Bandwidth Management Using IP Traffic Analysis:

A Case Study of the Ahmadu Bello University Zaria.

BY

Adedokun Emmanuel Adewale

FEBRUARY, 2009

TITLE PAGE

Bandwidth Management Using IP Traffic Analysis:

A Case Study of the Ahmadu Bello University Zaria.

BY

Adedokun Emmanuel Adewale

MSC/ENG/03952/2006-07

A THESIS SUBMITTED TO THE DEPARTMENT OF ELECTRICAL ENGINEERING, AHMADU BELLO UNIVERSITY, ZARIA, IN PARTIAL FUFILMENT OF THE REQUIREMENTS FOR THE AWARD OF A MASTER OF SCIENCE (M.Sc) DEGREE IN ELECTRICAL ENGINEERING

FEBRUARY, 2009

DECLARATION

I, Adedokun Emmanuel Adewale, hereby declare that this thesis " Bandwidth Management using IP traffic Analysis(A case Study of Ahmadu Bello University Zaria), presented to the department of Electrical Engineering ,Ahmadu Bello University Zaria is the result of my research and it has never been presented in any form anywhere for the award of a higher degree.

All quotations and sources of information as seen in this thesis are specifically acknowledged by means of references

Adedokun E. Adewale **Date**

CERTIFICATION

This Thesis titled “Bandwidth Management using IP traffic Analysis (A case study of Ahmadu Bello University Zaria)” satisfies one of the requirements for the award of a Master of Science (M.Sc.) degree in Electronic and Telecommunications and has been approved by the department of Electrical Engineering, Ahmadu Bello University, Zaria for its contribution to Knowledge and literary presentation.

Dr. M.B. Muazu	**Date**
(Supervisor)	
Prof. B. Bajoga	**Date**
(Supervisor)	
Dean Postgraduate School	**Date**
Dr. M.B. Muazu	**Date**
(Head of Department)	

DEDICATION

to my wife, 'ronke,

for the priceless gift of peace, love, encouragement, friendship and support.

ACKNOWLEDGEMENTS

To God the Father, Son and the sweet Holy spirit for grace and favour.

My supervisor, Dr M.B Muazu who painstakingly walked me through this course, he is not just my teacher but a brother and a friend, am most grateful.

Thanks to Dr D.D Dajab for his encouragement. Thanks to Prof. B.G. Bajoga, Dr. B. A. Adegboye, Dr Boyi Jimoh, Engr. Akinsanmi and Engr. S. G. Garba.

I acknowledge the contributions of authors, so referred in the field of this research work.

Many thanks to my colleagues at work, Akin, Al-Hassan, Philip, Maryam, Adeolu, Keji, Chris and Tamon; for your contributions and support. Special thanks to Emike for being a good friend, colleague and aburo, very grateful for your help and friendship.

I appreciate the efforts of Dele, Henry, Lanre and Jide who handled a lot of my commitments during the period of this course.

I am grateful to the families of Dr & Dr (Mrs.) Olayinka, Dr & Dr (Mrs) Keshinro and Pastor and Mrs Adeshina.

I appreciate my lovely parents, Prof and Dr. (Mrs) Onaolapo, Mrs C.O. Adedokun

I also appreciate my wife and kids ('Ronke, Dara and Joba) Thanks and God bless

This work has proved to me again and again that God is Faithful!

Adedokun Adewale

Electrical Engineering Dept.

