SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
NETWORK AND COMPUTER SYSTEMS DEPARTMENT

Continues Usage Based on Internet Traffic Control

A PROJECT SUBMITTED AS ONE OF THE REQUIREMENTS FOR OBTAINING A BACHELOR OF HONOR IN COMPUTER SYSTEMS AND NETWORKS

AUGUST 2014

بسم الله الرحمن الرحيم

SUDAN UNIVERSITY OF SCIENCE AND TECHNOLOGY
COLLEGE OF COMPUTER SCIENCE & INFORMATION TECHNOLOGY
NETWORK AND COMPUTER SYSTEMS DEPARTMENT

Continues Usage Based on Internet Traffic Control

PROPOSED BY:

MNASIK IBNOMER ALDSOOGY GAFFAR

OLA HUSSIEN ZEYAD BAKHEET

EIMAN OSMAN OMER MOHAMMED

SIGNATURE OF SUPERVISOR:

DR. ABU AGLA BABKER MOHAAMED

CO SUPERVISOR. MOHAMMED ALKHATIM OMER AHMED

AUGUST 2014

آيـــــــه

قال تعالي:

{وَقَالَ الَّذِينَ أُوتُوا الْعِلْمَ وَيْلَكُمْ ثَوَابُ اللَّهِ خَيْرٌ لِمَنْ آمَنَ وَعَمِلَ صَالِحًا وَلَا يُلَقَّاهَا إِلَّا الصَّابِرُونَ}
{القصص الايه 40}

الحمد

الحمد لله الذي جعل لنا من العلم نورا نُهدى به و بعد:

نتقدم ببحثنا هذا الي كل من يجمعنا بهم رباط العلم من مستمعين و قراء و معلمين ,إذ نضع بين أيديكم هذا البحث الذي نرجوأن يكون في المستوى المطلوب ..راجين من الله سبحانه وتعالى التوفيق والعون.

العلم مغرس كل فخر فافتخر ... واحذر يفوتك فخر ذاك المغرس

واعلم بأن العلم ليس يناله ... من همه في مطعم أو ملبس

إلا أخو العلم الذي يُعنى به ... في حالتيه عاريا أو مكتسي

فاجعل لنفسك منه حظا وافرا ... واهجر له طيب الرقاد وعبّسِ

فـ لعل يوما إن حضرت بمجلس ... كنت أنت الرئيس وفخر ذاك المجلس

شكر وتقدير

لابد لنا ونحن نخطُوا خُطواتنا الأخيرة في الحياة الجامعية من وقفة نعود إلى أعوام قضيناها في رحاب الجامعة مع أساتذتنا الكرام الذين قدموا لنا الكثير باذلين بذلك جُهداً كبيراً في بناء جيل الغد لتُبعث الأُمة ,وقبل أن نمضي نتقدم بأسمى آيات الشكر والامتنان والتقدير والمحبة...

إلى الذى حمل أقدس رسالة في الحياة رسول الله ﷺ...

إلى الذين مهدوا لنا طريق العلم والمعرفة...

إلى جميع أساتذتنا الأفاضل...

"كن عالما ... فإن لم تستطع فكن مُتعلماً، فإن لم تستطع فأحب العلماء ،فإن لم تستطع فلا تبغضهم"

وأخُص بالشكر والتقدير:

الدكتور ابوعاقله بابكر محمد.

الذي نقول له بشراك قول رسول الله ﷺ:

"إن الحوت في البحر ، والطير في السماء ، ليُصلون على معلم الناس الخير"

وكذلك نشكر كل من ساعدنا على إتمام هذا البحث وقدم لنا العون ومد لنا يد المساعدة وزودنا بالمعلومات اللازمة لإتمام هذا البحث ونخص بالذكر:

الاستاذ:محمد الخاتم والاستاذ:عمر بشري والاستاذ:مروان يوسف

الذين كانوا عونا لنا في بحثنا هذا ونوراً يُضيء الظلمة التي كانت تقف أحيانا في طريقنا.

الإهداء

إلى من بلغ الرسالة وأدى الأمانة .. ونصح الأمة .. إلى نبي الرحمة ونور العالمين

سيدنا محمد ﷺ

إلى من كلله الله بالهيبة والوقار، إلى من علمني العطاء بدون إنتظار، إلى

من أحمل إسمه بكل إفتخار

والدي العزيز

إلى معنى الحب وإلى معنى الحنان والتفاني ، إلى

بسمة الحياة وسر الوجود

إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي

أمي الحبيبة

إلى من به أكبر وعليه أعتمد ، إلى شمعة متقدة تنير ظلمة حياتي

إلى من بوجوده أكتسب قوة ومحبة لا حدود لها

أخي

إلى توأم روحي ورفيقة دربي .. إلى صاحبة القلب الطيب والنوايا الصادقة

إلى من رافقتني منذ أن حملنا حقائب صغيرة ومعها سرت الدرب خطوة بخطوة

أختي

إلى الأخوات اللواتي لم تلدهن أمي .. إلى من تحلوا بالإخاء وتميزوا بالوفاء

والعطاء إلى ينابيع الصدق الصافي إلى من معهم سعدت ، وبرفقتهم في دروب

الحياة الحلوة والحزينة سرت إلى من كانوا معي على طريق النجاح والخير صديقاتي

ABSTRACT

Network traffic monitoring and control play very important rule in bandwidth optimization and QoS assurance. Network monitoring has many benefits like knowing about the services available in the network put just the availability or interruption for users, enabling to appease the users, also provides information about users of the network. This project focus on monitoring the network to providing useful information about usage of the users, analyze the traffic to know the usage of the users, and finally find out the heavy users who used network bandwidth heavily and then restrict them by reducing their bandwidth. So that the normal users will be satisfied. In this project, practical implementation for control the users based internet traffic has been done, tested and evaluated. The result is significant according to the current test-bed. The benefits of this project are to provide QoS where Each user don't use bandwidth more than planned one during the peak time, while allowing them to freely utilize the bandwidth at the non-peak hours, moreover, it saves the cost by avoiding upgrading the bandwidth and it is suitable for the non-profit organizations, universities.

المستخلص

شبكة المراقبة والتحكم تلعب قاعدة مهمة جدافي تحسين عرض النطاق الترددي وضمان جودة الخدمة. شبكة المراقبة لها فوائد كثيرة مثل معرفة معلومات حول الخدمات المتوفرة في الشبكة وتوفرها أوانقطاعها عن المستخدمين، مما يتيح فرصة لإرضاء المستخدمين، ويوفر أيضا معلومات حول المستخدمين في الشبكة.هذا المشروع يركزعلى مراقبة الشبكة لتوفير معلومات مفيدة حول استخدام المستخدمين، وتحليل كمية البيانات التي تمر عبر الشيكة لمعرفة إستخدام المستخدمين، ومعرفة المستخدمين الذين يستخدمون نطاق ترددي عالي ومن ثم حصرهاعن طريق الحد من عرض النطاق الترددي. حتى أن المستخدمين العاديين سوف يكونون راضين. في هذا المشروع، تم التنفيذ العملي له واختباره وتقييمه. فوائد هذاالمشروع توفيرجودة الخدمة (حيث يتم ارضاء المستخدمين بتوفير الخدمة التي يحتاجونها بجودة عالية)حيثلكل مستخدملا يستخدمعرض نطاق ترددياكثرمما كان مخططا لهخلالوقت الذروة، مع السماح لهم بالتمتعبحريةعرض النطاق الترددیفيغير ساعاتالذروة، علاوة على ذلك، فإنه يحفظ تكلفةمناسبةللمنظماتغير الهادفة للربح، والجامعات وما شابه ذلك.

LIST OF TERMS

Term	Description
P2P	Peer to peer
QOS	Quality of service
Ubuntu	Operating system
IPFM	Ip flow meter
TC command	Traffic control
C sharp	Programming language
LAN	Local Area Network
HTTP	Hyper Text Transfer Protocol
NETFLOW	a network protocol developed by Cisco for the collection and monitoring of network traffic flow
IFTOP	a command-line system monitor tool
PFTOP	is a small, curses-based utility for real-time display of active states and rule statistics for pf, the packet filter. for OpenBSD
PINGSTING	is an application that monitors networks for ICMP Echo Requests and attempts to determine what application generated the ICMP packets.
TCPSPY	is an administrators' tool that logs information about selected incoming and outgoing TCP/IP connections
Nomad	Nottingham Online Maps And Dataand its Tool for monitoring networks and analysis

FLOWSCAN	A Network Traffic Flow Reporting and Visualization tool
MRTG	Multi Router Traffic Grapier and its Tool for monitoring networks and analysis
NTOP	It is a tool that shows the network usage, is based on pcapture and it has been written in a portable way in order to virtually run on every Unix platform.
WIRESHARK	is an open source tool for profiling network traffic and analyzing packets
Angry IP	Angry IP is a very lightweight program that allows you to quickly scan a range of IP addresses
NMAP	Networked Messaging Application Protocoland its Tool for monitoring networks and analysis
PRTG	Paessler Router Traffic Grapher and its Tool for monitoring networks and analysis
IPFIX	Internet Protocol Flow Information Export
PSAMP	Puget Sound Assessment and Monitoring Program
EPON	Ethernet passive optical networks
DBA	dynamic bandwidth allocation
P-EPON	penetrated-EPON
OPNET	Optimized Network Engineering Tool
OLSR	Optimized Link State Routing
Cisco	Computer Information System company
IP voice	voice applications provided over the Internet

VPN	Virtual Private Network
MPLS	Multi-Protocol Label Switching
IT	Information Technology
SAN	Storage Area Network
Amazon EC2	Elastic Cloud Computing Platform
VM-level	Virtual machine level
MySQL	open source database software
AIMD	Additive Increase and Multiplicative Decrease
ECN	Explicit Congestion Notification.
OMNET++	extensible, modular, component-based C++
TCP	Transmission Control Protocol
UCON	usage control model
IPTRAF	is a console-based network monitoring program for Linux that displays information about IP traffic
R-VBR	Renegotiable Variable Bit Rate
VBR	Variable Bit Rate
RED-VBR	renegotiated deterministic VBR
BEB	binary exponential back
SFLOW	a multi-vendor sampling technology embedded within switches and routers. It provides the ability to continuously monitor application
ASICs	Application Specific Integrated Circuit
CPU	Central Processing Unit

SARG	Squid Analysis Report Generator
HTML	Hyper Text Markup Language
ICMP	Internet Control Message Protocol
NAGIOS	monitoring and alerting services for servers, switches, applications, and services
SNMP	Simple Network Management Protocol
PPP	Point-to-Point Protocol
WINPCAP	Windows Packet Capture package
OSPF	Open Shortest Path First
UDP	User Datagram Protocol
IPFM	IP FLOW METER
RAM	Random Access Memory
DUMP	keyword specifies the interval at which to create log files use in IPFM tool
NAC	Network Access Control
OS	Operating system
Squid	caching proxy server
DNSPERF	Authoritative Domain Name services
PESPERF	is designed specifically to simulate Caching Domain Name services
DHCPERF	Dynamic Host Configuration Protocol
VoIP	Voice over Internet Protocol

PNG	penetrated-EPON
C	Program language
BPMN	Business Process Management
UML	Unified Modeling Language
SYSML	SystemsModelingLanguage
QA	Quality Assurance
MPLS	Multi-Protocol Label Switching
ISP	Internet service provider

LIST OF FIGURES:

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1. Introduction

Network monitoring provides the information necessary for network management. It is important to find network trends and locate network problems quickly.

The purpose of network monitoring is the collection of useful information from various parts of the network so that the network can be managed and controlled using the collected information.

Most of the network devices are located in remote locations. These devices do not usually have directly connected terminals so that network management application cannot monitor their statuses easily. Thus, network monitoring techniques are developed to allow network management applications to check the states of their network devices. As more and more network devices are used to build bigger networks, network monitoring techniques are expanded to monitoring networks as a whole.

Bandwidth [1] on the internet can only beconceptualized over time, and the amount of time that you talk about can greatly change the user experience. For reliable data transmission within computer network and internet forms the basis for management and control of bandwidth. Without bandwidth management, a user will not be able to handle all available bandwidth on the networks. It will be impossible to differentiate between various network traffics, and it will also be difficult to control which user or application has priority on the network.

Applications which require specific quantity and quality of service may not be predicted in terms of available bandwidth, thus making some applications run poorly due to improper bandwidth allocation.

Bandwidth management from Managed Communications enables our business to benefit by getting:

a) Get better information –that is can better understand your bandwidth usage with comprehensive bandwidth management tools.

b) Faster application speed - bandwidth management can allocate bandwidth to key critical applications enabling better performance.

c) Reduce unwanted traffic –by isolate P2P users or bandwidth hogs on your network so that you control the quality of performance seen across your data connections.

d) More bandwidth –that is can achieve up to 35 times the throughput with bandwidth management services [26].

The flowing figure [1.1] show Amount of bandwidth used in week one of Trinity term 2005 to 2011:

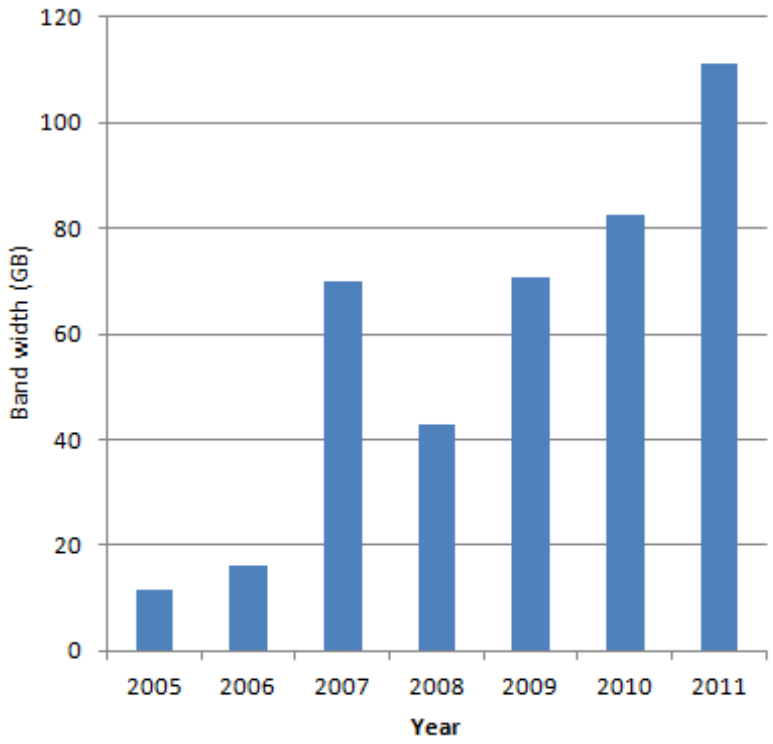


Figure 1.1:Amount of bandwidth used in week one of Trinity term 2005 to 2011

A new Internet traffic trends report released by the Canadian broadband management company Sandvine reveals [2] that global P2P traffic is expanding, with Bit

Torrent as the key player. In North America, more than half of all upstream traffic (53.3%) on an average day can be attributed to P2P.

The normalized aggregate of all traffic (up/down) during peak hours puts P2P traffic at 19.2% during the first months of 2010. Interestingly, this is up from 15.1% in 2009, which shows that P2P traffic is growing strongly, not only in absolute numbers but also as a share of total Internet traffic in North America.

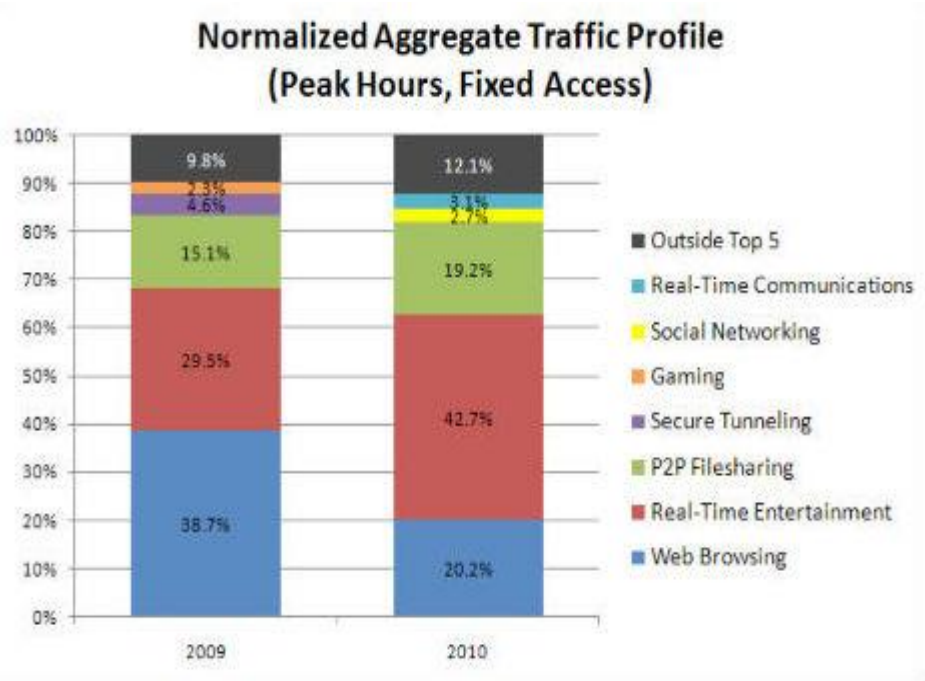


Figure 1.2: Normalized aggregate traffic profile

Network monitoring is a difficult and demanding task that is a vital part of a Network Administrators job.[3] Network Administrators are constantly striving to maintain smooth operation of their networks. If a network were to be down even for a small period of time Productivity within a company would decline, and in the case of public service departments the ability to provide essential services would be compromised. In order to be proactive rather than reactive, administrators need to monitor traffic movement and performance throughout the network and verify that security do not occur within the network.

