ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

Traffic Analysis of IP Core Networks: the Case of Ethio Telecom

By

Mehretu Daka

Advisor

Dr. -Ing. Dereje Hailemariam

A Thesis Submitted to the School of Electrical and Computer Engineering in Partial Fulfillment of the Requirements for the Degree of Masters of Science in Communication Engineering

May, 2017

Addis Ababa, Ethiopia

ADDIS ABABA UNIVERSITY

ADDIS ABABA INSTITUTE OF TECHNOLOGY

SCHOOL OF ELECTRICAL AND COMPUTER ENGINEERING

Traffic Analysis of IP Core Networks: the Case of Ethio Telecom

By: Mehretu Daka

Approval by Board of Examiners

_____	_____
Chairman, School Graduate Committee	Signature
Dr. -Ing. Dereje Hailemariam_____	_____
Advisor	Signature
_____	_____
Internal Examiner	Signature
_____	_____
External Examiner	Signature

Declaration

I, the undersigned, declare that this MSc thesis is my original work, has not been presented for fulfillment of a degree in this or any other university, and all sources and materials used for the thesis have been acknowledged.

Mehretu Daka___ _____

Name Signature

Place: **Addis Ababa, Ethiopia**

Date of submission: May 29, 2017

This thesis has been submitted for examination with my approval as a university advisor.

Dr. -Ing. Dereje Hailemariam__ _____

Advisor's Name Signature

Abstract

According to the Internet World Status report, number of Internet users is increasing at about 10% annually, and the trend is the same in Ethiopia. Beside, most networks in telecom companies are converging to Internet Protocol (IP)-based core networks.

To get maximum possible capability of IP-based core network, operators work on capacity development projects like expanding the bandwidth of their core networks. However, doing expansion project usually needs high cost that increases Capital Expenditure (CAPEX) of the operators. So, rather than doing capacity development projects frequently, core network traffic should be regularly analyzed in order to understand its' usage level; to improve the functionality of the network; to be aware of the operational aspects of the network; and to identify a way that uses maximum possible level of the network.

In this thesis, IP core network traffic analysis is conducted. To do this, data is obtained from the IP core network performance monitoring tools. After studying real time data and getting average values of key parameters, the network Key Performance Indicators (KPIs) are simulated using Matlab software environment. The real time data obtained from the monitoring tools is analyzed by comparing with simulated results.

The study results in usage level evaluation of core network, indicates the vendor tools reliability and gives better recommendation on core network architecture that helps to obtain maximum possible level of the network. Accordingly, the study shows that almost all tested service quality indicators are below the International Telecommunication Union (ITU) standards and vendors' tools are reliable. However,

enormously increasing number of subscribers will make core network traffic congested in a near future. So, this study recommended better core network architecture. As there will be a need to deploy new core networks or expand existing core network, findings in this study can be used as reference for new build as well as expansion on IP core network.

Keywords—IP Core Network, Traffic Analysis, Performance Monitoring, Active Monitoring, Passive Monitoring, KPIs.

Acknowledgement

First of all, I would like to thank the almighty God for letting me finish this thesis.

Secondly, I would like to express my sincere and special thanks of gratitude to my advisor Dr. -Ing. Dereje Hailemariam, who has given me great help, excellent advice and has treated me with infinite patience throughout this thesis work. It would be very difficult and might have taken longer time to finish this paper without his attentive guidance.

I also want to thank my brothers for their material support, indispensable guidance and moral advice. Beside them, I want to thank my wife for her patience during the thesis work. My gratitude also goes to my friends for their help and best wishes during the whole program, and particularly during this thesis work.

Finally, I want to give my endless gratitude to Addis Ababa University for giving me the chance to study in this program and ethio telecom for permission of data gathering.

Table of Content

List of Figures

List of Tables

List of Acronyms

ASCI	Application-Specific Integrated Circuits
ASG	Aggregation Service Gateway
ATN	Access Transmission Node
Bps	Bits per Second
BSC	Base Station Controllers
BTS	Base Transceiver Station
CAPEX	Capital Expenditure
CDMA	Code Division Multiple Access
CSG	Cell Site Gateway
DSLAM	Digital Subscriber Line Access Multiplexer
EPON	Ethernet Passive Optical Network
FCFS	First Come First Served
FMC	Fixed-Mobile Convergence
IC	Integrated Circuit
ICT	Information Communication Technology
IDC	Internet Data Center
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISP	Internet Service Provider
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LAN	Local Area Network
MAN	Metropolitan Area Networks
MPLS	Multiprotocol Label Switching

MSC	Mobile Switching Center
MSAG	Multiple Service Access Gateway
MSAN	Multiple Service Access Node
ONU	Optical Network Units
OSI	Open System Interconnection
PMF	Probability Mass Function
PoP	Point-of-Presence
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RNC	Radio Network Controller
RSG	Radio Service Gateways
RTN	Radio Transmission Node
SLA	Service Level Agreement
SPAN	Switch Port Analyzer
S-R	Short-Reach
TAP	Test Access Point
USR	Universal Service Router
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing

Chapter 1: Introduction

Telecommunication network basically contains three layers in its structure; namely, access layer, aggregation layer and core network layer. This layer arrangement helps to easily manage functions in each layer and also identify problems [1, 2].

Access layer is a layer that contains network elements (NEs) that can support end users [1]. Aggregation layer, as its name indicate, aggregates the access layer network elements to the core network [2]. A core network, or network core, is the central part of a telecommunication network that interconnects multiple network components such as aggregation components, wide area networks (WAN) and data centers. It provides path for the exchange of information between different sub-networks [3, 4].

Nowadays, core network is changing into an Internet Protocol (IP)-based network cloud, so that the name IP Core Network is used in this thesis and other recent works [5, 6]. As IP core network is center for all network nodes and interconnects many network components, there is a very high traffic flow or rate in the core network. Network traffic rate or flow refers to the amount of data in bits per second (bps) moving across a network at a given point of time [7].To follow up traffic usage and network performance level, to get maximum possible capacity of the network, this thesis proposes to do traffic analysis of the IP core network by collecting real time data from IP core network monitoring tools and simulating by computer-aided Matlab simulation. The study also proposes to do mathematical modeling of KPIs so that this modeling is used during simulation work.

Network traffic analysis is the process of capturing network traffic performance data and inspecting it closely to determine the network performance level and to examine its service quality with respect to International Telecommunication Union (ITU) standards [8]. The primary purpose of continuous performance analysis is usually to find out the usage levels on different parts of the network. In addition to this, general goals of network traffic analysis are [8]:

- Improving the functionality of the network,
- Performing user level behavioral studies,
- Being aware of the operational aspects of the network.

In addition to the above general goals, network traffic analysis also helps to identify the network path, link or devices with saturated capacity (those with the point where the flow of data is impaired or stopped entirely). At this saturated point, there is no enough data handling capacity to handle the current volume of traffic. So, after analysis is done, recommendations are given to the concerned body so that they can use this study to examine the existing core network architecture and change accordingly, or use it when they deploy new network core.

This thesis will mainly focus on IP core network traffic analysis. Since performance data for KPIs are usually fetched from vendor tools, their accuracy will be cross checked using mathematical modeling, which is developed by using mathematical equations for IP core network KPIs. Using these mathematical models, simulation on Matlab will be held. Common KPIs that are simulated using the developed models are end-to-end packet loss, packet delay and jitter. Data for these KPIs are collected in a file using passive monitoring method although in some situations it may be collected using active monitoring method. Passive monitoring is a data collection method that collects data

using devices that are connected to the network. Active monitoring method is collecting data from the network elements in a real time, which may introduce its own traffic into the network, and it is intrusive [9, 10, 11].

1.1. Statement of the Problem

There is very high and increasing demand in Internet and data usage throughout the Ethiopia, especially in the capital city Addis Ababa. This is because of the increase in Information Communication Technology (ICT) companies and organizations that need Internet and data and also the increase in number of smart phone users. To provide enough coverage and quality network for these continuously increasing customers, ethio telecom does continuous expansion projects in its network. For example, ethio telecom has recently expanded the existing backhaul for mobile customers, Multiple Service Access Gateway (MSAG) and Multiple Service Access Node (MSAN) plantation projects for PSTN and broadband internet users.

However, if capacity of the core network is saturated, expansion of access networks has no much effect on quality and performance. That is, if capacity of the core network is less than or nearly equal to the summation of network capacities of all the access networks, the flow encounters congestion. This, in turn, causes network delay since network flow is usually governed by First Come First Served (FCFS) discipline. If this happens in the network, subscribers that are connected to access networks cannot get satisfying services. So, there should be continuous "checkup" on core network so as to identify its bottlenecks and take remedial actions. Traffic analysis is used to inspect the capacity of core network and to identify traffic jam at a point.

However, usually practical analysis is done when there is a problem on some points such as a specific server. Besides this, capacity problems and quality cases are traced when there is complain from an affected customer. This causes maintenance time delay, hence, customer dissatisfaction. These points motivate this thesis. To be aware of capacity levels and service quality of the core network, traffic analysis is done using different KPIs. This study attempts to address the above problems by doing traffic analysis on core network.

1.2. Objective

1.2.1. General Objective

The main objective of this study is to do traffic analysis of IP core network in ethio telecom so as to find out the usage levels of the IP core network.

1.2.2. Specific Objectives

The specific aims of this thesis are:

- To do mathematical modeling of the network KPIs;
- To do analysis of traffic of roots that interconnect core NEs to get traffic analysis of the core network;
- To demonstrate the importance of regular and overall analysis of network and;
- To recommend better core network architecture.

1.3. Literature Review

There are several authors and researchers that have put forward their own ideas on the area of IP core network traffic analysis. Some of them have tried to describe core

network of a single network, such as core network of mobile network, core network of Code Division Multiple Access (CDMA), and so on. Some authors depicted the significance of core network analysis, rather than doing detail analysis. In this section some related works are reviewed to put bench mark to this study.

The investigation of traffic patterns in wireless data networks presented in [12]. In this thesis, analysis of network traffic was done for wireless data. It demonstrated that the wireless traffic is statistically different from traffic generated by traditional traffic models. However, the study does not include core network traffic. Not only that, it does not include analysis on each network KPIs rather it generally studied patterns of the wireless data network traffic.

Network traffic and infrastructure analysis was done in Software Defined Network (SDN) in [13]. The primary aim of the study was to bind out monitoring and measuring mechanisms by focusing only on SDN and through selected number of user cases.

A detailed analysis was done by Toni Janevski [14] on every Wireless IP networks. The paper mentioned analysis methods and network modeling for Wireless Access Networks. The content and its approach are very good but the problem is that it used to analyze the Wireless Network only. Besides, it has showed analysis in access network, not in Core network. It also used already existing service data, but not real time service data. He also did traffic analysis for voice in wireless IP network in collaboration with Boris Spasenovski [15]. Their study mainly focused only on voice service.

Young Choi and Sue Moon [16] on their magazine for Institute of Electrical and Electronics Engineers (IEEE) in 2004 carried out very good analysis on point to point

packet delay in a network. Their main work was focusing on router to router delay only but not on other parameters like packet loss, jitter and traffic rate. Another researcher, called Akhigbe-Mudu, with his colleagues, studied the behavior of packet loss using passive measurement technique. Their main focus was measurement technique, called passive measurement, not the trend of packet loss [9].

Very interesting analysis on IP Core devices was done by Francesco Musumeci and Massimo Tornatore [17]. They focused on parameters like Wavelength Division Multiplexing (WDM) transponders, Short-reach (S-R) interfaces, Electronic Processing to analyze power consumption on the network. However, they focused only on IP over WDM Core Network. Not only this but also their focus area was only on power consumption of the network.

On the paper "Rethinking of IP Core Network" [6], Saurav Das with his colleagues studied structural problems of IP core networks. Focusing on Capital Expenditure (CAPEX) of network backbone, they briefly studied how to reduce number of routers to optimum level. In order to get good insight of the core network, they did analysis on IP based core network versus Wavelength Division Multiplexing (WDM) based core network. However, in general their paper tried to show the structural problems and design issues of IP backbone infrastructure rather than the network's KPIs.

The performance of IPv6 compared with IPv4 has been analyzed in laboratory using 3G mobile in Stockholm, Sweden [18]. The study mainly focused only on IP data, Signaling and Web load time. That is, its primary focus was protocol, not whole performance. It described the advantage of IPv6 over IPv4 for future need of IP appliances. In the same way, performance analysis of triple play services has been conducted over IP using

OPNET simulator [19]. In the paper, the author mainly focused on performance analysis of services, not the network itself, using IP.

Some writers have been conducted the effect of certain KPIs on a specific services, or technologies. For example, Alexander F. Ribadeneira has studied the effect of delay, jitter and packet loss [20]. Krzysztof Perlicki also studied the impact of packet loss and delay on voice transmission quality [21]. Mansour J. Karam, with his friends, carried out analysis of the delay and jitter of voice traffic over the Internet [22]. These all tried to do analysis based on a specific KPI for a certain service but not core network.

Timo Viipuri [23] and Mohamed Faten Zhani [24], on their separate works, have conducted analysis for almost all IP Core network. Timo Viipuri has done analysis of the whole IP core network in a very good manner, except he left out simulation for future work. Mohamed, on the other hand, focused on prediction of network traffic in addition to real network analysis. Using behavior of training-based model, he studied the prediction of throughput of a single link of a real network. Then he tried to do analysis of his models with the existed predicting models. However, his work was not directly focused on IP core network traffic analysis.

Network traffic data analysis for backbone links are presented using real traffic data collected from publicity available anonymized traces in [25]. Data analysis and visualization are carried out using Matlab at packet level and flow level. However, the study did not include details. The analysis is also focused only on data not on all services.

Residential network traffic and user behavior analysis has been performed by considering end users in Stockholm, Sweden [26]. The main aim of the thesis is finding the hidden pattern of traffic and user behavior in a residential fiber based access network. However, it did not include traffic analysis on the network traffic pattern but on the users' traffic pattern.

This thesis tries to combine different methods and procedures that are used in the above literatures as input and works on analysis of traffic of IP core networks.

1.4. Methodology

In this thesis, we use different data that are related with performance analysis, particularly with traffic analysis of IP core network, such as books written for network traffic analysis, journals that are published for the study of network traffic analysis, different IEEE articles, documents and previous researcher's studies on this subject.

Using related works as an input and the statement of problem as main and basic benchmark for this study, the methodology of this paper is organized as follows.

Overview of the network structure and system design

- Investigate the network backbone and IP core network architecture so that clear environment is established for the whole work.

- Grasping general structure of the network, IP core network architecture is studied in detail with its elements and measurement indexes (KPIs).

- Data collection for KPIs is another method using different techniques mentioned in [9].

Preparation of mathematical modeling of the KPIs is done.

Simulations

- Prepare general outline for simulation
- Conduct Simulation using mathematical models of KPIs.
- The simulation is carried out using Matlab software.

Results and analysis

- Show levels of IP core network usage level
- Do analysis of the network by comparing their usage level with ITU standards
- Depict busy hour and slow hour using traffic rates
- Compare levels of actual IP core network KPIs and simulated results

1.5. Scope and Limitation

1.5.1. Scope of the Thesis

There are so many network elements (NEs) and each NE has many interfaces in one telecom operator. Even in one telecom operator, core network contains many NEs as it is backbone of the network. So, addressing each NE in the telecom is very challenging job, not only for thesis but also for day to day operation. So, usually network operation, monitoring and maintenance are done by classifying on their levels like core, aggregation and access. This thesis also addresses core network elements only.

1.5.2. Limitation of the Thesis

The mathematical modeling in this thesis considered main contributors like queueing delay, and transmission delay, not all parameters that contribute for each KPI. Assuming their effect is very little, this paper ignores parameters like propagation and processing delays. Their contribution amount is clearly cited in the development part (Section 5.2) so that a reader can understand why this paper ignored them.

In addition to this, simulation uses mathematically developed models and randomly generated variables for packet arrival rate. Indeed, these variables are generated after close inspection of the real network scenario.

1.6. Contribution of the Thesis

Core network is one of areas that need very strict follow up in telecommunication industries. This is because every telecom service is connected into core network through its ports. This in turn increases network traffic on core network. Hence, an attention has to be given to core network. To utilize maximum possible capacity of the core network and know its usage level after deploying network, there should be continuous and organized traffic analysis on core network.

This thesis work contributes such a study that helps to have an organized examination on traffic analysis of IP core network. It gives detailed analysis on traffic usage of IP core network using different KPIs. Furthermore, computer-aided simulation of the common KPIs is done to show performance monitoring tools' reliability.

1.7. Thesis Layout

This thesis paper contains seven chapters. Chapter one deals with introduction of the whole thesis. It clearly cites statement of the problem, objective of the study, related works, scopes and limitation of the thesis and the methods how this paper will achieve its objective.

Chapters 2 and 3 cover general structure of a telecom network and IP core network architecture respectively. The network elements that are going to be studied in IP core network are viewed in Chapter 3. Fourth chapter presents parameters that are used in IP core analysis in detail. Every performance indexes that are used for analysis are presented here in detail.

Following parameters study, mathematical modeling for each of them is developed in Chapter 5. Chapter 6 shows Matlab simulation of the developed models for each parameter presented in Chapter 4. This chapter also presents analysis and result parts. The final part of the thesis is presented in Chapter 7. In this chapter, conclusion is drown from the analysis part. It then recommends core network architecture to get optimum services regarding quality.

Chapter 2: Network Architecture in Telecommunication

2.1. Introduction

Network architecture represents the topology or hierarchical connection of network elements starting from core network to access network. Usually all telecom service providers use almost the same type of hierarchical architecture in their service. The following figure represents the most common type of network hierarch in telecom service providers [1, 2, 27].

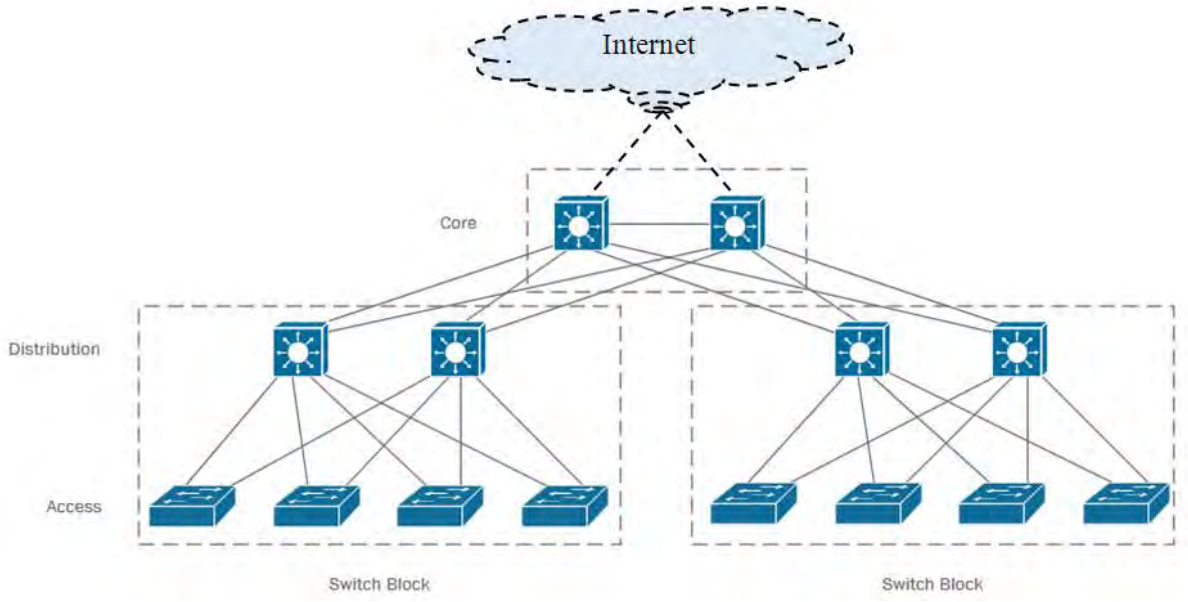


Figure 2.1: Common type of network architecture in a telecom network [1].

According to the above figure, Figure 2.1, general architecture of telecom network contains three hierarchal network layers. These are core network, aggregation (distribution) network and access network. The brief discussion of each network layer is presented in the following section.

2.2. Main Components of Network Architecture

As we have seen, there are three main contents in any telecom network architecture. In the following section, these three network components are discussed in detail.

2.2.1. Core Network

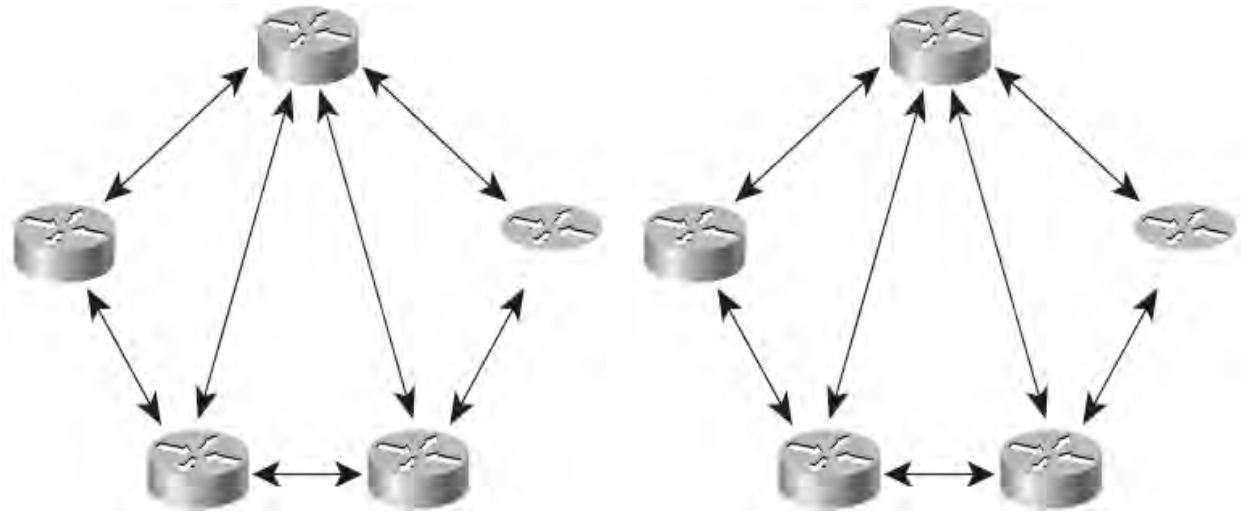
Core network of a three-layer hierarchical topology is also referred to as the network backbone of a service provider [1]. It consists of high-speed network devices which are designed to switch packets as fast as possible. Core network is also responsible to provide reliability and fault tolerance.

In an enterprise Local Area Network (LAN), the core layer may connect multiple buildings or multiple sites and may provide connectivity to the server farm. The core layer includes one or more links to the devices at the enterprise edge to support Internet, Virtual Private Networks (VPN), extranet (a controlled private network allowing customers to gain information about specific company. It can be viewed as intranet mapped onto the public Internet), and Wide Area Network (WAN) access [27]. According to Kenneth D. Stewart III and Aubrey Adams [27], core layer can be very big that can cover large area, or can provide connectivity to a certain sites or even local buildings. So, its place of location in a network architecture may vary.

As core network covers very large areas, it should provide a high-speed connection between the different distribution layer devices. Because of the need of high-speed connections, the core consists of high-speed switches [2, 27]. These switches are more commonly layer 3 switches with Gigabit connectivity. Layer 3 switches are basically routers that perform their switching using Application-Specific Integrated Circuits

(ASICs) instead of a central CPU. ASIC is an Integrated Circuit (IC) customized for a particular use, rather than intended for general-purpose use.

Most core layers in a network are connected using either full or partially mesh topology [27]. A full-mesh topology is one in which every device has a connection to every other device. It offers good performance because there is just a single-link delay between any two sites [2].Although full-mesh topologies provide the benefit of a fully redundant network, they can be difficult to wire and manage and are more costly. For larger installations, a modified partial-mesh topology is used. In a partial-mesh topology, each device is connected to at least two others, creating sufficient redundancy without the complexity of a full mesh.



A) Full-Mesh Topology B) Partial-Mesh Topology

Figure 2.2: Full-mesh topology (A) and partial-mesh topology (B) [2].

2.2.2. Aggregation Network

The aggregation (or distribution) layer of the network is the demarcation point between the access and core layers of the network [2, 27]. It aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination [1]. This layer is associated with routing, filtering, and is the communication point between the core layer and the access layer. A network designer must create a distribution layer design that complements the needs of the other two layers.

The aggregation layer is usually built using Layer 3 switches. Layer 3 switches are those switches that share much in common with traditional routers. Layers in this point of view are the hierarchical places that indicate where network elements in an Open System Interconnection (OSI) model should be placed. The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology. It consists of 7 layers; physical layer at bottom of the model and application layer at the top. Each layer has its own distinct function and network elements are placed in their respective layers according to their functions [28].

Accordingly, aggregation layer needs switches that are at layer 3 in OSI model. This is because; switches at layer 3 have switching and routing technologies. Since aggregation layer in a network architecture should aggregate and route packets, switches in this layer shall be layer 3 switches [28].

The distribution layer allows the core layer to connect sites that run different protocols while maintaining high performance. To maintain good performance in the core, the

distribution layer can redistribute between bandwidth-intensive access layer routing protocols and optimized core routing protocols.

Routers or switches, located at the distribution layer, provide many functions critical for meeting the goals of the network design. Some of functions provided by devices in aggregation layer are [2]:

- ✓ Filtering and managing traffic flows
- ✓ Enforcing access control policies
- ✓ Summarizing routes before advertising the routes to the Core
- ✓ Isolating the core from access layer failures or disruptions
- ✓ Routing between access layer VLANs

Distribution layer devices are also used to manage queues and prioritize traffic before transmission through the core network [27].

The other function of aggregation layer is providing WAN access and to determine how packets can access the core. It also defines broadcast and multicast domains in a network [28] that are explained as follows.

Broadcast Domain

Broadcast is a type of communication, where the sending device send a single copy of data and that copy of data will be delivered to every device in the network segment. A broadcast domain is a domain in which a broadcast is forwarded. A broadcast domain contains all devices that can reach each other at the data link layer, a second layer in an Open System Interconnection (OSI) model, by using broadcast. All ports on a hub or a switch are by default in the same broadcast domain. All ports on a router are in the

different broadcast domains and routers don't forward broadcasts from one broadcast domain to another [28].

The following figure clarifies the concept of broadcast domain in a good manner

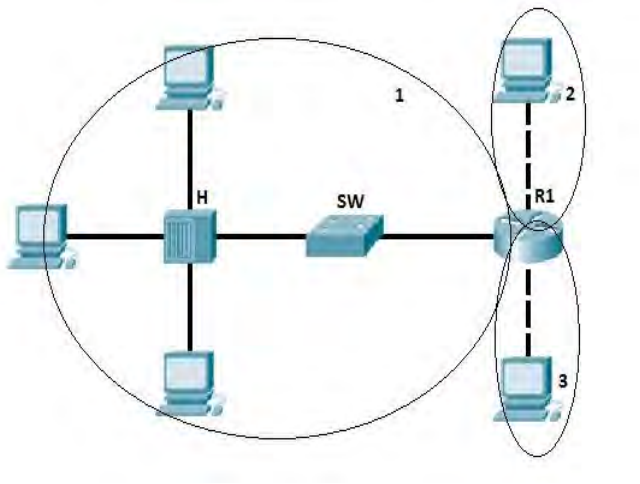


Figure 2.3: How network elements are interconnected in a broadcast domain [28].

