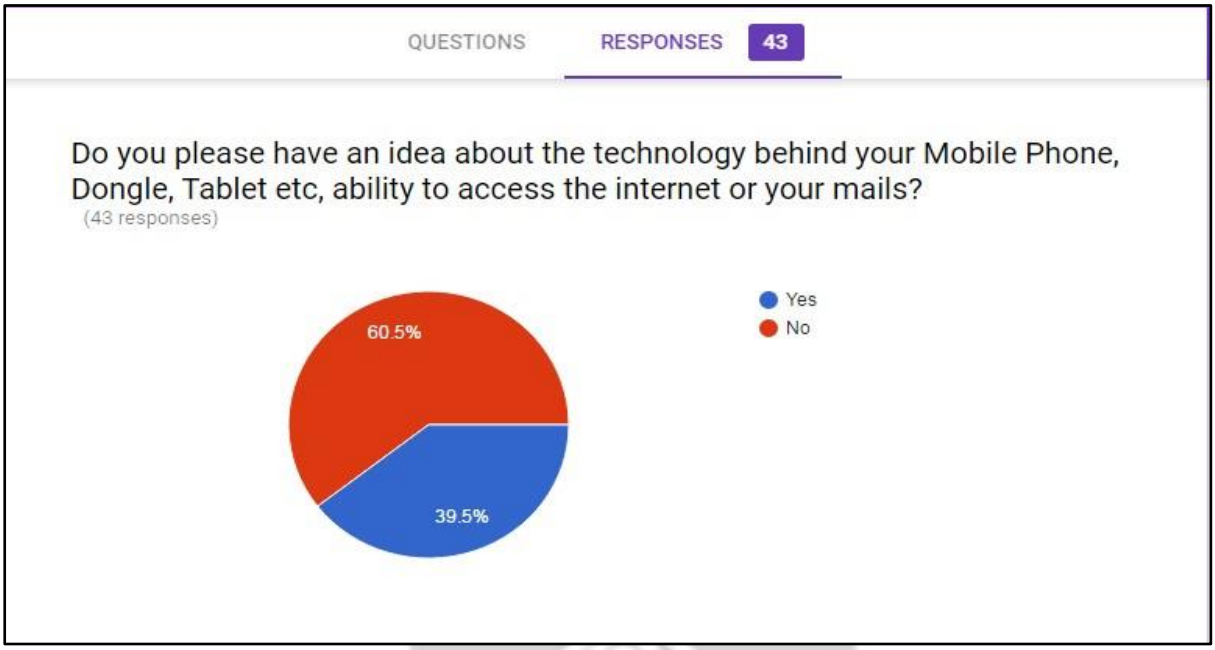


Figure 4.13: MBB Technical Awareness

The 60.5% respondents that had no technical knowledge of the mobile broadband is expected.

100% of respondents use mobile data with their handhelds and dongles as shown in Figure 4.14. This figure is expected.