It is a fact that the users always require a very high quality of service, very high speed internet access to satisfy their application's needs. On the other hand in most of the cases the Internet link has a limited bandwidth due to the budget constraints.

1.2. Problem Statement

Controlling the use of bandwidth among users is a challenging task,For example, if we assume the existence of a number of users in the network running different applications (some of them are bandwidth intensive while the others are considered light applications) accordingly, their offered traffic will vary. Thus, if the bandwidth is limited, the link will be congested and the heavy behaviour of some of the users will affect the performance of the rest. Therefore, a mechanism for monitoring and controlling the usage of the users must be exist so as to achieve the goals of balancing between performance (acceptable perceived QOS for the users) and cost (avoiding the link upgrading due to the users complains).

1.3. Research objectives:

1. To Monitor and control the user behaviors in the network.
2. To enhance the usage of bandwidth in the organization.
3. Torestrictthe user who have a heavy behavior in the network.

1.5. Scope of Research

The project will be implemented and tested in Sudan University of Science and Technology (College of Computer Science and Information Technology) network.

1.6. Research Methodology

At the first the implementation of the projectneeds to install OSand some tools to monitoring the network and some to apply some policy and other to write the code.

1.7. Thesis Layout

Chapter 2 is divided into two Sections. The first Section discusses the general introduction to the network monitoring, analysis, control and Tools usein traffic monitoring and analysis. The Second section is previousstudy.

Chapter 3 explores the issues for traffic monitoring and analysis.it also shows the tool use in the project and why we are choice it.

Chapter 4 explains the system structure and analysis the system.

Chapter 5 clarifiesthe implementation of system and the result of project.

Chapter 6 compares our project with the related studies. Also shows our recommendations for the future studies.

CHAPTER 2

BACKGROUND AND PREVIOUS STUDIES

2.1. Introduction

This chapter explains the concepts of Traffic Control, Bandwidth Management, Traffic Congestion and Traffic Monitoring…ETC ,and finally the previous studies and explain the work for each studies ,also advantage and disadvantage of each one of them.

2.1.1. Background

In this section define the basic concepts of traffic control, bandwidth management, and quality of Service. These three concepts are related but distinct.

2.1.1.1.Traffic Control

Traffic control is an agreement between a source and a destination to limit the flow of packets without taking into account the load on the network. The purpose of traffic control is to ensure that a packet arriving at a destination will find a buffer there.

Without any control, the source may send packets at a pace too fast for the destination. This may cause buffer overflow at the destination leading to packet losses, retransmissions, and degraded performance. A flow control scheme protects the destination from being flooded by the source [1].

2.1.1.2.Bandwidth Management

Bandwidth is a term used in much of the telecommunications industry as a measure, usually expressed in bits per second, of the rate at which information moves from one electronic device to another.

Without proactive management of bandwidth, network capacity fills with viruses and inappropriate traffic, problems cannot be diagnosed and the connection becomes ineffective.

Managing bandwidth improves the performance of an internet connection by removing unnecessary traffic: "improving bandwidth management is probably the easiest way for universities to improve the quantity and quality of their bandwidth for educational purposes". Bandwidth is like a pipe, it doesn't matter how big the pipe is, if the traffic in the pipe is not managed it will clog up with unwanted traffic and be hijacked by viruses, spam, peer-to-peer file-sharing traffic and problems on the network will not be accurately diagnosed. Bandwidth management requires three activities: Policy, Monitoring and Implementation. If any one of these is activities is missing then the management of bandwidth is significantly compromised. The activities inform and reinforce each other it is not enough to right-size the bandwidth. In order to properly manage this scarce resource, IT departments need a complementary budget for supporting infrastructure and staff. In particular, adequate budget will be needed to enforce policies and to use technology smartly [2].

2. 1.1.3. TrafficCongestion

Congestion is said to occur in the network when the resource demands exceed the capacity and packets are lost due to too much queuing in the network. During congestion, the network throughput may drop to zero and the path delay may become very high. A congestion control scheme helps the network to recover from the congestion state.

A congestion avoidance scheme allows a network to operate in the region of low delay and high throughput.The problem of congestion control is more difficult to handle in networks with connectionless protocols than in those with connection-oriented protocols. In connection-oriented networks, resources in the network are reserved in advance during connection setup. Thus, one easy way to control congestion is to prevent new connections from starting up if congestion is sensed [3].

2.1.1.4. Traffic Monitoring

The term network monitoring describes a range of techniques by which it is sought to observe and quantify exactly what is happening in the network, both on the

microcosmic and macrocosmic time scales. Data gathered using these techniques provides an essential input towards:

• Performance tuning: identifying and reducing bottlenecks, balancing resource use, improving QOS and optimizing global performance.

• Troubleshooting: identifying, diagnosing and rectifying faults.

• Planning: predicting the scale and nature of necessary additional resources.

• Development and design of new technologies: Understanding of current operations and trends motivates and directs the development of new technologies.

• Characterization of activity to provide data for modelling and simulation in design and research.

• Understanding and controlling complexity: to understand the interaction between components of the network and to confirm that functioning, innovation, and new technologies perform as predicted and required. The introduction of persistent HTTP connections, for instance, was found in some cases to reduce overall performance.

• Identification and correction of pathological behaviour.

2.1.1.5.Traffic analysis

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.Traffic monitoring and analysis is essential in order to more effectively troubleshoot and resolve issues when they occur, so as to not bring network services to a stand still for extended periods of time. Numerous tools are available to help administrators with the monitoring and analysis of network traffic [5].

2.1.1.6. Usage control

The term usage control is a generalization of access control to cover obligations, conditions, continuity (on going controls) and mutability. Traditionally, access control has dealt only with authorization decisions on a subject's access to target resources. Obligations are requirements that have to be fulfilled by the subject for allowing access. Conditions are subject and object-independent environmental requirements that have to be satisfied for access. In today's highly dynamic, distributed environment, obligations and conditions are also crucial decision factors for richer and finer controls on usage of digital resources. Traditional authorization decisions are generally made at the time of request but typically do not recognize ongoing controls for relatively long-lived access or for immediate revocation. Moreover, mutability issues that deal with updates on related subject or object attributes as a consequence of access have not been systematically studied [6].

2.1.1.7. Network Capacity planning

Network planning is determining how much bandwidth the network actually needs.

2.1.1.8. The Benefits of Capacity Planning

1. Budgeting

Capacity planning outlines the personnel and equipment your small business will need in order to maintain current operations and reach goals.

2. Scalability

Scalability is the process of planning for expansion.

3.Dynamic Change

The process of capacity planning collects a significant amount of data on how your company currently operates. One of the ways in which you can stay competitive in the

marketplace is to use that capacity data to make changes to your organization to keep up with your competition. For example, if your prime competitor expanded its customer service staff by 20 percent, then your capacity planning information can let you know exactly what you would need it terms of money, facilities and personnel to keep up with the competition's level of support.

The following figure2.2 shows Capacity Planning Methodology

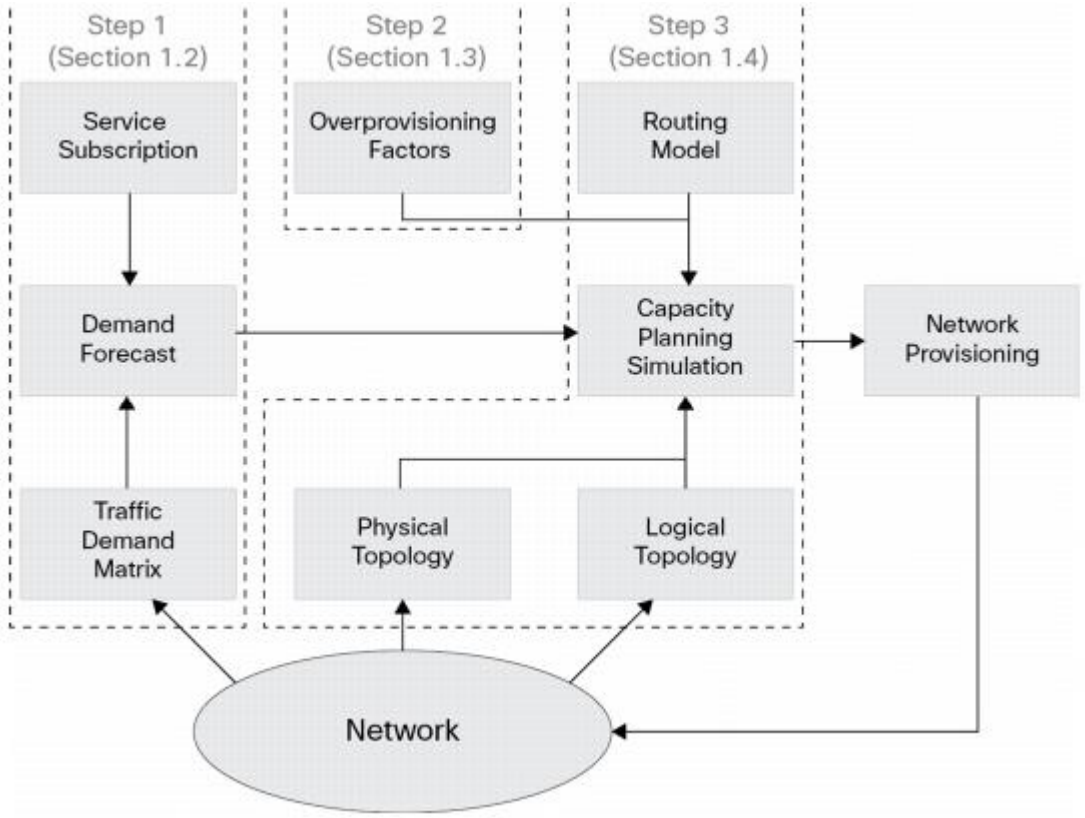


Figure2 .2: Capacity Planning Methodology [25]

2.2. Previous Studies

Raj Jain, K. K. Ramakrishnan [7] they compare the concept of congestion avoidance with that of flow control and congestion control.

Similar with the project in applying efficiency, fairness, but there are not applying their aims.

Shuo Fang, ChuanHengFoh, and KhinMiMiAung [16], their aims at designing a congestion and priority solution for Ethernet congestion management.

Different with this project their aims manage Ethernet congestion but us aims to manage congestion within user's level.

2.3 conclusions

The outcomes of this chapter are: the first one is understand the related concepts such as traffic controlling, bandwidth management and network monitoring etc. the second outcome is to have knowledge about other efforts on the project problem and their methodologies to obtain better result based on their results.

CHAPTER 3

NETWORK TRAFFIC CONTROL TECHNIQUES AND TOOLS

3.1. Introduction

The network monitoring directory contains software which allows a system administrator to monitor a network for the purposes of security, billing, and analysis (both online and offline).

Network analysis is the process of capturing network traffic and inspecting it closely to determine what is happening on the network.

A networkanalyser decodes, or dissects the data packets of common protocols and displays the network traffic in human-readable format. Networkanalysis is also known by several other names: traffic analysis, protocol analysis, packet sniffing, packet analysis, and eavesdropping to name a few.

Network analysis tools enable diagnosis of problems or allow exploration of all hardware on a computer network.

Network traffic control is the process of managing, prioritizing, controlling or reducing the network traffic, particularly Internet bandwidth, e.g. by the network scheduler. It is used by network administrators, to reduce congestion, latency and packet loss. This is part of bandwidth management. In order to use these tools effectively, it is necessary to measure the network traffic to determine the causes of network congestion and attack those problems specifically.

Networktraffic measurement is the process of measuring the amount and type of traffic on a particular network. This is especially important with regard to effective bandwidth management.

3.2. Network Monitoring and analysing Tools

3.2.1. NETFLOW

Netflow is another option for bandwidth usage analysis. Netflow is a standard means of traffic accounting supported by many routers and firewalls. You need a Netflow collector running on a host inside your network to collect the data. PfSense can export Netflow data to the collector using the pfflowd package, or softflowd [26].

3.2.2.SFlow

SFlow is a multi-vendor sampling technology embedded within switches and routers.It provides the ability to continuously monitor application level traffic flows at wire speed on all interfaces simultaneously.

The SFlow Agent is a software process that runs as part of the network management software within a device. It combines interface counters and flow samples into SFlow datagram's that are sent across the network to SFlow Collector. Packet sampling is typically performed by the switching/routing ASICs, providing wire-speed performance. The state of the forwarding/routing table entries associated with each sampled packet is also recorded.

The SFlow Agent does very little processing. It simply packages data into SFlow Datagram's that are immediately sent on the network. Immediate forwarding of data minimizes memory and CPU requirements associated with the SFlow Agent [27].

3.2.3. SARG

SARG is an open source tool that allows you to analyze the squid log files and generates beautiful reports in HTML format with information's about users, IP addresses, top accessed sites, total bandwidth usage, elapsed time, downloads, access denied websites, daily reports, weekly reports and monthly reports.

The SARG is very handy tool to view how much internet bandwidth is utilized by individual machines on the network and can watch on which websites the network's users are accessing [28], as show bellow in figure 3.1thatshow Screen Snapshot of Sarg.

Figure 3.1: Screen Snapshot ofSarg.

3.2.4. Cacti

Cacti are a complete network graphing solution designed to harness the power of RRDTool's data storage and graphing functionality. Cacti provides a fast poller, advanced graph templating, multiple data acquisition methods, and user management features out of the box. All of this is wrapped in an intuitive, easy to use interface that makes sense for LAN-sized installations up to complex networks with hundreds of devices [29].

3.2.5. Nagios

Nagios is a system and network monitoring application. It watches hosts and services that you specify, alerting you when things go bad and when they get better.

Nagios was originally designed to run under Linux, although it should work under most other unices as well.

Nagios was designed as a rock solid framework for monitoring, scheduling and alerting. Nagios contains some very powerful features, harnessing them is not only a matter of understanding how Nagios works, but also how the system you're monitoring also works. This is an important realization. Nagios can't automatically teach you about complex systems, but it will be a valuable tool to help you in your journey,as show bellow in figure 3.2that show Screen Snapshot of Nagios.

Figure 3.2: Screen Snapshot of Nagios.

3.2.6.Nomad

Nomad is a network mapping program designed to automatically discover a local network, using SNMP to identify network devices and work out how they are physically connected together. The network is then presented as a topology diagram with simple integrated monitoring. Changes in the network are reflected in the diagram which continuously updates, and you can customize your own views of the network map with various views and filters.

3.2.7.Ntop

Ntop is a tool that shows the network usage, similar to what the popular top UNIX command does. Ntop is based on capture and it has been written in a

portable way in order to virtually run on every UNIX platform, as show bellow in figure 3.3that shows Screen Snapshot of Ntop.

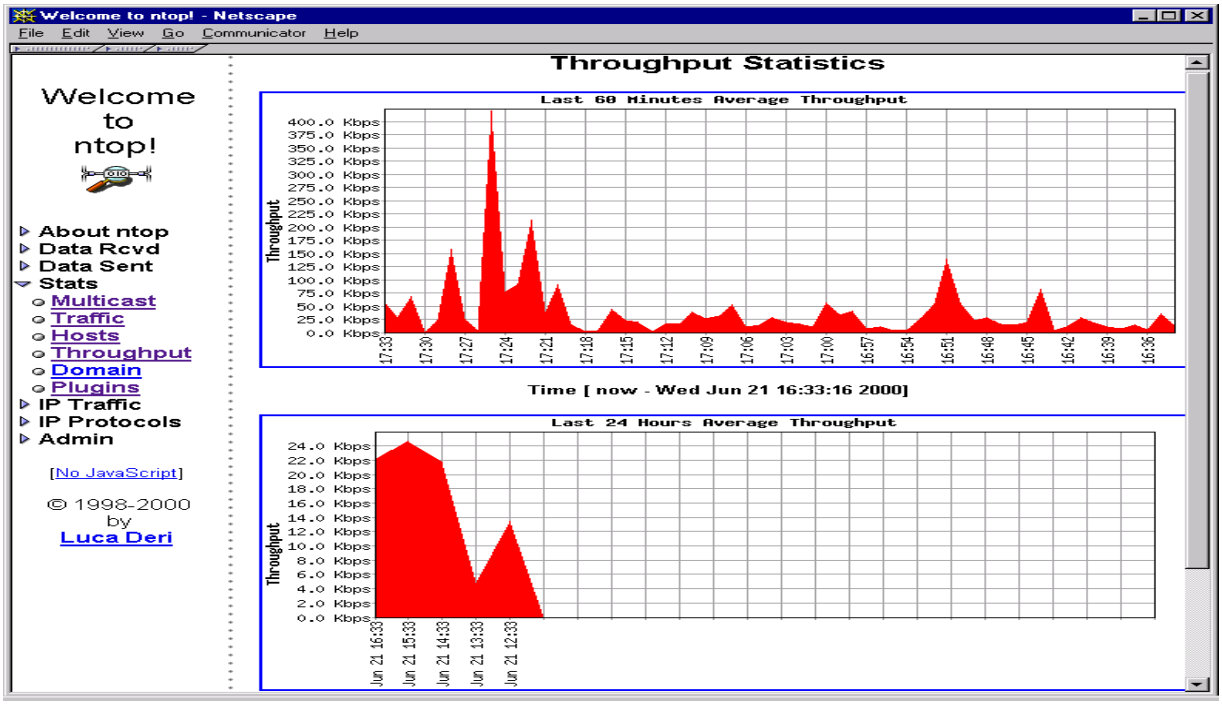


Figure 3.3: Screen Snapshot of Ntop.