In the picture above we have three broadcast domains, since all ports on a hub or a switch are in the same broadcast domain, and all ports on a router are in a different broadcast domain.

Multicast Domain

Multicast is the term used to describe communication where a piece of information is sent from one or more points to a set of other points. In this case there is may be one or more senders, and the information is distributed to a set of receivers (there may be no receivers or any other number of receivers). The difference between broadcast and multicast is that in the former case, the sender is only one where as in the latter case; the sender can be more than one. The information is sent to all connected receivers in a network in both broadcast and multicast [29].

After having briefly seen the difference between broadcast and multicast domains, we have to explain why it is mentioned in this section. The only reason is that these two methods of transferring packets in a network are defined in an aggregation layer. For large scale convergence layer networking application, routers that have higher capacity in switching are used in an aggregation layer so that they are suitable for metro network aggregation layer applications [30].

2.2.3. Access Network

Access layers are usually end-stations and servers that connect subscriber side through different devices. These devices are usually multi-service elements so that they support end users to get different services. Access layer gives users access to the network [1].

The access layer provides users on local segments with access to the internetwork. The access layer devices can include routers, switches, bridges, shared-media hubs, and wireless access points. As mentioned, switches are often implemented at the access layer in a network to divide up bandwidth domains to meet the demands of applications that need a lot of bandwidth or cannot withstand the variable delay characterized by shared bandwidth [2].

For internetworks that include small branch offices and telecommuter home offices, the access layer can provide access into the corporate internetwork using wide-area technologies such as ISDN, Frame Relay, leased digital lines, and analog modem lines [2].

Access layer network devices are usually small scaled in capacity. They are directly connected to aggregation network layer elements through medium scaled switches.

2.1.Network Architecture in Ethio Telecom

Ethio telecom, sole telecom operator in Ethiopia, uses all the above layers in its network architecture. There are two vendors in ethio telecom. These two vendors use two different types of architectures to provide the telecom service. The following figure, Figure 2.4, shows the general architecture of one of the two vendors' network in ethio telecom.

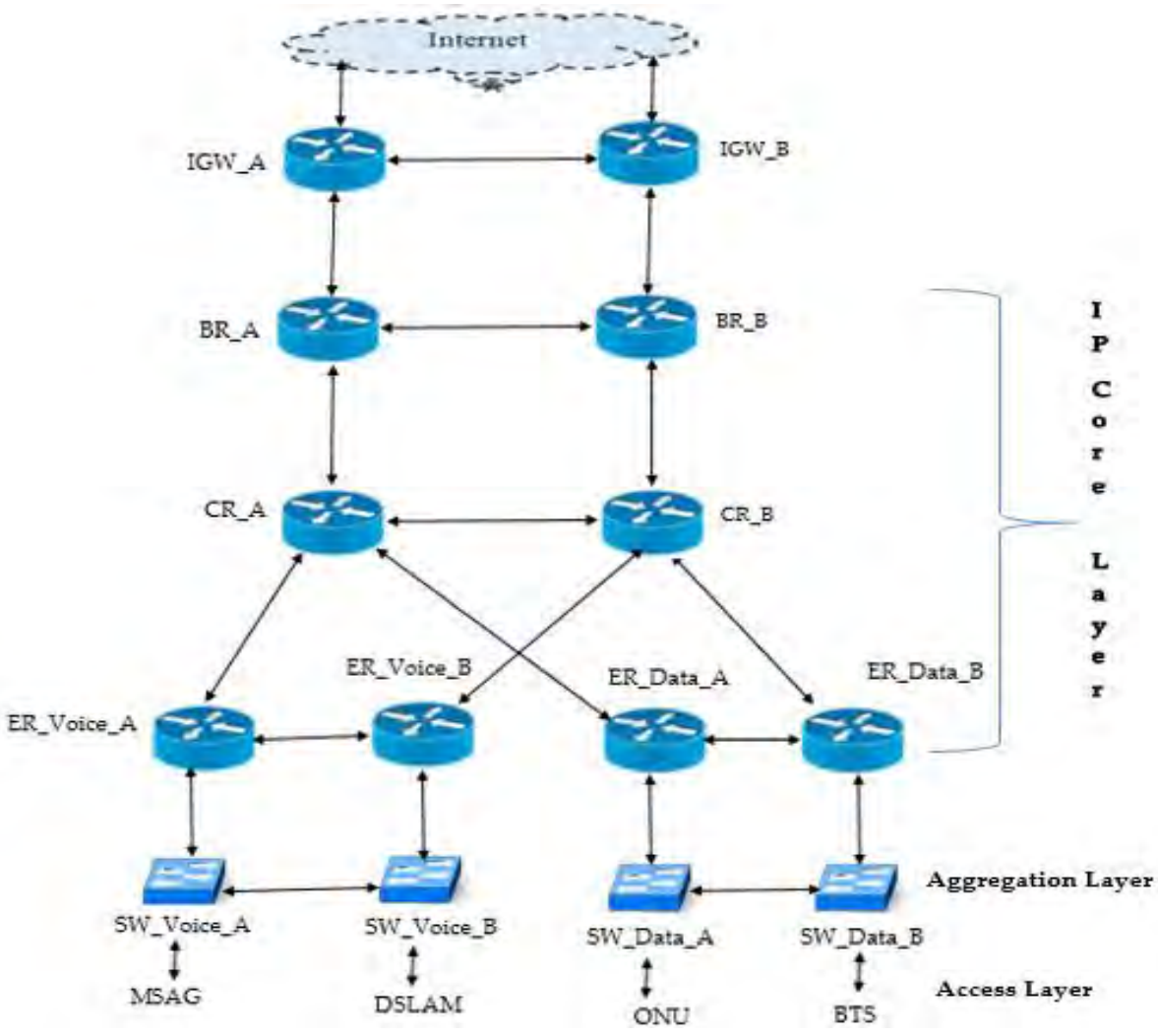


Figure 2.4: One of the two network architectures in ethio telecom [32].

In the above figure, IGW represents international gateway, BR represents bearer router, CR is core router, ER is edge router and SW represents switch. BR, CR and ER all together are the NEs of IP core network.

The following figure shows network architecture of the second vendor in ethio telecom. It differs only by NEs from Figure 2.4.

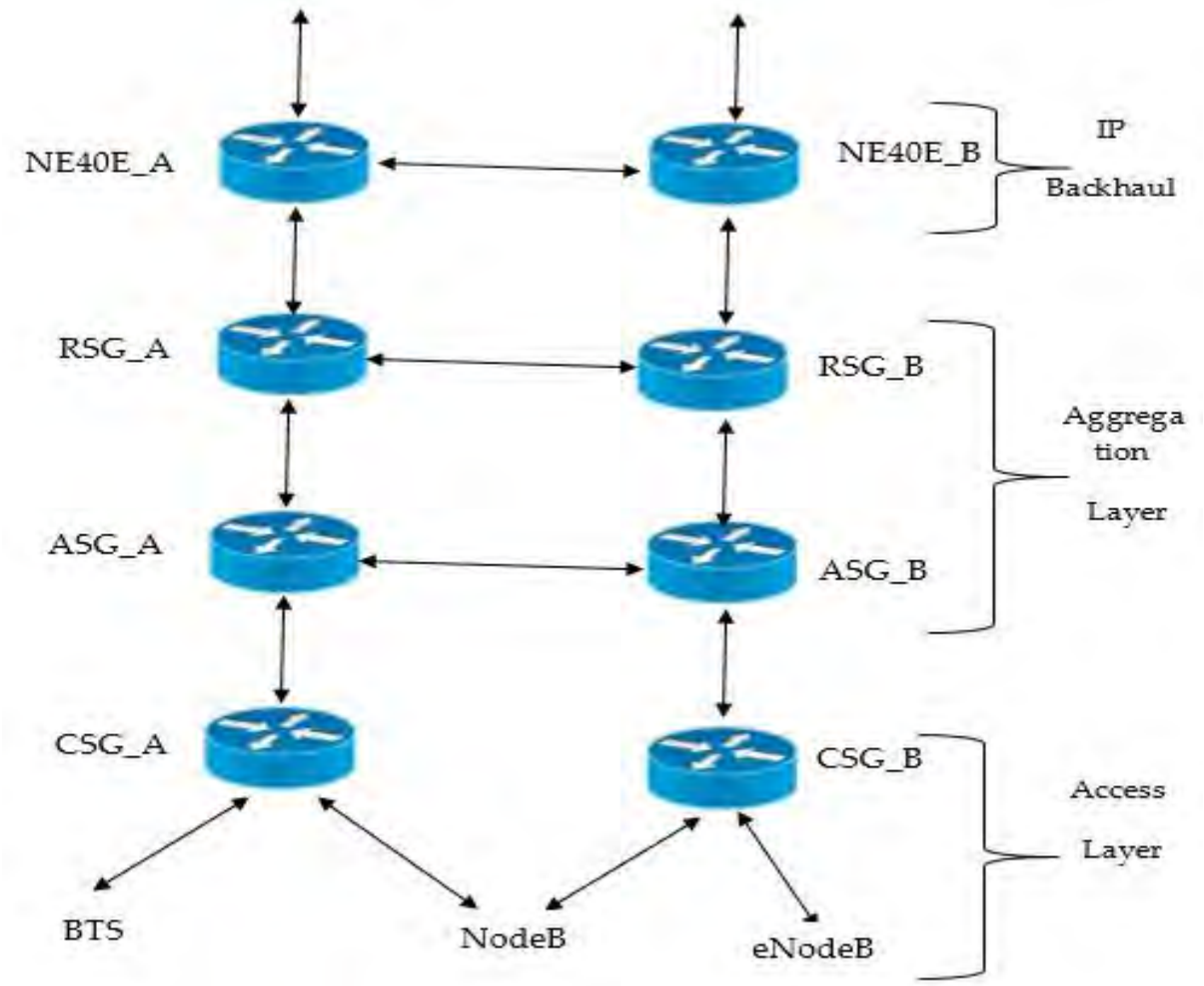


Figure 2.5: The second network architecture in ethio telecom [33].

Here, NE40E represents NetEngine40E Universal Service Router for large scale IP-based networks. There are 5 NE40Es in ethio telecom network each with one backup. RSG is radio side gateway, ASG is aggregation side gateway and CSG is cell side gateway [34]. Core layer in Figure 2.5 is IP backhaul just to distinguish it from IP core layer in Figure 2.4. This separate is necessary since IP backhaul in Figure 2.5 is again connected to IP core network in Figure 2.4. That is, IP backhaul is not directly connected into the Internet via IGWs rather, it is connected to IP core network. This can be seen from the following figure.

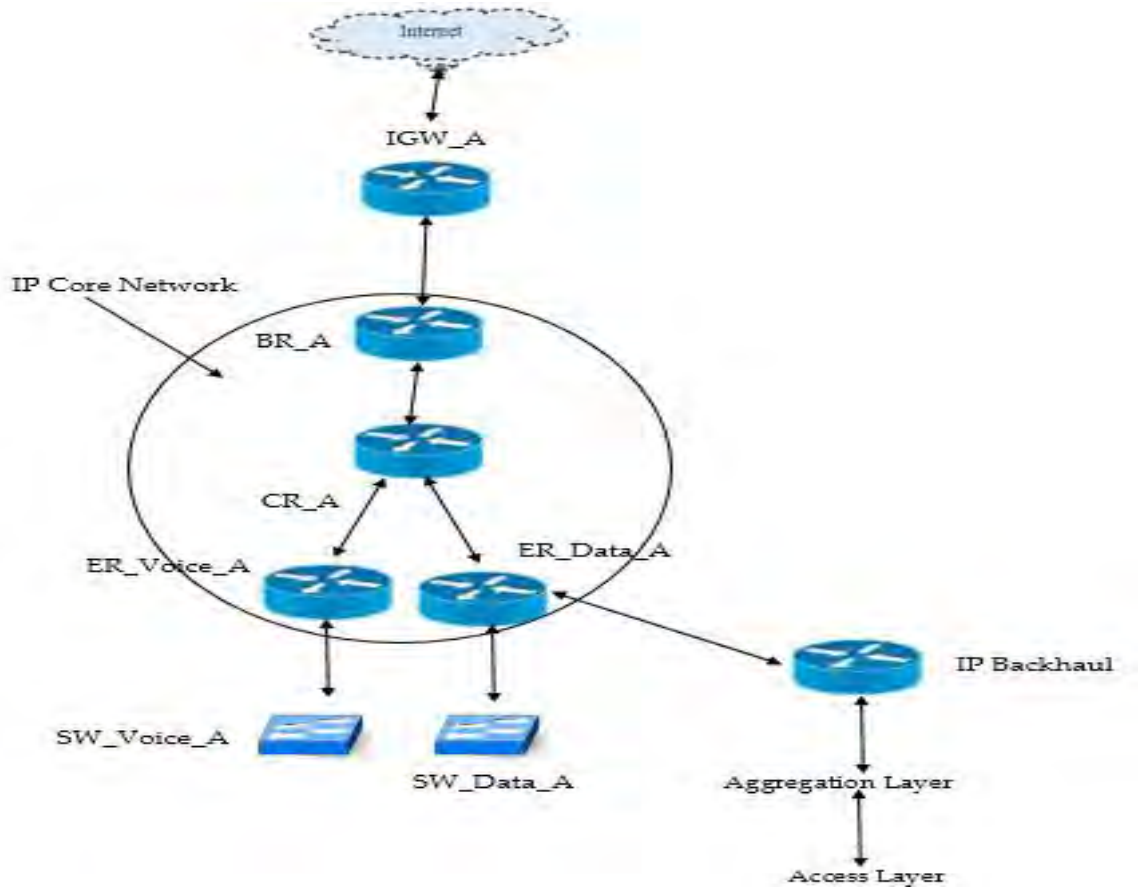


Figure 2.6: The general architecture of network in ethio telecom [34].

Chapter 3: IP Core Network Elements

3.1. Overview

As we have seen in Chapter 2, there are three main network layers in any telecommunication service provider's network architucture. One and the backbone of the network is core layer. Core layer is usually IP based nework, so the name IP core network is given.

Since there are many other subnetowrks such as mobile network, PSTN network, that are connected in IP core network [31], network elements in IP core should have very high capacity and performance.

In this chapter, we describe network elements in IP core layer, their property, their perfromance indicators in general, their capacity and so on, as core layer is the focus of this thesis work. Finally, methods to collect perfromance data from these network elements are depicted.

3.2. IP Core Network Elements

Depending on the services provided by a telecom operator, there may be more than one core networks in a total network. That is, there is its own core for mobile service, for example. All core networks are connected to the center of a network called the backebone of a network. This can be seen in the following figure, Figure 3.1. According to the figure, mobile service, enterprize network, local network and regional network have their own core.

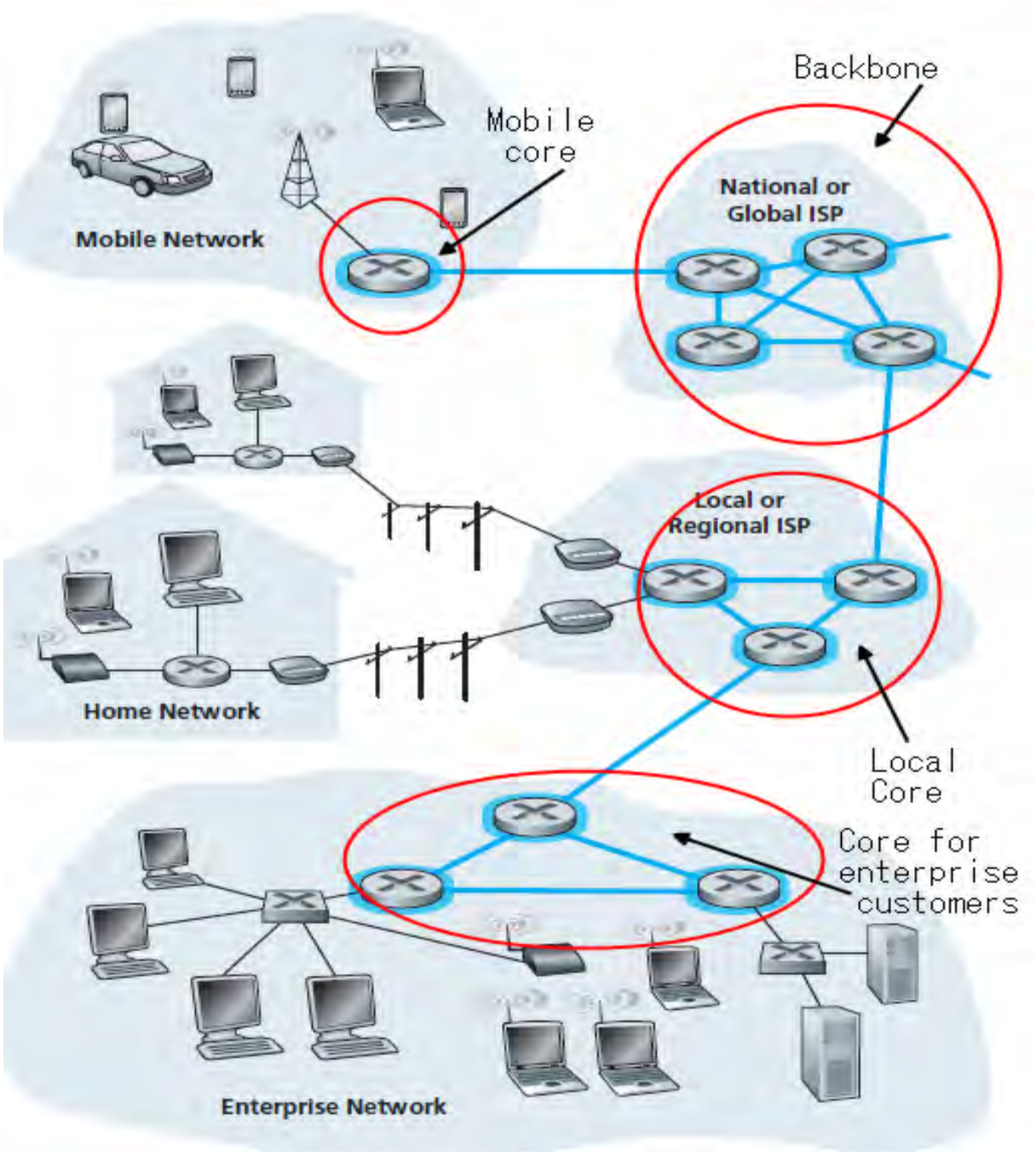


Figure 3.1: How the network core is incorporating other network components [31].

These all divide the network into sub network. These sub networks are connected into the central core, called national/global core.

Depending on the location of core network, there are many elements that are suitable for IP core network layer. Based on their level, their capacity and performance may vary. That is, when their level is higher in the netowork topology, their capacity is high and their performance must also be reasonable.

Core network elements, as we have presented in Chapter 2, are very high speed routers. There are three types of network elements in core network depending on the functions that they support and their capacity. These are backbone/bearer routers (BRs), core routers (CRs) and edge routers (ERs).

i. Bearer Routers (BR)

These are core routers that are directly connected to the Internet via international gateways (IGW). They are also called as back bone routers. These routers are devices that determines the next network point to which a packet should be forwarded toward its destination [32]. They have many ports that can support data transfer up to 10Gbps.

As BRs are very few in number (usually 5-6), located in a center (national Internet Service Provider (ISP) in Figure 3.1) and incorporate many lower level network elements, they need to be highly protected. That is, if one BR is down or get faulty, there should be an alternative path through which communication continues. In order to support this, each BR is connected with each other in a full mesh scenario. Besides, each BR has its own backup that helps to take over all functions when the main BR fails. Each BR is connected with other BRs through its port.

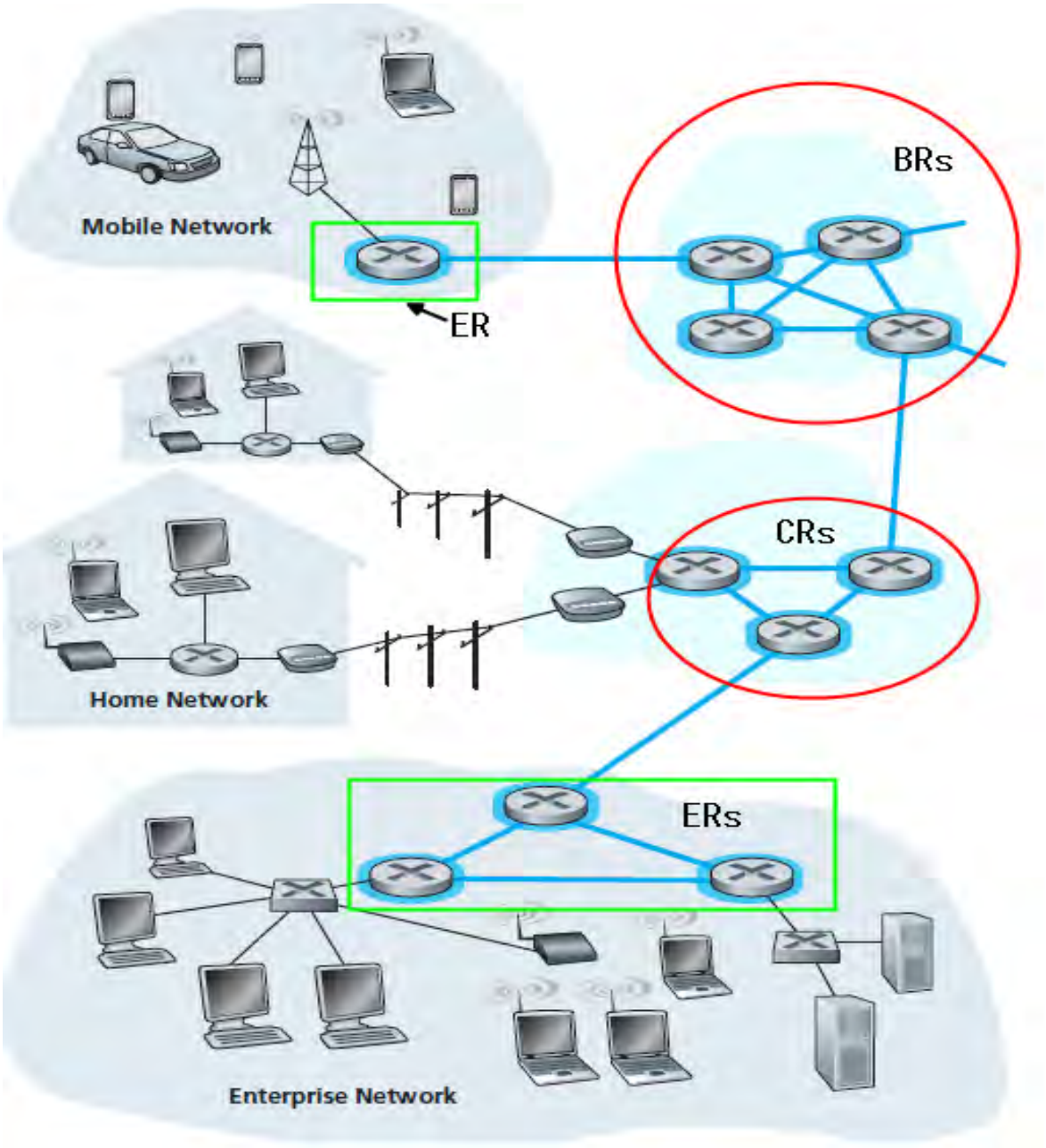


Figure 3.2: BR as core network element in a telecom network [31].

In the above figure, red circled parts indicate core network with clarifying BRs as backbone of a network.

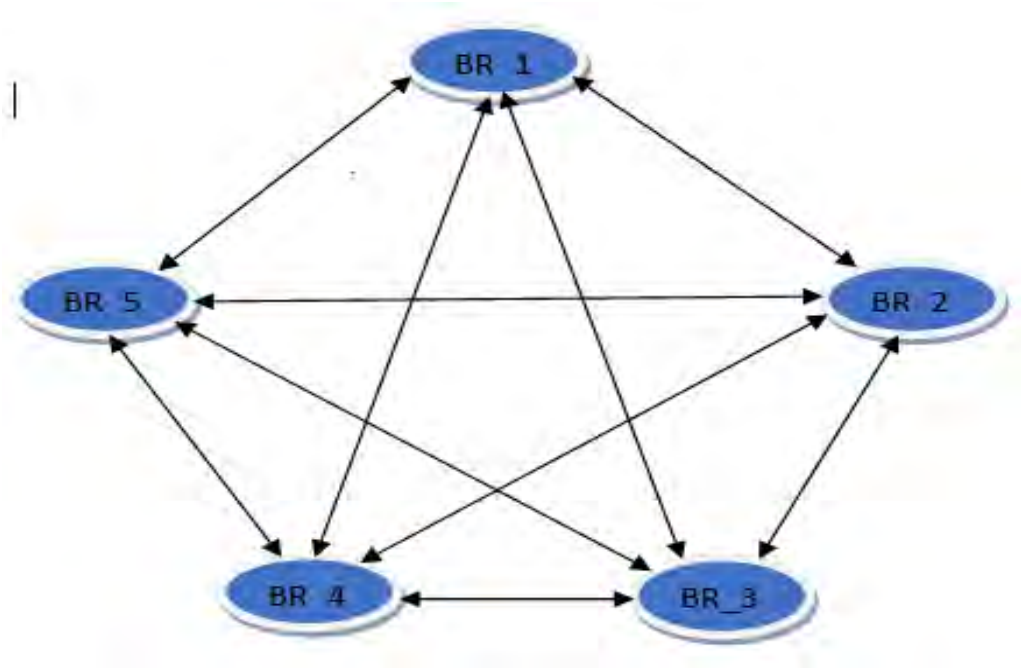


Figure 3.3: Core BR interconnection with each other in a mesh topology [32].

Each BR is also connected with its CR router. The difference here is that there are many nearby CR routers that are connected with each BR routers.

ii. Core Routers (CR)

The CR router has the same role as BR except capacity difference. As it is seen in Figure 3.2, usually 3 or 4 CRs are connected to each BR. They are used as local cores so that each service has its own core [31]. All CRs are interconnected with each other in a full mesh [2].

Since each services can have their own core, there are more than one CRs that are connected into one BR. Figure 3.4 shows connection of CR with BR and ER. ER is an edge router that disprses service types [30].