ABU Zaria

Table of Contents

TITLE PAGE ii

DECLARATION iii

CERTIFICATION iv

DEDICATION v

ACKNOWLEDGEMENTS vi

LIST OF FIGURES x

LIST OF TABLES xi

LIST OF SYMBOLS xii

ABSTRACT xiii

CHAPTER ONE 1

GENERAL INTRODUCTION 1

1.0 Introduction 1

1.2 Motivation 2

1.3 Problem Definition 2

1.4 Methodology 3

1.5 Thesis Outline. 5

CHAPTER TWO 6

THEORETICAL BACKGROUND 6

2.0 History of the Internet. 6

2.2 What Is an Internetwork 7

2.2.1 History of Internetworking 8

2.2.2 Internetworking Challenges 9

2.2.3 Internetworking Models 9

2.3 OSI Model 10

2.3.1 Characteristics of the OSI Layers 11

2.4 Transport Control Protocol/Internet Protocol (TCP/IP)Reference Model 11

2.5 Data Encapsulation 15

2.6 Internet Protocol (IP) 16

2.6.1 IP Addressing 17
2.6.2 IP Terminology 18
2.6.3 The Hierarchical IP Addressing Scheme 18
2.6.4 Network Addressing 19
2.6.5 Network Address Range: Class A 20
2.6.6 Network Address Range: Class B 20
2.6.7 Network Address Range: Class C 21
2.7 Bandwidth 21
2.8 The University current Network Setup 23
2.9 Detailed Configuration on the devices in the network 24
CHAPTER THREE. 26
METHODOLOGY 26
3.0 Proposed Model and Methodology 26
3.2 Installations and Configurations 27
3.2.1 Installing *ntop* from Source 27
3.2.2 Using *ntop* as a NetFlow Collector 29
3.2.3 Configure *ntop* NetFlow Plugin to receive NetFlow Data 29
3.2.4. Configure the NetFlow Probe to export Data to *ntop* 30
3.2.5 Configure *ntop* to Analyze the NetFlow Data 31
CHAPTER FOUR. 326
4.0 Sample of Results and Data collected 32
4.2 Analysis of Sample data 40
4.3 Additional configuration of ntop 42
4.4 Results obtained with the additional configuration 43
4.5 Deduction from Results of Data Analysis 44
4.6 Experimental solution 45

CHAPTER FIVE..... 48

RECOMMENDATIONS AND CONCLUSION 48

5.0 Introduction..... 48

5.1 Limitations..... 48

5.2. Conclusion 48

5.3 Suggestion for Further Work..... 49

Appendix A..... 53

LIST OF FIGURES

Fig.2.1	Different Network Technologies connected to Create Internetwork	7
Fig 2.2	Open System Interconnection model (OSI)	10
Fig 2.3	Sub Divisions of the OSI Layer	11
Fig 2.4	Data Encapsulation	16
Fig 2.5	IP Header	17
Fig 2.6	Three Classes of Networks	19
Fig 2.7	Schematic of University's current Network	23
Fig 3.1	Proposed Network Setup	26
Fig 4.1	Network Load Statistics (Test Data)	32
Fig 4.2	IP Protocol Distribution	33
Fig 4.3	Network Load Statistics (Live Data)	36
Fig 4.4	Remote to Local Network Traffic (Test Data)	40
Fig 4.5	Remote to Local Network Traffic (Live Data)	41
Fig 4.6	Summary of Network Traffic	44
Fig 4.7	Network Load Statistics (Experimental)	45
Fig A1	Network Load Statistics	70

LIST OF TABLES

Table 2.1	Three Classes of IP	19
Table 3.1	List of dependencies required by ntop	28
Table 4.1	Local Traffic (Test Data)	33
Table 4.2	Remote to Local Traffic	34
Table 4.4	IP Protocol Distribution (Live)	37
Table 4.5	Remote to Local Traffic	38
Table 4.6	Local to Remote Traffic	39
Table 4.7	Summary of Extract from Table 4.2(Test Data)	40
Table 4.8	Summary of Extract from Table 4.5(Live Data)	41
Table 4.9	Summary of Network Traffic	43
Table 4:10	Network Load Statistics (Live Data)	46
Table A1	Network Traffic (all Protocols)	52
Table A2	TCP/UDP Local Protocol Usage	57
Table A3	Last contracted Peers	66
Table A4	TCP/UDP Service/Protocol	67
Table A5	TCP/UDP Traffic on Ports	69
Table A6	TCP/UDP Recently Used Ports	69