3.2.8.WireShark

WIRESHARK (formerly Ethereal) has established itself as the premier packet analyzer. It can capture packets of standard Ethernet, PPP and VPN interfaces. I have used it many times to identify people running heavy reports bringing servers down to a crawl.

WireShark requires installation of Windows Packet Capture package (WINPCAP). WinPcap allows for other software to 'listen' secretly to the information coming and going through the network card on the computer. I found it better to install the latest WinPcap first, rather than versions included with the

programs, as show bellow in figure 3.4 thatshow Screen Snapshot of Wireshark.

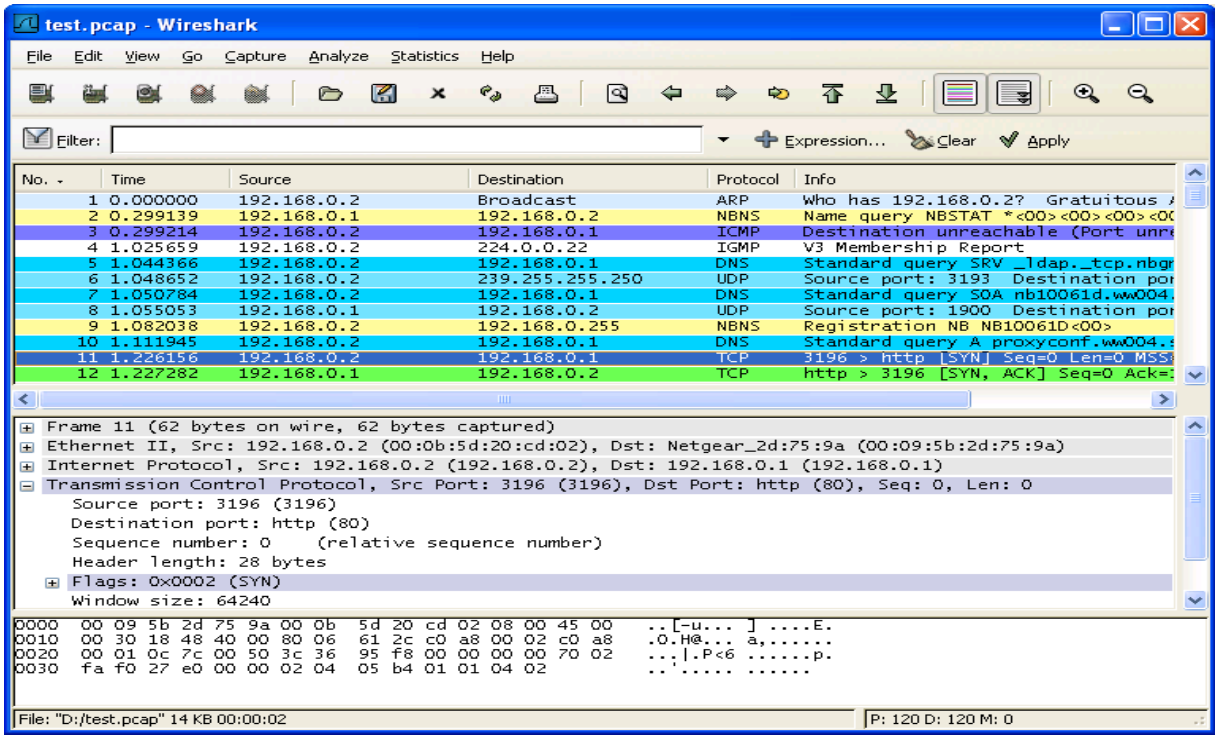


Figure 3.4: Screen Snapshot of Wireshark.

3.2.9.Angry IP

Angry IP Scanner (or simply ipscan) is an open-source and cross-platform network scanner designed to be fast and simple to use. It scans IP addresses and ports as well as has many other features.

It is widely used by network administrators and just curious users around the world, including large and small enterprises, banks, and government agencies.

It runs on Linux, Windows, and Mac OS X, possibly supporting other platforms as well [30].

3.2.10. IPTraf

IPTraf is a menu driven utility that allows you to monitor your TCP network. Information such as ICMP, OSPF, TCP and UDP counts can be displayed easily. Interfaces can be monitored. Monitor connectivity and traffic with ease.

IPTraf cannot create the configuration file. The most likely cause of this is that you didn't properly install the program, and the necessary directory /var/local/iptraf does not exist. Can also be generated if you have a disk problem or if you have too many files open [31], as show bellow in figure 3.5 thatshow Screen Snapshot of IPTraf.

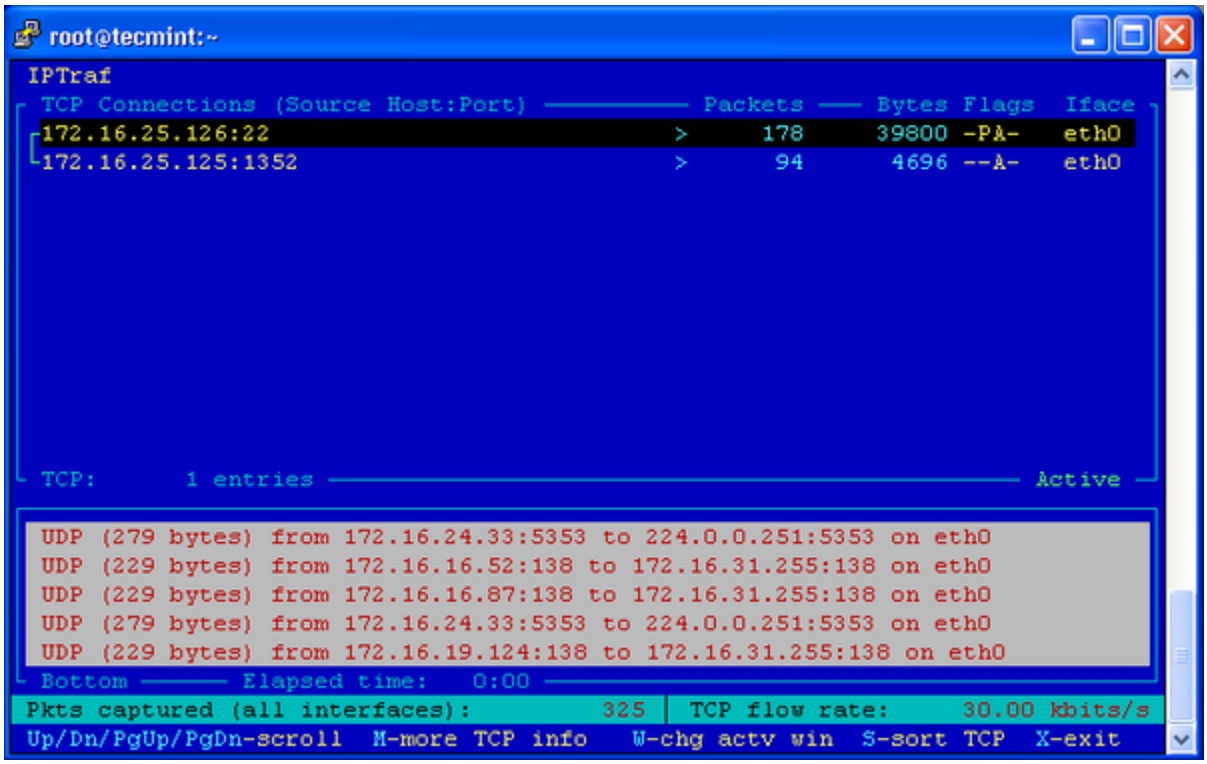


Figure 3.5: Screen Snapshot of IPTraf.

3.2.11. IPFM

IP Flow Meter (IPFM) is a bandwidth analysis tool which outputs a list of hosts with their respective bandwidth usage. IPFM uses libpcap and aims to be portable. It features multi-filtering rules and name resolving, and runs on Linux, FreeBSD, and IRIX [32].

3.3. Network Usage Control Tools

3.3.1. NAC

Network Access Control (NAC) is a complete standards-based, multi-vendor interoperable pre-connect and post-connect Network Access Control

solution for wired and wireless LAN and VPN users. Using Extreme Networks NAC Gateway appliances and/or NAC Gateway Virtual Appliance with NetSight NAC management configuration and reporting software, IT administrators can deploy a leading-edge NAC solution to ensure only the right users have access to the right information from the right place at the right time including time of day, location, authentication types, device and OS type, and end system and user groups [33].

3.3.2. Squid

Squid is caching proxy server, which improves the bandwidth and the response time by caching the recently requested web pages. Now a day's many servers in the world are configured with squid in order to provide high delivery speeds to the clients. Configuring the squid in transparent mode, special configuration is not required on the client side. All the requests originatinating from client and going to internet on port 80 are automatically redirected by proxy. Depending on the requirement we need to configure the squid as transparent or non-transparent proxy. This lab aims to enable readers implement a Proxy server in the network so that other users of the LAN can leverage the functionalities of accessing internet through proxy [34].

3.3.3. TC command

Traffic control is the name given to the sets of queuing systems and mechanisms by which packets are received and transmitted on a router. This includes deciding which (and whether) packets to accept at what rate on the input of an interface and determining which packets to transmit in what order at what rate on the output of an interface.

1.3.4. IP TABLE

Iptables is a generic table structure that defines rules and commands as part of the netfilter framework that facilitates Network Address Translation (NAT), packet filtering, and packet mangling in the Linux 2.4 and later operating systems. NAT is the process of converting an Internet Protocol address (IP address) into

another IP address. Packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols. Packet mangling is the ability to alter or modify packets before and/or after routing [24].

3.4. Network Traffic Measurement Tools

3.4.1. DNSPerf

DNSPerf measures Authoritative Domain Name services and is designedsimulate network conditions by self-pacing the query load.

3.4.2.ResPerf

It is designed specifically to simulate Caching Domain Name services. To test a caching server, ResPerf systematically Increases the query rate and monitors the response rate.

3.4.3. DHCPerf

DHCP performance testing provides a means of predicting server behavior under load and verifying server performance. The most important elements in a DHCP performance test tool are:

• Accuracy the tool's results should correlate strongly with the server's "real-world" Performance.

• Reproducibility Successive testing runs with the tool should produce strongly similar results.

• Simplicity Good results should not be dependent upon configuration options, and the tool should be easy to use and understand.

3.4.4. PRTG

PRTG is an indispensable network traffic logger that makes life for network administrators much easier. In addition to measuring network traffic, PRTG also monitors the availability and performance of network devices, checks the quality of VoIP connections, monitors CPU and RAM usage, etc. Each PRTG license includes various remote probes which allow you to monitor multiple

locations with just one installation of the monitoring software, as show bellow in figure 3.6 thatshow Screen Snapshot of PRTG.

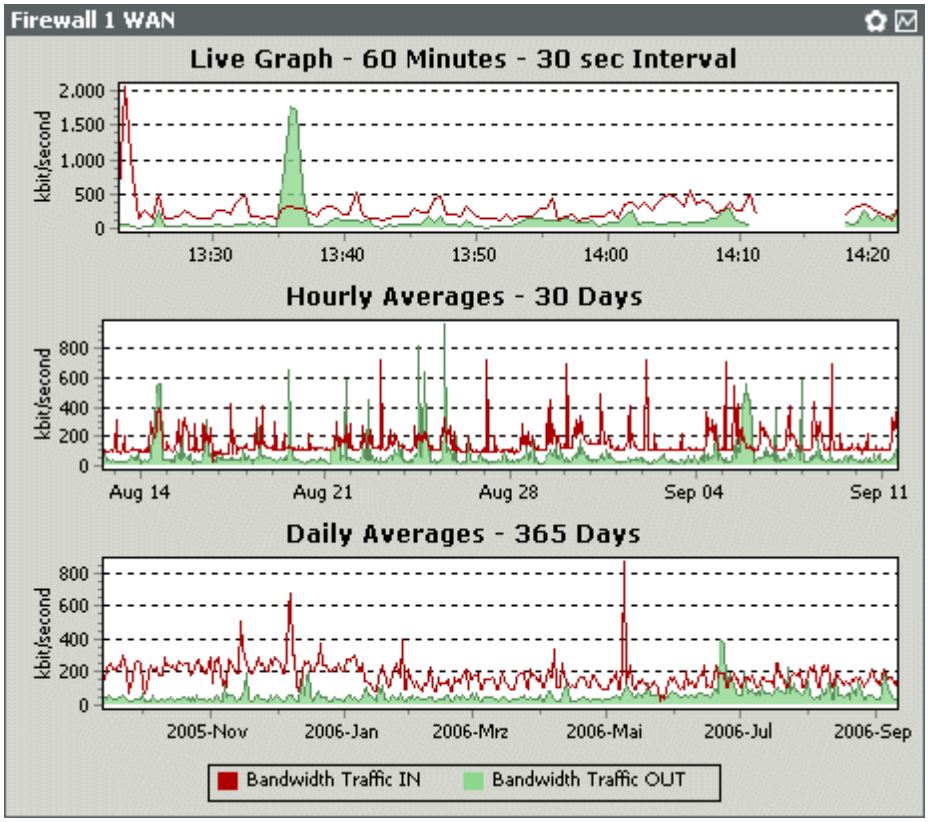


Figure 3.6: Screen Snapshot of PRTG [PRTG06]

3.4.5. MRTG

The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images which provide a LIVE visual representation of this traffic.

MRTG consists of a Perl script which uses SNMP to read the traffic counters of your routers and a fast C program which logs the traffic data and creates beautiful graphs representing the traffic on the monitored network connection. These graphs are embedded into WebPages which can be viewed from any modern Web-browser.

MRTG is not limited to monitoring traffic, though. It is possible to monitor any SNMP variable you choose. You can even use an external program to gather the data which should be monitored via MRTG. People are using MRTG, to

monitor things such as System Load, Login Sessions, Modem availability and more. MRTG even allows you to accumulate two or more data sources into a single graph.

3.5. The Best Tools for This Project

IPFM package makes use of the pcap library to obtain network data for processing.

IPFM serves as a useful tool for analyzing bandwidth usage by hosts on a network, as it stores a table of all IP host pairs communicating and the total amounts of traffic following in each direction. This table is periodically output to disk in text format which can be further processed. Tools such as this can be invaluable in determining which hosts on one's network are responsible for the majority of traffic, and which external hosts are popular. The pcap library filter logic allows for the selection of traffic (such as the exclusion of traffic between hosts on the local LAN) if required.

We chose IPFM because it save user data that is needs to use in the project (such as IP address and the traffic (in and out) of each device) in a file.

When properly employed, traffic control should lead to more predictable usage of network resources and less volatile contention for these resources. The network meets the goals of the traffic control configuration. Bulk download traffic can be allocated a reasonable amount of bandwidth even as higher priority interactive traffic is simultaneously serviced. Even low priority data transfer such as mail can be allocated bandwidth without tremendously affecting the other classes of traffic and we choice TC command to control and shape the traffic of users and we use IP TABLE because it have option to limited the bandwidth for specific user by determining his IP address .

3.6. Summary

This chapter explain some tool use in Network Monitoring and analysing, Network Usage Control, Network Traffic Measurement and the tool will use in the project and why we are choice it.

CHAPTER 4

SYSTEM STRUCTURE

4.1. Introduction

4.1.1. ENTERPRISE ARCHITECT

Enterprise Architect is a very powerful Visual Modeling Platform for Comprehensive UML analysis and design tool, Rich modeling for business, software and systems, Full traceability from requirements to deployment, Code engineering in over 10 languages, Scalable, team-based repository, Enterprise frameworks, mind maps, BPMN. The flowing figure 4.1 show picture of Enterprise Architecture:

Figure 4.1: Enterprise Architecture

4.2. SYSTEM ANALYSIS

4.2.1. Introductions

The key components of the system are: monitoring algorithm, analysing algorithm, decision function, and increase/decrease algorithms, as show below on figure 4.2:

Figure 4.2: Component of the system

The system contains server and many clients, the client request service via server then the server monitoring the traffic in the network and analysis the result of monitoring to specify heavy users in the network then the system will control the heavy usage users.

The following figure 4.3 show simple network has server and many clients.