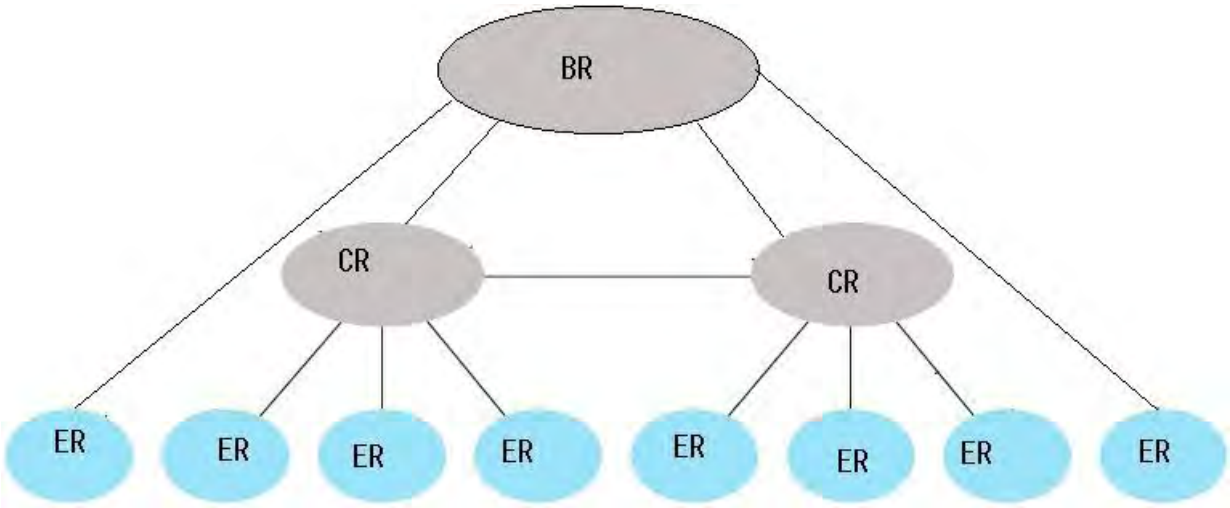


Figure 3.4: Interconnection of core network elements in a telecom network [31].

iii. Edge Routers (ER)

An edge router (also called access router) is a network device located at the boundary of a network that connects to external networks, wide area networks (WANs) and the internet.The IP edge is the service point that sits at the most critical juncture between metro IP Multiprotocol Label Switching (IP/MPLS) network and customer access networks, and this service point is under the most extreme pressure. The IP edge is the support of the IP edge router (PE router), the home of subscriber management and control central of service definition and service delivery. It is the point of service differentiation and service quality, and the pressure point for increasing scale and service granularity [30].

Service providers are trying to make more efficient their network operations, principally by reducing multiple networks to a few or ideally one using their IP edge routers to concentrate multiple services, such as subscribers' broadband and mobile backhaul, or business servicesand WiFi hotspot backhaul. The right router makes it easier to accelerate the delivery of new services and new service bundles. Just as

important as service velocity (the ability to quickly roll out new services), the IP edge router is the key to developing varied and more granular types of services through customization or personalization. As these new services generate more traffic, the IP edge router mustaccommodate the future with high density 10Gbps and 100Gbps capacities, with an eye toward the future at 400Gbps or 1Tbps [30].

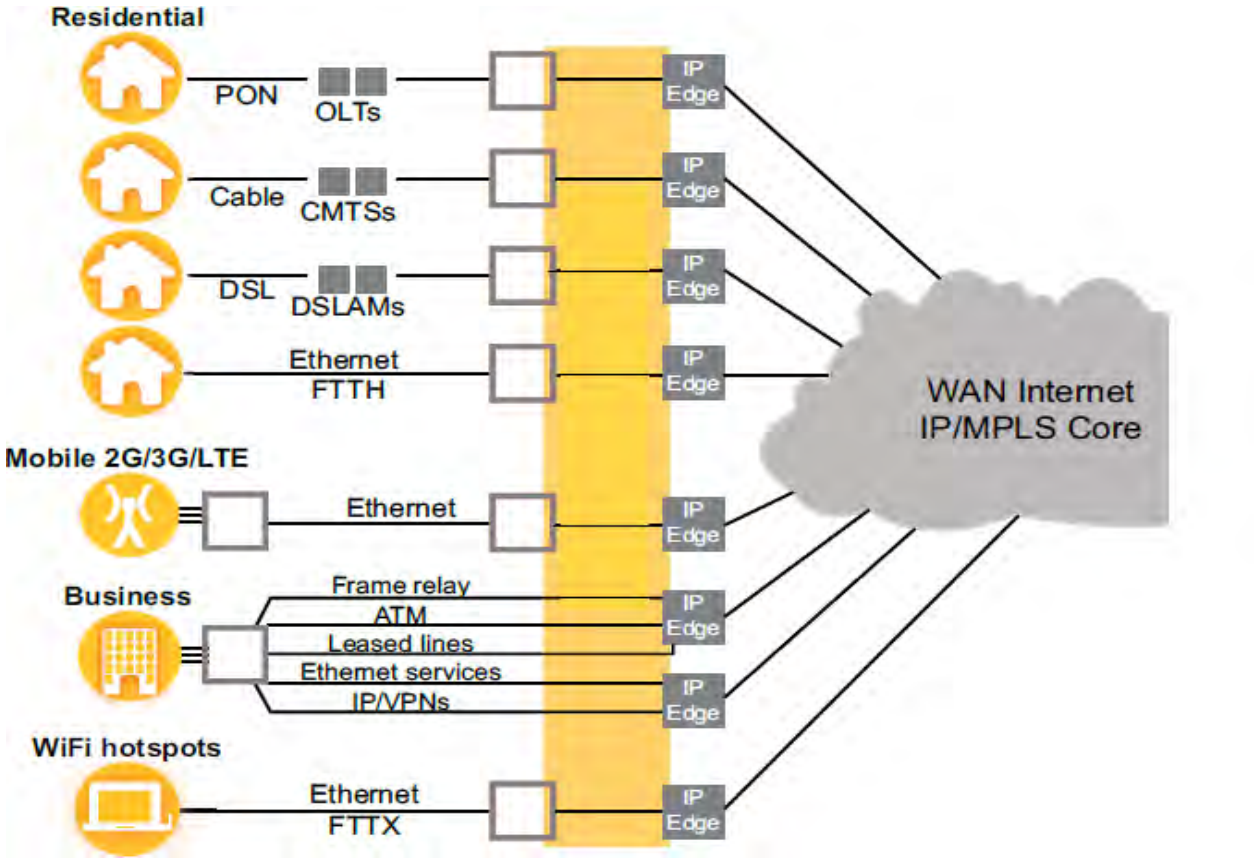


Figure 3.5: ER routers are core routers that are used to divide services [30].

Ethio telecom, one of telecom operators, uses the same architecture as we have seen in the above sections.

3.3. IP Core Network Architecture in Ethio Telecom

The network architecture in ethio telecom incorporates BR, CR and ER in its IP core and NE40E in its IP backhaul [32, 33]. The following figure shows how NEs in IP core network and IP backhaul are interconnected in SiteA.

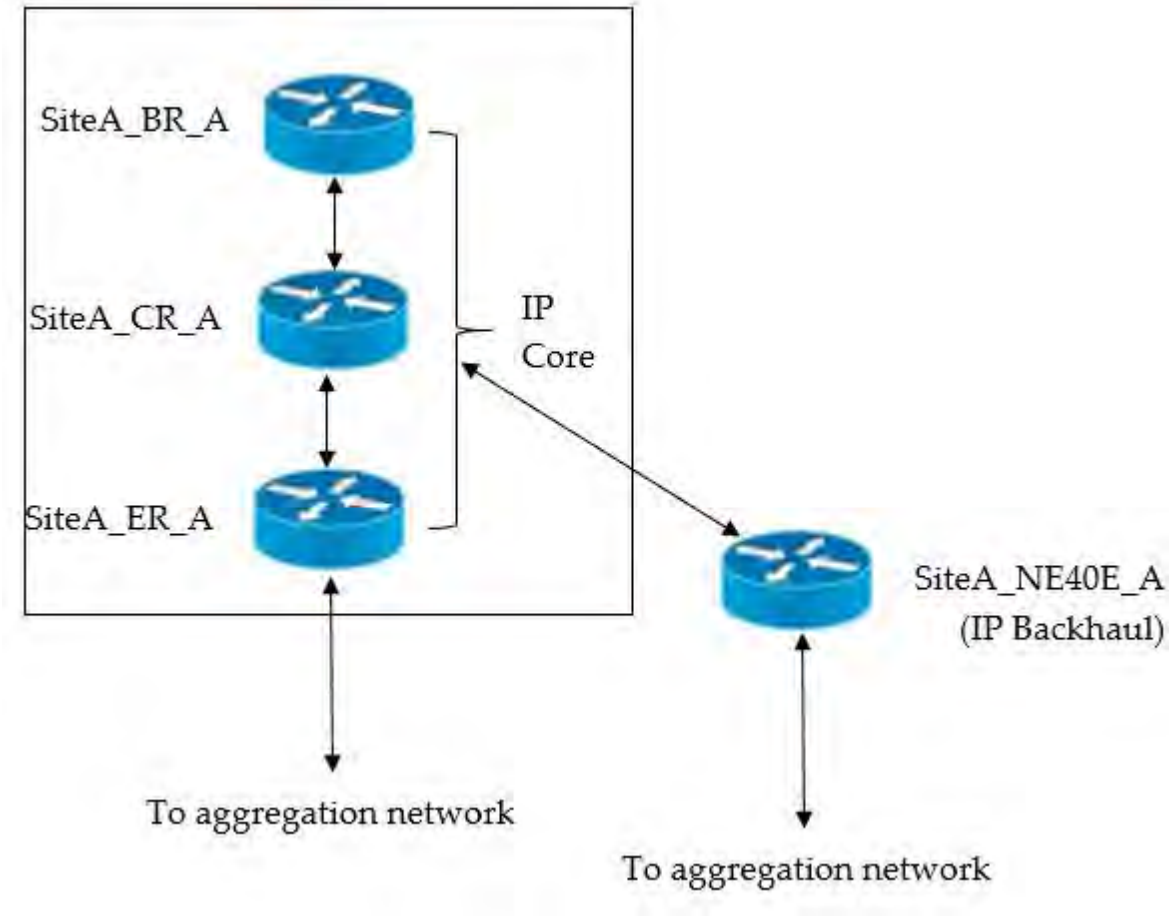


Figure 3.6: Interconnection of NEs in IP core and IP backhaul [32].

There are 5 BRs in five sites that are interconnected with each other in a full-mesh topology. Three or four CRs are connected to one BR. CRs are regional core network elements. Then three or more edge routers (ERs) are connected into one CR to bisect service into voice and data [32]. Aggregation layer NEs are directly connected to ER so that all access NEs that serve one type of service are connected.

IP backhaul is another core network that is deployed to carry mobile services. NE40Es are universal service routers that can be used in metropolitan area networks [34].

3.4. Methods of Monitoring a Network

There are two basic methods for measuring and monitoring a network. These are active and passive monitoring methods, each with its own set of challenges [9, 10, 11].

a. Active Monitoring Method

Active monitoring method is packet measuring techniques that use special probe packets that are sent over the network. Unlike passive measurements, active measurements generate additional network traffic so they may possibly disturb the normal traffic flow. This is why active measurements have to be carefully planned before execution and usually the bandwidth reserved for the probe packets is limited to fewer than 5 percent of the path's total capacity [10, 11].

b. Passive Monitoring Method

The idea behind passive methods is to capture packets in order to store and collect information from various fields within the packet header. Unlike active methods, passive monitoring systems are non-intrusive and do not load the network [10, 11]. That means, in a passive monitoring technique, no packets are sent to the network by the monitor.

Passive monitoring is usually performed in two alternative ways: by using existing network devices to gather statistics or by introducing separate monitoring equipment to the network [11, 23]. Using existing network devices relies on switches and routers to gather statistics of the traffic. The statistics are fetched from the devices for analysis. The second alternative, using separate equipment, is more effective and customizable

way of passive analysis. It can be used to store all the traffic traversing through the monitoring point or just collecting the statistics required for the analysis.

Combining the above two methods, we can use a hybrid method to monitor and measure a network. In this thesis, we used both active and passive methods to collect data, even though passive data collection method is used in most. Active method is used to cross check the data reality collected using passive monitoring method.

3.5. Connecting to a Network

To monitor the IP core network performance and do analysis, we have to get its data. To get data from really existing system, we have to have connection with the real network. In this section, we present methods of connection of IP core network to a real network in order to get its performance data. There are two main methods to connect a certain system to the real network [23]. These are:

- Using link taps
- Mirroring a port

a. Using Link Taps

A Network Test Access Point (TAP) is a hardware device which provides a way to access the data flowing across a computer network. It is a passive splitting mechanism installed between a 'device of interest' and the network. It should have at least three ports: an **A** port, a **B** port, and a **monitor** port. TAPs transmit both the send and receive data streams simultaneously on separate dedicated channels, ensuring all data arrives at the monitoring device in real time. This is shown using Figure 3.6.

b. Mirroring a Port

This is a method by which switches copy the activity of one or more ports through a Switch Port Analyzer (SPAN) port, also known as a mirror port. An analysis device can then be attached to the SPAN port to access network traffic.

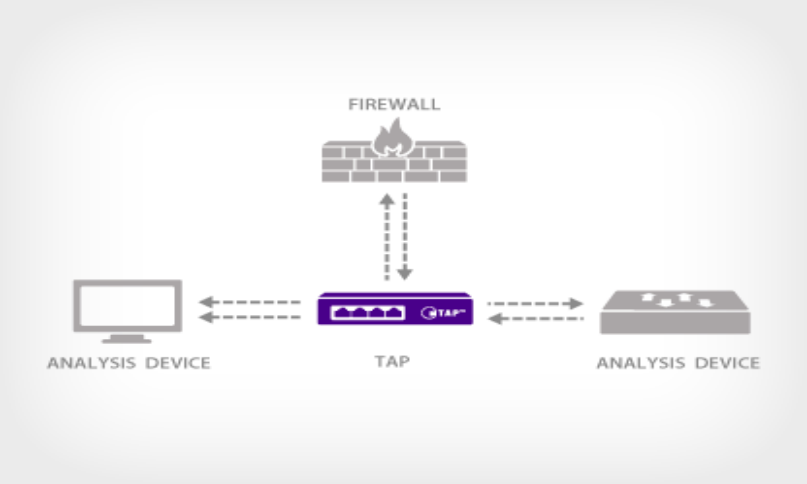


Figure 3.7: Connecting to the network using TAP [23].

A port mirror is active packet duplication, meaning that a network device physically has the duty to copy packets onto a mirror port. This means that the device has to carry on this task by using some resources (e.g. CPU) and that both traffic directions will be copied into the same port.

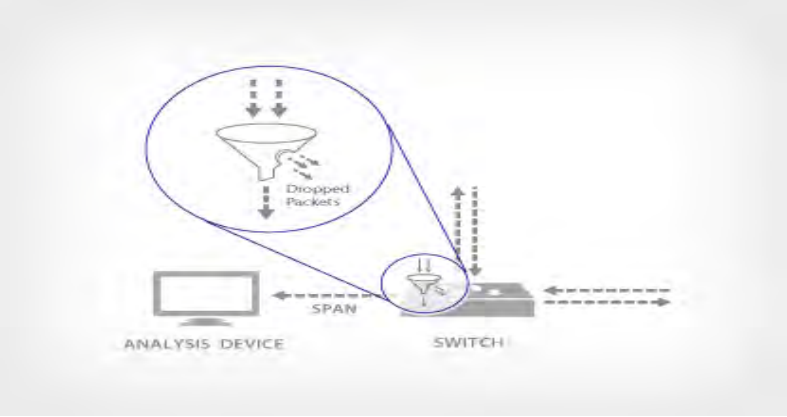


Figure 3.8: Connecting to the network using mirroring [23].

In ethio telecom, we use mainly link TAP method to collect data from IP core network devices and to monitor them. There is also active data collection (e.g. network mirroring) method in ethio telecom as supportive network monitoring and data collection method. This method usually is used to confirm the data reality that is collected using passive data collection method. This is because, if we use active data collection method, like port mirroring, as main data collection method, it generates its own load on the network. This in turn may lead into miss judgment on the network analysis.

The following figure shows how U2000, one of the monitoring tools of IP core network, is connected to real network system as network TAP in ethio telecom IP core network [33].

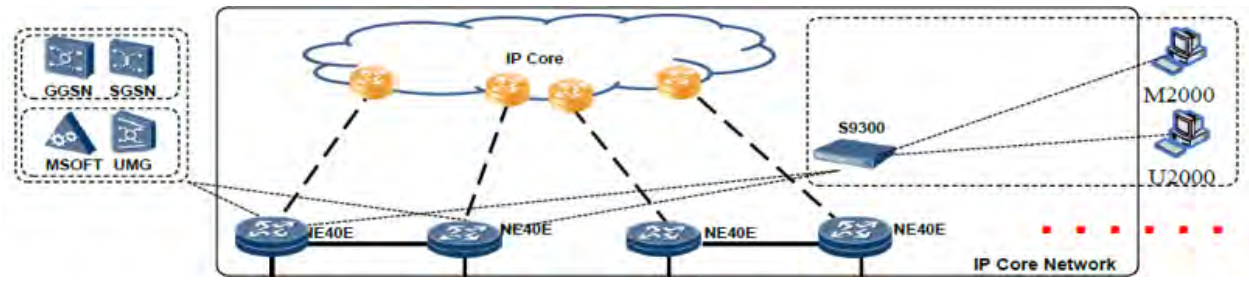


Figure 3.9: Network TAP in IP core network [5, 34].

Chapter 4: IP Core Network Performance

4.1. Introduction

After connecting to the network, we have to know which parameters are used to monitor network performance. The most basic parameters (Key Performance Indicators, KPIs) are described in the following part.

4.2. Packet Loss Ratio

Packet Loss Ratio is one of the most important parameters for identifying poor network conditions since it affects data throughput performance and the overall end-to-end data transfer quality.

Packet loss occurs when one or more packets of data travelling across a network fail to reach their intended destination. It occurs if network discards packets when a router or other network device is overloaded and cannot accept additional packets at a given moment. Figure 4.1 describes the concept of packet loss in brief.

Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion, and so on. However, many studies generally characterize five primary causes of packet loss in IP based networks [35, 36].

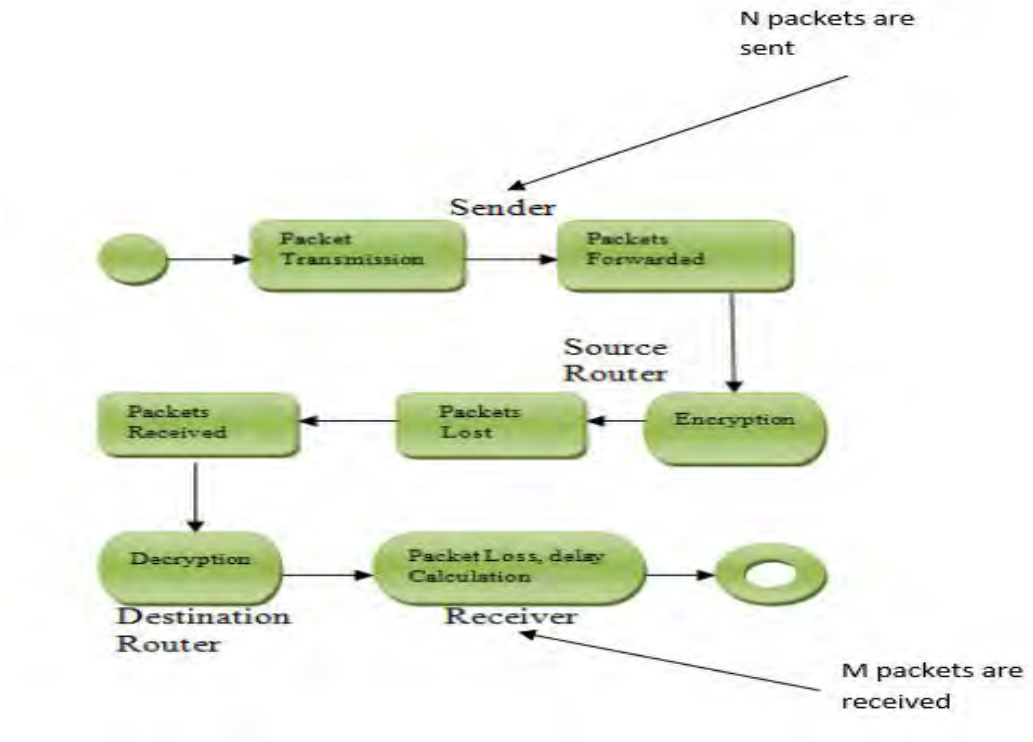


Figure 4.1: Concept of the occurrence of packet loss in a packet switched network [35].

These five main causes of packet loss are:

1. **Congestive Loss**

This type of loss results when the network is unable to support the amount of traffic that it receives. Router buffers become full, forcing it to drop packets. Rarely is just a single packet dropped—usually congestion-related packet loss is characterized by patterns consisting of sequences of consecutive dropped packets. This is because data travels through multiple devices and links during its trip across the network.

The effect of congestive loss starts from minor to very serious problem depending on the network application. Most applications are able to gracefully handle this, and the user probably won't ever notice it. The user's application realizes that a packet was lost, slows down its transfer speed, and re-transmits the data. If this was a file download, an

email, or another non real-time application, the effect will be minimal as long as the packet loss doesn't continue to happen.

If the network application is a phone call and the network loses some data, there is no time to resend the packets since it is a real-time conversation. The user will typically hear breaks in the audio during small packet loss, and potentially lose the phone call if the packet loss is severe.

Another critical application that has a low threshold for packet loss is video conferencing. If data is lost between the two end points, the video will show artifacts and the audio will be distorted.

There are two main ways to help reduce the effect of packet loss due to network congestion:

- Increase the bandwidth of the congested link(s).
- Implement Quality of Service (QoS) to give priority to real-time traffic. This will not help the congestion of the link, but it can give priority to applications like voice or video which lowers the likelihood of a drop.

2. **Device (Router/Switch/Firewall/etc.) Performance**

The effect of network congestion on packet loss can be minimized by increasing the bandwidth. If the network bandwidth is adequate, user can still face an issue if router/switch/firewall is not able to keep up with the traffic.

In some scenario, after a link's bandwidth is upgraded, users can still experience performance issues. To check if the link's bandwidth is really upgraded or not, usually

users look at traffic report but they can get that they were at full capacity during peak hours of the day. The issue could be that the device is not able to keep up with the traffic, and users have hit the maximum throughput that their hardware can provide. The traffic is reaching the device, but the device's CPU or memory is maxed out and not able to handle extra traffic. This results in packet loss for all traffic that is beyond the capacity of the box.

Usually replacing hardware with a new appliance that can handle the maximum throughput, or potentially clustering additional hardware to increase the throughput are the two most followed solutions to reduce the effect of device's performance on packet loss.

3. **Software issues on a network device**

While we can hope that the software written for our network devices is perfect, sometimes it can be assured that it is not. These network devices are extremely complex, and it is a matter of time before a user falls upon a bug (malwares). These bugs can cause new features to not work at all when users deploy them, or can go undetected for a while before user may notice performance issues.

Once the performance issue is detected and troubleshooting has started, these types of issues are usually found using system logs and packet captures. User must upgrade the software on the affected device(s).

4. **Faulty Hardware or Cabling**

Sometimes, traffic report may show that network links are not over-utilized, and the hardware utilization is within specification. The next common issue that can lead to packet drops would be a physical component that is malfunctioning.

If hardware is not working properly, it will usually lead to error messages being seen on the console of the device or within system logs. If there is a link issue, it can usually be seen as errors on an interface. This can be seen on both copper cabling and fiber optic.

Best recommendation is replacing the faulty hardware, or repairing the faulty link.

5. **Loss due to transmission bit errors**

Bit errors result from transmission channel noise, distortion, signal weakness, bit synchronization, or attenuation. Packet loss resulting from bit errors is characterized by low-density individual packet drops at random intervals. Unlike the case with congestive loss, packet loss resulting from transmission bit errors (as measured in loss percentage) usually remains constant and does not change with the level of network utilization.

These are the most common reasons for packet loss on a network, but there are many other reasons that can contribute to packet drops. The best way to determine the root cause is through a network assessment and detailed troubleshooting.

4.3. Packet Transfer Delay

Packet transfer delay in point-to-point communication is the time between a packet entering a router in one PoP (an ingress point) and its leaving a router in another PoP (an egress point). It measures the one-way delay experienced by packets from an ingress point to an egress point across an ISP's network and provides the most basic information regarding the delay performance of the ISP's network.

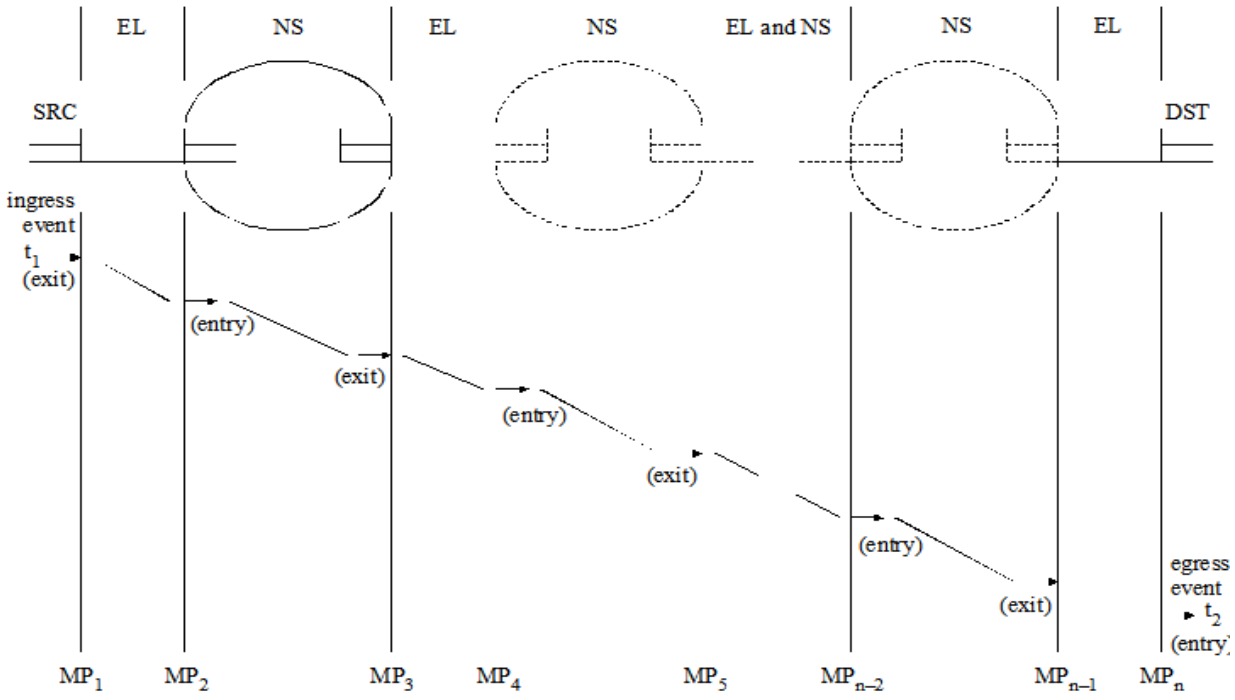
Packet transfer delay is usually a concept in packet switching technology. The sum of store-and-forward delay that a packet experiences in each router gives the transfer or queueing delay of that packet across the network. It is the time, $(t_2 - t_1)$ between the occurrence of two corresponding IP packet reference events, ingress event at time t_1 and egress event at time t_2, where $(t_2 > t_1)$.