LIST OF ABBREVATIONS

IP	Internet Protocol
HTTP	hypertext Transfer Protocol
FTP	File Transfer Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
LAN	Local Area Network
WAN	Wide Area Network
ISDN	Integrated Services Digital Network
OSI	Open System Interconnect
VSAT	Very Small Aperture Terminal
DVB	Digital Video Broadcast
SNMP	Simple Network Management Protocol
PDU	Protocol Data Unit
ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DNS	Domain Naming System
OSPF	Open Shortest Path First
FTP	File Transfer Protocol
TFTP	Trivial File Transfer Protocol
ARPANET	Advanced Research Projects Agency Network

ABSTRACT

This research studied the Internet Protocol traffic on the Ahmadu Bello University Zaria network in order to develop a strategic Bandwidth Management model. This work used a packet sniffer on the network for the investigation of different types of Internet Protocol (IP) traffic in order to device a bandwidth management strategy that will be based on the characteristics of the different types of protocols, their usage and the bandwidth consumed by each of these protocols. It was found that more than 75% of the total IP traffic on the university network are HTTP traffic while about 19% of the traffic were termed “other IP protocol”. A closer look at the constituents of the HTTP traffic revealed that internet mail sites like Yahoo, Google, MNS etc constitute not less that 50 % of the total HTTP traffic while online socialising sites like YouTube, Facebook etc also constitute a very significant amount of traffic on the network, other sites are Microsoft and various antivirus software sites . Based on the analysis of the data collected, it is suggested that access to less relevant sites to academic and research activities be restricted to off peak period (5pm -9am).It is also suggested that FTP server and Microsoft update servers be deployed on the network to ensure that software download and updates are restricted to local traffic. The official e-mail for the University should be accessed only during working hours while access to all internet free mail sites are denied.

CHAPTER ONE

GENERAL INTRODUCTION

1.0 Introduction

The internet was the result of some visionary thinking by people in the early 1960s that saw great potential value in allowing computers to share information on research and development in scientific and military fields(5). The internet is an innovation (or rather a series of innovations) that enables communication and transmission of data between computers at different locations. It is an extremely new scientific development.

The internet revolution has permanently and fundamentally altered the way in which Universities among others function. At a conceptual level, they remain (or ought to remain) what they have always been, but the way in which information is produced, shared and consumed is now so heavily intermediated by information technology that a university depends utterly on the quality of its connections to both the commodity Internet and the global research network(2)

Where a researcher resides or works is at one level, irrelevant: the same technology imperative applies, to the extent that the applications, the clients, the protocols and the operating systems are substantially the same. However, the available bandwidth is not the same. The regulatory and competitive environments, the availability of terrestrial infrastructure, the distance from the global network cores and the cost and quality of bandwidth are all very different. The consequence of weak infrastructure is a dramatic disparity in bandwidth provisioning between the developed and developing worlds. Remedying this by buying more bandwidth is usually out of the question. Hence, the challenge and research investigation on bandwidth management

1.2 Motivation

Towards the end of year 2005, the Ahmadu Bello University (henceforth referred to as the University) management entered into a bandwidth consortium agreement under the auspices of the Africa Virtual University (AVU) with five other universities in Nigeria; such as Obafemi Awolowo University (OAU) Ife, University of Jos, University of Portharcourt, Bayero University Kano (BUK) and University of Ibadan (UI) to acquire a 6.5mbps of bandwidth to improve on the 512kbps it had before the formation of the consortium. For more than 18 months after that, the bandwidth consumption of the University community was less than 25% of the purchased capacity. However in the past 12 months, a pattern of traffic congestion was noted on the University network especially during work hours (10am-3:30pm) even though less than 50% of the University community have access to the internet and it was found that during the periods of congestion, the University traffic is between 99% and 103%(due to burst capacity) of her purchased capacity (3). This work is an attempt to solve the traffic congestion by devising a bandwidth management strategy based on the analysis of the IP traffic on the network

This gets worsened with the current rate in the price of satellite bandwidth affected by the global financial crisis and inflation, which may obviously hinder the University management from being able to afford to buy more bandwidth for the next few years.