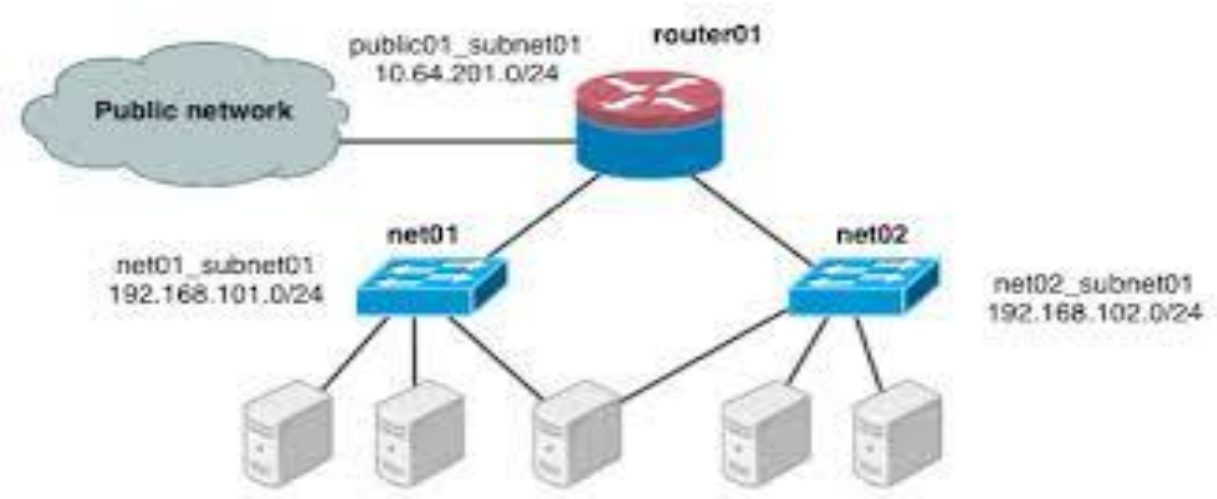


Figure 4.3: simple network

To explain the idea of the project Suppose that pc0 want to download video require very high bandwidth and pc1 in same LAN wantBrowsing and he/she uses few bandwidth, by monitoring the network Appearsthat is pc0 disturbs the other users and uses more than allowed bandwidth and must be restricted by reducing his bandwidth and give a chance to others to work better.

4.2.2 UML diagram

This section covers how the system will work using UML diagrams. Enterprise Architect has been used to create the following UML Diagrams for theoretical analysis to the project.

4.2.2.1 THE USE CASE DIAGRAM

The use case diagram display all function of the system (login, start system, monitoring, collection data, analysis, restriction, view report, stop system) as show in Figure 4.4.

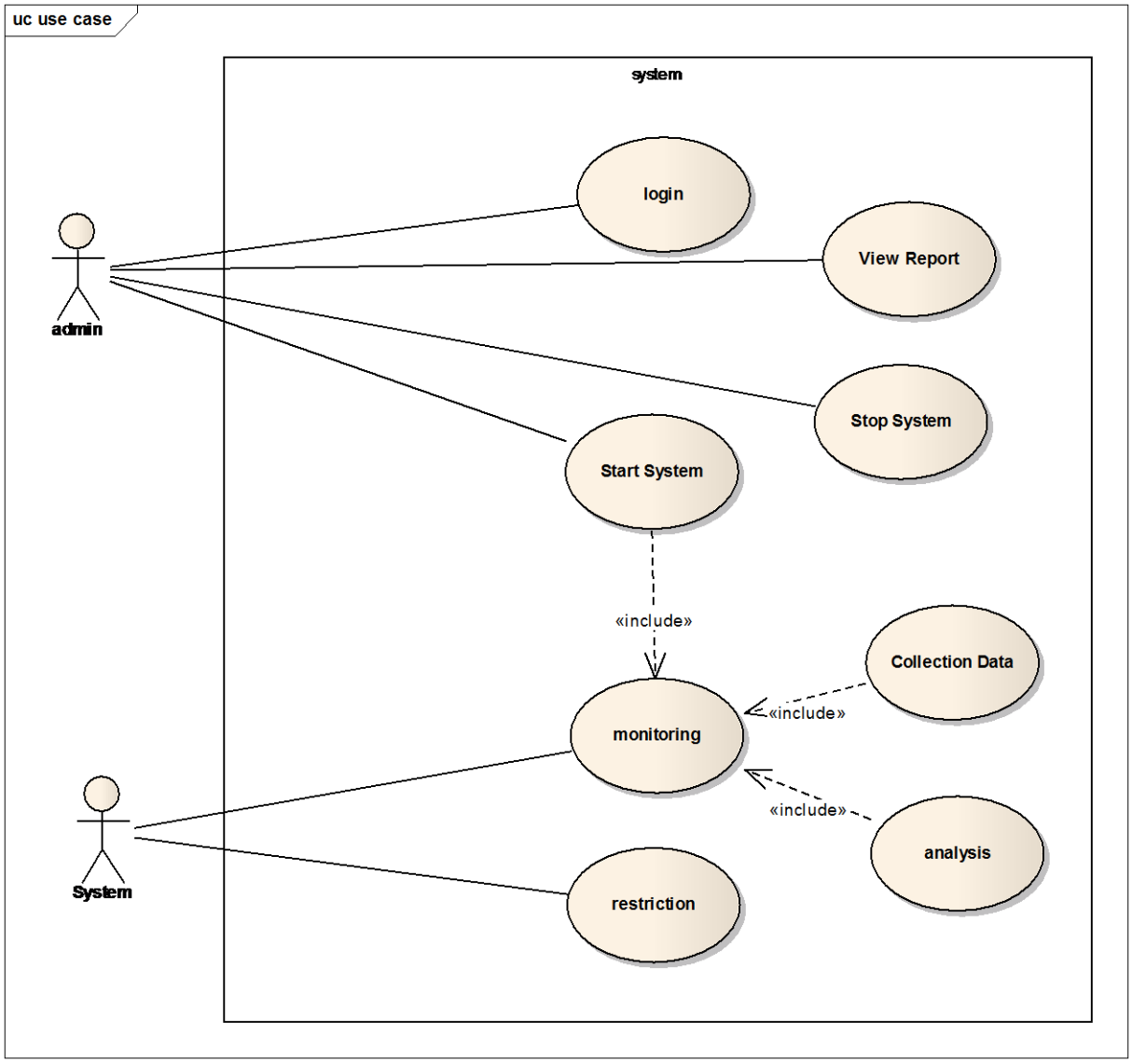


Figure 4.4: use case diagram.

4.2.2.2. UML Description

4.2.2.2.1. Login Use case

Login to system by enter username and password in system interface.

4.2.2.2.2. Start system Use case

Is to make IPFM start to start all function of system.

4.2.2.2.3. Monitoring Use case

Monitoring the network to known useful information about network.

4.2.2.2.4. Analysis Use case

Analysis data to known heavy usage users.

4.2.2.2.5. Collection data Use case

That is data collected about the user in the network.

4.2.2.2.6. Restriction Use case

Restrict heavy usage user.

4.2.2.2.7. View report Use case

Is view report of system that contains the black list (heavy usage users).

4.2.2.2.8. Stop system Use case

Is terminating the system (stop all function in the system)

4.2.2.3. THE SEQUENCE DIAGRAMS

The following figures 4.5 show the sequence of login use case, that show the action happens when the administrator want to login to system:

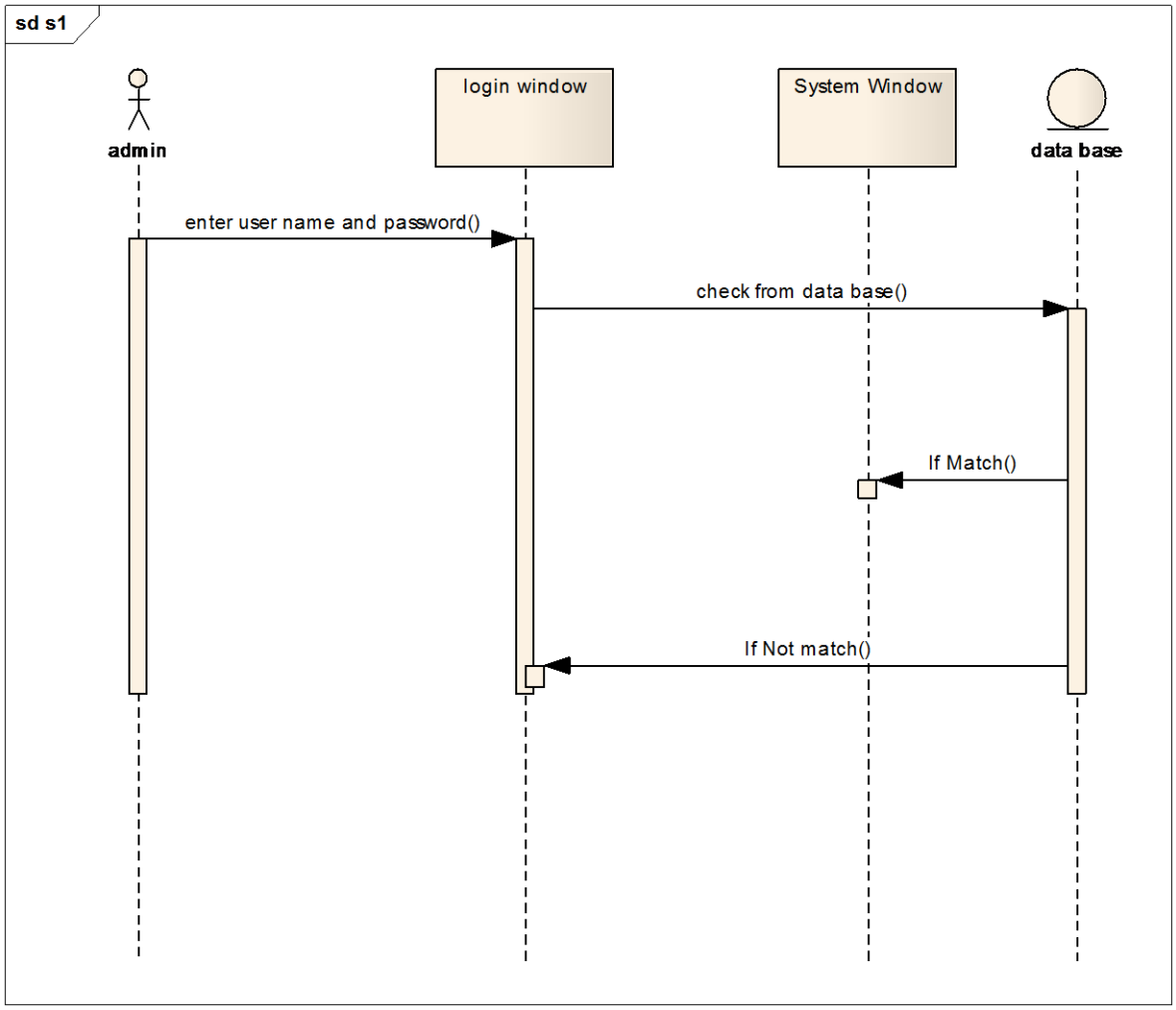


Figure 4.5: login diagram.

In this sequence will display the actions that happen when the administrator enter username and password in login window then the system will check it's from database ;if match it will display system window else it will return to login window and send error message.

The following figures 4.6 show the sequence of start system use case, which shows the action to start the system:

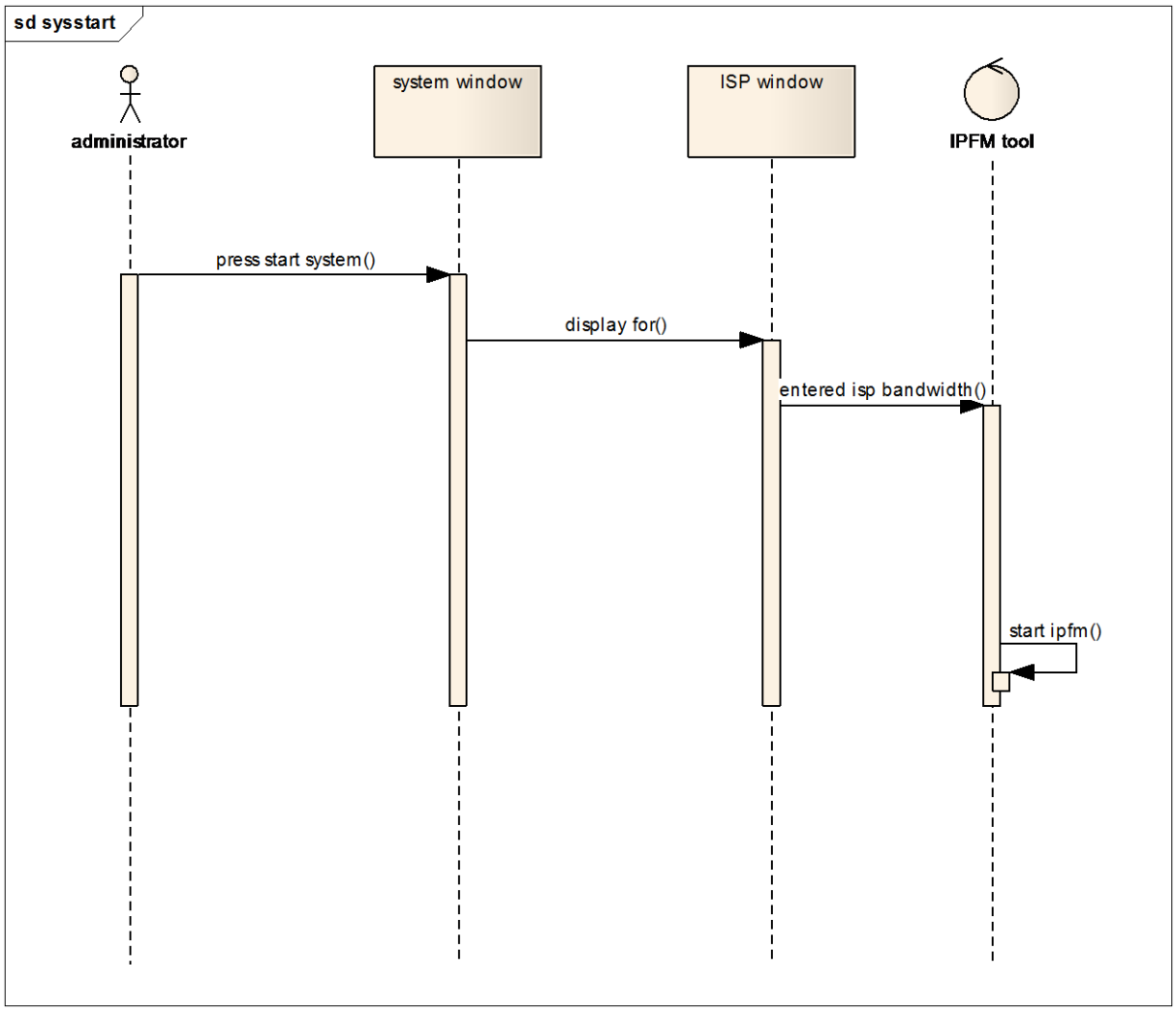


Figure 4.6: Start system

In this sequence will display action happens when the administrator will press start system button on system window, the system will display ISP window then administrator will be entered ISP quota (bandwidth) then the IPFM (tool of monitoring) will be start to monitor the network.