The most adopted delay condition for any real communication system is

$(t_2 - t_1) \leq T_{max}$ where T_{max} is the ITU standard

That is, the time difference between the occurrence of two corresponding IP packet reference events, (or delay) should not be exceeded the international delay standard set by ITU. The ITU standard for end to end packet delay is 150ms [37].

Packet transfer delay provides a basis for determining whether a service provider has implemented an efficient network design with sufficient levels of network resources for its IP network.



DST	Destination Host
EL	Exchange Link
MP	Measurement Point
NS	Network Section
SRC	Source Host

Figure 4.2: Concept of the packet transfer delay in a packet switched network [37].

The end-to-end IP packet transfer delay is the one-way delay between the MP at the SRC and DST

Packet transfer delay is influenced by:

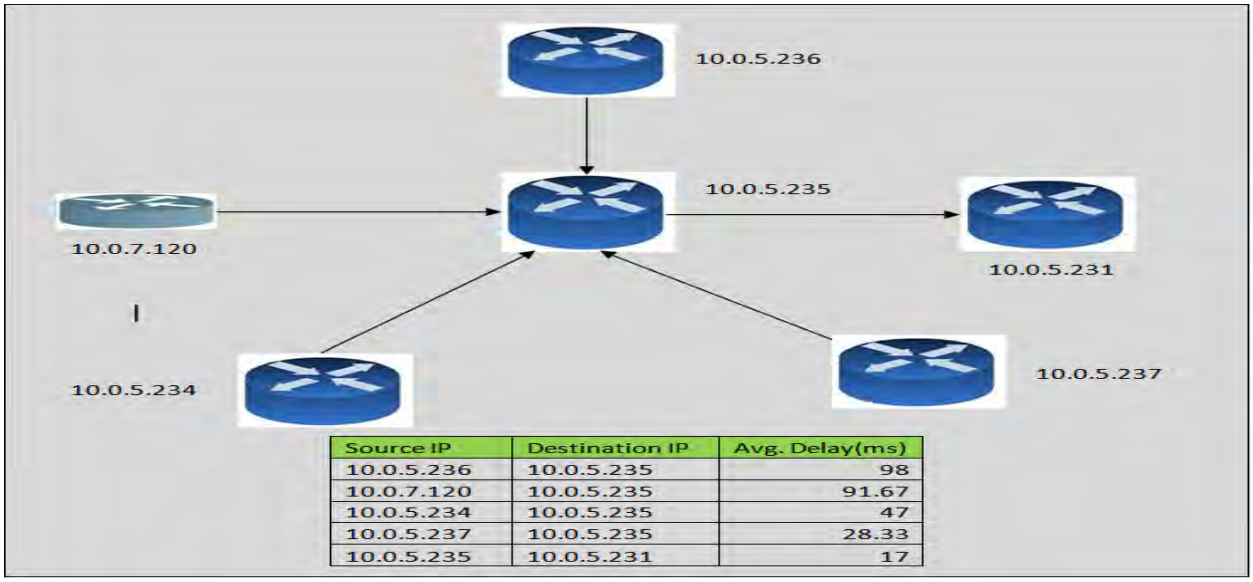
- The level of network congestion and
- The number of routers along the way of transmission

There are four sources of packet transfer delay:

1. Nodal processing:
   - ✓ During processing of a packet, routers may check for bit-level errors in the packet that occurred during transmission as well as determining where the packet's next destination is.
     - ❖ Check bit errors
     - ❖ Determine output link
2. Queueing:
   - ✓ **Queueing delay** is the time a job waits in a queue until it can be executed.
     - ❖ Time waiting at output link for transmission
   - ✓ Depends on congestion level of router
3. Transmission delay:
   - ✓ Is the amount of time required to push all the packet's bits into the wire.
   - ✓ Or, this is the delay caused by the data-rate of the link.
   - ✓ It is proportional to the packet's length in bits.
   - ✓ Let:
     - ❖ R=Link bandwidth (bit/s)
     - ❖ L=Packet length (bits)
     - ❖ Time to send bits into link = L/R
4. Propagation delay:
   - ✓ It is the amount of time it takes for the head of the signal to travel from the sender to the receiver.
   - ✓ It can be computed as the ratio between the link length and the propagation speed over the specific medium.

- ✓ Let:
  - ❖ d = Length of physical link
  - ❖ s = Propagation speed in medium
  - ❖ Propagation delay = d/s

The following figure shows practical example of packet transfer delay from and to the particular router (whose IP address 10.0.5.235).



Source IP	Destination IP	Avg. Delay(ms)
10.0.5.236	10.0.5.235	98
10.0.7.120	10.0.5.235	91.67
10.0.5.234	10.0.5.235	47
10.0.5.237	10.0.5.235	28.33
10.0.5.235	10.0.5.231	17

Figure 4.3: Practical example of packet transfer loss of a given router.

4.4. Jitter

Jitter is a variation in packet transit delay caused by queuing, contention and serialization effects on the path through the network.

In general, higher levels of jitter are more likely to occur on either slow or heavily congested links.

Main types of jitter:-

- ✓ Type A

- ✓ Type B
- ✓ Type C

Type A – constant jitter.

- This is a roughly constant level of packet to packet delay variation.

Type B – transient jitter.

- This is characterized by a substantial incremental delay that may be incurred by a single packet.

Type C – short term delay variation.

- This is characterized by an increase in delay that persists for some number of packets, and may be accompanied by an increase in packet to packet delay variation.
- Is commonly associated with congestion and route changes.

The following picture shows the comparison of jitter and delay for one route.

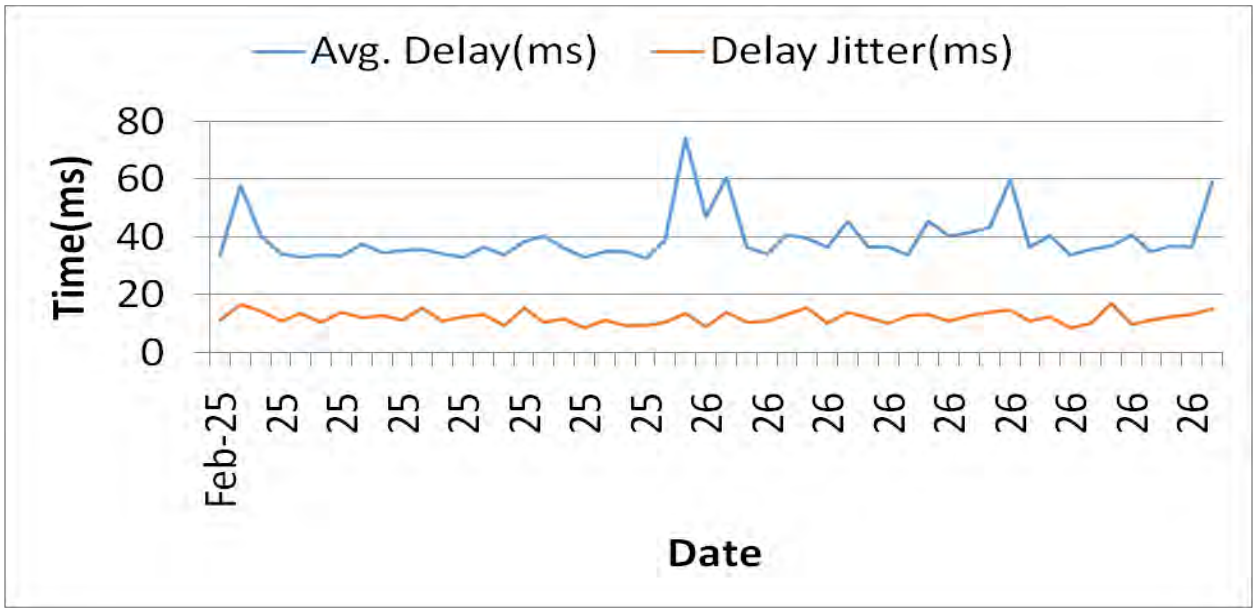


Figure 4.4: How jitter and delay is interrelated in a real scenario.

4.5. Bandwidth Utilization

Bandwidth is the amount of data that can be carried from one point to another in a given time period, usually expressed in bps [7]. A network in a given link (interface) with an allocated bandwidth can use some amount from its total capacity. For example, if an interface A has 10 Gbps, it can support data flow up to 10G in a second. If a flow uses n bits per second and the capacity of the network is N bits per second, then the Bandwidth Utilization of the network is:

$$BW\ (\%) = (n/N)*100 \quad \text{.....(4.1)}$$

A network path usually consists of a succession of links, each with its own bandwidth, so the end-to-end bandwidth is limited to the bandwidth of the lowest speed link (the bottleneck).

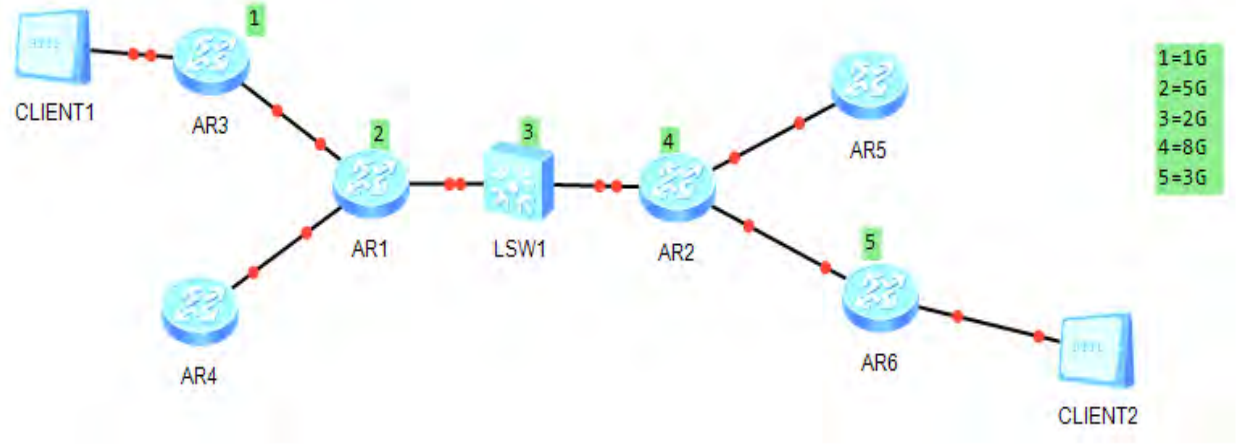


Figure 4.5: How link bandwidth is limited to the lowest link [7].

For example, CS_01_CS_A.HW.Microwave.CAAZ.AA/Giga bit Ethernet has many interfaces. Among them, 3/0/16 uses its 1G interface speed as the following fig.

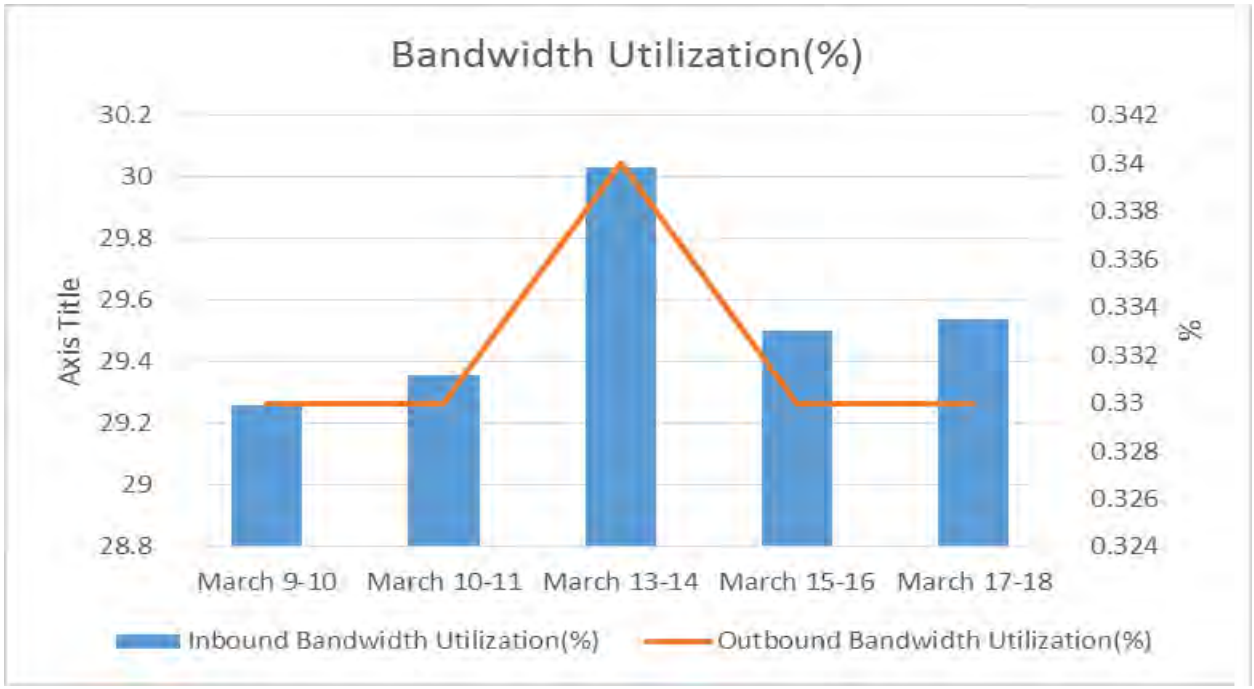


Figure 4.6: Example of Bandwidth utilization for particular port.

4.6. CPU Usage

The CPU executes operating system instructions, such as

- System initialization,
- Routing functions, and
- Switching functions.

CPU usage refers to a device's usage of processing resources, or the amount of work handled by a CPU. Actual CPU utilization varies depending on the amount and type of managed computing tasks. Certain tasks require heavy CPU time, while others require less because of non-CPU resource requirements.

For example, in the two gateways the CPU usages in their particular slots are shown as follows.

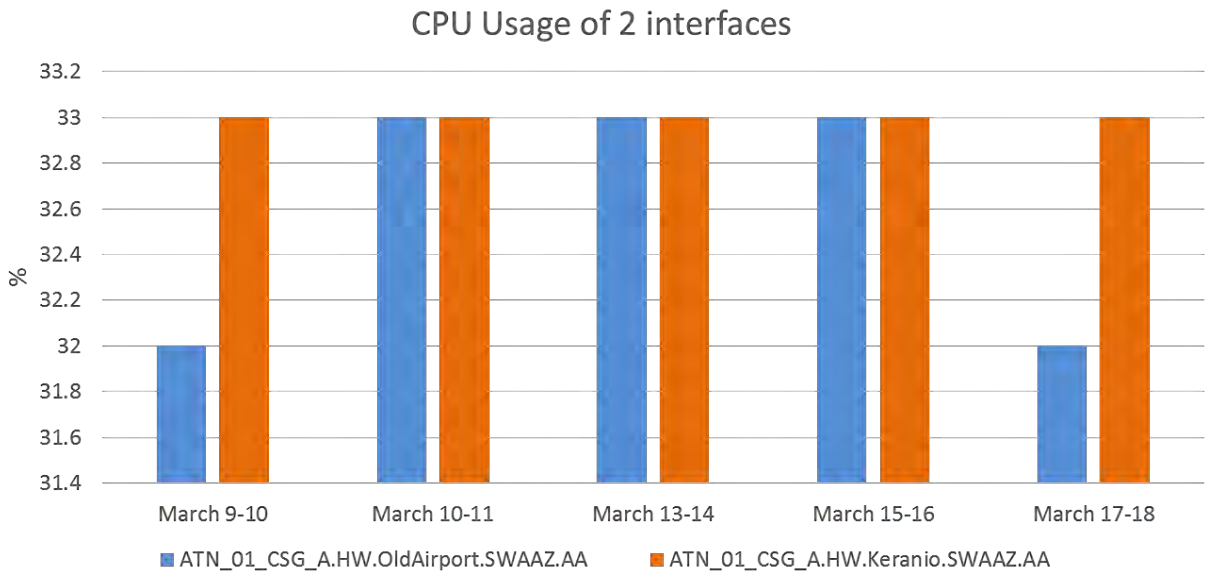


Figure 4.7: CPU usages of a specific network element in one week.

4.7. Memory Usage

There are two main types of memory, as any computing devices, in routers. These are:

- Random-Access Memory (RAM)
  - ✓ Stores the instructions and data needed to be executed by the CPU.
  - ✓ RAM is used to store these components:
    - ❖ Operating System
    - ❖ Running Configuration File.
    - ❖ IP Routing Table
    - ❖ Packet Buffer
- Read-Only Memory (ROM)

This type is a form of permanent storage. There are many slots in one network element. For example, in a specific gateway the memory usage of slot 1 and 4 is as shown in the below picture.

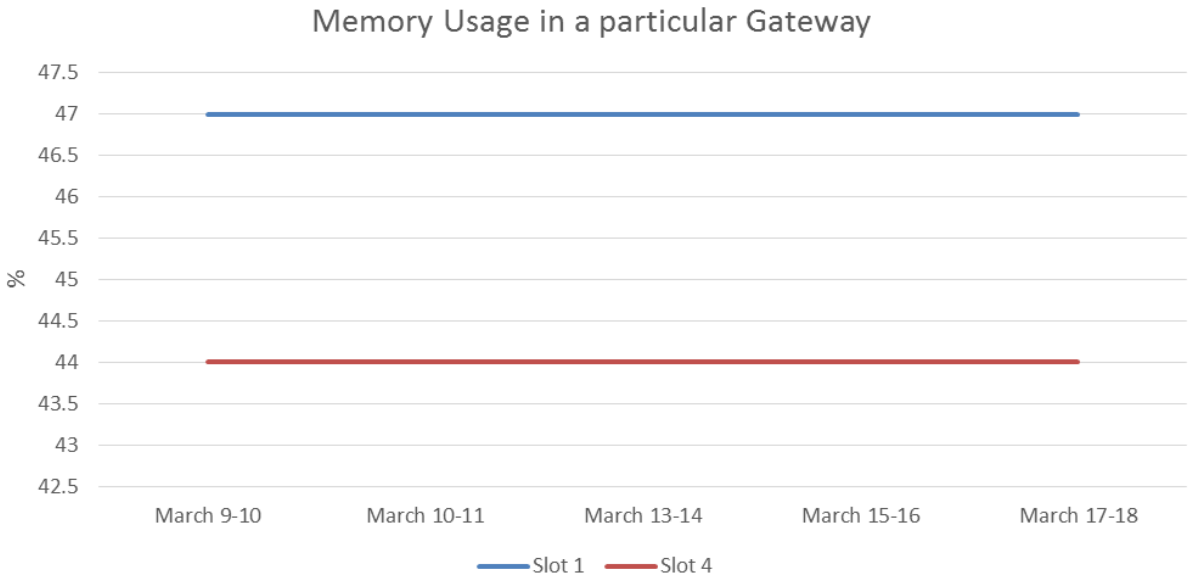


Figure 4.8: Memory usage of a specific router in a week.

Chapter 5: Modeling of the Network KPIs

5.1. Introduction

Modeling is generally the process of representing a real-world, or systematic description of object or phenomenon that shares important characteristics with the object or phenomenon [46]. In science and engineering, there are three main types of system modeling. These are:

- Mathematical modeling,
- Physical modeling and
- Process modeling

Mathematical modeling describes systems by using mathematical symbols and relations. Mathematical modeling is constructed using procedures (or algorithms) and mathematical equations.

Physical modeling usually describes systems by physical structures (e.g. aircraft by its physical body) and relations. This type of modeling is applied to high fidelity (detailed) system simulations.

Process modeling is a type of modeling that models the process a system performs. It represents dynamic relations by mathematical and logical functions.

Modeling network is usually done by mathematical modeling using mathematical equations and procedures. But sometimes the mathematical modeling of network parameters is secret for users and even for operators. This is because tools that are used

in network performance monitoring and analysis of network parameters are vendor based. It is black body that gives output for a given input. Nobody knows the real mathematics, hence the algorithm, that this black body does to yield value for a specific KPI, except the vendor.

In addition to this, it is very difficult to deploy a third party performance analysis tool because of the agreement between vendors and telecom operators. Vendors usually force telecom operators to use their own tools to do their respective performance analysis. This may result in blind judgment on the measured values of the parameters.

This chapter focuses on mathematical modeling of the performance parameters that have been described in Chapter 4.

5.2. Packet Delay Modeling

One of the most important performance analysis parameter in a network is the average delay required to deliver a packet from origin to destination [38]. So it is very important to understand the nature and mechanism of packet delay.

There are many mechanisms to model network parameters. Among them, Queuing Theory [39, 40, 41] gives a framework for analyzing packet delay. Its use often requires simplifying assumptions since more realistic assumptions make meaningful analysis extremely difficult. For this reason, it is sometimes impossible to obtain accurate quantitative delay predictions on the basis of queuing models. Nevertheless, these models often provide a basis for adequate delay approximations, as well as valuable qualitative results and meaningful approaching.

As we have seen in Chapter 4, there are four main sources of delay in a network. These are processing delay, queuing delay, transmission delay and propagation delay. These all can happen in a single link. That means, total delay in a single link is the summation of each delay components in that link. The overall delay is the sum of delays on each subnet link traverse by the packet.

The following assumptions have been set before developing the model of packet delay in a network.

Assumptions

- Ideal channel conditions (no transmission errors or hidden stations)
- The contending stations are of fixed number n and
- Each station has always a packet available for transmission of the same fixed size.
- The collision probability of a data packet transmission is constant
- Independent of the number of collisions the packet has suffered in the past

The Delay Equation

The delay equation below describes the packet delay at a single node along its route from source to destination.

$$D_{total} = D_{proc} + D_{queue} + D_{trans} + D_{prop} \quad \text{.....5.1}$$

Let's see each of them in detail:

Processing Delay (D_{proc})

The nodal processing delay, D_{proc}, is the time that a node spends processing a packet. This includes time for error checking, time for reading the packet header, and time for

looking up the link to the next node, based on the destination address. Although the processing may sound complicated, the nodal processing delay is usually **negligible** compared to other terms in the delay equation.

Transmission Delay (D_{trans})

The transmission delay, D_{trans}, is the time required to put an entire packet into the communication media. In another word, it is the amount of time required for the router to push out the packet. If L denotes the length of the packet by bits, and R (bits/sec) denotes the transmission rate of the link from first router to second router, then transmission delay will be:

$$D_{trans} = \frac{L}{R} \quad \text{.....(5.2)}$$

Where, L is the length of a packet in bits and R is the transmission rate in bits per time unit.

Queueing Delay (D_{queue})

The queueing delay, D_{queue}, is the time that a packet spends in a queue at a node while waiting for other packets to be transmitted. If the node is a high-speed router then there is one queue for each outgoing link, so a packet waits only for other packets that are going across the same link.

Propagation Delay (D_{prop})

The propagation delay, $D_{prop,}$ is the time that it takes a signal change to propagate through the communication media from a node to the next node. That is, it is the time it takes a bit to propagate from one router to the next router. It can be computed using the

following equation. If d denotes the distance between two routers and s denotes the propagation speed, the propagation delay will be:

$$D_{prop} = \frac{d}{s} \quad \text{.....(5.3)}$$

The total average delay as indicated in (5.1) is the sum of these all delays. That is:

$$D_{total} = D_{proc} + D_{queue} + D_{trans} + D_{prop}$$

The propagation delay (D_{prop}) depends on the physical characteristics of the link and is independent of the traffic carried by the link. The processing delay (D_{proc}) is also independent of the amount of traffic handled by the corresponding node if computation power is not a limiting resource. Beside this, propagation and processing delays are very small compared to the rest two. These can be justified by comparing the figurative values of all delay sources.

Examples 1:

If the distance between two routers is 10km, and since usual medium between two routers is fiber, we can calculate the time taken to travel for one bit from one router to another as follows. Assume

- Refractive index of the fiber~1.5
- Speed of light in fiber = 3x10^8 / 1.5 = 2x10^8 m/s

Then the propagation delay can be calculated using Equation (5.3) as follows.

$$\frac{d}{s} = \frac{1000}{2*10^8} = 0.00005s == 0.05ms = \mathbf{50\mu s}$$

Example 2:

Given that average transmission rate of routers= 291930992bits/sec≈ 300X10^6bits/sec and average length of packets= 15200 bytes=15200X8= 121600 bits, then we can compute transmission delay using Equation (5.2) as follows.

$$D_{trans} = \frac{121600 bits}{300 * 10^{6} bits / \sec} \approx 4 * 10^{-4} \sec = 0.4 ms$$

In the same way, we can calculate and get typical values for processing delay and queueing delay. Moreover, most networking books mention values for the four sources of delay as the following table.

Delay Sources	Delay
Transmission Delay	1ms
Propagation Delay	10μs
Processing Delay	10μs
Queueing Delay	100μs-∞

Table 5.1: Typical values of delay sources.

From the above table, we can see that values of propagation delay and processing delay are very small (order of micro) compared to the rest two sources of delays. So, we can ignore them for practical usage and modeling of total delay. So the total delay in Equation (5.1) can be reduced to

$$D_{total} = D_{queue} + D_{trans} \quad \text{.....(5.4)}$$

To compute this mathematics, we have to use Queueing Theory. This theory puts bench mark to model network. Queueing model is a system where packets assigned to a communication link for transmission. The following picture symbolizes queueing model using a buffer.

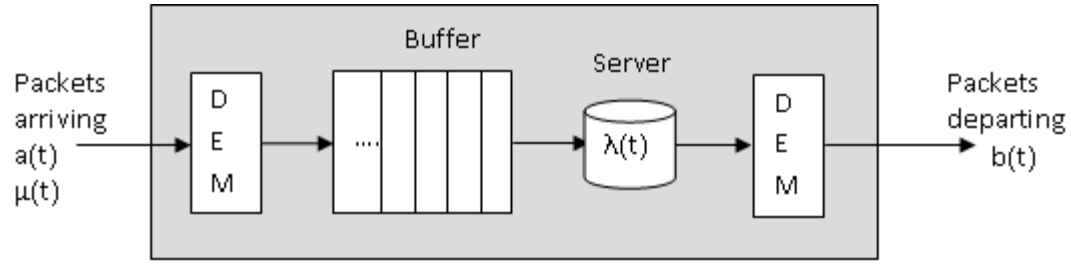


Figure 5.1: The buffer inside a switch or router to symbolize queuing model [41].