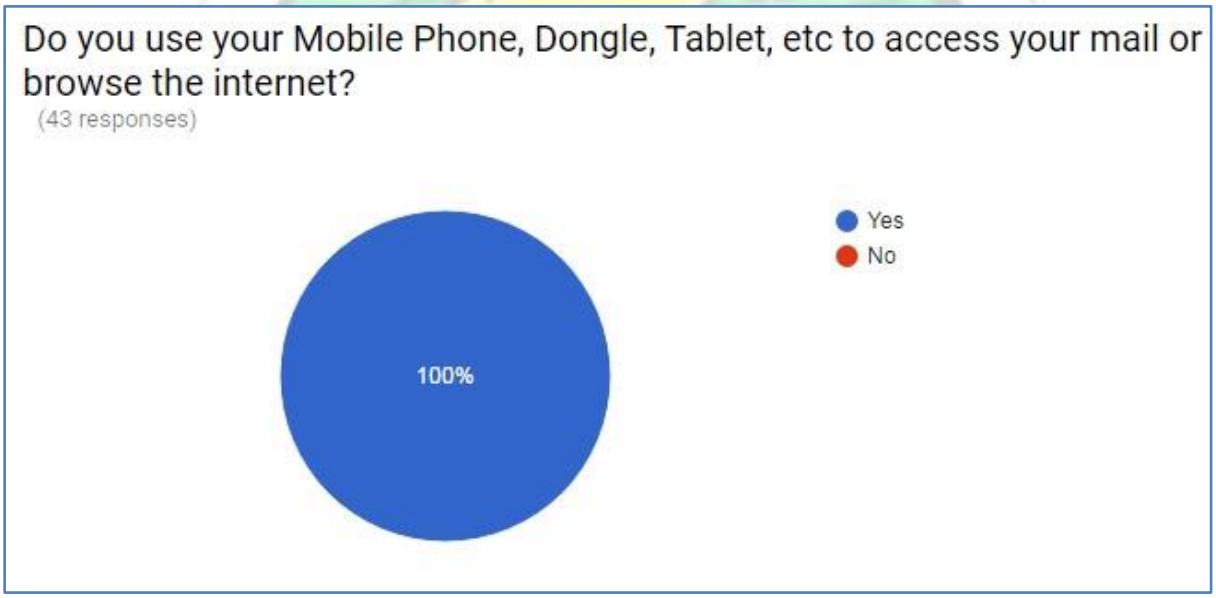


Figure 4.14: MBB Popularity

Conclusion

Mobile broadband is quite popular in Ghana but its usage is limited to personal online activities and not being used as private IP networks backbone, which this thesis is attempting to address.

CHAPTER 5. CONCLUSION & RECOMMENDATION

5.1. Summary of Findings

The best source of data for the study could have been obtained using industry standard telecommunications measurement tools. The acquisitions of these tools are beyond the financial capability of this study.

These tools are able to lock onto specific encoding schemes for MBB which in turn provide more accurate data for analysis.

Mobile handhelds and dongles were used for drive tests and data collection.

Speeds recorded for MBB most of the time varied at same location. This could be attributed to:

- The inability to lock on to a specific encoding scheme, i.e GPRS, EDGE, HSDPA, HSPA+, etc. during drive test or
- Cell resource availability

The virtual lab with GNS3 could not account for packet capture and analysis for Gb and Iu interfaces.

It accounted mainly for the internet facing interface, i.e. Gi. In fact, this is the focus of the study since the IP network design and deployment for businesses or for home use, occurs mainly over this logical interface.

The research showed that mobile broadband technologies are great sources for data access over IP networks. It provided the needed throughput, quality of service, upload and download speeds and security for use as an alternative to the fixed broadband technology.

5.2. Flexibility

MBB, per its nature of being mobile, offered greater flexibility in its deployment for doing business. It's available almost everywhere, flexible and able to integrate detached remote business entities where FBB is non-existent.

5.3. Security

MBB is composed of mainly two parts for data access, i.e RAN facing part, which is highly secured and had proven over the years to be virtually impossible to hack. Literature available only points to Lab setup where a little success was chalked in hacking. For live setup, we are yet to observe hacking.

The other is the internet facing part (Gi). This part is equally secured for every user.

FBB does not provide this level of security in what we have in Ghana today. Elsewhere operators only try to provide some level of protection by proving anti-virus applications. Users are exposed to possible hacking unless they deploy their own sophisticated level of protection in the form of Stateful Firewalls, Intrusion Detection and Prevention Systems. These are capital intensive systems.

Service providers for MBB had already invested in these systems on users stead for packets from the internet.

5.4. Conclusion

MBB has come to stay and it's making strides and fast becoming the default choice for data access over LAN, WAN and internet in Ghana. When this thesis commenced about two years ago, LTE, which is known as 4G, was not operational in Ghana. Today the world of MBB

technology is testing 5G and LTE is gaining roots in Ghana. As stated in the abstract of this thesis, the choice for experimenting MBB viability as alternative to FBB is UMTS.

Largely, favourable results were obtained and expectations were met from analysis of experiments conducted that emphasise the points made in page ii of the thesis abstract.