The following figures 4.7 show the sequence of monitoring system use case, which shows the actions,happens to monitoring the network and analysis the data that is collected form monitoring tool:

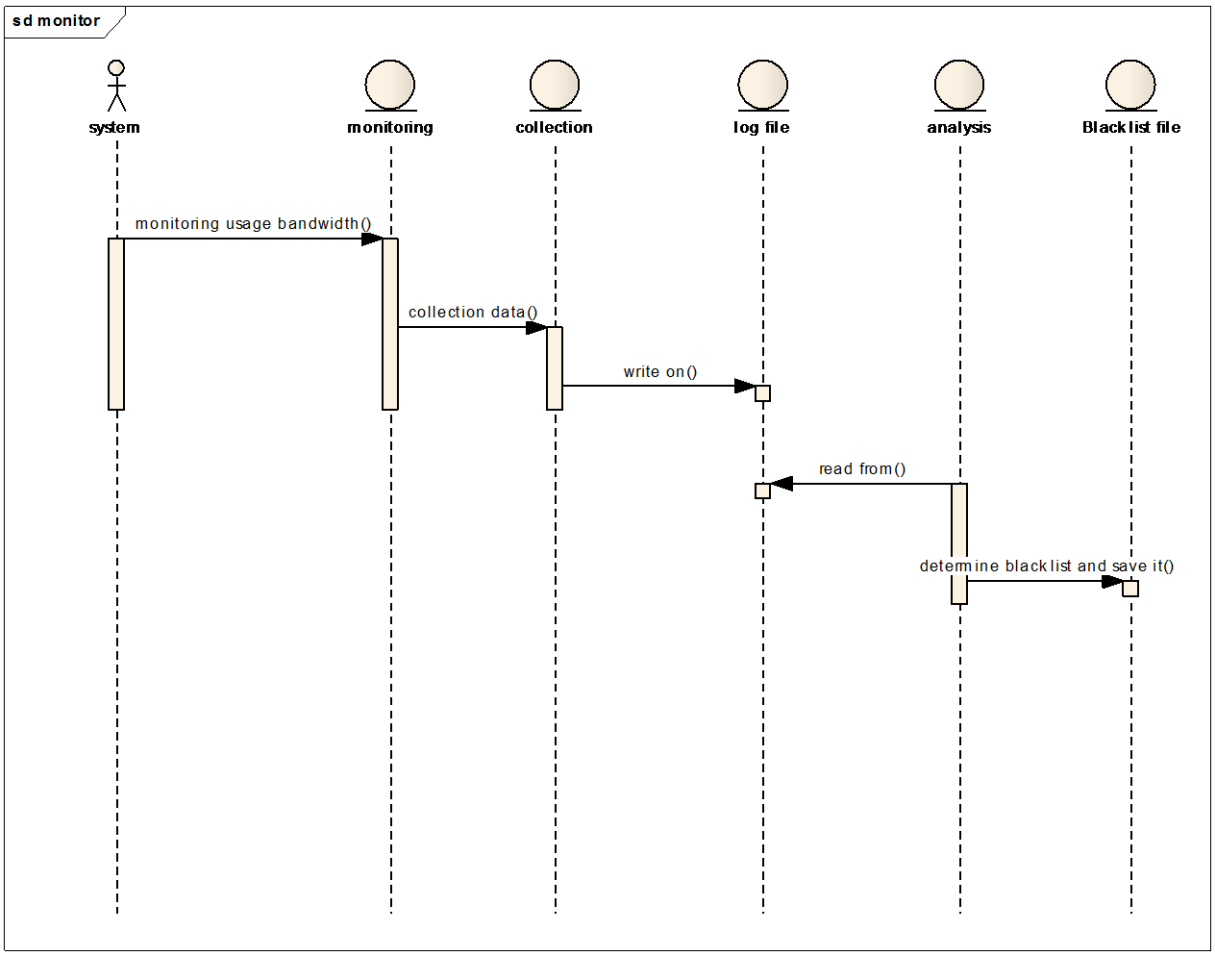


Figure 4.7: Monitoring system

In this sequence the system will start IPFM to monitor the network and collection data, write it in log file then read this data to analysis it, and then if there are heavy users must save them in black list file.

The following figures 4.8 show the sequence of Restriction use case, which shows the action of restriction process in the system:

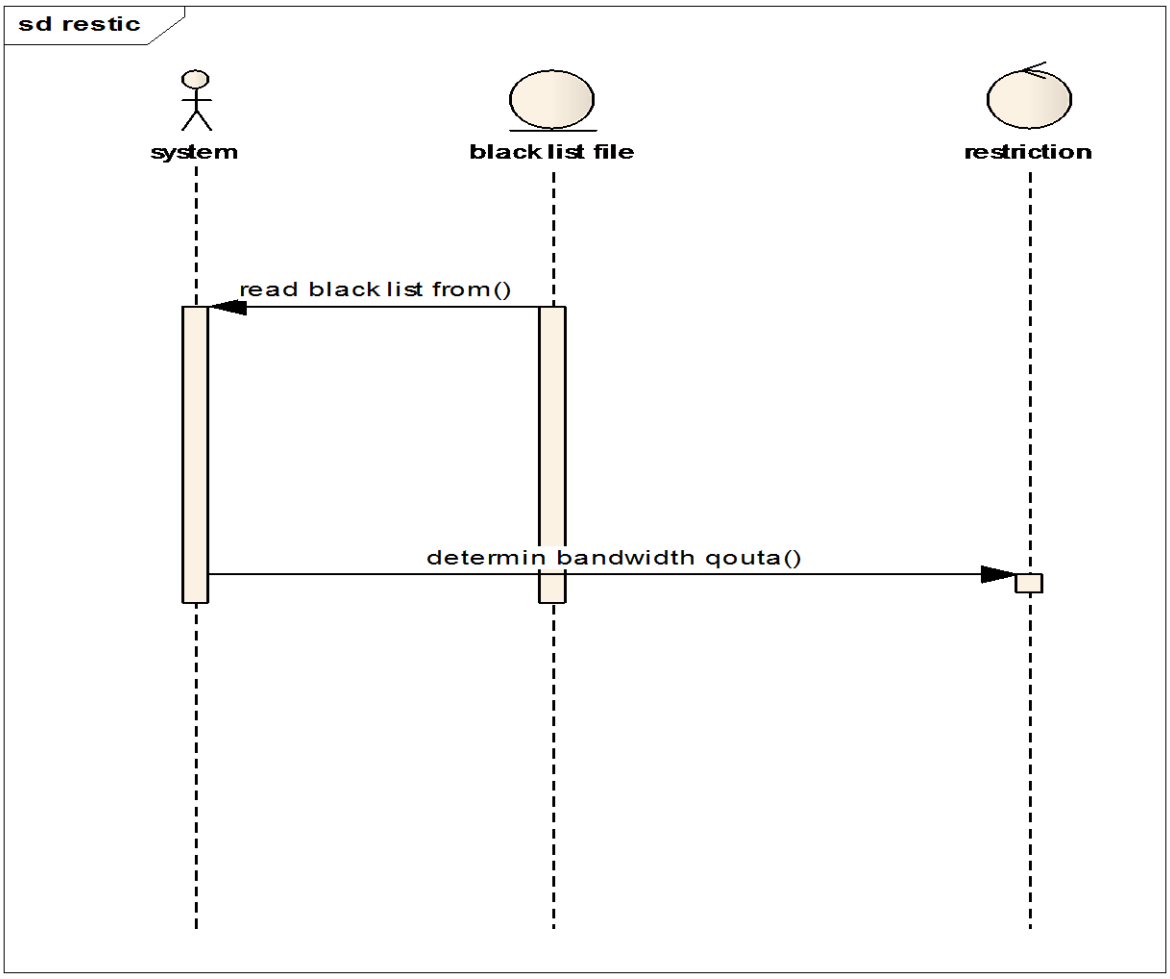


Figure 4.8: Restriction process in the system

In this sequence the system will read the black list from black list file then determine the quota (bandwidth) and restrict them.

The following figures 4.9 show the sequence of stop systemuse case, which show action happen when the administrator wants to stop system:

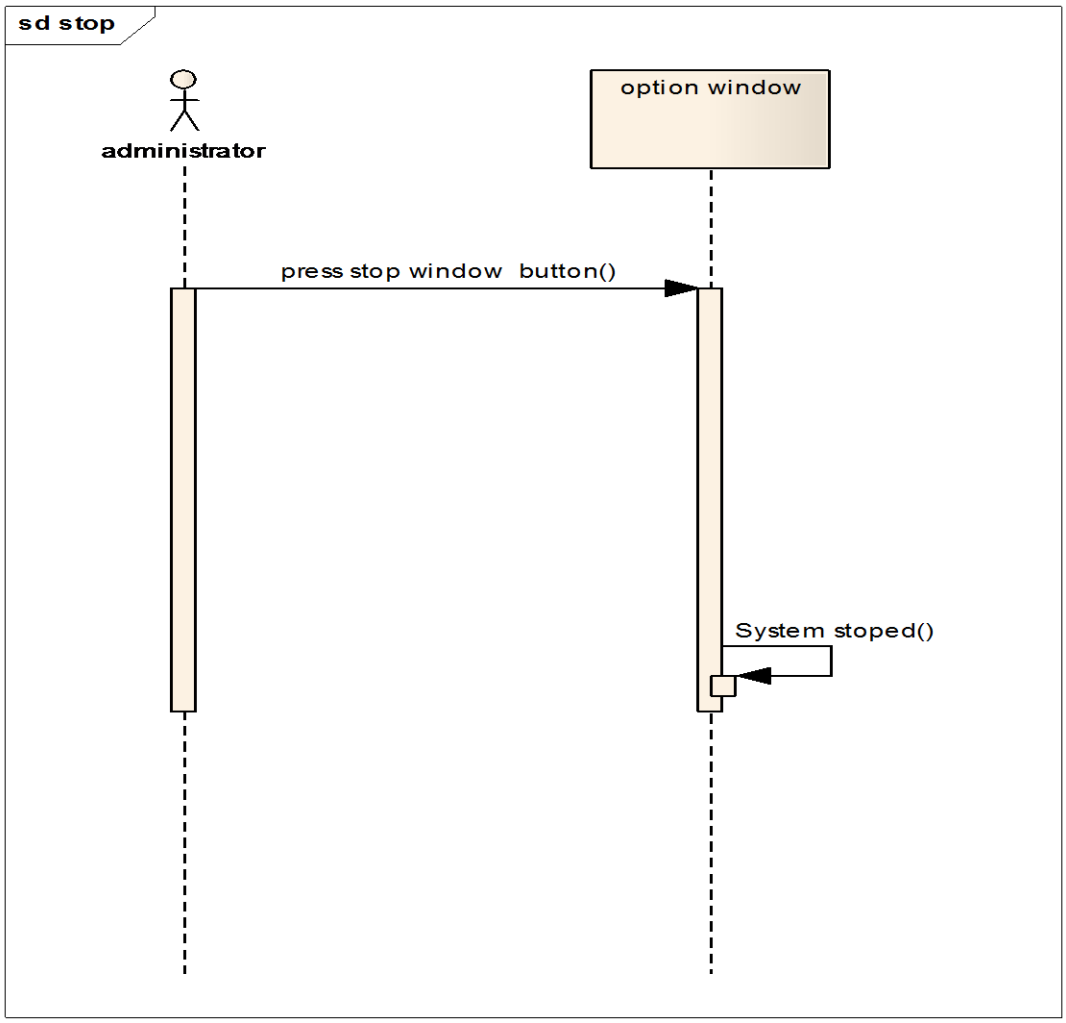


Figure 4.9: Stop system

In this sequence the administrator will press stop system button on option window, the system will be stop all actions (functions) in it.

The following figures 4.10 show the sequence of view reportuse case, which show action to view report about heavy users in the system:

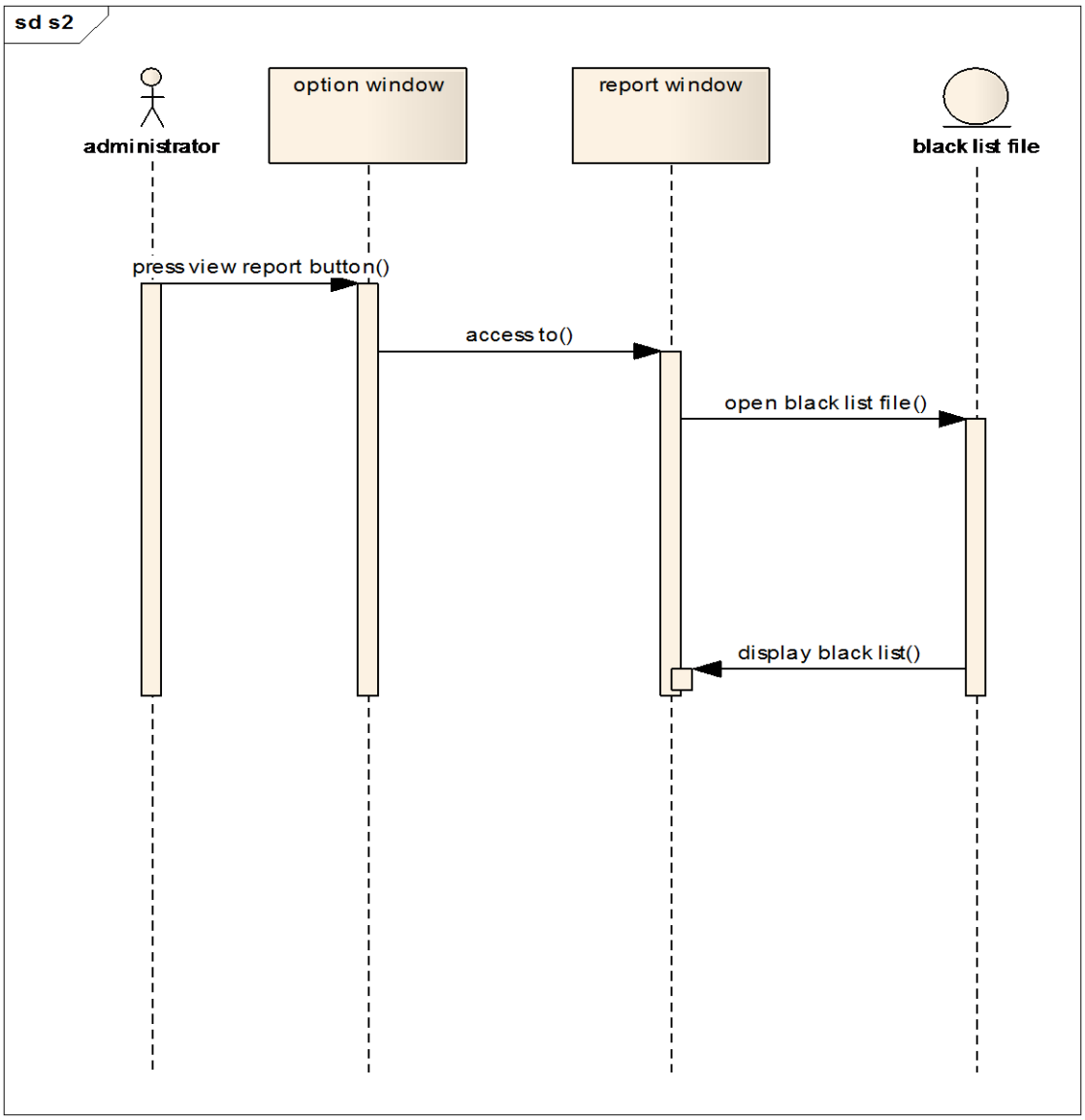


Figure 4.10: View report

In this sequence the administrator view report button on option window then display report window the system will open the blacklist file then display it in report window.

4.2.2.4. THE ACTIVITY DIAGRAM

The following figures 4.11 show the activity diagram for system:

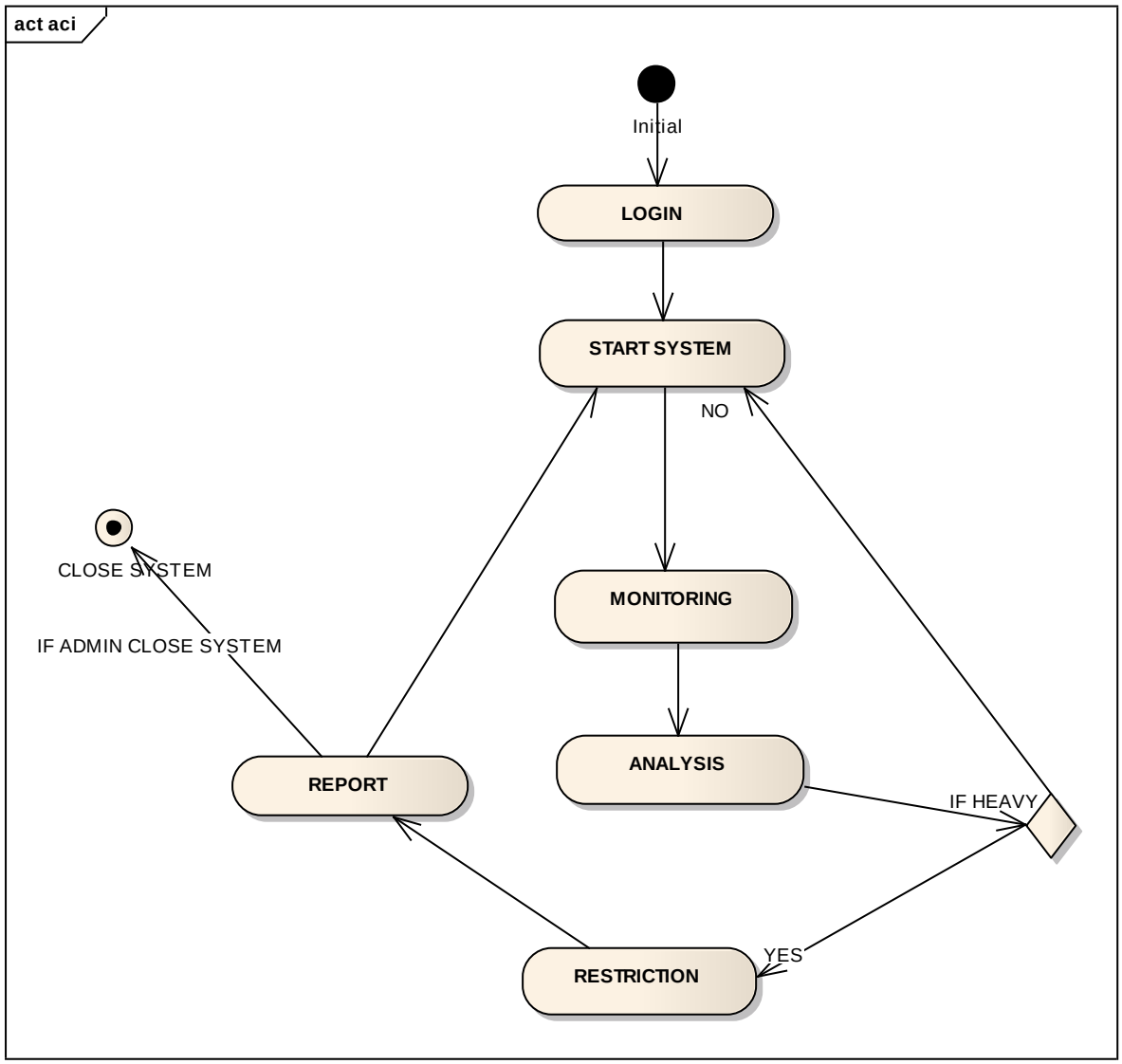


Figure 4.11: activity diagram.