1.3 Problem Definition

Traffic congestion is as a result of bandwidth constraint, and the challenge for solution such that an average network user will have a fairly smooth browsing experience while on the University network.

What actually causes a slow internet connection or traffic congestion? Obviously, the capacity of a given connection is finite, so if too many people request information

simultaneously, then someone will have to wait. In an ideal world, organizations would simply order more bandwidth to accommodate the increased traffic. However, internet access costs money, and most organizations do not have infinite budgets.

It is an interesting fact of online life that users tend to consume more bandwidth over time. It is very rare to find a user who, once they have had access to a broadband connection, is satisfied with going back to a low speed dialup line (13).

Over a period of time it has been noticed that even though the University may need to pay for more bandwidth, that will never be a final solution to congestion because no matter how large the bandwidth is, it will be oversubscribed within a very short period. Hence, there may not be a better solution until the traffic and browsing habit of the University community is monitored, analysed and a strategic bandwidth management policy is put in place based on the data collected from the monitoring.

This could be addressed in several ways. However this work seeks to study the IP traffic pattern on the University network, analyze the type of traffic using the protocol they communicate with over the Internet.

1.4 Methodology

This work will focus mainly on the different communication protocols used by Internet traffic for data transmission on the internet; the analysis of these protocols will be used to develop a strategic management which will seek to maximize bandwidth for research and scholarly traffic data, at least during work hours to reduce the congestion experienced on the network. The research methods are:

1. Selection of monitoring software: A software that will monitor and adequately report in details the network usage will be identified and preferably an open source software to take care of licensing and virus issues
2. Installation and Configuration of monitoring software: A traffic monitoring software(ntop) will be installed and configured as a monitoring server on the network, it will be accessible from any part of the network
3. Testing of Server: The server will be tested on a small office network to ensure that the configuration works well.
4. Installation of Server on Live network: The server will the installed on the university live network in the network operating centre
5. Data collection: Data shall be collected from the monitoring server daily over a period of forty five (45) days continuously.
6. Extraction of Data: Since the point of interest is the analysis of network usage by different protocols, the protocols usage distribution shall be extracted from the collected data for analysis.
7. The collected data will be analysed to figure out the type of IP traffic on the network.
8. The result of the analysis will be used to recommend a bandwidth management strategy that will best suit the objectives of the University.

An attempt will be made to suggest a simple configuration of the core server on the university network that will implement the recommended strategy.

1.5 Thesis Outline

The whole work is divided into five chapters. Chapter One contains the introduction to the thesis; Chapter Two explains the theoretical background of internetworking and internet traffic transmission and protocols. Chapter There discusses the methodology adopted in carrying out the research. Chapter Four, presents the data collected, its analysis and results. Chapter Five contains recommendations, problems encountered and recommendations for further work and conclusions.

CHAPTER TWO

THEORETICAL BACKGROUND

2.0 History of the Internet.

The conceptual foundation for creation of the internet was significantly developed by three individuals and a research conference, each of which changed the way we thought about technology by accurately predicting its future:

- *Vannevar Bush* wrote the first visionary description of the potential uses for information technology with his description of the "memex" automated library system [22].

- *Norbert Wiener* invented the field of Cybernetics, inspiring future researchers to focus on the use of technology to extend human capabilities [22].

- *The 1956 Dartmouth Artificial Intelligence conference* crystallized the concept that technology was improving at an exponential rate, and provided the first serious consideration of the consequences [22].

- *Marshall McLuhan* made the idea of a global village interconnected by an electronic nervous system part of our popular culture [22].

The first networking protocol used on the Advanced Research Projects Agency Network (ARPANET) was the *Network Control Program*. In 1983, it was replaced with the *TCP/IP* protocol developed by *Robert Kahn*, *Vinton Cerf*, and others, which quickly became the most widely used network protocol in the world, the use of the Internet exploded after

1990, causing the US Government to transfer management to *independent organizations* starting in 1995[22]

The Internet workings include a technical design and a management structure. The management structure consists of a generally democratic collection of loosely-coupled organizations and working groups with mostly non-overlapping responsibilities. The technical design is founded on a complex, interlocking set of hierarchical tree-like structures like Internet Protocol addresses and domain names, mixed with networked structures like packet switching and routing protocols, all tied together with millions of lines of sophisticated software that continues to get better all the time.