MBB could really be used as an alternative IP backhaul to traditionally known FBB. It competes favourably in speed, throughput and quality of service throughout the experiments. All is not rosy with MBB. Results obtained showed it has challenges where signal is quite low and also where a lot of people are contending for radio resource. Example, crowded areas such as depicted in page 90 under Unfavourable Result.

Research carried out by Vujic et al. (2014) suggested how radio resource challenges, which he referred to as "high user density", could be overcome. Their research stated that: Special events such as music festivals, sports etc. are characterised as "high user density" where user behaviour is determined by the dynamics of the event. This is the reason that it is necessary for a mobile network operator to dimension its network based on maximum expected resource requirements instead on averaged values.

Mobile broadband technology has good quality of service, secure, and good data speeds. MBB could be used as alternative to IP networking for businesses and individuals.

5.5. Recommendation

The conclusion arrived at for this study primarily points to the following recommendations:

Businesses could obviously prefer MBB as alternative to FBB for their IP networking but must be done based on feasibility studies. Businesses must be sure of MBB signal levels which could easily be done with modern smartphones before deploying it as IP backhaul. MBB use is also not recommended for lower technologies below UMTS and businesses must ensure where their office share same cell site with crowded areas, FBB should be the preferred choice.

LTE could have been the ideal MBB technology to use for the study but it was absent in Ghana during the commencement of the study. The study could be expanded to include LTE and direct tunnel where SGSN is eliminated to improve throughput

As of now, LTE is present in Ghana but has a very low market penetration and network coverage. Checks from National Communications Authority web site made no mention of LTE as one of the benchmarks for measuring MBB penetration in Ghana.

Figure 5.1 is a summary of MBB market penetration as of November 2015 referenced from NCA web's site http://www.nca.org.gh/73/34/News.html?item=581