System activity

The administrator login to system and start it then the system will start all function automatically monitoring, analysis and restriction if there are heavy users, also the administrator can stop the system if he/she want.

4.2.2.5. THE DEPLOYMENT DIAGRAM:

The following figures 4.12 show the deployment diagram for system:

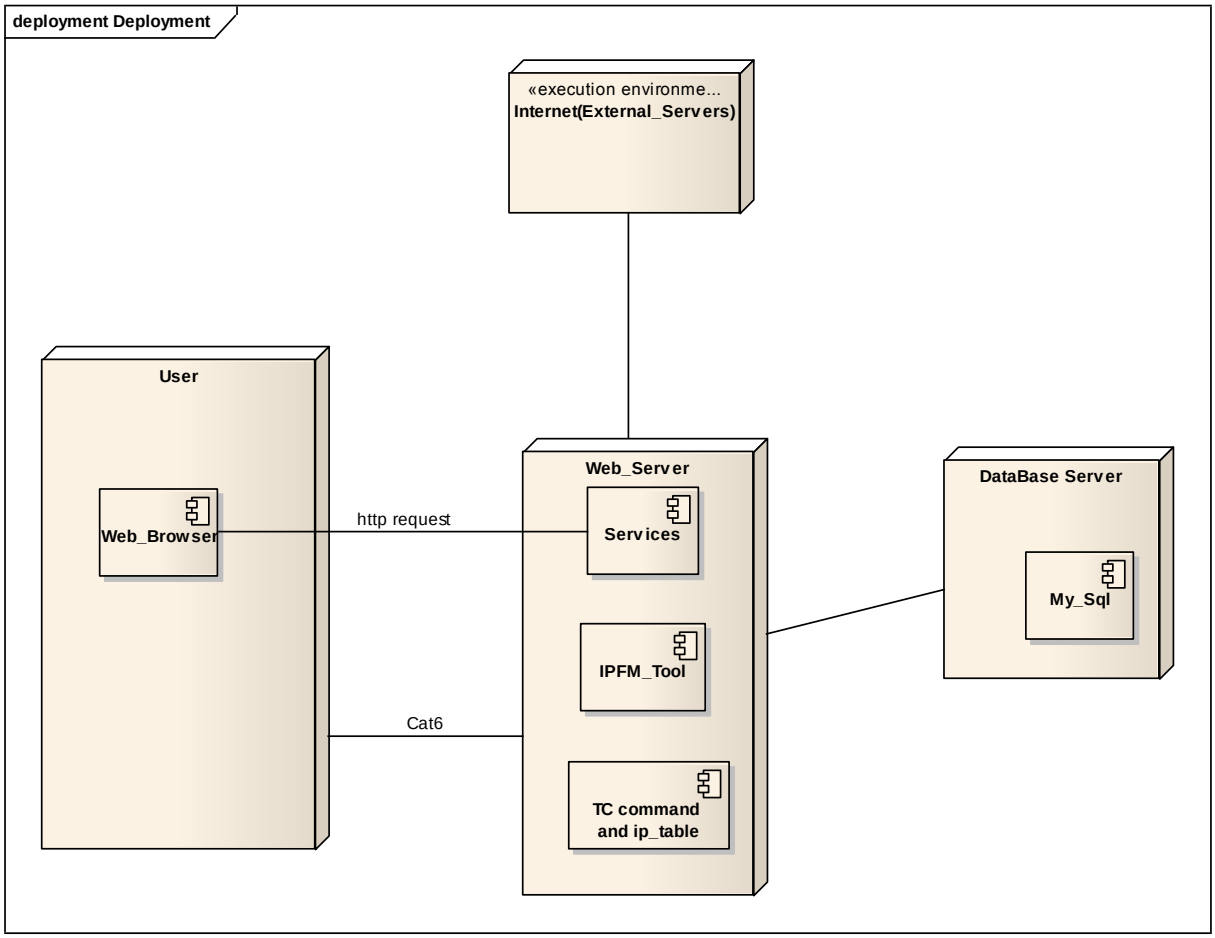


Figure 4.12: deployment diagram

System Deployment

The deployment show the software using in the system ,first the users use web browser for requesting service from server .in monitoring the system use IPFM tool ,after monitoring system save the result of monitoring in data base to use in the analysis step and control the users using TC command and IP table to limitation users bandwidth.

4.3. Summary

This chapter first explain the ENTERPRISE ARCHITECTthat we are using to analysis the system and them show UML diagram for the system to analysis and explain system, then show sequence diagram for all function in the system and show activity diagram for system then show the deployment diagram for the system and explain each of its.

CHAPTER 5

SYSTEM IMPLEMENTATION

5.1. Introduction

This chapter discusses the implementation of the project, testing and the results of the project.

5.2. Implementation

5.2.1. System description

System has the following specification.

5.2.1.1. Server

- 4 GB of ram
- NICs (10/100 Mb)
- UBUNTU SERVER 14.04
- IPFM monitoring tool

5.2.1.2. Transmission Media

- Twisted pair cat 6
- Layer 2 switch 24 ports

5.2.1.3. Clients

- 10 PCs [lap 13]
- Windows 8 Windows 7 OS and Ubuntu OS

5.3. Network Configuration

A small Subnet inside university LAN was created and the server connected to the university LAN.

University LAN has Network ID (172.27.129.0), all clients in The Subnet connect throw the switch (layer 2 switch 24 port) to server with interface (**eth0**) and IP address (172.27.129.153).

All connections between our server to switch and from clients to the switch with cat 6 twisted pair cable. The DHCP server (which installed in system server) gives IP address to clients.

5.4. Server Configuration

We install Ubuntu server 14.04 in the server and the system installed in the server to monitoring, analysis and control users in the network. This system have two modes : first online system using terminal this one works in real time (very short time) and offline system is GUI system works for long time (1 hour) is not in real time. the following figures show the Sequence of systems and the interface of systems.

5.4.1 ONLINE SYSTEM (TERMINAL)

After run the system it ask the admin to enter the total bandwidth from isp in kilobytes.

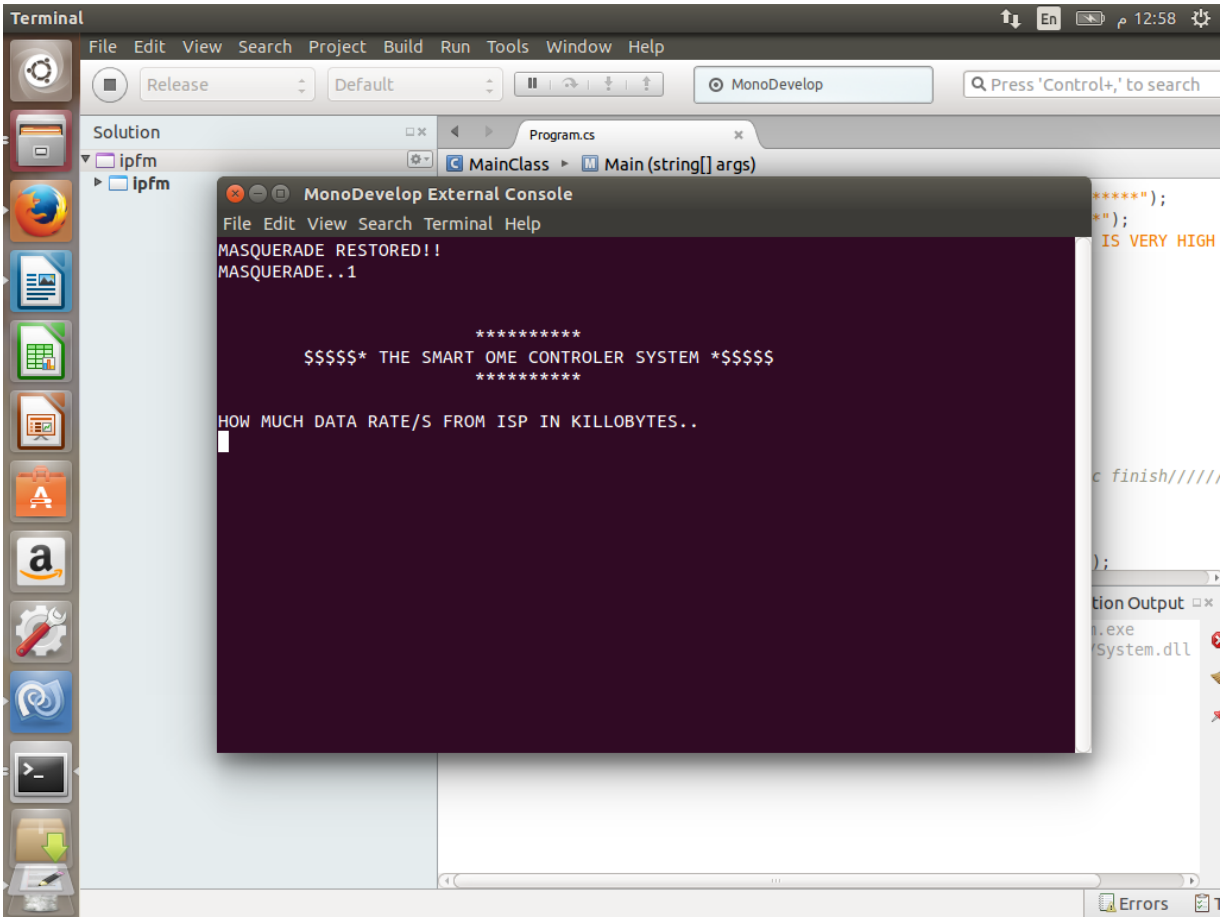


figure 5.1:Enter total bandwidth from isp

then admin enter the bandwidth from isp and the system calculates the allow in 1 minute, after that start the ipfm monitoring tool

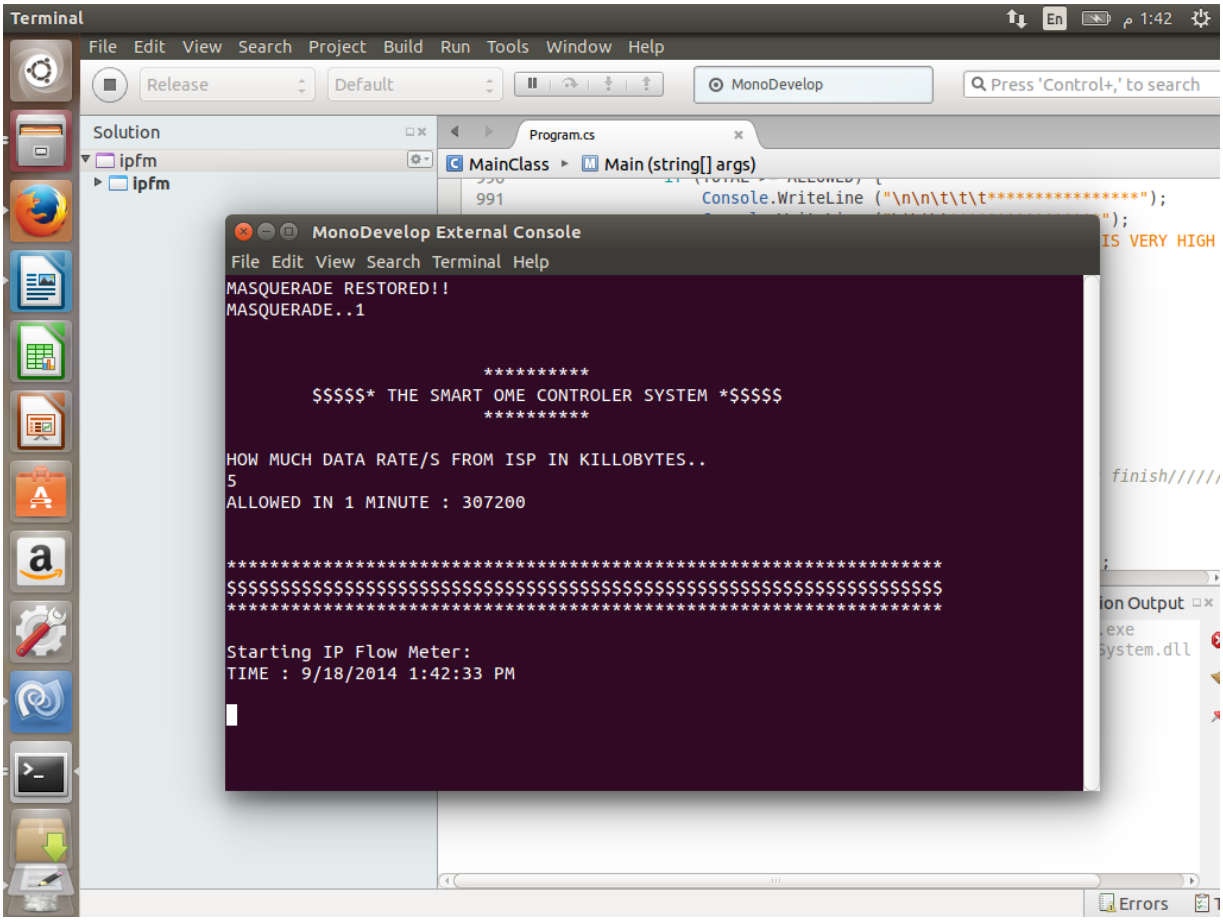


figure 5.2: Calculates the allow bandwidth and start ipfm

After the ipfm write its log file the system read it to calculate the total load of the network and determines if the network is over utlization or not .If is over utlization it read the log file again to finds the black list (the heavy usage users), it do that by comparing their downloads bytes. Then restrict the speed of black list users to specific qouta which it calculates it by divid the total bandwidth from ISP on the number of active users.

In figure 5.3 it finds the 172.27.130.225 is the most heavy usage user and then restrict it.

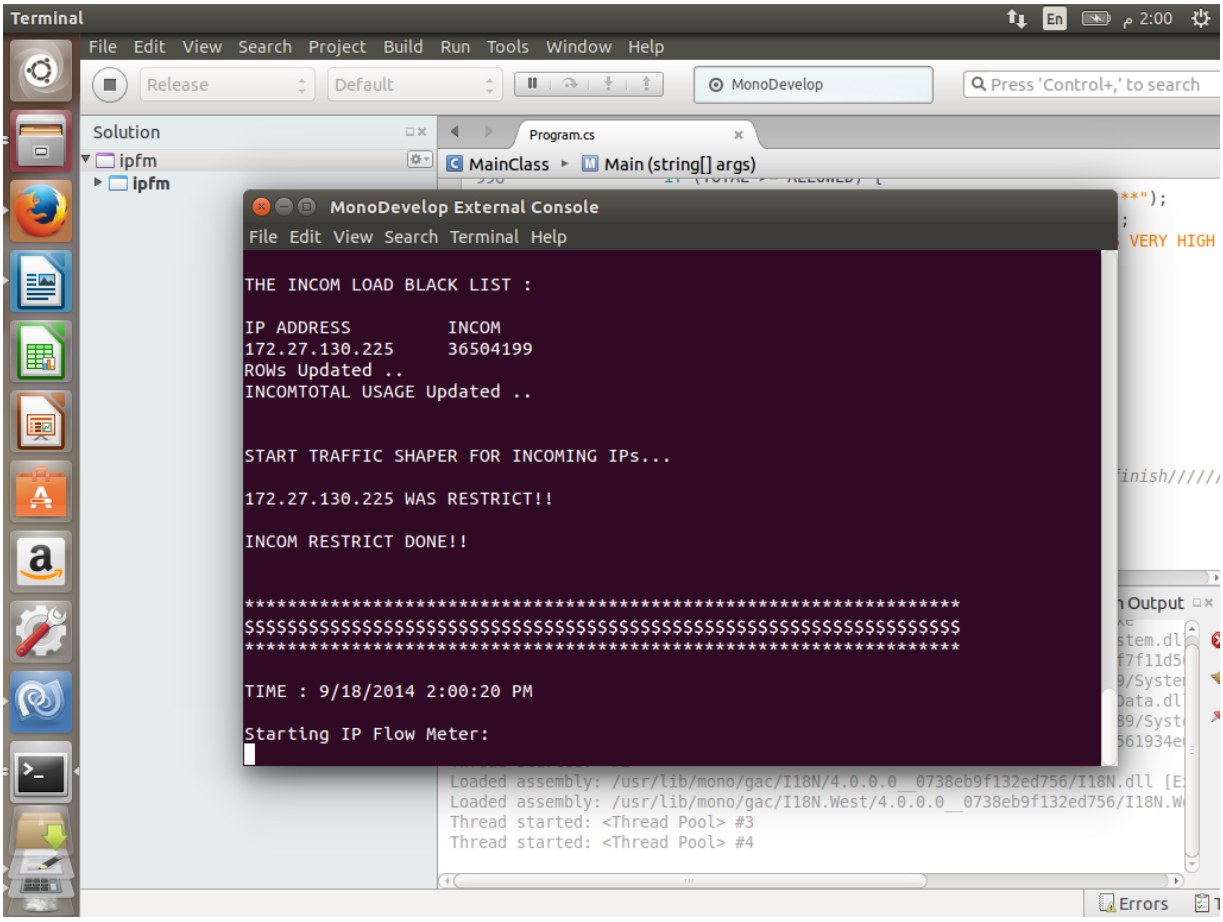


Figure 5.3: Find black list users and Restrict them

The next figure (figure 5.4) shows the quota which the system restricted the 172.27.130.225 to it.