So far this combination of management and technical structures has worked well, providing the reliable, powerful communication platform on which the rest of the complexity of the Internet is built [22]

2.2 What is an Internetwork?

An *internetwork* is a collection of individual networks as in Figure 2.1, connected by intermediate networking devices, that functions as a single large network. Internetworking refers to the industry, products, and procedures that meet the challenge of creating and administering internetworks [23].

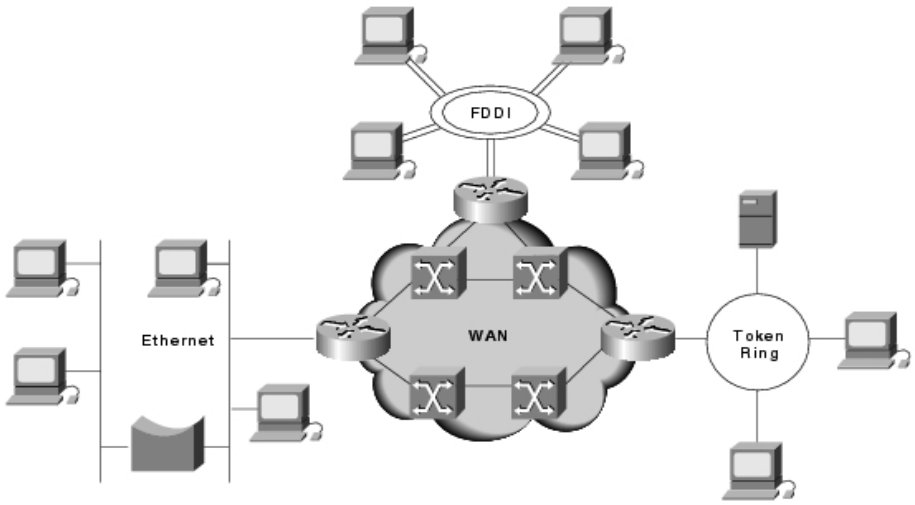


Figure2.1 Different Network Technologies Can Be Connected to Create an Internetwork

2.2.1 History of Internetworking

The first networks were time-sharing networks that used mainframes and attached terminals. Such environments were implemented by both IBM's Systems Network Architecture (SNA) and Digital's network architecture.

Local-area networks (LANs) evolved around the PC revolution. LANs enabled multiple users in a relatively small geographical area to exchange files and messages, as well as access shared resources such as file servers and printers.

Wide-area networks (WANs) interconnect LANs with geographically dispersed users to create connectivity. Some of the technologies used for connecting LANs include T1, T3, ATM, ISDN, ADSL, Frame Relay, radio links, and others. New methods of connecting dispersed LANs are appearing every day [23].

Today, high-speed LANs and switched internetworks are becoming widely used, largely because they operate at very high speeds and support such high-bandwidth applications as multimedia and videoconferencing.

Internetworking evolved as a solution to three key problems: isolated LANs, duplication of resources, and a lack of network management. Isolated LANs made electronic communication between different offices or departments impossible. Duplication of resources meant that the same hardware and software had to be supplied to each office or department, as did separate support staff. This lack of network management meant that no centralized method of managing and troubleshooting networks existed [23].

2.2.2 Internetworking Challenges

Implementing a functional internetwork is no simple task. Many challenges must be faced, especially in the areas of connectivity, reliability, network management, and flexibility. Each area is critical in establishing an efficient and effective internetwork.

The challenge when connecting various systems is to support communication among disparate technologies. Different sites, for example, may use different types of media operating at varying speeds, or may even include different types of systems that need to communicate. There is nothing stagnant in this world, internetworks must be flexible enough to change with new demands.