We are interested in estimating quantities such as:

- *N*: The average number of packets in the system i.e. the typical number of packets that are either waiting in the queue or undergoing the service.
- T: The average packet delay i.e. the time a packet spends waiting in queue plus the service time (transmission delay).

These parameters will depend mainly on known information such as:

- μ: packet arrival rate (the number of packets entering into the system per unit time)
- *λ*: packet transmission rate (the number of packets transmitted by the systems per unit time)

Moreover, statistical information about the packet arrival will be needed to be more precise in predicating average delay.

To continue deriving mathematical model of packet delay using queuing theory, let us use the following technical definition of end-to-end delay.

End-to-end delay of the i^{th} packet, denoted by D_i, is the difference between the time instant of the i^{th} packet arrival (the last bit or the most significant bit of the packet that has been received) at a network, denoted by E_i, and the time instant of the i^{th} packet

departure (the last bit or the most significant bit of the packet that has been transmitted) from the network, denoted by V_i. That is:

$D_i=V_i-E_i$

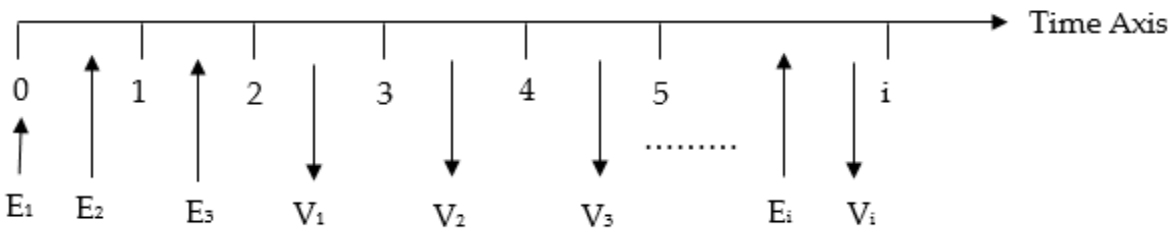


Figure 5.2: Packet arrival and departure in packet switched network [41].

The time average of the number of packets in the system (both in queue and server) is given by:

$$N_t = \frac{1}{t}\int_0^t N(\tau)\,d\tau \quad \text{.....(5.5)}$$

where N(t) is the number of packets in the system at time t and, its probabilistic formula is expressed as follows.

$$\bar{N}(t) = \sum_{n=0}^{N} np_n(t) \quad \text{..... (5.5a)}$$

where $p_n(t)$: probability that n packets are in the system at time t.

$$P_n = \lim_{t->T} p_n(t)$$

N is the number of nodes

As the above equation (Equation (5.5)) depends on packet arrival rate and departure rate, let us see arrival process and departure process in detail.

Arrival Process, a(t)

Let us consider the situation where the time slot is divided into slots of length δ. Here δ is very small quantity (δ<<1) that illustrates Poisson process. This is because the packet arrival follows Poisson process.

What is Poisson process?

Poisson process is a type of random mathematical object that consists of points randomly located on a mathematical space [43, 44]. It is widely used to model random points in time and space, such as the times of radioactive emissions, the arrival times of customers at a service center, and the positions of flaws in a piece of material.

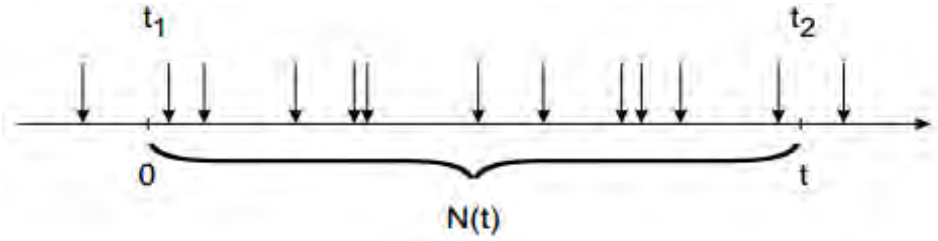


Figure 5.3: Poisson process is a random process of discrete events [44].

Now let us seen a situation where a packet arrival is Poisson process. Let us model the times between the arrivals of consecutive packets to a router by random variables Ei. Thus, E1 is the time between the starting of the router and the arrival of the first packet, E_2 is the time between the arrival of the first packet and the arrival of the second one, etc. It is reasonable to assume that E_i are independent identically distributed random variables [41].

Poisson process is a very important model used in a queuing theory. It is a viable model when the packets originate from a large network of independent users [39].

When packets are arriving according to Poisson process with the rate of λ, we have the following relations.

$$\begin{aligned} P\{a(t+\delta)-a(t)=0\} &= 1-\lambda\delta+o(t) \\ P\{a(t+\delta)-a(t)=1\} &= \lambda\delta+o(t) \\ P\{a(t+\delta)-a(t)\geq 2\} &= o(t) \end{aligned} \quad \text{.....(5.6)}$$

where o(δ) is a function such that

$$\lim_{\delta\to\infty}\left(\frac{o(\delta)}{\delta}\right)=0 \text{.....(5.7)}$$

Departure process, b(t)

When the system is not idle at time t, we have the following relations

$$\begin{aligned} P\{b(t+\delta)-b(t)=0\} &= 1-\mu\delta+o(t) \\ P\{b(t+\delta)-b(t)=1\} &= \mu\delta+o(t) \\ P\{b(t+\delta)-b(t)\geq 2\} &= o(t) \end{aligned} \quad \text{.....(5.8)}$$

In the steady-state, the probability that the system is in i state and makes a transition to i+1 state has to be equal to the probability that the system is in i+1 state and makes a transition to i state.

State transition diagram

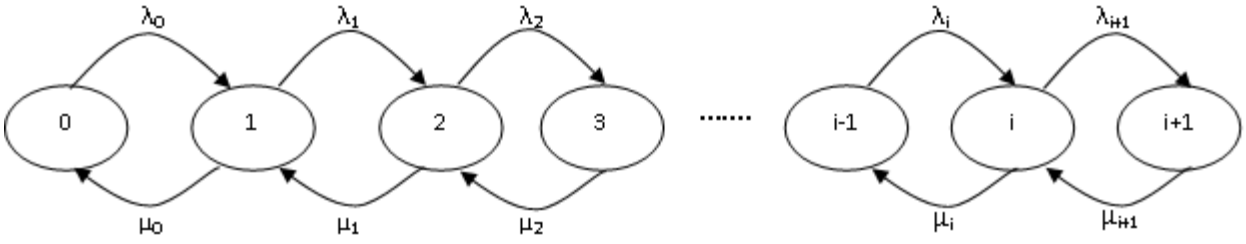


Figure 5.4: State transition diagram of packet arrival and departure [39].

That is,

$$P_i \lambda \delta = P_{i+1} \mu \delta \quad i = 0,1,2,\ldots \quad \text{.....(5.9)}$$

Or

$$P_{i+1} = P_i \lambda / \mu \quad \text{..... (5.10)}$$

Setting ω=μ/λ, (the ratio of arrival rate to service rate)

$$P_{i+1} = P_i \omega \quad \text{..... (5.11)}$$

We can derive an equation for P_i from Equation (5.11) using recursive method. i.e.

For i=0,

$$P_1 = P_0 \omega \quad \text{.....(5.12a)}$$

For i=1,

$$P_2 = P_1 \omega = (P_0 \omega)\omega = \omega^2 P_0 \quad \text{.....(5.12b)}$$

For i=2,

$$P_3 = P_2 \omega = (\omega^2 P_0)\omega = \omega^3 P_0 \quad \text{.....(5.12c)}$$

Following the same trend, we can get the i^{th} probability as follows

$$P_i = P_{i-1} \omega = (\omega^{i-1} P_0)\omega = \omega^i P_0 \quad \text{..... (5.12)}$$

Using the rule of probability, that is, the sum of probabilities of each item is unity,

$$\sum_{i=0}^{T} (P_i) = 1 \quad \text{.....(5.13a)}$$

From equation (5.12), this equation can be written as

$$\sum_{i=0}^{N} (\omega^i P_0) = 1 \quad \text{.....(5.13b)}$$

Since ω=μ/λ is usually less than one for stable system, $\sum_{i=0}^{N} (\omega^i P_0)$ converges to $\frac{P_0}{(1-\omega)}$

That is;

$$\sum_{i=0}^{N} \omega^i P_0 = \frac{P_0}{1-\omega} \quad \text{..... (5.14)}$$

From Equations (5.13b) and (5.14)

$$\frac{P_0}{1-\omega}=1$$

$$\Rightarrow P_0 = 1-\omega \quad \text{..... (5.15)}$$

Inserting this equation into Equation (5.12), we get

$$P_i = \omega^i P_0 = \omega^i (1-\omega) \quad \text{..... (5.16)}$$

The number of packets in the system can be calculated as follows

$$N = \sum_{i=0}^{T} iP_i = \sum_{i=0}^{T} i(\omega^i (1-\omega)) = (1-\omega)\sum_{i=0}^{T} i(\omega^i)$$

Using some manipulation,

$$N = (1-\omega)\sum_{i=0}^{T} i(\omega^i)\frac{\omega}{\omega} = (1-\omega)\omega\sum_{i=0}^{T} i\frac{\omega^i}{\omega} = (1-\omega)\omega\sum_{i=0}^{T} i\omega^{i-1} \quad \text{...(5.17)}$$

Looking carefully at the right most part of Equation (5.17), i.e. $i\omega^{i-1}$, it is the derivative of ω^i with respect to ω

That is,

$$i\omega^{i-1} = \frac{d}{d\omega}(\omega^i) \quad \text{..... (5.18)}$$

From this,

$$N = (1-\omega)\omega\sum_{i=0}^{T} i\omega^{i-1} = (1-\omega)\omega\sum_{i=0}^{T} \frac{d}{d\omega}\omega^i \quad \text{..... (5.19)}$$

Applying the rule of differentiation of sum of series, i.e.

$$\frac{d}{dx}\left(\sum_{i=1}^{T} f(X_i)\right) = \sum_{i=1}^{T}\left(\frac{d}{d} f(X_i)\right) \quad \text{..... (5.20)}$$

We get

$$\sum_{i=1}^{T}\left(\frac{d}{d\omega}\omega^i\right) = \frac{d}{d\omega}\left(\sum_{i=1}^{T}\omega^i\right) \quad \text{..... (5.21)}$$

So,

$$N = (1-\omega)\omega \frac{d}{d\omega}(\sum_{i=0}^{T} \omega^i) \quad \text{..... (5.22)}$$

Since ω=μ/λ, it is usually less than 1. So its summation is Taylor Series. That is,

$$\sum_{i=0}^{T} \omega^i = \frac{1}{1-\omega} \quad \text{..... (5.23)}$$

Replacing Equation (5.23) into Equation (5.22)

$$N = (1-\omega)\omega \frac{d}{d\omega}(\frac{1}{1-\omega}) \quad \text{..... (5.24)}$$

Now again using the rule of differentiation of reciprocal, i.e.

$$\frac{d}{dx}\frac{1}{f(x)} = \frac{-(f(x))'}{(f(x))^2}$$

$$\frac{d}{d\omega}(\frac{1}{1-\omega}) = \frac{-\frac{d}{d\omega}(1-\omega)}{(1-\omega)^2} = \frac{-(-1)}{(1-\omega)^2} = \frac{1}{(1-\omega)^2} \quad \text{..... (5.25)}$$

Inserting this into Equation (5.24)

$$N = (1-\omega)\omega(\frac{1}{(1-\omega)^2}) = \frac{\omega}{1-\omega} \quad \text{..... (5.26)}$$

Now we have to relate this number of packet with the arrival rate, μ. To find their relation, it is very useful to use Little's Theorem that puts a great foundation on the relationship between the number of packets (N) in the system, the arrival rate (μ), and the delay (T). These three parameters are related by a simple formula that makes it possible to determine one parameter when the other is given. This result, known as Little's Theorem, has the form:

$$N = \mu T \quad \text{..... (5.27)}$$

Equating Equations (5.26) and (5.27), we get the general formula for delay as follows.

$$\frac{\omega}{1-\omega} = \mu T$$

$$\Rightarrow T = (\frac{\omega}{1-\omega}) / \mu = \frac{\omega / \mu}{(1-\omega)} = \frac{(\mu / \lambda) / \mu}{(1-\mu / \lambda)} \quad \text{.....(5.28)}$$

$$\Rightarrow T = \frac{1/\lambda}{(\lambda-\mu)/\lambda} = \frac{1}{\lambda-\mu}$$

So the general mathematical model for packet delay is given by

$$T = \frac{1}{\lambda-\mu} \quad \text{..... (5.29)}$$

5.3. Jitter Modeling

Jitter is a measure of the packets' transfer delay variation. It can depend on the packets' routes and is caused by multiplexing several flows in the node queues. The following example shows how jitter is computed from delay of a flow from one node to another through Internet.

Figure 5.5: Routers' connection to show how jitter is measured in a network [22]

Let

Router1 sends packet1 at T_1

Router3 receives packet1 at T_2

Delay at this instant is given by

$$\Rightarrow D_1 = T_2 - T_1 \quad \text{..... (5.29)}$$

Router1 sends packet2 at T_3

Router3 receives packet2 at T_4

Delay at this second instant is given by

$$=> D_2 = T_4 - T_3 \quad \text{..... (5.30)}$$

From the definition, jitter is given by:

$$J = D_2 - D_1 = \left(T_4 - T_3\right) - \left(T_2 - T_1\right) \quad \text{..... (5.31)}$$

Equation (5.32) shows the transient time between two consecutive packets. That is,

$$J_i = T_{i+1} - T_i \quad \text{..... (5.32)}$$

The average end-to-end delay jitter is the mean of the absolute value of the differences of the transient delays. That is:

$$J = E\left[\left|T_{i+1} - T_i\right|\right] \quad \text{..... (5.33)}$$

For N nodes, the total average packet delay jitter is given by

$$\mathrm{J(N)} = \mathbf{E}\left\{\left|\sum_{n=0}^{N}\left(T_{i+1}^{(n)} - T_{i}^{(n)}\right)\right|\right\} \quad \text{..... (5.34)}$$

where $T_i^{(n)}$ is i^{th} delay of node n.

We can have three cases depending on the Equation (5.35). These are

(i) Small arrival rate and

(ii) large arrival rate

(iii) intermediate rate

Suppose K streams of packets are arriving to a specific queue by FCFS discipline. Our interest is in the jitter of a particular stream k, called tagged stream. All streams are assumed to have behavior of Poisson distribution with arrival rates μ_m.

Let

$$\mu = \sum_{m=1}^{K} \mu_m \quad \text{..... (5.35)}$$

Where K (capital K) is the total number of packet arriving into the queue

μ is the total arrival rate

μ_k is the arrival rate of the tagged stream

When packet arrival rate of a selected flow (a tagged stream) is very small, i.e. $\mu_k << \mu$, two packets of stream k are separated by a large number of packets from the other streams so that we can ignore the correlation between the transit delays of two consecutive packets and assume that$T_{i+1}$and T_i are two independent random variables. Using one of the common properties of exponential distribution, we can get simple formula for jitter. This property of exponential distribution is stated as follows:

Let X_1 and X_2 are two independent and identically distributed random variables whose common distribution is f, which is the same as that of random variable X. The distribution of random variable $|X_2-X_1|$ is the same as that of X if and only if f is the exponential distribution [39, 42].

SinceT_{i+1} and $T_i$are two independent random variables, we can apply this theory. So, when the arrival rate of a selected stream is small, jitter is given by,

$$J = E\left[|T_{i+1} - T_i|\right] = \frac{1}{\lambda - \mu} \quad \text{..... (5.36)}$$

Setting λ-μ=η,

$$J = \frac{1}{\eta} \quad \text{..... (5.37)}$$

For large arrival rate, that is when arrival rate of a selected stream is almost equal to the arrival rate of the whole packets ($\mu_k \approx \mu$), we can neglect the presence of the other streams and consider that we have a queue with only one flow.

So jitter can be expressed as

$$J = E\left[|T_{i+1} - T_i|\right] = \frac{1}{\lambda} \quad \text{..... (5.38)}$$

For the case where the arrival rate of the tagged flow takes values between the above two extreme points, let us define total traffic load, ρ .

$$\rho = \frac{\mu}{\lambda} \quad \text{..... (5.39)}$$

Let's have packets P_i and P_{i+1}that are two consecutive packets with delays T_i and T_{i+1} respectively. Given that the arrival process is Poisson with parameter μ_k, the average time between P_i and P_{i+1} is:

$$\Gamma_k = 1/\ \mu_k \quad \text{..... (5.40)}$$

The end-to-end jitter of a packet with intermediate arrival rate is given by

$$J_k \approx \frac{1}{\eta} f(\Gamma_k, \eta) \quad \text{..... (5.41)}$$

Where

- $\eta = \lambda - \mu$
- Γ_k is he average time between two consecutive packets

- $f(\Gamma_k, \eta)$ is the function that estimates the degree of correlation of two successive packets, P_i and P_{i+1}, and it is given by

$$f(\Gamma_k, \eta) = 1 - e^{-\eta\Gamma_k}(\eta\Gamma_k + e^{-\eta\Gamma_k}) \quad \text{..... (5.42)}$$

We can examine two extreme conditions from approximation in (5.41).

1. When $\mu_k \approx 0$, that is, when packet arrival rate of a selected flow, k, is very small
   In this condition, the average time between two packets is very large. That is, $\Gamma_k = 1/\mu_k \approx \infty$.

Inserting this expression into Equation (5.41), we can get 1. From Equation (5.40), we can get

$$J_k \approx \frac{1}{\eta} \quad \text{..... (5.43)}$$

Which is equivalent with jitter when arrival rate of a stream is small (Equation (5.37)).

2. When the arrival rate of a tagged stream is dominant in the flow, that is, when $\mu_k \approx \mu$,

$$\eta\Gamma_k \approx (1-\rho)/\rho \quad \text{..... (5.44)}$$

In this case,

$$J \approx \frac{1}{\eta}\left[1 - e^{(\rho-1)/\rho}\left(\frac{1-\rho}{\rho} + e^{(\rho-1)/\rho}\right)\right] \quad \text{..... (5.45)}$$

Here we can again see two cases by considering two values for ρ

   a. **when $\rho \approx 0$**

      In this case, the exponential part will be very small

$$\Rightarrow J \approx \frac{1}{\eta}$$

That is, when ρ is small, the jitter does not depend much on the proportion of tagged traffic.

b. **when $\rho \approx 1$,** inserting this into Equation (5.44) we get,

$$\eta \Gamma_k \approx 0$$

And after expanding the exponentials inside the braces into the first order, we get

$$J \approx \frac{1}{\lambda}$$

5.4. Modeling of Packet Loss Ratio

Packet loss ratio is the ratio of packets lost per the packets received. i.e.

$$PLR = \frac{N^o \ of \ packets \ lost}{N^o \ of \ packets \ offered} \quad \text{..... (5.46)}$$

The number of packets offered to the buffer is equal to the number of packets arriving into the buffer. The number of lost packets is the difference between packets departing the server and the packets arrived to the buffer. Let the average number of packets arrived in [0, t] to the system is a(t) and the average number of packets departed in [0, t] from the system is b(t). Then the number of packets lost is equal to

$$PL = a(t) - b(t)$$

$$\Rightarrow PLR = \frac{PL}{a(t)} * 100\% = (\frac{a(t) - b(t)}{a(t)}) * 100\%$$

$$\Rightarrow PLR = (1 - \frac{b(t)}{a(t)}) * 100\% \quad \text{.....(5.47)}$$

Chapter 6: Simulation, Results and Analysis

6.1 Introduction to Simulation

In communication and computer network research, network simulation is a technique where a program models the behavior of a network either by calculating the interaction between the different network entities (hosts/packets, etc.) using mathematical formulas, or actually capturing and playing back observations from a production network. The behavior of the network and the various applications and services it supports can then be observed in a test lab; various attributes of the environment can also be modified in a controlled manner to assess how the network would behave under different conditions.

There are three types of simulation based on entitles involved. These are live simulation, virtual simulation and constructive simulation. In this paper, we use constructive type of simulation to simulate KPIs of core network elements. This type of simulation helps to resemble the real system.

In this chapter, simulation of KPIs of core NEs is done, results are obtained from existing core network monitoring tools and analysis is done by using compare and contrast method.

6.2 Simulation of KPIs used in IP Core Network

There are five IP core NEs (BRs) and five IP backhaul NEs (NE40E) in ethio telecom network architecture. All five BRs and five NE40Es are interconnected in a full-mesh topology. As it is shown in Figure 2.4, there are three or four CRs that are connected

into one BR and three or four ERs that are connected to a CR. CRs in one site are interconnected in a full mesh topology and ERs in one site too. In the same way, as figure 2.5 shows, RSG and ASG are NEs in an aggregation layer and CSGs are NEs in access layer in IP backhaul network.

6.2.1 Packet Delay Simulation

Using the model for packet delay developed in Chapter 5, (Equation (5.28)), we can simulate real network packet delay. According to the equation, there are two variables that determine packet delay. These are packet arrival rate (μ) and packet transmission rate (λ)

Packet transmission rate of a router is taken from the real system for 9 days. Then maximum packet transmission rate is taken at each day. Finally, the maximum value is taken out of nine days. This can be shown in Table 6.1. All routers indicated in the table are interconnected to each other in a full mesh topology.

Date	Router_A	Router_B	Router_C	Router_D	Router_D	Max. Packet Tx Per S
23/5/2016	619988	305251	540768	1463237	418968	1463237
24/5/2016	1988252	921452	875412	891527	1452154	1988252
25/5/2016	356178	7845112	4552134	3825452	126398	7845112
26/5/2016	4587841	1057830	4212247	4025481	1257854	4587841
27/5/2016	512437	5878451	1468782	1023545	895624	5878451
30/5/2016	874591	325698	937845	725431	784562	937845
31/5/2016	234789	894512	894512	874563	365441	894512
6/1/2016	2213841	1913801	1725484	1257484	256389	2213841
6/2/2016	310841	365487	405784	102125	1265341	1265341
Grand Average(Packets per Second)						7845112

Table 6.1: The trend of packet transmission rate for one week.

According to the above table, the maximum real time packet rate in the existing routers is 7845112pps. So, we can take up to 80,000,000pps for packet transmission rate of a router which is the maximum rate of core routers.

Packet arrival rate is random. We took one week traffic arrival rate of routers in a real system and generated random variables.

Other usual variable in a real system is time. Time taken when some situation happens is usually correlated with other dependent variables. In this paper, we used time variable according to real system dates. That is, for example, for one day, the paper uses 24*60=1440 minutes range starting from 0 to 1440.

Taking these all in account, we can simulate packet delay. Result for packet delay simulation is shown as follows. Figure 6.1 below shows the simulated result of delay in one day.

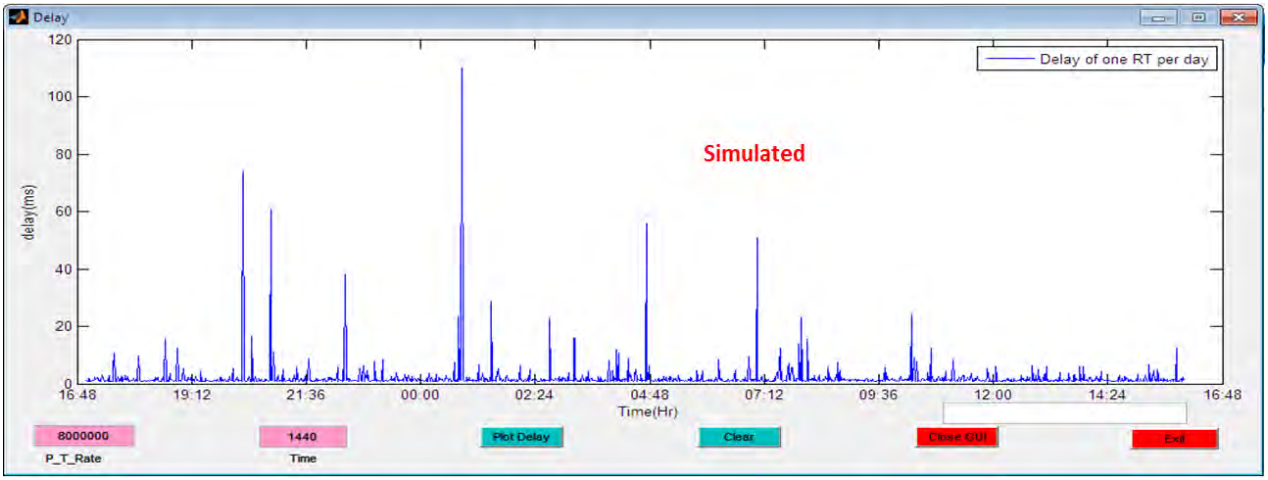


Figure 6.1: Simulation result of packet delay of one router in one day.

6.2.2 Packet Jitter Simulation

As jitter is the measurement of the difference of delay at one point from the other point in time reference, it can be simulated using the difference between delay at one point of time and the delay prior that point of time. That is, all the parameters used in delay simulation remains the same, and the first value of jitter is taken as of the delay value at that point. Then, the next values are calculated by subtracting delay value at previous point from that of the current point. Accordingly, the simulation of jitter for a particular link is shown in the following figure.

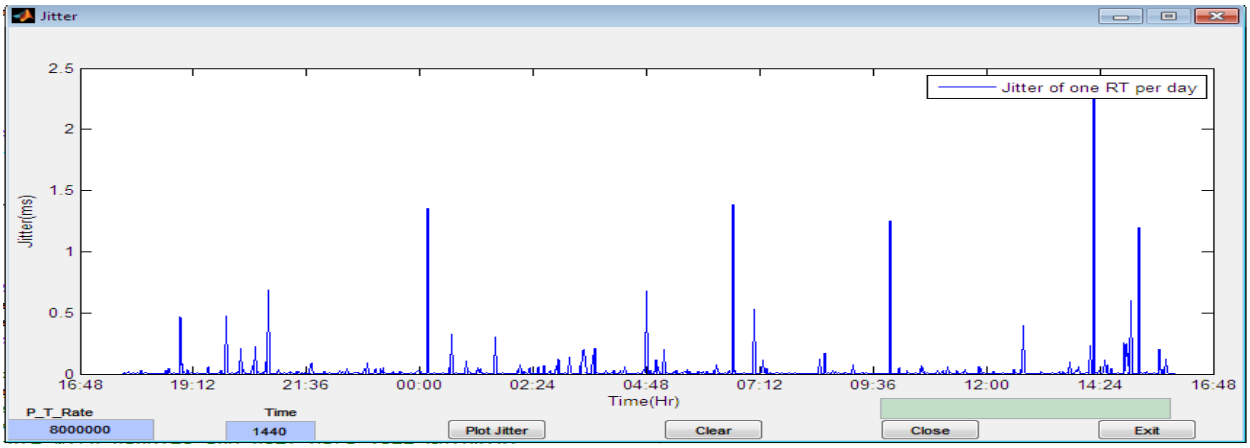


Figure 6.2: Simulation result of packet jitter of one router in one day.