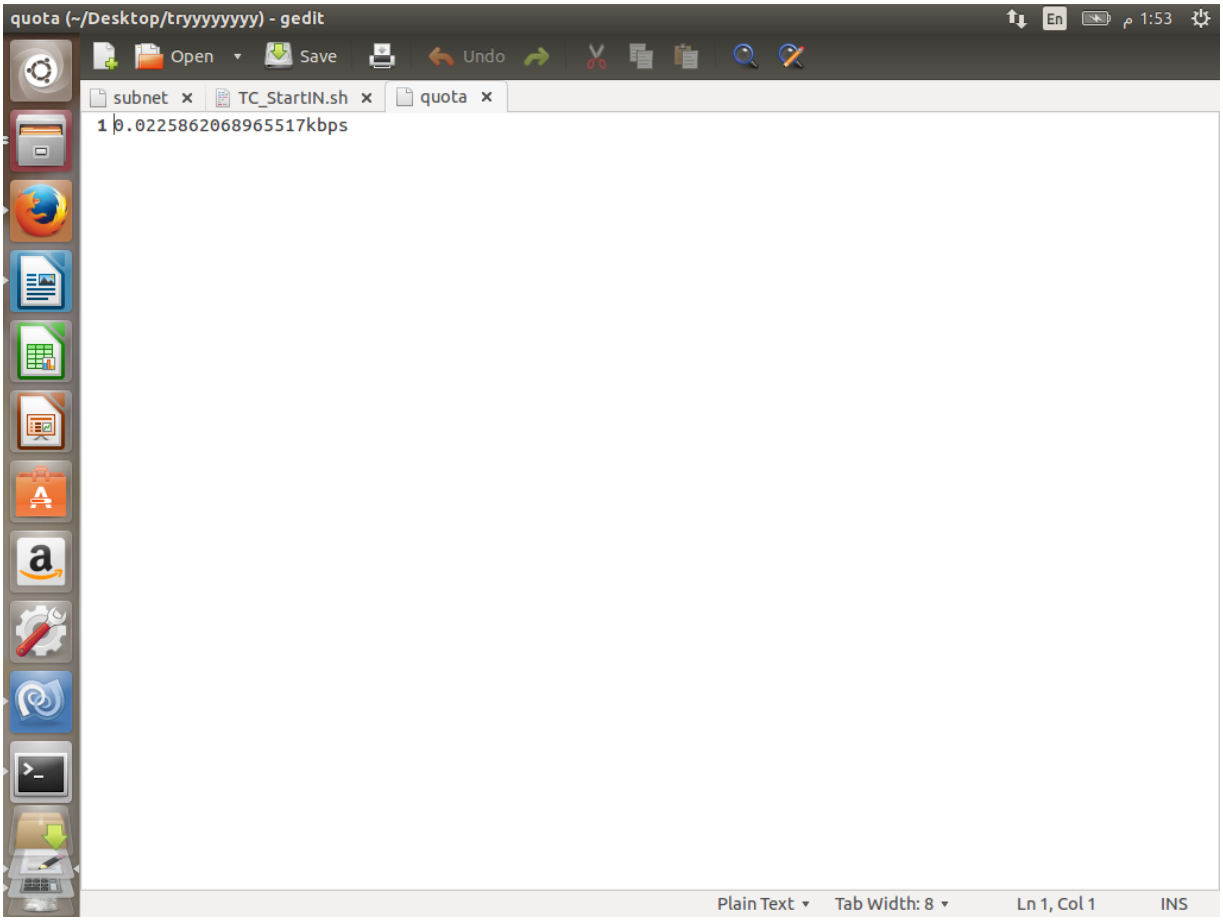


Figure 5.4: Restriction quota

The system still workonglik that until it finds the total load of the network is under utlization and here it stop restriction and allow users to work freely, finally it continuos its work (monitoring, analayzing and controlling).

5.4.1.1. analyzingnetwok status

In this section the status of netwok before the system and after it will be compared. The comparing will be done based of above black list that is mean the comparing will be done on the usage of 172.27.130.225ip address before and after system implementation because of challenges which faced the system implementation.

5.4.1.1.1. Before sysem implementation

To understand and the system work be clear take this for example :

if the total bandwidth from ISP = 5kBps, then the total usage in 5 minutes must be 1536000 kbytes.

The following table show the usage of 172.27.130.225 during the time (5 minutes):

IP	1 MIN	2 MIN	3 MIN	4 MIN	5 MIN	Total(5 minutes)
172.27.130.225	16224	1470594	19729014	512005	15362911	37090748

The above table show that the total usage of the ip is more than the total usage must be in 5 minutes, that is mean the network needed to be monitored and controlled.

5.4.1.1.2. After system implementation

here the system will be monitor and control the network usage, its controlling by restrict speed (bandwidth).

The following table show the usage of 172.27.130.225 during the time (5 minutes) after system implementation :

IP/USAGE	I min speed	I min restrict	2 min speed	2 min restrict	3 min speed	3 min restrict	4 min speed	4 min restrict	5 min speed	5 min restrict	Total
172.27.130.225	13mbps	0.153kbps	o.153kbps	no_restriction	10mbps	0.153kbps	0.153kbps	no_restriction	4mbps	0.153kbps	_
Usage	798720 kB	921.6kB	921.6kB		614400 kB	921.6kB	921.6kB		245760 kB	921.6kB	4608 kB

The above table show clearly the system impact on network usage, in the table as be explained on above sections the restriction qouta calculated based on the number of active users that maens it changes with number of active users changing. Also, the implementation done based on one ip address but keep in mind there large number of ips in this network which impacted on the system implementation and restriction qouta and the system can not manage those users because the system server is not a gateway for the network, this is on of challenges faced this system implementation.

5.4.2. OFFLINE System (GUI)

5.4.2.1. LOGIN

The following figures [5.1] show login to system:

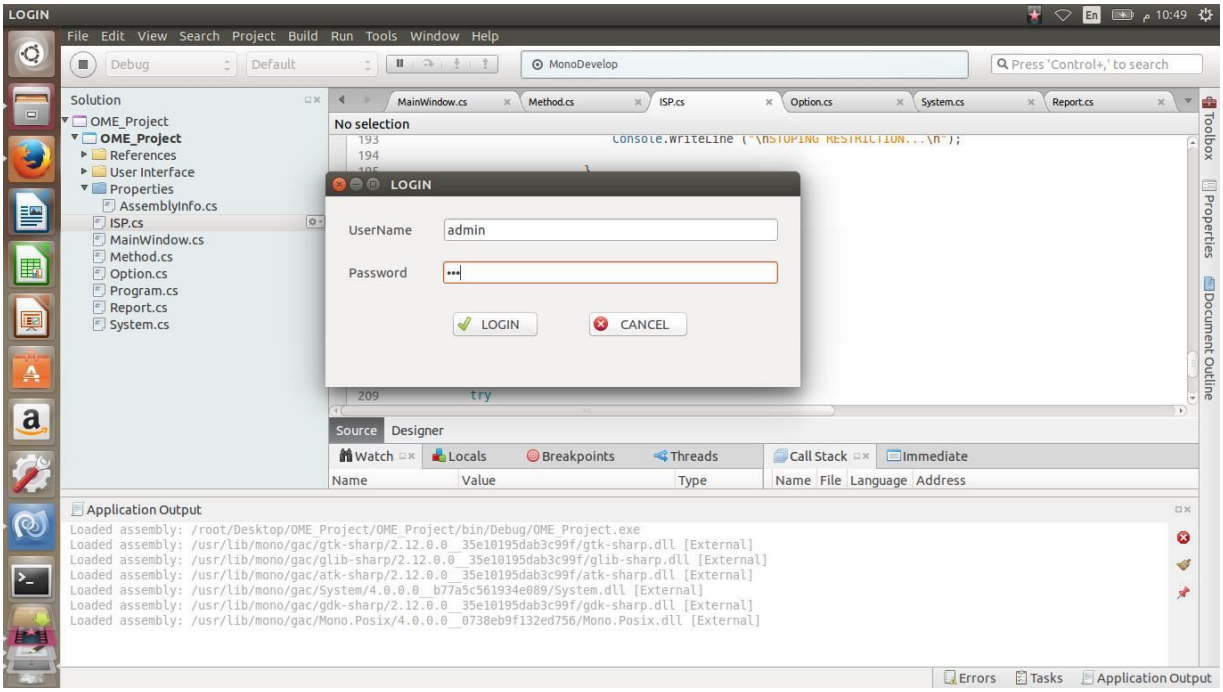


Figure 5.5: login to system

5.4.2.1.1. LOGIN Button

Press this button to login to system, the administrator must enter user name and password the system checked it, if it write data the system will display system window.

5.4.2.1.2. CANCEL Button

If press this button it close application.

5.4.2.2. The main system window

The following figures [5.2] show system window:

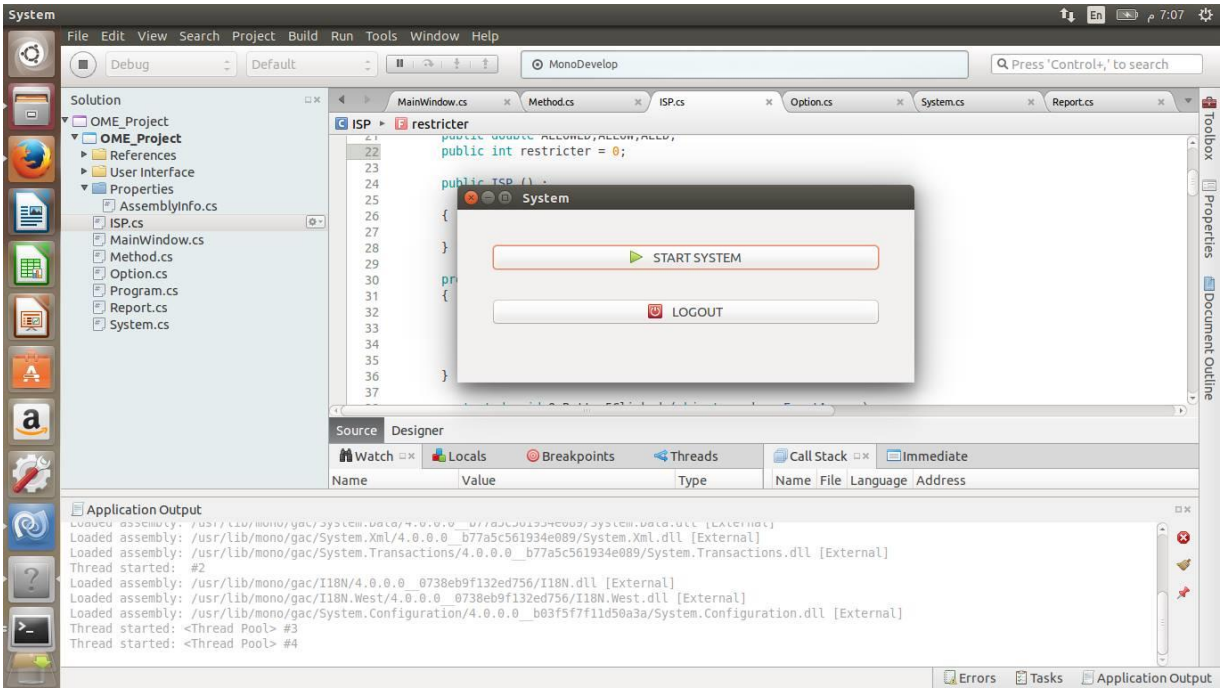


Figure 5.6: system window

5.4.2.2.1. START SYSTEM Button

On click on this button it will display ISP window.

5.4.2.2.2. LOGOUT Button

On click on this button it will display login window.

5.4.2.3. ISP window

The following figures [5.3] show window to enter ISP bandwidth to system:

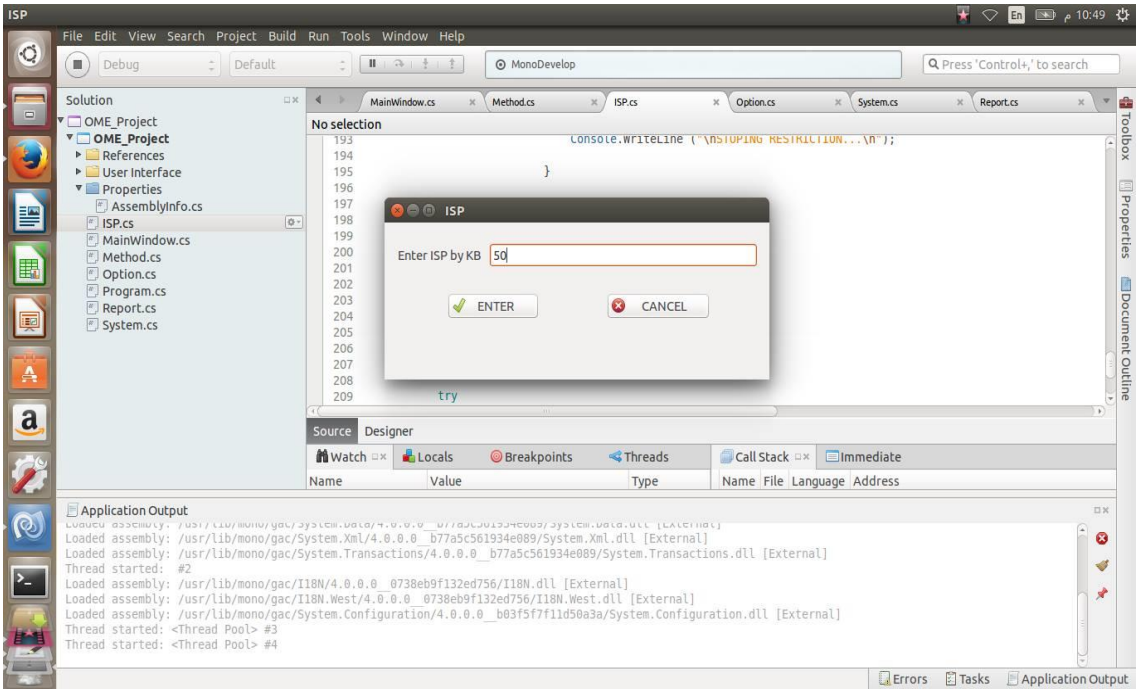


Figure 5.7: ISP window.

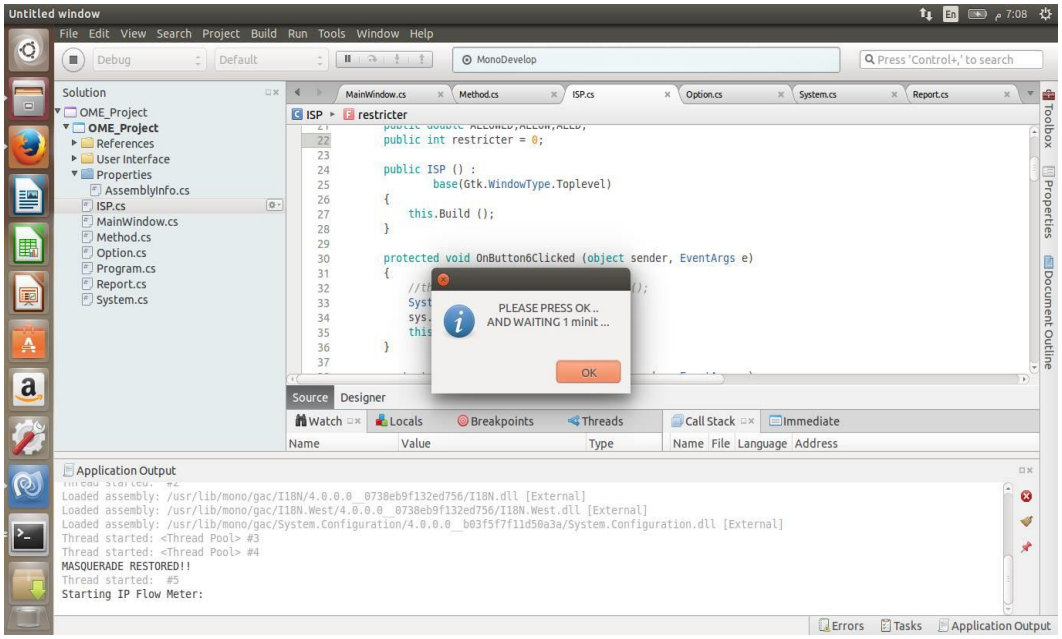
5.4.2.3.1. ENTERButton

Enter ISP quota then press this button to display the show below in figure 5.4.