2.2.3 Internetworking Models

When networks first came into being, computers could typically communicate only with computers from the same manufacturer. For example, companies ran either a complete DECnet solution or an IBM solution—not both together. In the late 1970s, the *Open Systems Interconnection (OSI) reference model* was created by the International Organization for Standardization (ISO) to break this barrier [23].

The Open Systems Interconnection (OSI) model was meant to help vendors create interoperable network devices and software in the form of protocols so that different vendor networks could work with each other. The Open Systems Interconnection (OSI)

model is the primary architectural model for networks. It describes how data and network information are communicated from an application on one computer, through the network media, to an application on another computer. The OSI reference model breaks this approach into layers [17].

2.3 OSI Model

The *Open System Interconnection (OSI) reference model* describes how information from a software application in one computer moves through a network medium to a software application in another computer. The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for inter-computer communications. The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups. A task or group of tasks is then assigned to each of the seven OSI layers. Each layer is reasonably self-contained so that the tasks assigned to each layer can be implemented independently. This enables the solutions offered by one layer to be updated without adversely affecting the other layers. The following list details the seven layers of the Open System Interconnection (OSI) reference model as in Figure 2.2:

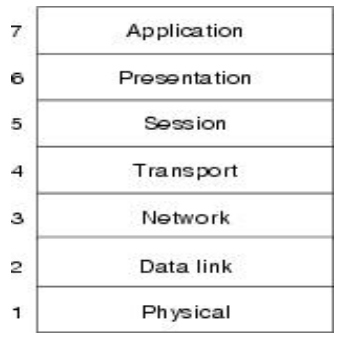


Figure 2.2 Open Systems Interconnection (OSI) Model

2.3.1 Characteristics of the OSI Layers

The seven layers of the OSI reference model can be divided into two categories: upper layers and lower layers as in Figure 2.3.

The *upper layers* of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application layer processes interact with software applications that contain a communications component. The term upper layer is sometimes used to refer to any layer above another layer in the OSI model [18].

The *lower layer*s of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the network cabling, for example) and is responsible for actually placing information on the medium [18].

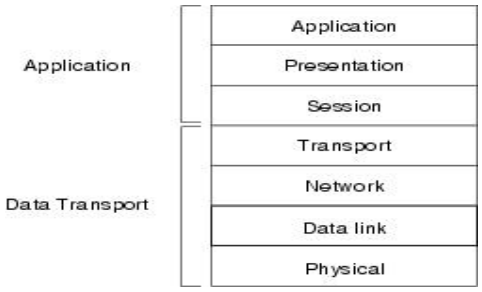


Figure 2.3 Sub-division of the Open Systems Interconnection (OSI) Layer

2.4 Transport Control Protocol/Internet Protocol (TCP/IP)Reference Model

The TCP/IP model is not the same as Open Systems Interconnection (OSI) model. There is no universal agreement regarding how to define TCP/IP with a layered model but it is generally agreed that there are fewer layers than the seven layers of the OSI model. [20]

TCP/IP model defines 4 layers that are as follows:

1) Internet layer:

Packet switching network depends upon a connectionless internetwork layer. This layer is known as internet layer, is the linchpin that holds the whole design together. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. They may appear in a different order than they were sent in each case it is job of higher layers to rearrange them in order to deliver them to proper destination. The internet layer specifies an official packet format and protocol known as internet protocol. The job of internet layer is to transport IP packets to appropriate destination. Packet routing is very essential task in order to avoid congestion. For these reasons it is said that TCP/IP internet layer performs the same function as that of OSI network layer [20].

2) Transport layer:

In the TCP/IP model, the layer above the internet layer is known as transport layer. It is developed to permit entities on the source and destination hosts to carry on a conversation. It specifies two end-to-end protocols

i) TCP (Transmission Control Protocol)

ii) UDP (User Datagram Protocol)

i) TCP

It is a reliable connection-oriented protocol that permits a byte stream originating on one machine to be transported without error on any machine in the internet. It divides the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination, the receiving TCP process collects the received message into the output stream. TCP deals with flow control to make sure a fast sender cannot swamp a slow receiver with more message than it can handle.

ii) UDP

It is an unreliable, connectionless protocol for applications that do not want TCP's sequencing on flow control and wish to offer their own. It is also used for client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video [20].