6.2.3 Packet Loss Ratio Simulation

Packet loss ratio is calculated using measuring probes in every common network measuring tools. That is, this KPI is counted using counters that trap network and measure how much packets are sent and how much are received. From these two quantities, packet loss ratio is calculated as shown in Equation (5.45).

$$PLR = (1 - P_{rec} / P_{sent}) * 100\% \quad \text{.....(6.1)}$$

Since it is a bit complicated to design counter in this thesis work, this paper uses number of packets sent and received by a router in a given time, the simulation is done taking the consideration of queueing theory. Accordingly, simulation for packet loss ratio of a typical link is as shown in Figure 6.3.

6.2.4 Memory Usage and CPU Utilization Simulation

In the same concept as packet loss ratio, memory usage and CPU Utilization is simple in that a metric system checks the level of various memory and CPU units and sends information to the monitoring tool.

However, it is very difficult to insert probes that measure memory usage in simulation tool (Matlab) in our case, we left simulation of memory usage and CPU Utilization for further study.

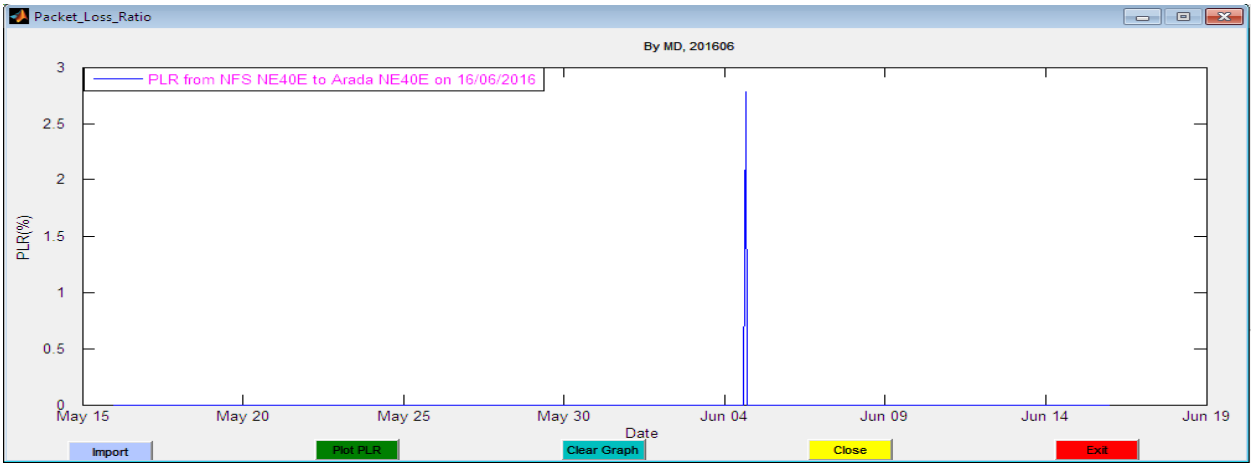


Figure 6.3: Simulation of PLR of a specific router (one link).

6.3 Results

This subsection is concerned with results of simulated and actual values. It slightly compares the two results using statistical parameters like mean, standard deviation, and variance.

Mean

Mean of the KPI represents the average value of the data within the given range. For example, if we have 1440 different values in one day, we can get the mean of the values. Mean is useful to know the general tendency of the values so that designer/or planner/or optimization engineer can judge on cumulative quality rather than individual value.

In this paper, we exported simulated values to excel and computed mean for each KPI and compared it with the mean of real data for a given time [36].

Standard deviation (SD)

Standard deviation is a quantity expressing by how much the members of a group differ from the mean value for the group. It is the measure of spread of the numbers in a set of data from its mean value. It is also called SD and is represented using the symbol σ (sigma). This can also be said as a measure of variability or volatility in the given set of data [36].

Variance

The variance is one of the measures of dispersion that is a measure of by how much the values in the data set are likely to differ from the mean of the values. It is the average of

the squares of the deviations from the mean. Squaring the deviations ensures that negative and positive deviations do not cancel each other out [36].

6.3.1 Packet Delay

End to end packet delay is measured by taking the delay effect of one NE on other NEs. For example, the average delay of one NE40E is measured by considering each link that enters to it. So we should study delay behavior of each NE40Es that are connected to it. This delay is the average delay of all NEs in the telecom. This is because; other lower level NEs connected into this router are connected to it through their neighbor NE40Es. More specifically, for example, RSG in site A is connected at the first to NE40E in site A. Since all NE40Es are interconnected in full mesh manner, NE40E in site B is connected with NE40Ein site A. Since RSG in site B is connected to NE40E in site B, it can communicate with RSG in site A.

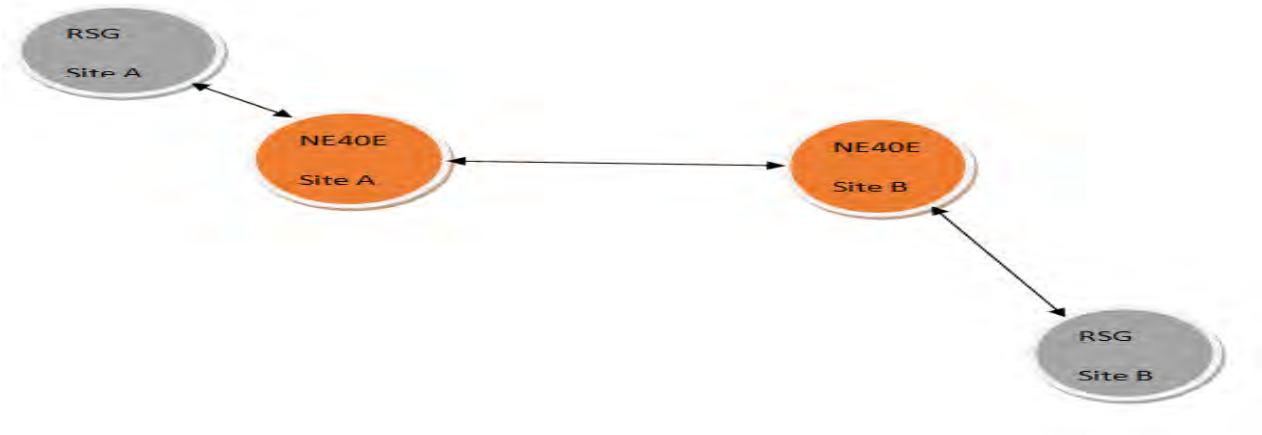


Figure 6.4: How NEs are interconnected in a single route.

Mean Delay of Core Routers

There are ten main IP core network elements at two different levels for two different purposes in ethio telecom. In the first level, five bearer routers (BRs) are directly

connected to international gateways. At the second level, there are 5 NE40Es that are connected directly to the above BRs and used as backhauls of the network.

	SiteA	SiteB	SiteC	SiteD	SiteE
SiteA	--	SiteA-SiteB	SiteA-SiteC	SiteA-SiteD	SiteA-SiteE
SiteB	SiteB-SiteA	--	SiteB-SiteC	SiteB-SiteD	SiteB-SiteE
SiteC	SiteC-SiteA	SiteC-SiteB	--	SiteC-SiteD	SiteC-SiteE
SiteD	SiteD-SiteA	SiteD-SiteB	SiteD-SiteC	--	SiteD-SiteE
SiteE	SiteE-SiteA	SiteE-SiteB	SiteE-SiteC	SiteE-SiteD	--

Table 6.2: Delay trend from one router to the other routers.

As it is mentioned above, the average packet delay of one core router is calculated taking all links that are connected to it. Table 6.2 shows the matrix that explains how the average delay is calculated.

Description to the above table

- SiteA, SiteB, SiteC, SiteD and SiteE indicate place names where core routers are deployed.
- First name indicates the NE from which the link whose delay is going to be calculated is started. The second name after '-' represents an NE to which the link is entering. For example, 'SiteA-SiteB' shows the link that started from router at site A and entered into router at site B. Delay is calculated when packet travels from router at site A to router at site B.

The actual average delay from each NE40E to the others is shown in the following table for the period of April 17 to May 16 2016, of one month.

	SiteA	SiteB	SiteC	SiteD	SiteE	Average
SiteA	--	6.037674	6.24427	11.1449	6.35056	7.444349
SiteB	8.91934	--	9.01538	13.5509	9.16205	10.16192
SiteC	8.181667	6.879896	--	13.573	7.02948	8.916016
SiteD	8.093854	8.491771	8.60545	--	8.60879	8.449965
SiteE	10.07181	10.06462	10.3274	15.3852	--	11.46227

Table 6.3: The average packet delay of each device from the others.

The above table (Table 6.3) shows delay of one router that occurred when the packet flows from one router to the other router. For example, a packet delay when packet travels from router at SiteA to router at siteB is 6.037674ms. This value is indicated in Column 3, Row 2. It is the average value of 30 days on the granularity of 1 Hr.

Taking average of all the four routers' delay values for one router, we can get the following table for one month.

Routers	Actual Mean Delay (ms)	Simulated Mean Delay (ms)
SiteA NE40E	7.444348958	9.78739
SiteB NE40E	10.1619184	10.277
SiteC NE40E	8.916015625	9.04147
SiteD NE40E	8.449965278	9.36171
SiteE NE40E	11.46226563	11.4905

Table 6.4: The average packet delay of NE40Es in one month (simulated and actual).

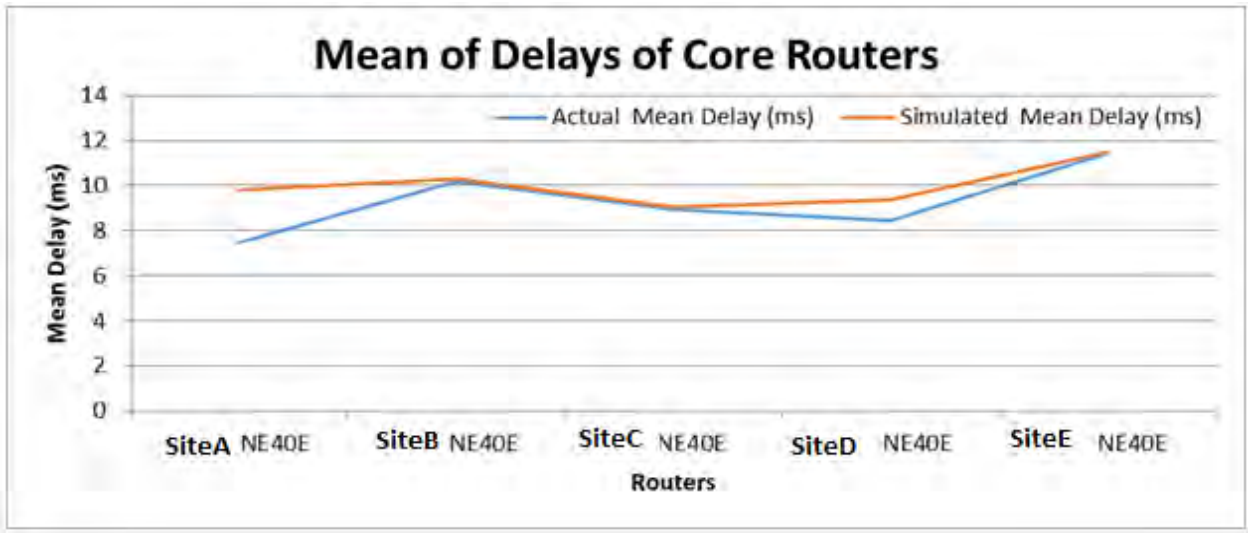


Figure 6.5: Simulated and actual mean delay comparison of routers.

According to the above figure, the delay mean for all core routers is almost the same with simulated delay mean.

In the same way as we have got mean for NE40s, we can get mean for BRs as the following table.

Routers	Actual Mean Delay(ms)	Simulated Mean Delay (ms)
SiteA BR	12.81056656	11.24561
SiteB BR	7.499542125	10.23491
SiteC BR	10.000845	9.98543
SiteD BR	11.39254814	12.74562
SiteE BR	9.971739067	11.02458

Table 6.5: The average packet delay of each BR in one month.

As the below figure shows, the simulated and actual mean delays of BRs are in a range from 8ms to 13ms. That means, the average delay values in a given day is far below from ITU standard, which is 150ms for end to end packet delay.

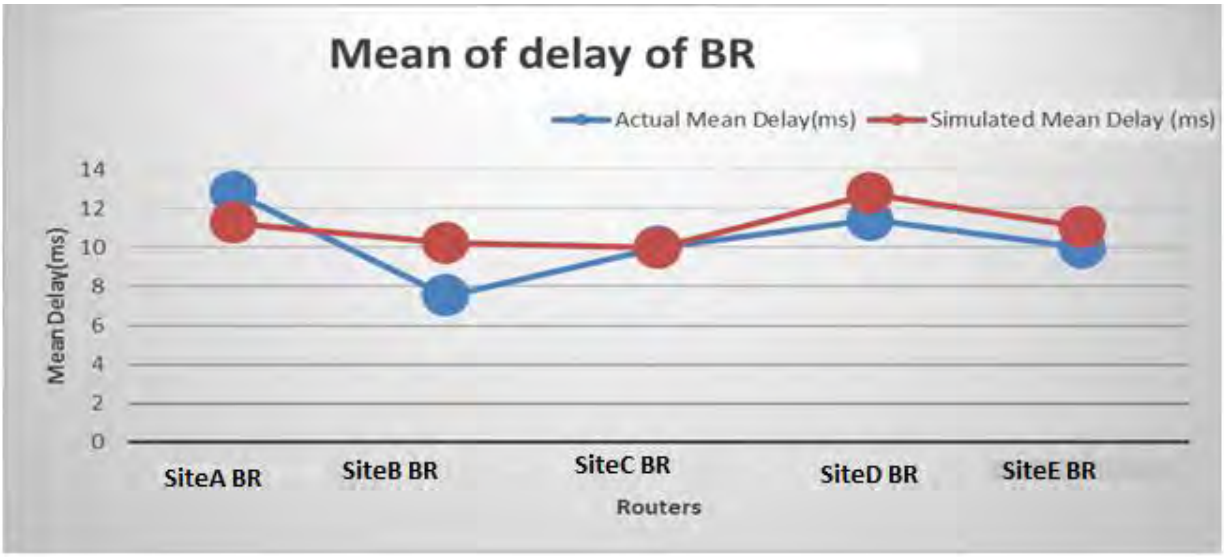


Figure 6.6: Simulated and actual mean delay comparison of BRs.

Variance, σ^2 of delay of IP core network

Mean alone will not be able to truly represent the Probability Mass Function (PMF) of any random variables. A probability Mass Function (PMF), or density of a discrete random variable, is counterpart of a probability distribution function (PDF) of continuous variables that describes the relative likelihood for this random variable to take on a given interval. Sometimes two variables with the same mean do not have the same distribution. Variance gives more clear meaning to the likelihood for random variables [43].

Variance is the sum of all average mean square deviations of the random variable around its mean. When variance is large, it shows the spread of the PMF around its mean. Thus as the variance of a random variable tends to zero, it will begin to concentrate more and more around the mean ultimately behaving like a constant [43,44]. The following figures show the difference in PMF when variance differs. Figure 6.7 a, whose variance is 1 seems concentrated more and more around the mean whereas

Figure 6.7 b shows that the PMF spread more wider around the mean as its variance is larger than that of f_{x1}

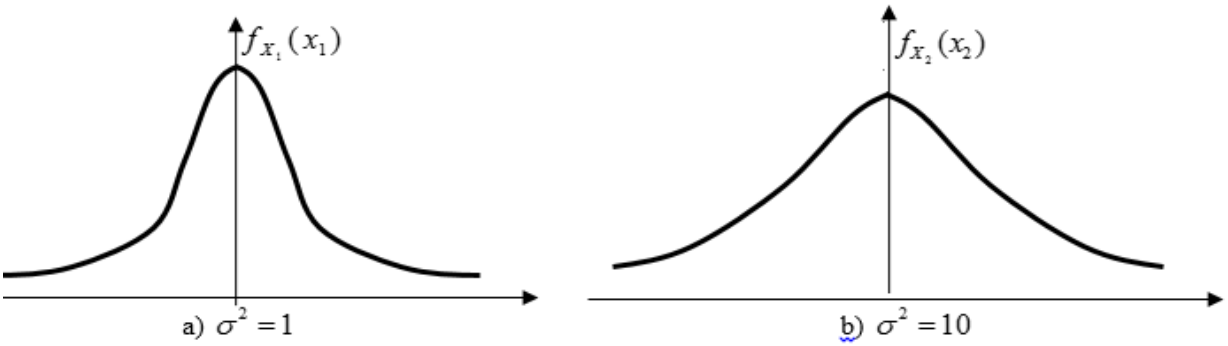


Figure 6.7: The difference of PMF for two different variances.

Since packet arrival is random, packet delay is also random. As mean of the packet delay is known, so we can calculate mean square deviation of the packet delay as follows. Let X represents random variable, i.e. delay, m represent mean of the delay. Then the sum of mean square deviation of the packet delay is given by.

$$\sigma^2 = \frac{1}{N}\sum_{i=1}^{n}(X_i - m)^2 \quad \text{.....(6.2)}$$

where n represents the number of random variables.

This equation is satisfied when the variable is discrete. If it is continuous, the summation is replaced by integration.

According to the above equation, Equation (6.2), we can get variance for both simulated and actual data of core routers. Taking mean for each router from Table 6.4, we can get the following table for variance.

Routers	Actual Variance of Delay	Simulated Variance of Delay
SiteA NE40E	168.02062	283.574
SiteB NE40E	374.7605878	405.095
SiteC NE40E	254.6041161	364.577
SiteD NE40E	84.23603358	177.07
SiteE NE40E	467.4174535	395.726
Average	**269.8077622**	**325.2084**

Table 6.6: The variance of delays of NE40Es.

Routers	Actual Variance of Delay	Simulated Variance of Delay
SiteA BR	36.40534033	41.34661
SiteB BR	60.28257364	56.29493
SiteC BR	62.17074991	79.08643
SiteD BR	64.0226915	56.71582
SiteE BR	32.81275793	36.22488
Average	**51.13882266**	**53.933734**

Table 6.7: Variance of packet delays of each BR in one month.

Standard deviation, σ , of delay of IP core network

Standard deviation is a measure that is used to quantify the amount of variation or dispersion of a set of data values [43, 44]. A low standard deviation indicates that the data points tend to be close to the mean of the set, while a high standard deviation indicates that the data points are spread out over a wider range of values.

The mathematical equation for standard deviation is the square root of the variance of given variables. Form Equation (6.2), standard deviation is given by

$$\sigma = \sqrt{\frac{1}{N}\sum_{i=1}^{n}(X_i - m)^2} \quad \text{.....(6.3)}$$

Accordingly, the following two tables show standard deviation of delays of each NE40Es and BRs.

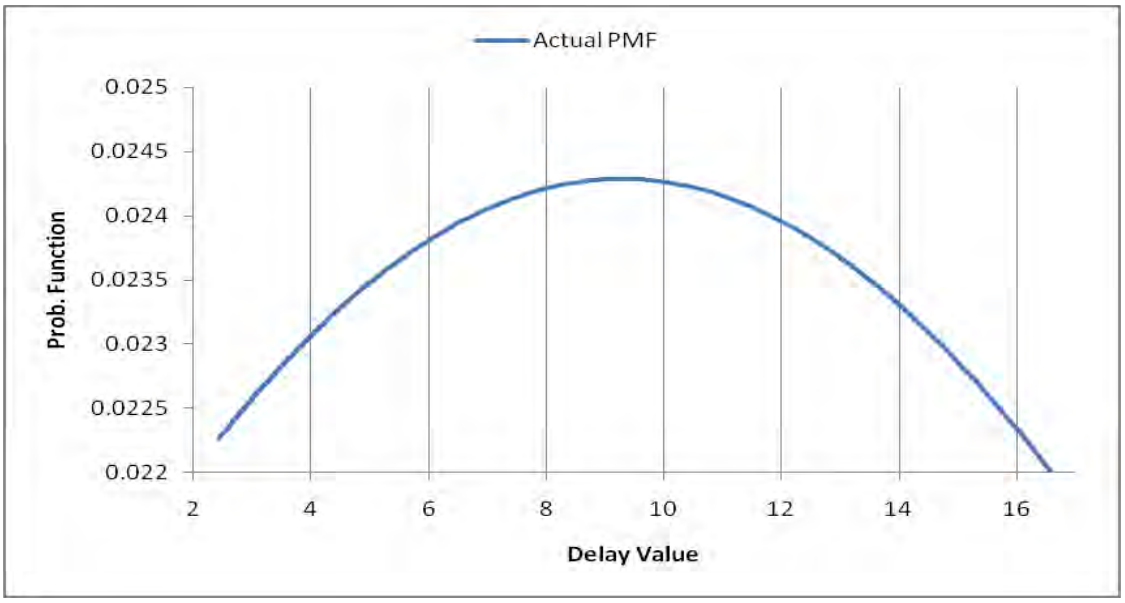
Routers	STD of Actual Delay values	STD of Simulated Delay
SiteA NE40E	12.96227681	16.83965558
SiteB NE40E	19.35873415	20.12697195
SiteC NE40E	15.956319	19.09389955
SiteD NE40E	9.178019044	13.3067652
SiteE NE40E	21.61983935	19.89286304

Table 6.8: The STD of delays of NE40Es.

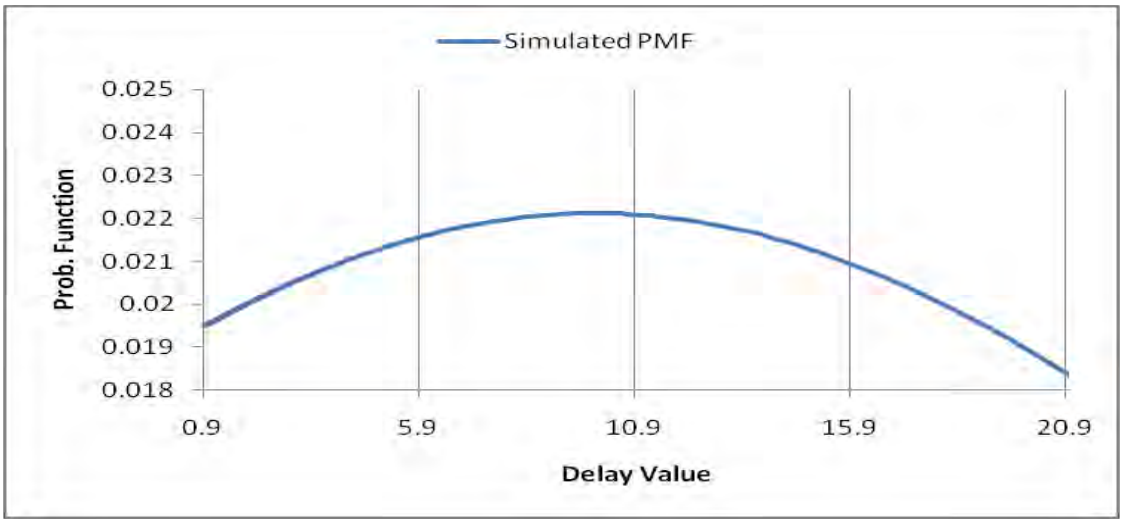
Routers	Actual STD of Delay	Simulated STD of Delay
SiteA BR	6.033683811	6.430132969
SiteB BR	7.764185317	7.502994735
SiteC BR	7.884843049	8.893055156
SiteD BR	8.001418093	7.530990639
SiteE BR	5.728242133	6.018710825
Average	**7.082474481**	**7.275176865**

Table 6.9: The STD of packet delays of each BR in one month.

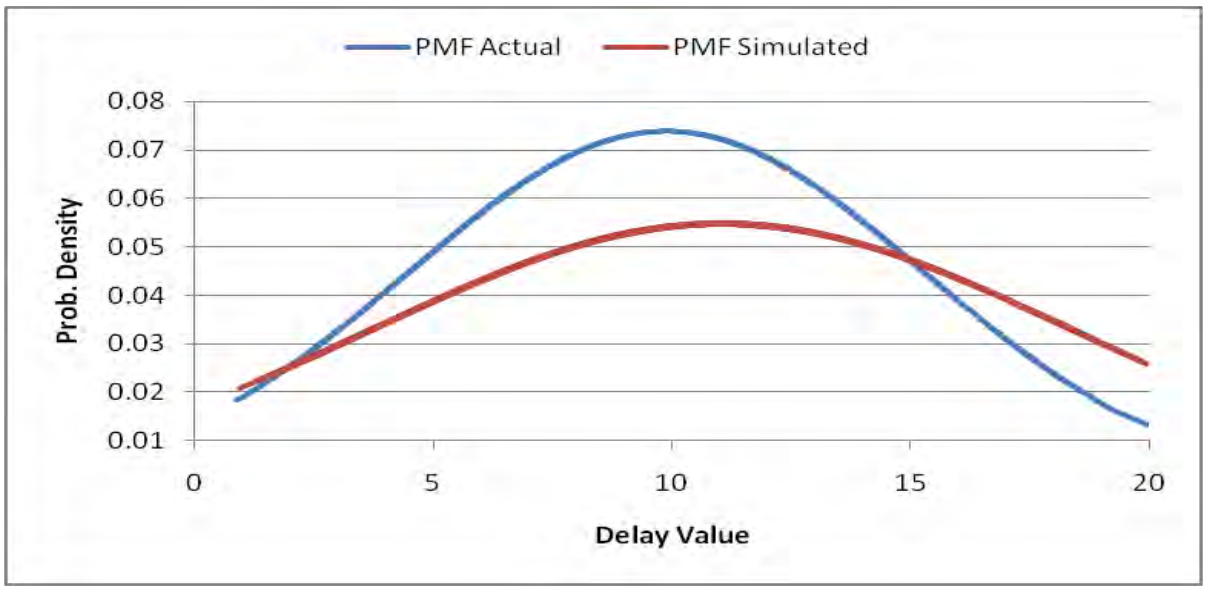
We have got enough parameters that can illustrate the real behavior of PMF for random variables. Using mean and standard deviation, the following figures show PMF of both simulated and actual delay results of core routers.



A) PMF of delay series in an actual case.



B) PMF of delay series in a simulated situation.



C) Actual and Simulated PMF of delays of BR routers.

Figure 6.8: PMF of actual and simulated delay series of IP core network.

According to Figures 6.8 A and 6.8 B, the PMF for the actual delay is more compacted near the mean of the delays (which is 9.2869) than the PMF of the simulated delays which is distributed in a wider plane from its mean (which is 9.9916). This shows that delay values in a real situation is near to their mean.

According to the Figure 6.8 C, all actual delay values are nearer to their mean value compared with the simulated delay values from the simulated delays mean.

6.3.2 Jitter

Mean of jitters of IP core network

Jitter simulation is also done according to the rule of delay simulation. Since there are 5 NE40Es, there will be 20 combinations in total. This is the same as we have seen in Table 6.2. Using the same scenario, we can get average jitter for NE40Es as the following table.