5.4.2.3.1.1. Waite Message

Press ok button to start system as the following figures [5.4] that show witting massage to tell administrator to Waite some time (one minute):

Figure 5.8: wait window



5.4.2.3.2. Cancel Button

On press this button will be back to system window.

5.4.2.4. Option window

The following figures [5.5] show option window:

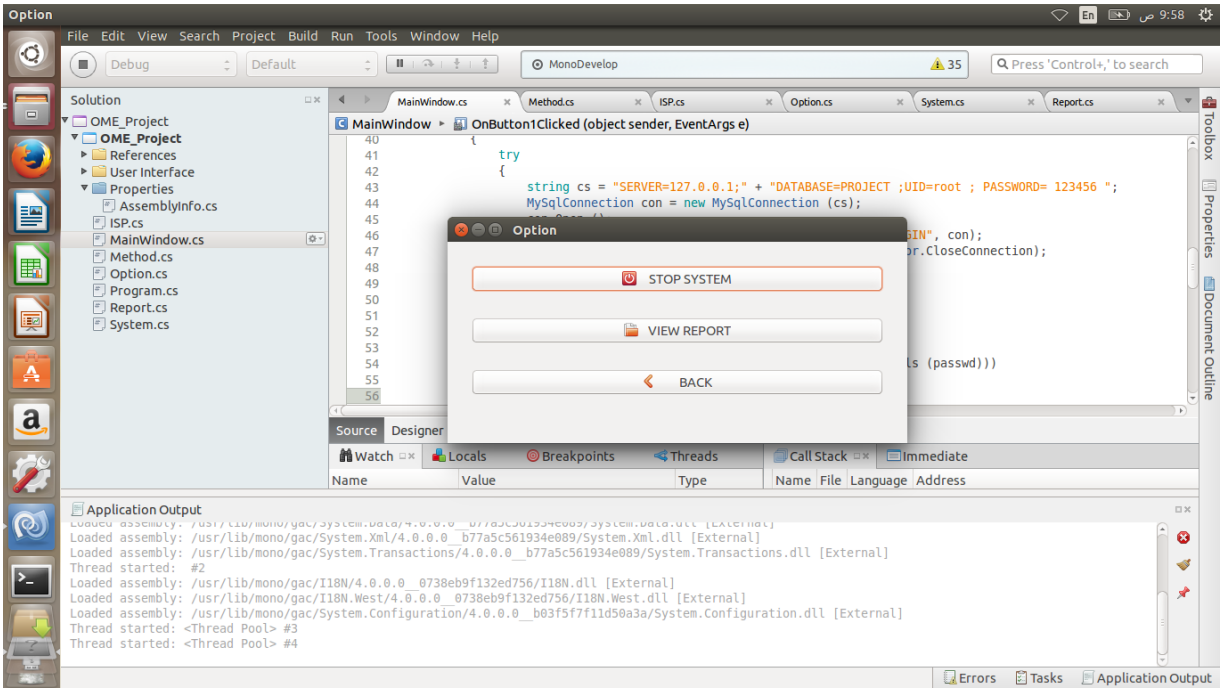


Figure 5.9: option window

5.4.2.4.1. STOP SYSTEM Button

This button will stop all system.

5.4.2.4.2. VIEW REPORT Button

On click this button will display report window.

5.4.2.4.3. Back Button

On click this button will display option window.

5.4.2.5. Report window

The following figures [5.6] show report about heavy user in the network:

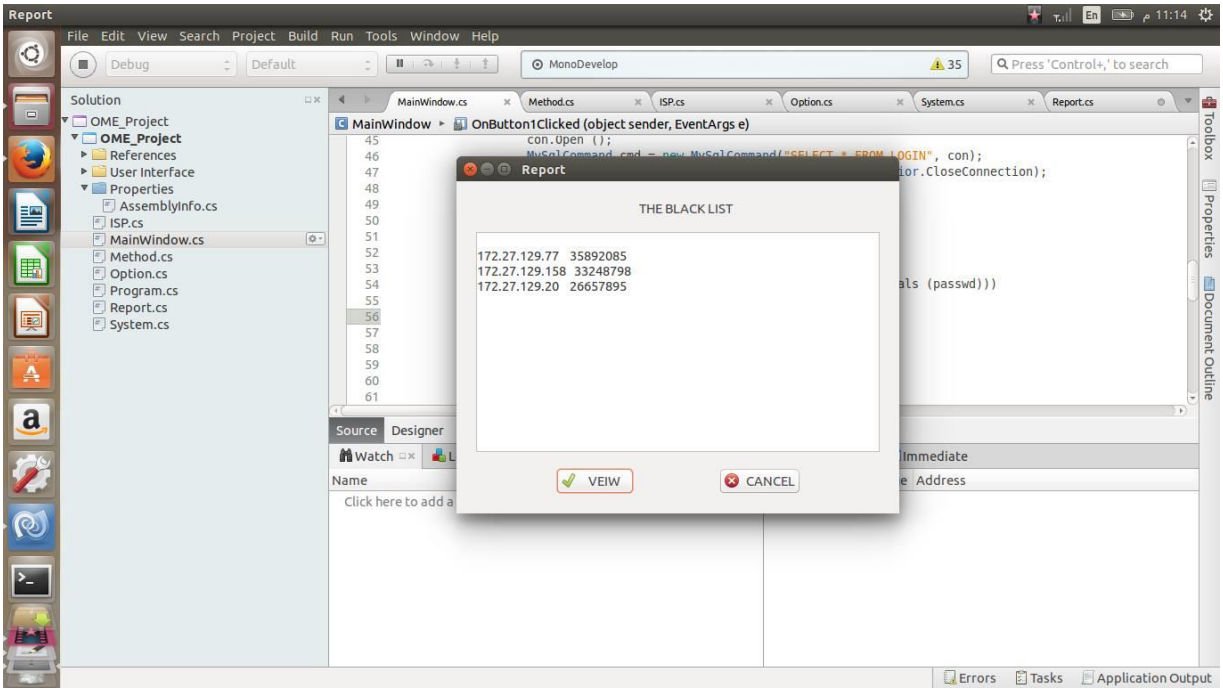


Figure 5.10: report window

5.4.2.5.1. VIEWButton

On press this button it will view report of back list.

5.4.2.5.2. CANCEL Button

On press this button it will display option window.

5.4.2.6. THE BLACK LIST IN DATA BASE

The following figures [5.7] show table in data base about heavy user for a long time:

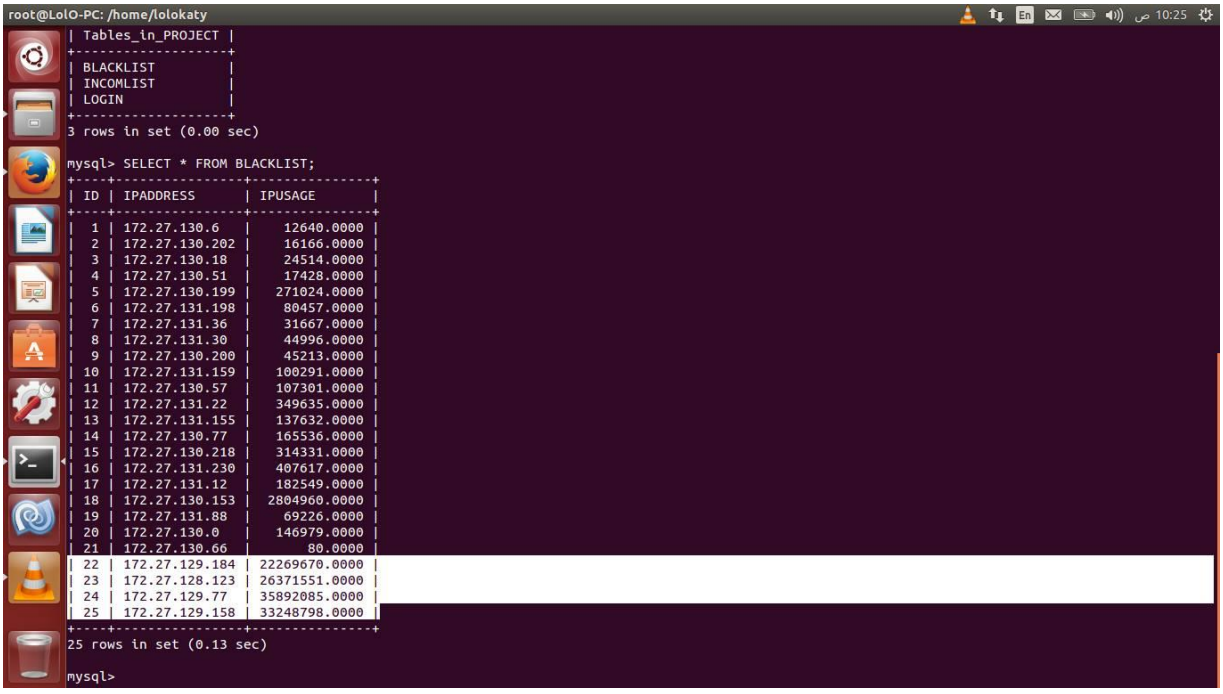


Figure 5.11: table of black list in data base

5.4.2.7. The implementation of system using IFTOP

The following figures [5.8] show IP address of users before apply system:

Figure 5.12: IP address of users before apply system

The following figures [5.9] show IP addresses of users after apply system:

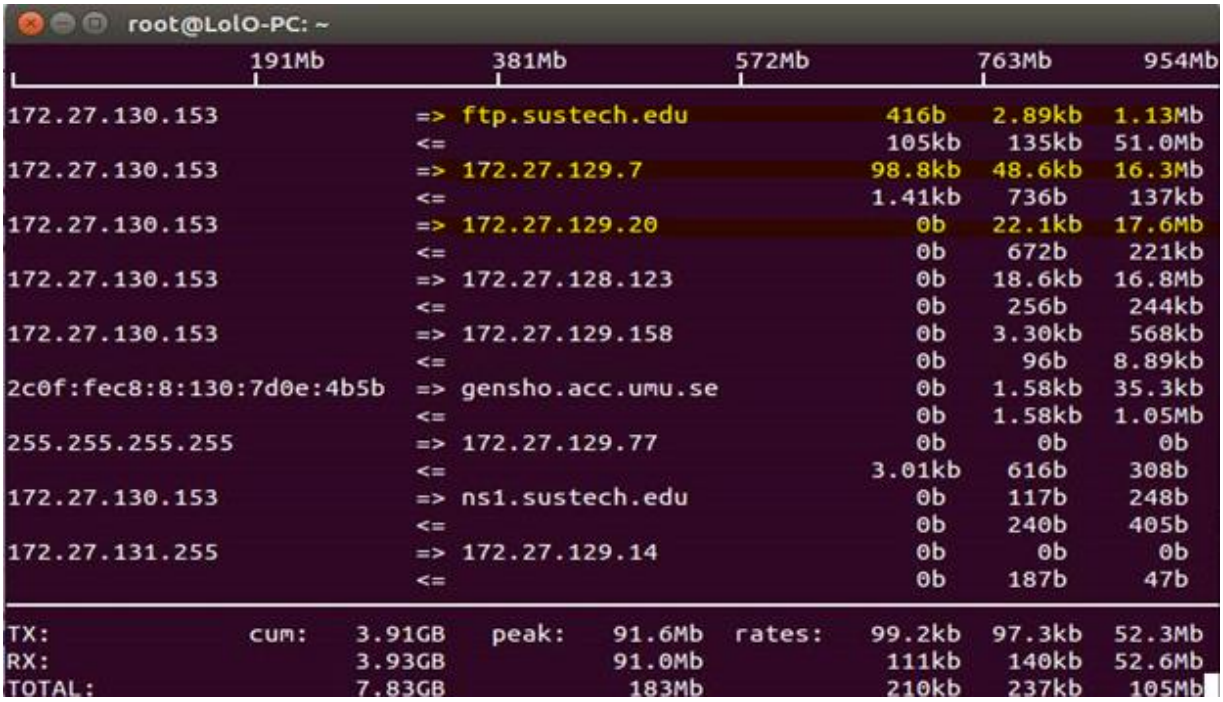


Figure 5.13: IP address of users after apply system

Observation on figure [5.8] the IP addresses (172.27.127.158), (172.27.129.77), (172.27.129.20) there bandwidth is higher than allowed bandwidth (by Mb/s) but on figure [5.9] that is IP addresses is controlled by system and there bandwidths is reduced (by Kb/s) after applying the system.

5.5. Summary

This chapter shows the implementation of the project system with interfaces explain, also is shows the result of the implementation of the system.

CHAPTER 6

CONCLUSION AND RECOMMENDATION

6.1. Conclusion

In this effort, a usage-based monitoring and control system has been implemented, tested and validated. Furthermore, according to the testbed (LAB 13) It works according to the expected objectives (identifies the heavy users and punished them in very short time (1 minute).

Moreover, this implementation allows the normal users to use the available bandwidth fairly, while at the same time saves the cost of upgrading the link by fully utilizing the available bandwidth.

When you compare this project with previous studies that have been mentioned in the second chapter, we found that the distinguish feature of the current one is to control the bandwidth according to the usage of the user in very short time which will be acceptable to university campus environment, while most of the studies did not mention the control of the user's process based on very short time (1 minute. Therefore this project is to monitor the network and analysed to find users who make over use for the network and then be punished by reducing bandwidth for them. The system has many benefits, which include the availability of QOS between users, and manager of organization need not to increase the bandwidth every time because of the bad use of users and other benefits. Also the good side effect of this implementation is that it can help the users to adapt themselves automatically by reducing their offered traffic in self based manner.

6.2.Recommendations

- By definition, the transfer rate is measured in ***bps***, reducing the control period will be very effective, although it can be implemented in our system (by controlling the usage in real time (go near by one second (the ideal situation))
  Rather than 1 minute, but an effort is required to measure the performance and practicality of the system.
- Modify and customize this project to help them in avoiding the overconsumption of the monthly/weekly quota provided by the ISPs such as ZAIN,MTN and SUDANI to give same benefit that is save customer money and provide good service to him.
- Monitoring the network for a long time to know the users that always make a problem in the network by using high bandwidth and accordingly, record their usage as history so that they will be given more/less punishment according to their history.
- Enhance the system to send Warningmassage “the extreme use of bandwidth will be exposed to punishment” before restricting the users. The outcomes of this warning message helps in making the users control themselves in self-healing.
- Add priorities to system like administration users, teachers and students so that punishes people with lower priority.
- Develop android application for this system with some updated to be available to regular users to monitoring and managing their own internet packets.

References

[1] A study of Bandwidth Management in Computer Networks DevajitMahantaMajidul Ahmed, UtpalJyoti Bora

[2] BITTORRENT STILL DOMINATES GLOBAL INTERNET TRAFFICBY ERNESTO ON OCTOBER 26, 2010

[3] V. Ahuja, \Routing and Flow Control in Systems Network Architecture," IBM Systems Journal, Vol. 18, No. 2, 1979, pp. 298 – 314.

[4] Multi-layer network monitoring and analysis

[5] A Summary of Network Traffic Monitoring and Analysis Techniques, Alisha Cecil, acecil19@yahoo.com

[6] Usage Control: A Vision for Next Generation Access Control, Ravi Sandhu, Jaehong Park, 2003, pp 17-31

[7] Congestion Avoidance in Computer Network with a Connectionless Network Layer, 1998.

[8] High-Speed Network Monitoring and Analysis, 2005

[9] A QOS-BASED BANDWIDTH MANAGEMENT SCHEME IN HETEROGENEOUS WIRELESS NETWORKS, 2007.

[10] Quality of Service Control Schemes for Two Stage Ethernet Passive Optical Access Networks, 2005.

[11] Quality-of-Service Routing in Ad-Hoc Networks Using OLSR, December 2002.

[12] Quality of Service for IP Voice and Video, 2007

[13] Local Area Network Traffic Characteristics, with Implications for Broadband Network Congestion Management, 1997.

[14] Programmable Host-Network Traffic Management, 2013.

[15] A study of Bandwidth Management in Computer Networks.

[16] Differentiated Congestion Management of Data Traffic for Data Center Ethernet, 2011.

[17] A Scalable Architecture for Network Traffic Monitoring and Analysis Using Free Open Source Software, 2009.

[18] Real-time update of access control policies, December 2003.

[19] On the Automated Analysis of Safety in Usage Control: a New Decidability Result.

[20] Usage Parameter Control Studies in an ATM Network Model, Box 118, S-221 00 LUND Sweden.

[21] Studies of Dynamic Bandwidth Allocation for Real-Time VBR Video Applications.

[22] A Survey of Network Traffic Monitoring and Analysis Tools

Chakchai So-In, so-in@ieee.org.

[23]http://www.sparxsystems.com/products/ea/index.html 8/7/2014 12:40 Pm

[24] http://searchenterpriselinux.techtarget.com/definition/iptables 20/8/2014 8:53 am

[25] C:\Users\mnasik\Desktop\Last Research\Best Practices in Core Network Capacity Planning - Cisco.html 2/6/2014 9:30 am

[26] A study of Bandwidth Management in Computer Networks