3) Application Layer

In TCP/IP model, session or presentation layer are not present. Application layer is present on the top of the Transport layer. It includes all the higher-level protocols which are virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP). The virtual terminal protocol permits a user on one machine to log into a distant machine and work there. The file transfer protocol offers a way to move data efficiently from one machine to another. Electronic mail was used for file transfer purpose but later a specialized protocol was developed for it. The Application Layer defines the following protocols [20]

i) File Transfer Protocol (FTP)

It was designed to permit reliable transfer of files over different platforms. At the transport layer to ensure reliability, FTP uses TCP. FTP offers simple commands and makes the differences in storage methods across networks transparent to the user. The FTP client is able to interact with any FTP server; therefore the FTP server must also be able to interact with any FTP client. FTP does not offer a user interface, but it does offer an application program interface for file transfer. The client part of the protocol is called the FTP and the server part of the protocol is known as FTPd. The suffix "d" means Daemon this is a legacy from UNIX computing where a daemon is a piece of software running on a server that offers a service [20].

ii) Hyper Text Transfer Protocol (HTTP)

HTTP permits applications such as browsers to upload and download web pages. It makes use of TCP at the transport layer again to check reliability. HTTP is a connectionless protocol that sends a request, receives a response and then disconnects the connection. HTTP delivers HTML documents plus all of the other components supported within HTML such as JavaScript, Visual script and applets [20].

iii) Simple Mail Transfer Protocol (SMTP)

SMTP provides extension to the local mail services that existed in the early years of LANs. It supervises the email sending from the local mail host to a remote mail host. SMTP makes use of TCP to establish a connection to the remote mail host [17].

iv) Simple Network Management Protocol (SNMP)

For the transport of network management information, SNMP is used as standardized protocol. Managed network devices can be cross examined by a computer running to return details about their status and level of activity [17].

4) The Host to Network Layer

Below the internet layer is great void. The TCP/IP reference model does not really say such about what happen here, except to point out that the host has connected to the network using some protocol so it can transmit IP packets over it. This protocol is not specified and varies from host to host and network to network [17].

2.5 Data Encapsulation

When a host transmits data across a network to another device, the data goes through *encapsulation*: it is wrapped with protocol information at each layer of the OSI model. Each layer communicates only with its peer layer on the receiving device.

To communicate and exchange information, each layer uses *Protocol Data Units (PDUs)*. These hold the control information attached to the data at each layer of the model. They are usually attached to the header in front of the data field but can also be in the trailer, or end, of it. Each Protocol Data Unit (PDU) is attached to the data by encapsulating it at each layer of the OSI model, and each has a specific name depending on the information provided in each header. This Protocol Data Unit (PDU) information is read only by the peer layer on the receiving device. After it has been read, it is stripped off, and the data is then handed to the next layer up [17].

Figure 2.4 shows the Protocol Data Units (PDUs) and how they attach control information to each layer. Figure 2.4 demonstrates how the upper-layer user data is converted for transmission on the network. The data stream is then handed down to the Transport layer, which sets up a virtual circuit to the receiving device by sending over a synch packet. Next, the data stream is broken up into smaller pieces, and a transport layer header (a PDU) is created and attached to the header of the data field; now the piece of data is called a segment. Each segment is sequenced so the data stream can be put back together on the receiving side exactly as it was transmitted. Each segment is then handed to the Network layer for network addressing and routing through the internetwork. Logical addressing (for example, IP) is used to get each segment to the correct network [18]

The Network layer protocol adds a control header to the segment handed down from the Transport layer, and what we have now is called a *packet* or *datagram*. Remember that the Transport and Network layers work together to rebuild a data stream on a receiving host,

but it is not part of their work to place their Protocol Data Units (PDUs) on a local network segment—which is the only way to get the information to a router or host. It is the Data Link layer that's responsible for taking packets from the Network layer and placing them on the network medium (cable or wireless) [18].