	SiteA	SiteB	SiteC	SiteD	SiteE	Average
SiteA	--	9.568	9.166	8.146	9.767	9.161763
SiteB	9.845	--	9.838	8.606	10.67	9.73981
SiteC	8.704	9.241	--	7.98	9.317	8.810701
SiteD	7.633	8.192	8.059	--	8.22	8.025794
SiteE	9.474	10.59	9.973	8.966	--	9.749487

Table 6.10: The average jitter of each device from the others.

Taking average for each router, we can get the following table which also contains mean value for simulated case.

Routers	Actual Jitter Mean(ms)	Simulated Jitter Mean(ms)
SiteA NE40E	9.161763021	9.62066
SiteB NE40E	9.739809896	10.9807
SiteC NE40E	8.810700521	8.35356
SiteD NE40E	8.025794271	8.35356
SiteE NE40E	9.749486979	9.67637

Table 6.11: Actual and simulated mean values of jitters of NE40Es.

Mean value is average value of all jitter values that occurred when the packet moves from source router to the other routers. For example, mean jitter of NE40E at SiteA is the average value of jitters that occurred during the flow of packets from SiteA NE40E to the other four NE40Es.

Actual jitter value is compared with the simulated values of mean jitter as the following figure.

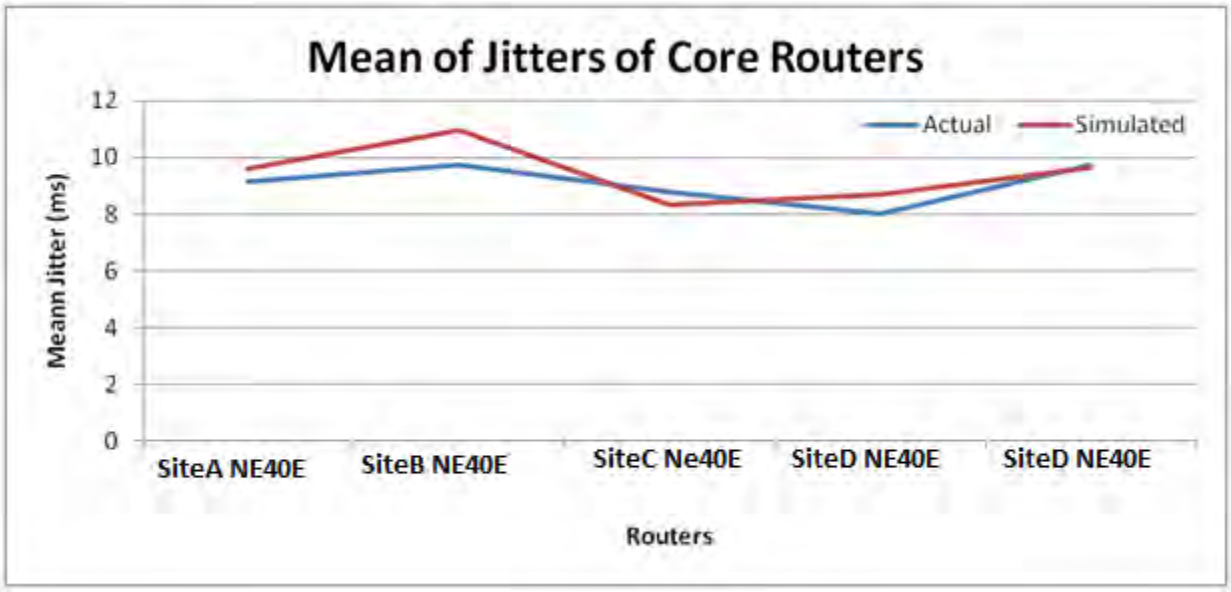


Figure 6.9: Simulated and actual mean jitter comparison of routers.

According to Figure 6.9, actual value and simulated result of jitter of all routers are almost the same except SiteB NE40E whose actual mean jitter is almost 1ms below than the simulated jitter value.

In the same way as we expressed mean jitter for NE40Es, mean jitter of BRs can be obtained as follows.

Routers	Actual Mean Jitter(ms)	Simulated Mean Jitter (ms)
SiteA BR	0.14217033	0.162158
SiteB BR	0.872481685	0.865521
SiteC BR	1.261904762	1.00583
SiteD BR	1.833562271	1.301589
SiteE BR	0.51717033	0.62458
Average	0.925457875	0.7919356

Table 6.12: Actual and simulated mean of BRs.

Variance and Standard deviation of jitters of IP core network

Variance and standard deviation of jitter is calculated according to the Equations (6.2) and (6.3) respectively. Accordingly, the following table shows actual and simulated jitter variance and standard deviation of NE40Es.

Routers	Actual Jitter Variance	Simulated Jitter Variance	Actual Jitter STD	Simulated Jitter STD
SiteA NE40E	1.753098465	1.09372	1.324046247	1.04581
SiteB NE40E	1.683938572	1.61303	1.297666587	1.27005
SiteC NE40E	1.294136781	1.0226	1.137601328	1.01124
SiteD NE40E	2.052666275	2.87008	1.432712907	1.69413
SiteE NE40E	2.072768715	2.17242	1.43971133	1.473913
Average	1.771321762	1.75437	1.32634768	1.2990286

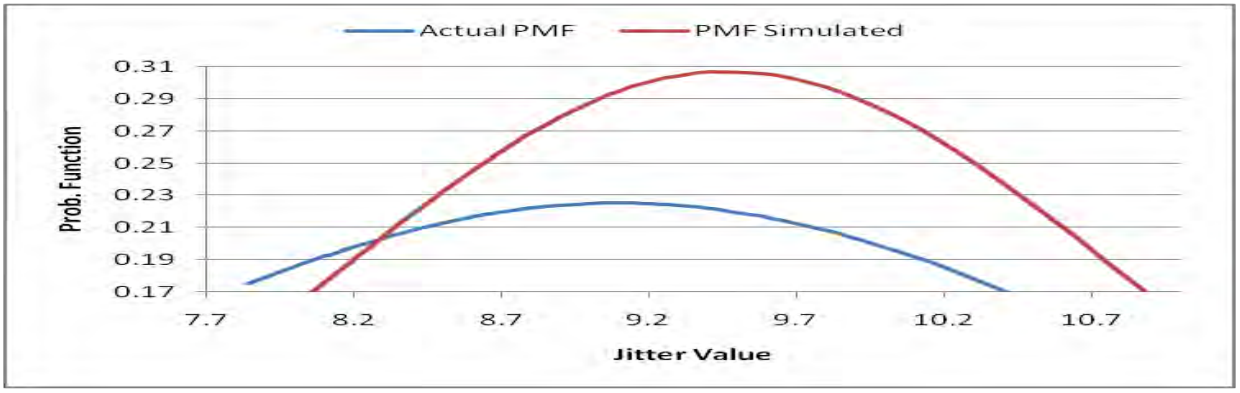
Table 6.13: Actual and simulated variance and STD of jitter values of NE40Es.

Variance and STD of BRs are also obtained using Equations (6.2) and (6.3) respectively.

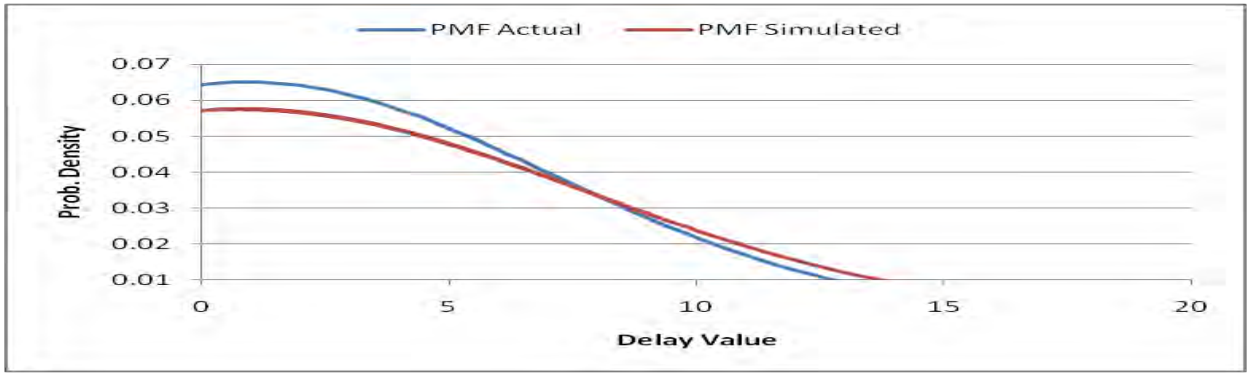
Routers	Actual Variance of Jitter	Simulated Variance of Jitter	Actual STD of Jitter	Simulated STD of Jitter
SiteA BR	0.321665268	0.205615	0.567155418	0.453447902
SiteB BR	89.51087069	66.19403	9.461018481	8.135971362
SiteC BR	81.76010555	78.58642	9.042129481	8.864898195
SiteD BR	88.08335236	89.71084	9.385273164	9.47158065
SiteE BR	4.815368039	5.58851	2.194394686	2.364002961
Average	52.89827238	48.057083	6.129994246	5.857980214

Table 6.14: Actual and simulated STD and variance of BRs.

The PMF of actual and simulated jitter of IP core devices is shown in the following figure.



a. PMF of NE40Es.



b. PMF of BRs.

Figure 6.10: PMF of simulated and actual jitter of IP core devices.

6.3.3 Packet Loss Ratio

Packet loss usually exists in a link that connects two devices. Since there are too many links from one device to the others, it is very time taking job to get whole packet loss for all devices. Not only for all devices, but also for core devices only, it may take one paper to realize whole packet loss. In this thesis, we take some links to show sample of packet loss in the existing network.

The following figure shows the average packet loss ratio of a link that connected SiteA-BR to SiteB-ER.

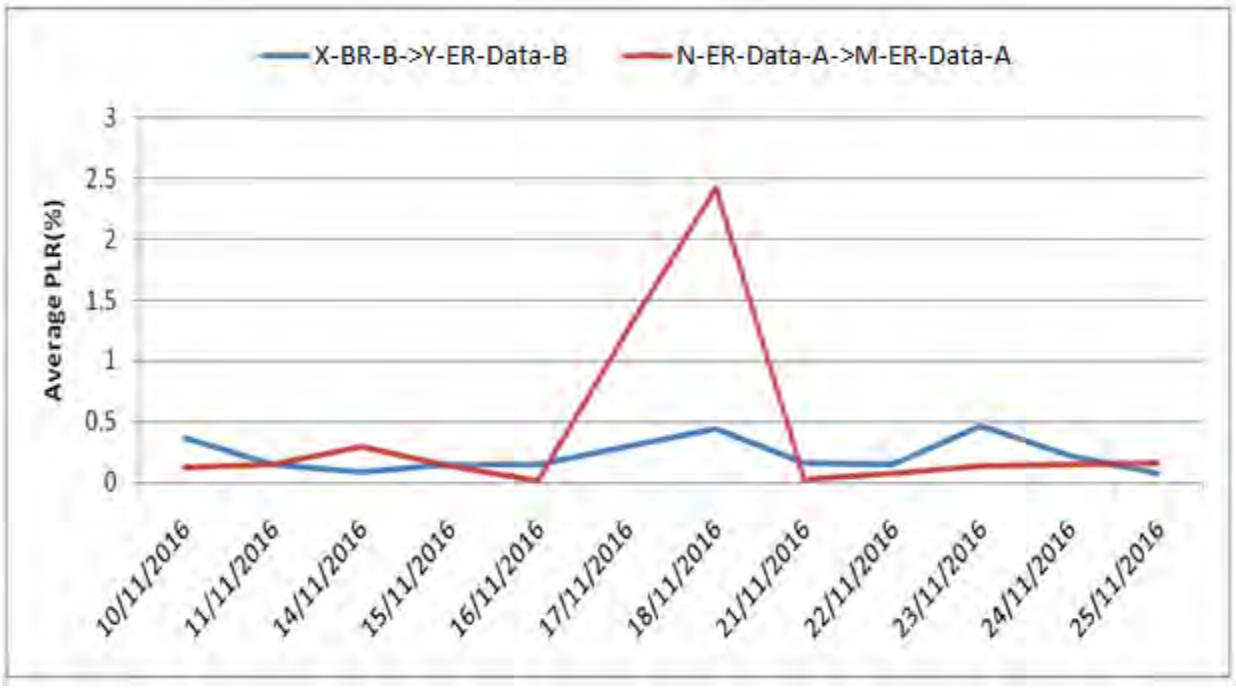


Figure 6.11: Average packet loss of the two links.

According to the above figure (Figure 6.11), average packet loss ratio (PLR) of the two selected links is below 0.5% in the whole test period except the PLR of a link. The average PLR of this link somewhat increased and finally reached to around 2.5%. This loss was occurred due to transmission medium between the two devices.

6.4 Analysis

In this section, detailed analysis of the KPIs of IP core network elements is done using results from Section 6.3. The result values are compared with the ITU standard values.

6.4.1 Packet Delay Analysis

ITU sets maximum of 150ms for end to end delay. It is tolerable if packet delay is below 150ms. Packets are discarded if the delay is above 150ms, so that results loss in packet. This in turn causes data reliability problem.

According to Table 6.4, the average packet delay of the five IP core network elements in NE40E is below ITU standard. The table also shows simulated result of packet delay of IP core network elements.

Both simulated and actual results in Table 6.4 are the average values of one day in a granularity of 1Hr. This means there may be a high value in a moment that may hinder the flow. To see the actual delay of one day, the snipping shoot of delay when packet flows from SiteA-NE40E-A to SiteB-NE40E-B is shown in the following figure.

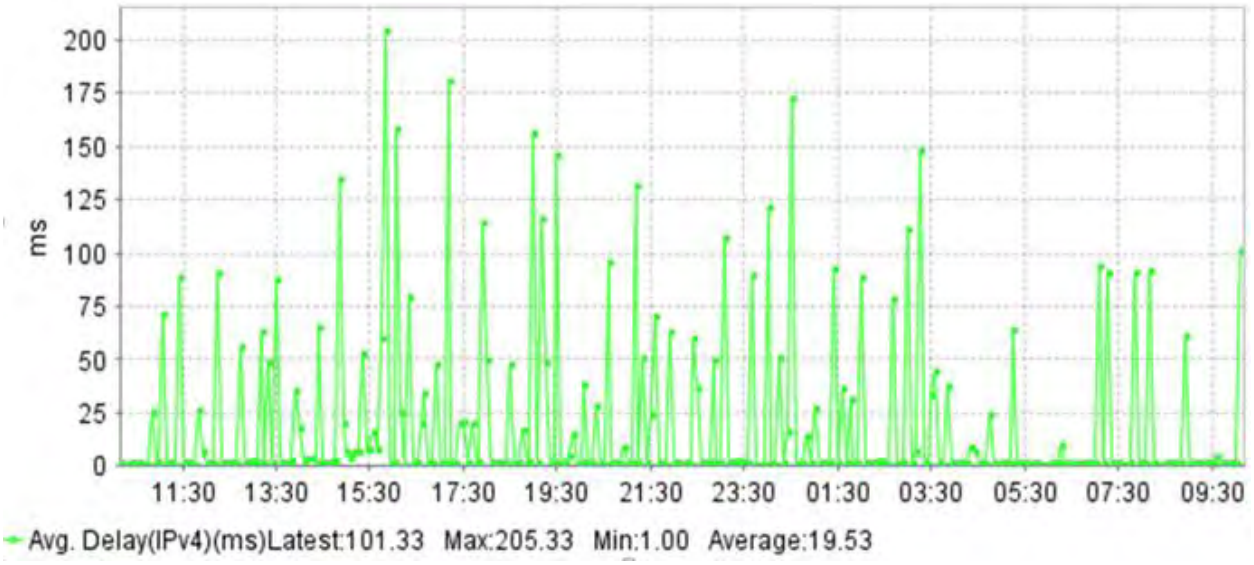


Figure 6.12: Delay when packet flows from SiteA-NE40E to SiteB-NE40E.

According to Figure 6.12, the maximum delay occurs at around 16:00 (4:00PM) which is 205.33ms in a link that connects SiteA NE40E and SiteB Ne40E. However, it may not affect the service quality since it is for a very short period of time. This delay is most probably the result of queueing delay as the time it occurred is at a peak hour. This can also be confirmed using the delay history on a link between RSG in a particular site and BR at that site as the following figure.

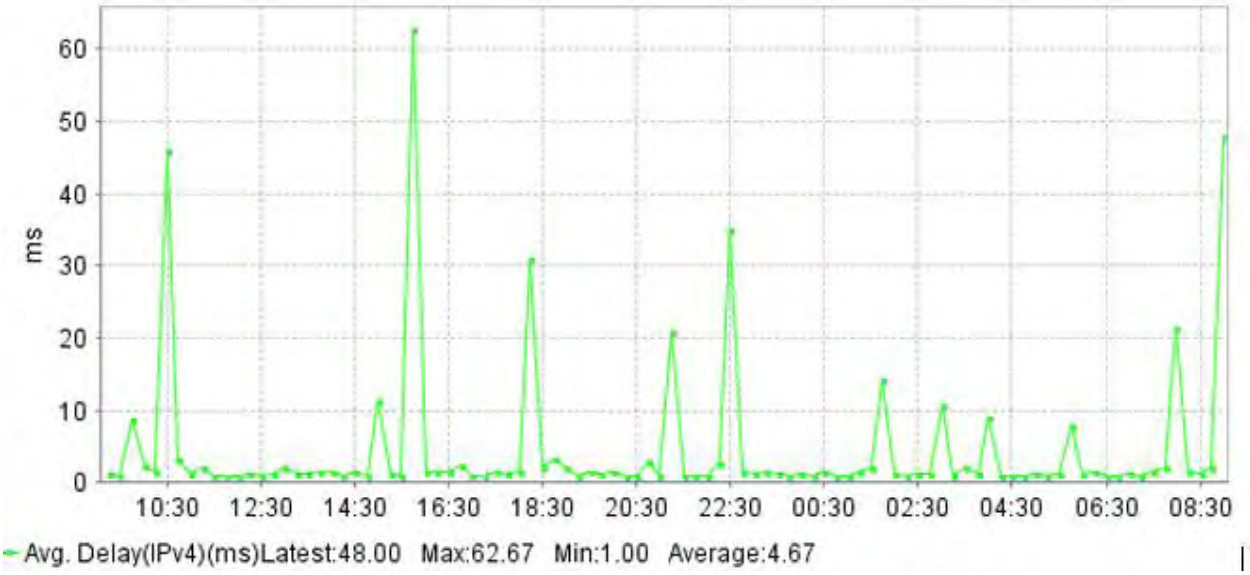


Figure 6.13: Actual delay history of a specific link.

According to the above two pictures, delay is higher in peak compared with other times in a day.

6.4.2 Analysis of Jitter

In the same was as it has been seen in packet loss analysis, we can do packet jitter analysis using average packet jitter of one day in Table 6.10 and ITU standard, which is 10ms for end to end connection. According to the table, all average values for the actual case is below 10ms which shows there is no feasible effect on real data communication.

As mentioned in a packet delay analysis part (Section 6.4.1), there may be jitter values above ITU standard in a link since the Table 6.10 shows average values. We can see this from the following figure.

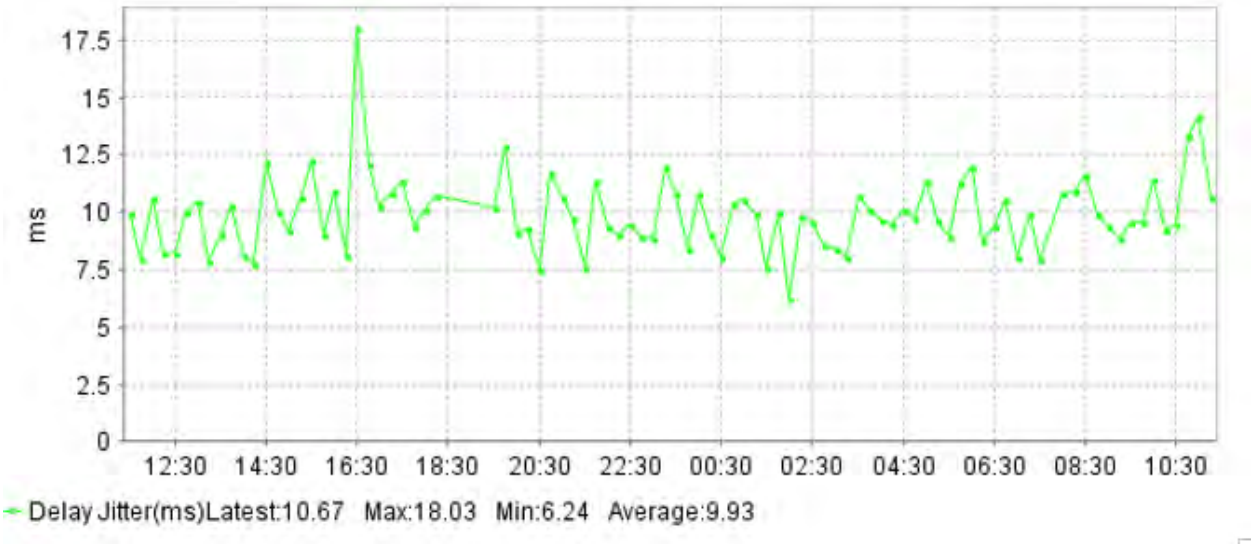


Figure 6.14: Actual packet jitter of a specific link.

As the above figure indicates, the average jitter is 9.93ms but there is a maximum value at 16:30 (4:30PM). This happened because of the packet delay at busy hours.

6.4.3 Traffic Analysis

Network traffic represents the total flow of packets in a given time through the network element. Traffic rate is a measure of how much bits are transmitted through a given network element per second [7, 45]. Hence it is measured by bps. In this section, IP core network traffic is analyzed using traffic rate fetched from two different tools.

Analysis of traffic rate is done based on weekly and daily traffic rate. Busy hour traffic is peaked from daily analysis and considered as a special case.

a. Weekly IP Core Traffic Analysis

The following figure shows the average traffic rate of core network in two weeks. The average traffic rate is done by taking the average of traffic rates of all IP core network elements from the two main vendors' performance monitoring tools.

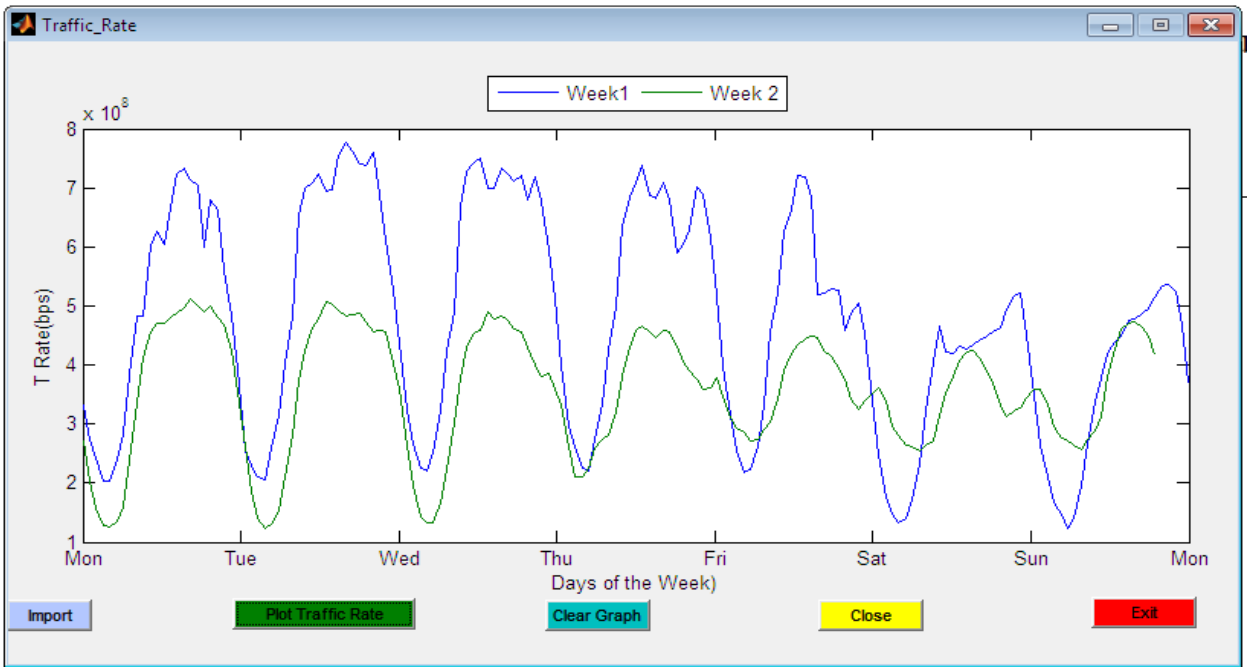
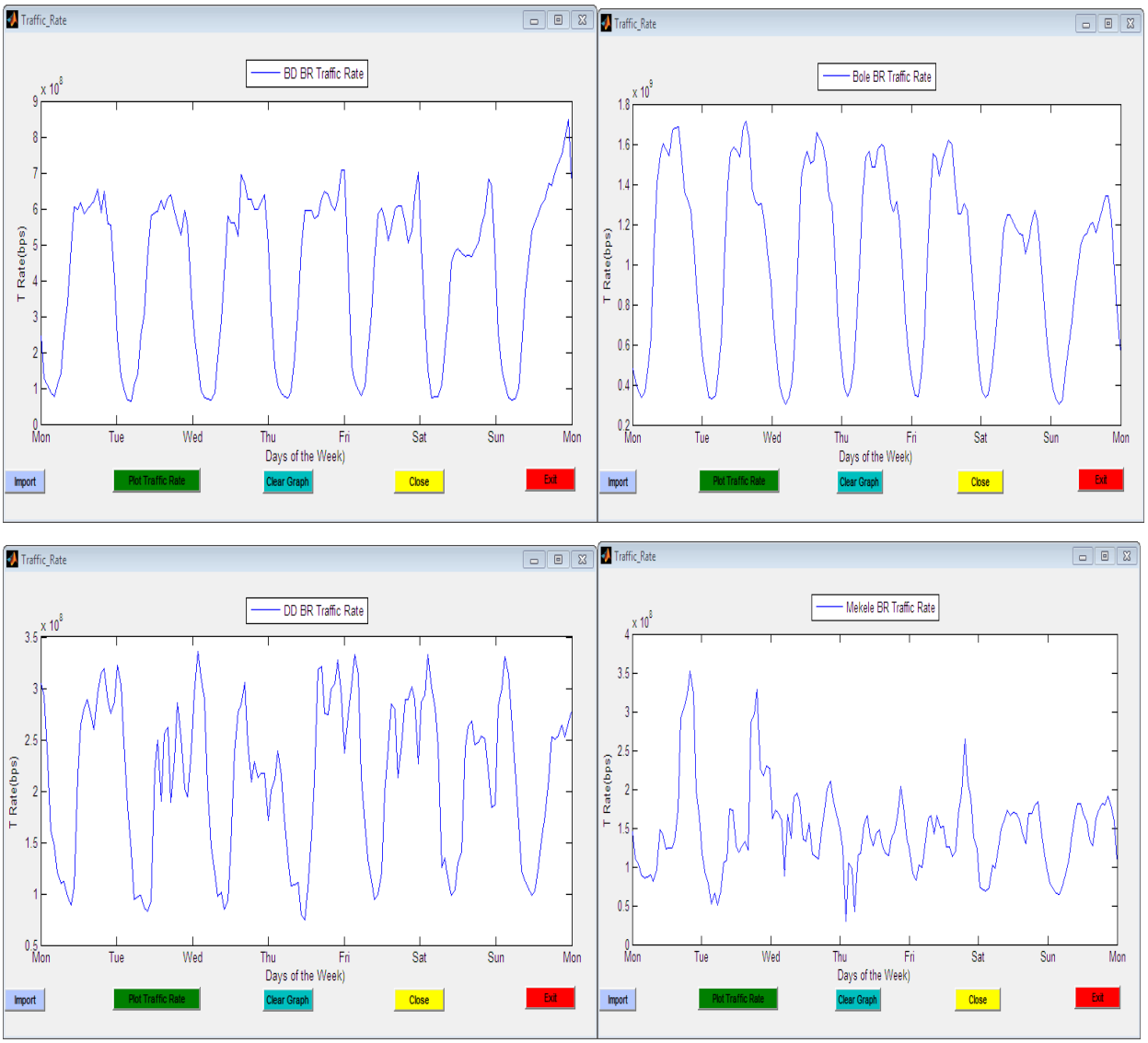


Figure 6.15: Traffic rate of core network in two weeks.