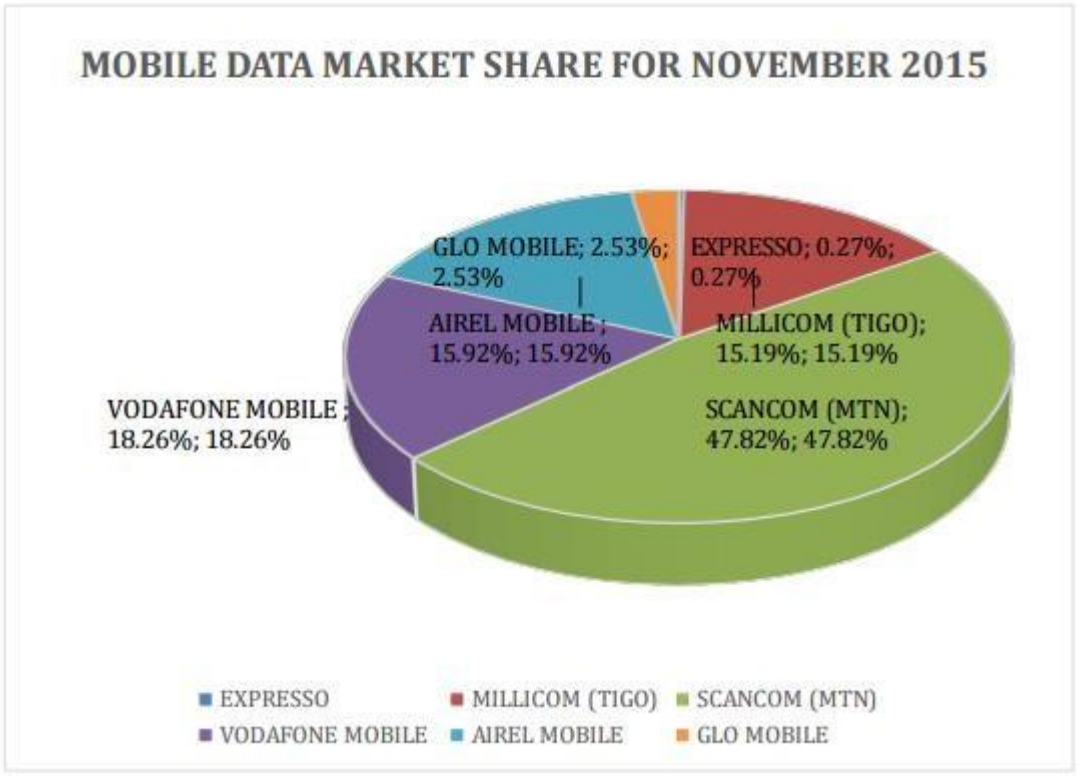


Figure 5.1: NCA MBB Penetration

5.6. Future Work

At the commencement of this exercise, LTE was non-existent in Ghana as a commercial service to users. Even the coverage of HSPA+ could only be felt in parts of Greater Accra, Ashanti and Western regions by then. As of now HSPA+ coverage had been extended by MBB service providers to all regional capitals and major cities. (NCA, 2016).

Unlike this research that primarily rode on 3G, HSPA+ and IP version 4; future research could be carried out within the mobile broadband space with primary focus on LTE and its potential impact on Ghanaian businesses with IP version 6 protocol and whether it is economically prudent for Telco's to continue investing in Fixed Broadband infrastructure.

REFERENCES

3GPP TR 25.848. (2003). "*3rd Generation Partnership Project. Technical Specification Group Radio Access Network. Physical layer aspects of UTRA High Speed Downlink Packet Access. (Technical Report)"*: 3GPP Organizational Partners.

Anandalingam, G., Raghavan, S. (2003). "*Telecommunications Network Design and Management"*: Kluwer Academic Publishers

Assad, M. (2007)."*TCP Performance over UMTS-HSDPA Systems"*: Taylor & Francis Group.

Behrouz, A. Forouzan. (2010). "*TCP/IP Protocol Suite"*. 4th ed. New York: The McGrawHill Companies, Inc.

Comer, D. E. (2014). "*Internetworking with TCP/IP"*, Volume One. 4th ed: Pearson.

Doyle, J., Carroll, J. D. (2006). "*Routing TCP/IP, Volume 1"*: Cisco Press, Inc.

Fitzek, F., Charaf, H.(2009). "*Mobile Peer To Peer(P2P)"*: John Wiley & Sons, Ltd.

Hunt, C. (2002). "*TCP/IP Network Administration"*: O'Reilly Media, Inc.

Kappler, C. (2009). "*UMTS Networks and Beyond"*: John Wiley & Sons, Ltd. pp. 30-39.

Kasera, S., Narang, N. (2004). "*3G Networks: Architecture, Protocols and Procedures"*: Tata McGraw-Hill Company Limited.

McGuiggan, P. (2004). "*GPRS in practice, A Companion to the Specifications"*: John Wiley & Sons, Ltd. pp. 44 - 62.

NCA. (2016, May). "*Industry Information - Telecom Subscriptions"*. Retrieved from http://www.nca.org.gh/downloads/Telecom_subscription_trends_for_May_2016.pdf

Odom, W. (2008). "*CCENT/CCNA ICND1 Official Exam Certification Guide, 2ed"*: Cisco Systems, Inc. pp 17.

Orebaugh, A., Ramirez, G., Burke, J., Morris, G., Pesce, L., Wright, J. (2006). "*Wireshark & Ethereal"*. Syngress Publishing.

Ouyang, Y., Fallah M. H, (2012). "*An Analysis of Traffic and Throughput for UMTS Packet Core Networks".* Stevens Institute of Technology.

Pandey. S . (2009). "*3GPP Wireless Standard"*: School of Technology and Computer Science, TIFR, Mumbai.

Perez, D., Pico, Jose. (2011). "*A practical attack against GPRS/EDGE/UMTS/HSPA Mobile Data. Communicatio*ns".

Punz, G. (2010). "*Evolution of 3G Networks, The Concept, Architecture and Realization of Mobile Networks Beyond UMTS"*: SpringerWien

RFC 3819. (2004). "*Internet Engineering Task Force: Advice for Internet Subnetwork Designers"*.

RFC 3819. (2004). "*Internet Engineering Task Force: Advice for Internet Subnetwork Designers"*.