The network traffic rate is higher on Monday in week 2, and On Tuesday on week one. This is due to the higher the network traffic users on the beginning of week days.

It is lower on Saturday and Sunday in both weeks. These days are holidays so that there is minimum user in these days. The reason to this is that most of the time, most users use network on Monday to Friday. For example, banks, governmental organizations, internet centers, and so on are constantly use on working days more than using on weekends.

Traffic rate in each BR (core router in the network) for one week is shown in the following figures. In all routers, the peak hour is around 16:00 (02:00PM) in every day. The figures also show that the traffic usage is higher in week days (Monday to Friday) than weekends (Saturday and Sunday).



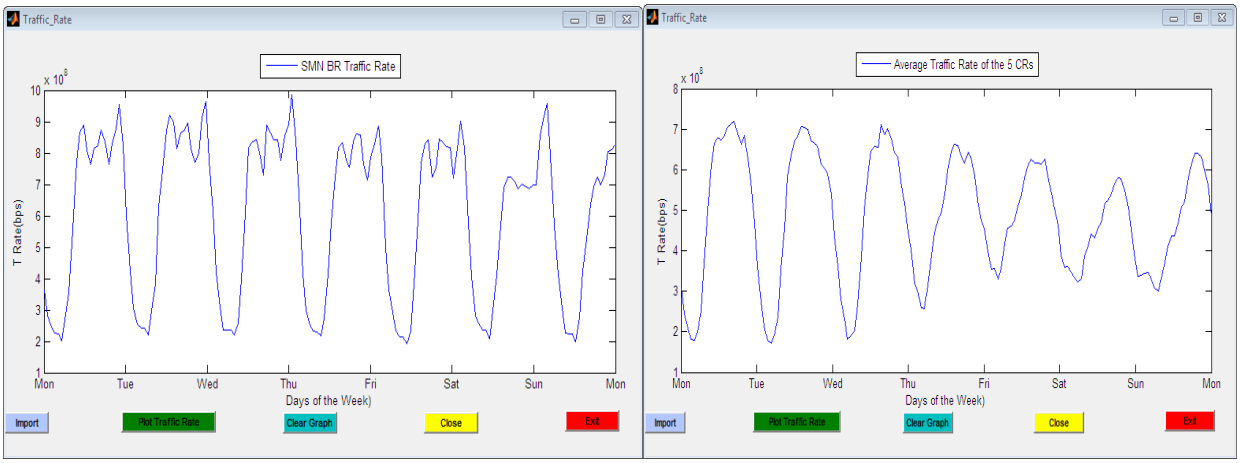


Figure 6.16: Traffic rate of BR on one week.

Traffic rate of the NE40Es, IP core (backhaul) network elements, is somewhat the same with that of BRS. However, it is slightly lower than the traffic rate of BRs. This is because, as it is mentioned in Chapter 2 (Section 2.3), IP backhaul devices are connected into BR. Since a BR has its own access network layer, additional traffic flow from backhaul elements makes the traffic flow in BR higher.

In addition to that, traffic rate is almost similar from Monday to Sunday. The reason for this is that IP backhaul is more for mobile services, and mobile phone users can use data on every day in a week. Other trend and peak hour of traffic rate is the same with that of BRs. This can be seen from the following figures.

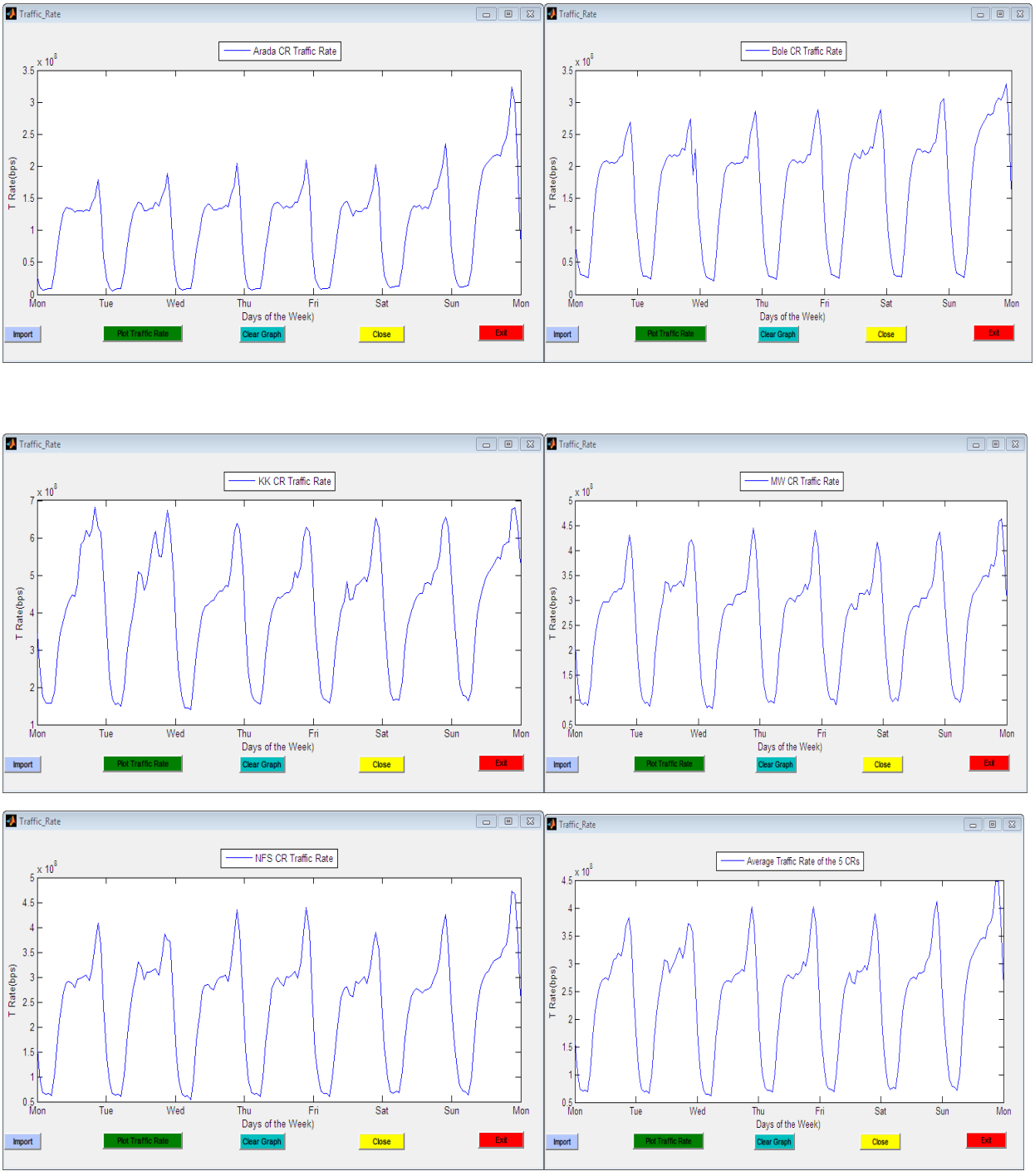


Figure 6.17: Traffic rate of IP core routers in one week.

b. Daily IP Core Traffic Analysis

Daily traffic analysis helps us to see the exact trend of traffic rate and to determine the peak hour in a day. According to Figure 6.16 below, the average traffic rate is higher in a day starting from 09:30 to 21:30 (09:30AM to 09:30 PM). It then reaches at peak around 16:00 (04:00PM).

The figure also shows the slow hour. The traffic rate starts to decline after 6:00PM and reaches to its slowest hour at 4:00AM. It then inclines up starting at the morning 06:00AM. The reason for this is that almost all subscribers do not use services specially data service at night.

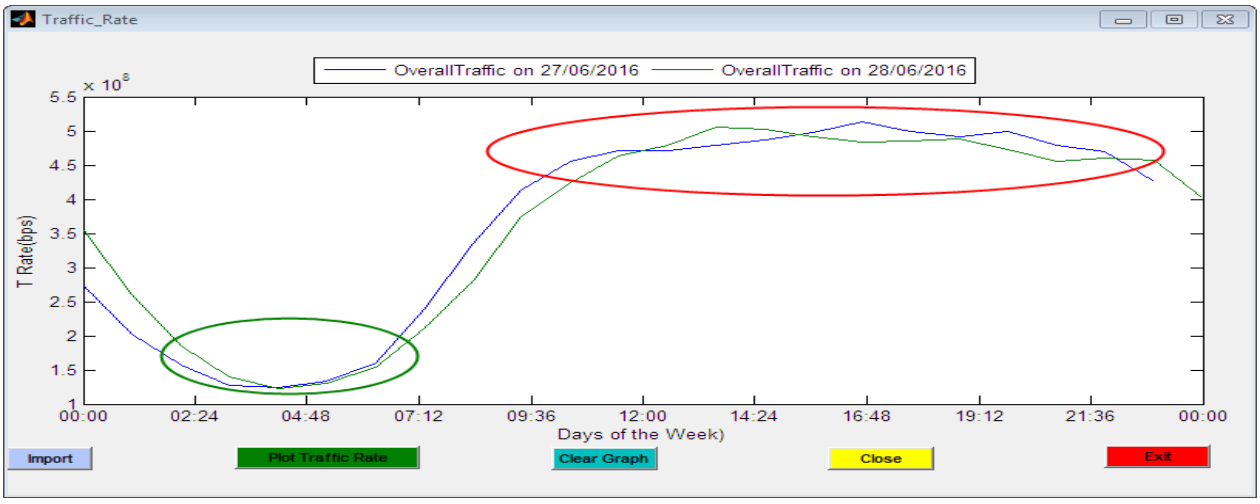


Figure 6.18: Average traffic rate of core network to show peak and slow hours.

Chapter 7: Conclusion, Recommendation and Future Work

7.1 Conclusion

In this thesis, traffic analysis of an IP core network in ethio telecom has been done. The core network actually contains multiple points as there are many hops between two core network elements. This thesis has dealt with issues related with end to end points excluding cases in middle hops. The issues are those that are commonly defined in IP network called KPIs like packet loss, delay, jitter and so on.

Before going directly into traffic analysis, mathematical modeling of defined IP network KPIs was done using Queueing theory. Then these mathematical models were used to do simulation of selected KPIs particularly packet delay, packet delay jitter and packet loss ratio to check if the real network KPIs resemble simulated KPIs or not.

Actual traffic and network performance KPIs data were obtained from the real network without affecting daily operation of the network and introducing its own traffic into the network. The data were collected for monthly, weekly and daily base so as to get enough lookup on the network.

Using simulated result obtained from Matlab simulation software and actual data collected from the existing IP core network monitoring tools (U2000 and U31), analysis was done comparing the simulated and actual results in collaboration with ITU standards. From the results, the following conclusions can be conducted.

- All service quality KPIs are in good conditions in average compared to the ITU standard.
- Traffic analysis of core network shows that BR is busier than the IP Backhaul. This is because; the IP Backhaul is connected to the BR as a one sub-network. In addition to BR's own access network traffic, IP Backhaul traffic enlarged traffic on BR's core network.
- Peak hours and slow hours occurred on those times in which regular activities are held. These hours are more or less at similar times on which peak hours of voice traffic occur.
- Simulation result that was done using vendor independent models showed that the two vendors' performance monitoring tools are neutral and not biasing. Because, mean values of the simulated and actual results are almost the same for all KPIs. Distribution of KPI values around the mean at each point is nearly the same for both simulated and actual result.

7.2 Recommendation

There are enormously increasing number of subscribers nowadays. The increase in smart phone users also increases the subscriber's number. Even though the existing IP core network capacity is not too congested, the increasing network traffic may cause subscribers to not satisfy. So, I recommend the following architecture to the existing IP core network.

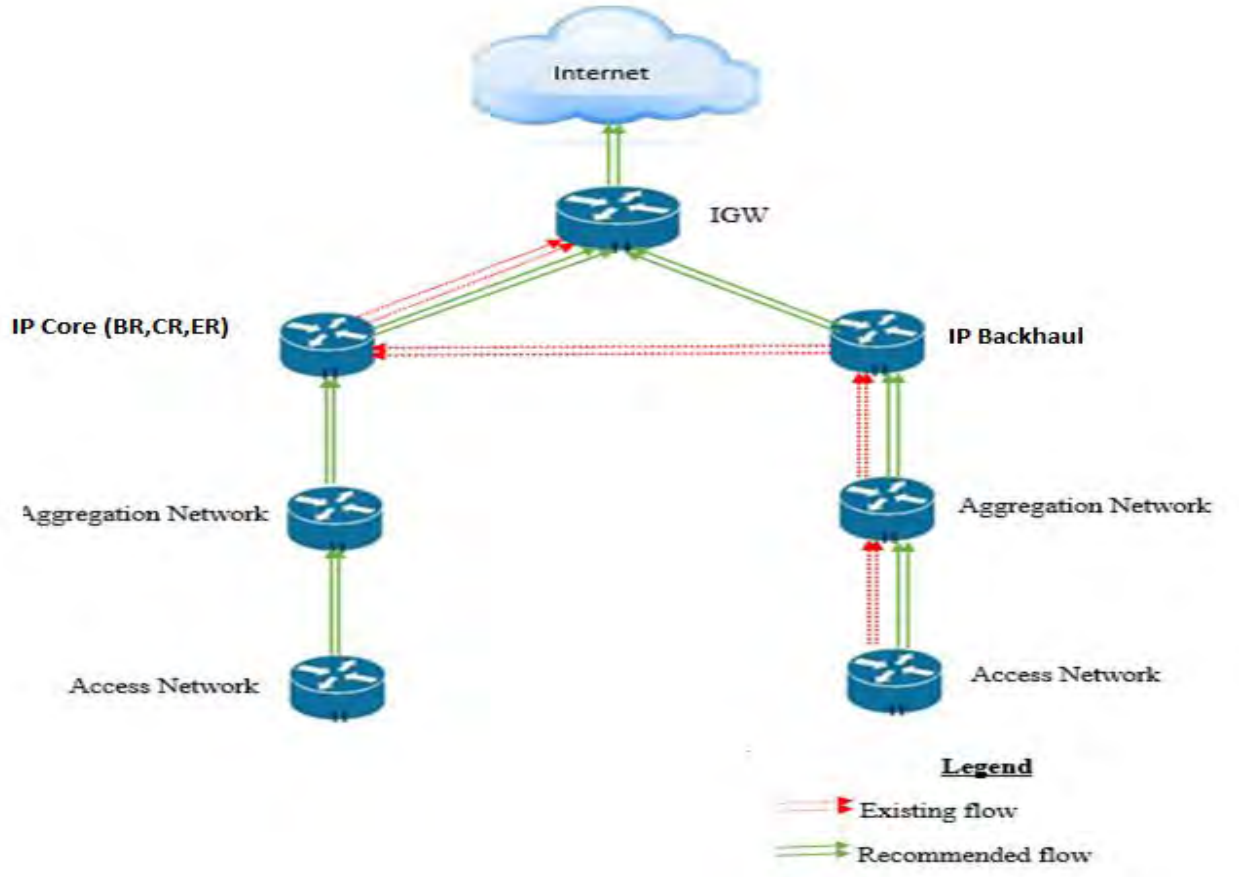


Figure 7.1: Recommended network architecture.

This recommendation is based on the packet delay and traffic rate that we have seen in Chapter 6, Sections 6.3.1 and 6.4.3 respectively. As we can see from Tables 6.4 and 6.5, average monthly delay of IP backhaul networks is slightly less than that of IP core network elements. Numerically, average delay of IP Backhaul core devices is 9.285ms where as that of IP core devices (BR) is 10.335ms. This difference is happened due to the queuing delay that occurs when packets arrive to the common point which is IP core network elements in the existing architecture.

The difference in traffic rate of IP backhaul and IP core network elements is one of the two causes for this paper to recommend the new architecture. This is because the traffic

rate is higher in IP core network elements than that of IP backhaul network elements as we have seen in Figures 6.16 and 6.17. This is because IP core network elements (BR, CR and ER) carry traffic from two directions, one from their access side and the other from the IP backhaul side. The difference in IP core (BR) and IP backhaul (NE40Es) traffic rates is shown in the below figure.

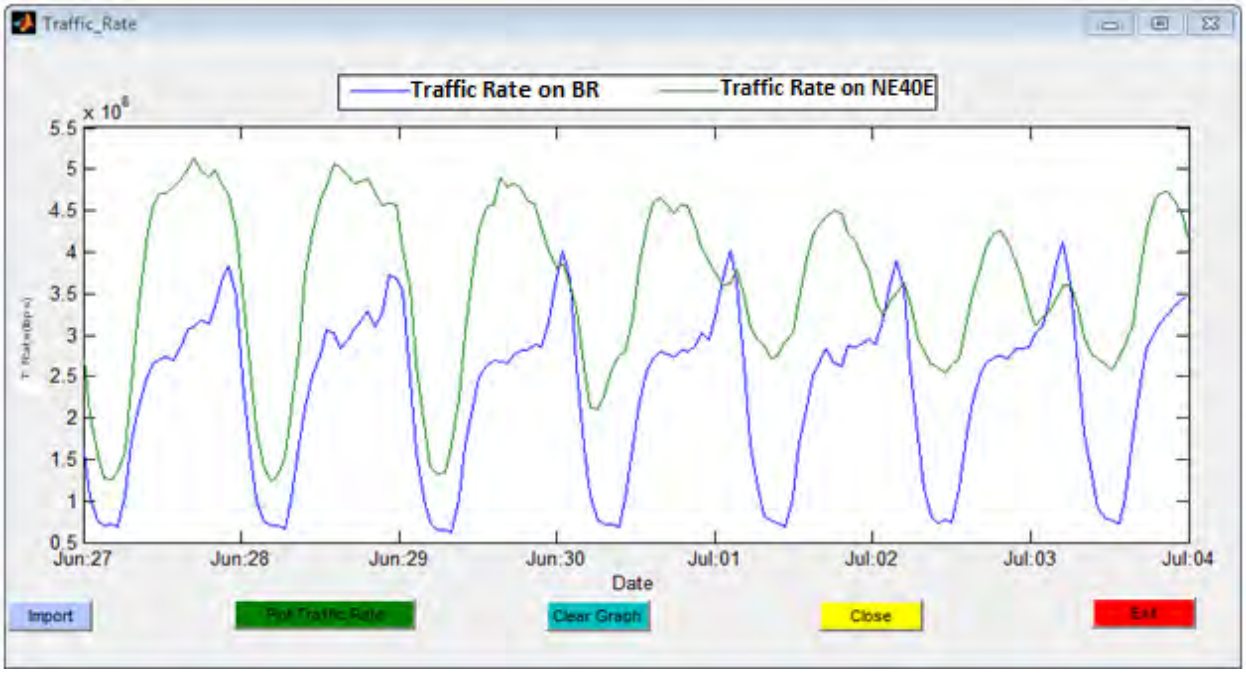


Figure 7.2: Traffic rate of BR and NE40E (one week).

7.3 Future Work

This paper has worked in a great effort to achieve the objective of the study. However, there are some works that are left for future. Some of these works are:

- Increasing the scope of analysis from core to the whole network
- Including all hops during end to end KPIs performance measurements
- Doing traffic analysis based on service types like mobile and fixed broad band

References

[1]. Cisco Networking Academy, "Connecting Networks", First Edition, Cisco Press, May 2014.

[2]. Priscilla Oppenheimer, "Top-Down Network Design", Third Edition, Cisco Press, 2012.

[3]. "Core Network", Retrieved on June 15, 2016, from https://en.wikipedia.org.

[4]. Albert Hankel, "Sustainability in networks", Version 1.1, February 2014.

[5]. Ethio Telecom, "Low Level Design for IP Backhaul".

[6]. Saurav Das, Guru Parulkar, and Nick McKeown, "Rethinking IP Core Networks", Vol. 5, December 2013.

[7]. Andreas Johnsson, Bob Melander, and Mats Björkman, "Bandwidth Measurements in Wired and Wireless Networks", Master Thesis, Mälardalen University, April 2005.

[8]. Jay Beale, Gilbert Ramirez, Angela Orebaugh, "Wireshark & Ethereal Network Protocol Analyzer Toolkit", Syngress, September 2006.

[9]. Akhigbe-Mudu, Ibharalu, Folorunso, "Analysis of Network packet loss using passive measurement technique augmented with parity-check", February 2012.

[10]. Venkat Mohan, Janardhan Reddy, Kalpana, "Active and Passive Network Measurements: A Survey", International Journal of Computer Science and Information Technologies, Vol. 2 (4), 2011.

[11]. Thomas Lindh, "A New Approach to Performance Monitoring in IP Networks–combining active and passive methods", Haninge, Sweden.

[12]. Michael Zhonghua Jiang, "Analysis of Wireless Data Network Traffic", Master Thesis, Simon Fraser University, April 2000.

[13]. Andreas Schmidt, "Network Traffic and Infrastructure Analysis in Software Defined Networks", Master Thesis, Saarland University, May 2015.

[14]. Toni Janevski, "Traffic Analysis and Design of Wireless IP Networks", Methodius University, April 2003.

[15]. Toni Janevski, Boris Spasenovski, "Traffic Analysis for Voice in Wireless IP Networks", Methodius University.

[16]. Baek-Young Choi, Sue Moon, Zhi-Li Zhang, Konstantina Papagiannaki, Christophe Diot, "Analysis of Point-To-Point Packet Delay in an Operational Network", 2004.

[17]. Francesco Musumeci, Massimo Tornatore, and Achille Pattavina, "A Power Consumption Analysis for IP-Over-WDM Core Network Architectures", Vol. 4, February 2012.

[18]. Daniel Abad, "Performance analysis of IPv4 / IPv6 protocols over the third generation mobile network", Master Thesis, Stockholm, August 2014.

[19]. Sarah A. Abdullah, "Performance Analysis of Triple Play Services Over IP Using OPNET Simulator", Master Thesis, May 2013.

[20]. Alexander F. Ribadeneira, "An Analysis of the MOS under Conditions of Delay, Jitter and Packet Loss and an Analysis of the Impact of Introducing Piggybacking and Reed Solomon FEC for VOIP", Master Thesis, Georgia State University, April 2007.

[21]. Krzysztof Perlicki, "Simple Analysis of the Impact of Packet Loss and Delay on Voice Transmission Quality", Warsaw University.

[22]. Mansour J. Karam, Fouad A. Tobagi, "Analysis of the Delay and Jitter of Voice Traffic over the Internet", Stanford University.

[23]. Timo Viipuri, "Traffic Analysis and Modeling of IP Core Networks", Master thesis, Helsinki University, December 2004.

[24]. Mohamed Faten Zhani and Halima Elbiaze, "Analysis and Prediction of Real Network Traffic", University of Quebec in Montreal, Canada November 2009.

[25]. Harish Kapri, "Network Traffic Data Analysis", Master Thesis, Louisiana State University, December 2011.

[26]. Yichi Zhang, "Residential Network Traffic and User Behavior Analysis", Master Thesis, Stockholm, 2010.

[27]. Kenneth D. Stewart III, Aubrey Adams, "Designing and Supporting Computer networks", April 2008.

[28]. Todd Lammle, "CCNA Cisco Certified Network Associate Study Guide", John Wiley & Sons, Inc., 2013.

[29]. Cisco Series, "Layer 2 WAN Technology Design Guide", August 2014.

[30]. Michael Howard, "Routers on the IP Edge Overcoming the Triple Challenge of Video, Mobility, and Cloud", October 2009.

[31]. James F. Kurose, Keith W. Ross, "Computer Networking: A Top-Down Approach", Sixth Edition, 2013.

[32]. ZTE Corporation, "ZXR10 T160G/T64G 10-Gb Routing switch User manual", Version 2.6, Jane2007.

[33]. Huawei, "Operation Guide for Router NE Management, version V100R002C01", November 2010.

[34]. Ethio Telecom, "High Level Design for IP Backhaul LOT1 Addis Ababa Swap and Build Project", Final Version II.

[35]. Gerhard Haßlinger, Oliver Hohlfeld, "The Gilbert-Elliott Model for Packet Loss in Real Time Services on the Internet", 2007.

[36]. Douglas C. Montgomery, "Applied Statistics and Probability for Engineers", Third Edition, John Wiley & Sons, 2003.

[37]. Jean-Chrysostome Bolot, "Characterizing End-to-End Delay and Loss Behavior in the Internet", In SIGCOMM Symposium on Communications Architectures and Protocols, San Francisco, September 1993.

[38]. Dimitri Bertsekas, Robert Gallager, "Data Networks", Prentice-Hall International

[39]. Ivo Adan and Jacques Resing, "Queueing System", March 2015.

[40]. Moshe Zukerman, "Introduction to Queueing Theory and Stochastic Tele traffic Models", 2000.

[41]. Robert B. Cooper, Yang Chen, Zengbin Zhang, "Introduction to Queueing Theory", Second Edition.

[42]. Hamza Dahmouni, André Girard, Brunilde Sanso, "An analytical model for jitter in IP networks", May 2011.

[43]. Athanasios Papoulis, "Probability, Random variables and Stochastic Processes", Third Edition, McGraw-Hill, 1991.

[44]. Leonid B. Koralov, Yakov G. Sinai, "Theory of Probability and Random Processes", Second Edition, 2007.

[45]. Shingo Ata, Masayuki Murata, Hideo Miyahara, "Analysis of Network Traffic and Its Application to Design of High-Speed Routers", Volume E83-D, May 2000.

[46]. Undeger C. "Introduction to Modeling & Simulation", Bilkent University, Turk, 2008.