Sanders, C. (2011). "*Practical Packet Analysis".* San Francisco: No Starch Press, Inc.

Sanders, G., Thorens, L., Reisky, M., Rulik, O., Deylitz, S. (2003). "*GPRS Networks"*: John Wiley & Sons, Ltd,

Seurre, E., Savelli, P., Pietri , Jean-Pierre. (2003). "*GPRS for Mobile Internet"*: Artech House.pp. 332-351.

Soldani, D., Li, M., Cuny, R. (2006). "*QoS and QoE Management in UMTS Cellular Systems"*: John Wiley & Sons, Ltd.

Stevens, R. W. (2009). "*TCP/IP Illustrated Volume 1"*: Pearson Education, Inc, pp. 46-60.

Tomsho, G. (2011). "*Guide To Networking Essentials"*. pp. 261 – 270.

Vujic, D,. Certic, J. (2014). "*UMTS RAN Capacity Analysis for Special Events"*: University of Belgrade

Welte, H. (2011). "*28th Chaos Communication Congress: Cellular protocol stacks for Internet [Powerpoint Presentation]"*. Retrieved From https://www.youtube.com/watch?v=Rk8Lc7-8Tbo

.

APPENDIX

KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY, KUMASI

MASTERS IN INFORMATION TECHNOLOGY QUESTIONNAIRE

INTRODUCTION: Dear Respondent, this questionnaire is for academic purpose only.

Mobile Broadband (MBB) is the marketing term for wireless internet access through a portable modem/dongle, mobile phone, USB wireless modem, tablet or other mobile devices. This is made possible by data enabled SIM cards.

Kindly answer the question below. It would take you not more than five (5) minutes to complete:

*Required

1. Please select your professional background * *[Mark only one radio button]*
   - ○ Legal
   - ○ Human Resource
   - ○ Academics
   - ○ Engineering
   - ○ Medical
   - ○ Information Technology
   - ○ Telecommunication
   - ○ Finance
   - ○ Marketing
   - ○ Student
   - ○ Other

2. Do you use your Mobile Phone, Dongle, Tablet, etc to access your mail or browse the internet?
   [Mark only one radio button]
   - ○ Yes
   - ○ No

3. How convenient is it when accessing internet or mails from your Tablet, Mobile Phone, Dongle, etc?
   [Mark only one radio button]
   - ○ Very Convenient
   - ○ Convenient
   - ○ Not Convenient

4. How fast is it when accessing internet or mails from your Tablet, Mobile Phone, Dongle, etc.?
   [Mark only one radio button]
   - ○ Very Fast
   - ○ Fast
   - ○ Slow

5. Do you feel secured when using Mobile Phone, Dongle/Modem, Tablet etc, to access your mails or internet? *[Mark only one radio button]*
   - ○ Yes
   - ○ No

6. Does your credit finish quite fast when using your Mobile Phone, Dongle/Modem, Tablet etc. to access your mails or internet. In order words, is it expensive?
   [Mark only one radio button]
   - ○ Expensive
   - ○ Not Expensive
   - ○ Moderate

7. Do you please have an idea about the technology behind your Mobile Phone, Dongle, Tablet etc., ability to access the internet or your mails? *
   [Mark only one radio button]
   - ○ Yes
   - ○ No

8. Please, which of the following Mobile Broadband Technologies are you familiar with?
   [Tick all that apply]
   - ☐ LTE
   - ☐ HSPA+
   - ☐ 3G
   - ☐ 2G/EDGE

9. Would you recommend Mobile Broadband Technology as main form of accessing internet for offices or businesses? *[Mark only one radio button]*
   - ○ Yes
   - ○ No

10. Could the speed of Mobile Broadband Technology match that of WiFi or Fixed Broadband (ADSL)?
    [Mark only one radio button]

- Yes
- No

11. Could the security of Mobile Broadband Technology match that of WiFi or Fixed Broadband?
[Mark only one radio button]
    - Yes
    - No

12. Please your general comments about Mobile Broadband Technology would be appreciated. *

[End of questionnaire. Thank you for the responses]