The Data Link layer encapsulates each packet in a *frame*, and the frame's header carries the hardware address of the source and destination hosts. If the destination device is on a remote network, then the frame is sent to a router to be routed through an internetwork. Once it gets to the destination network, a new frame is used to get the packet to the destination host [17]

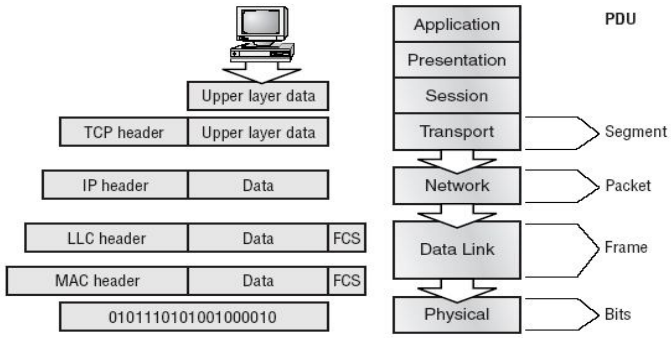


Figure 2.4 Data Encapsulation.

2.6 Internet Protocol (IP)

Internet Protocol (IP) essentially is the Internet layer. The other protocols found here merely exist to support it. IP holds the big picture and could be said to "see all," in that it's aware of all the interconnected networks. It can do this because all the machines on the network have software, or logical, address called an IP address. IP looks at each packet's address [17].

All hosts on a network have a logical ID called an IP address. This is the software or logical address and contains valuable encoded information, greatly simplifying the complex task of routing. IP receives segments from the Host-to-Host layer and fragments them into

datagram's (packets) if necessary. IP then reassembles datagram back into segments on the receiving side.

This will give you an idea of what the IP protocol has to go through every time user data is sent from the upper layers and is to be sent to a remote network.

The following fields make up the IP header:

Version IP version number.

Header Length: Header length (HLEN) in 32-bit words.

ToS with IP Precedence Bits: Type of Service tells how the datagram should be handled. The first 3 bits are the priority bits.

Total length: Length of the packet including header and data.

Identifier: Unique IP-packet value.

Flags: Specifies whether fragmentation should occur.

Flag offset: Provides fragmentation and reassembly if the packet is too large to put in a frame. It also allows different Maximum Transmission Units (MTUs) on the Internet [18]

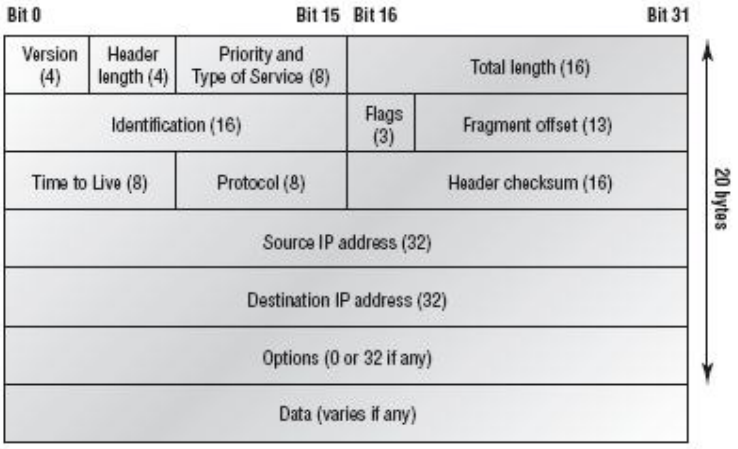


Figure 2.5 IP headers.

2.6.1 IP Addressing

One of the most important topics in any discussion of TCP/IP is IP addressing. An *IP address* is a numeric identifier assigned to each machine on an IP network. It designates

the specific location of a device on the network. An IP address is a software address, not a hardware address—the latter is hard-coded on a Network Interface Card (NIC) and used for finding hosts on a local network

2.6.2 IP Terminology

There are some important terms vital to your understanding of the Internet Protocol:

- **Bit** A *bit* is one digit, either a 1 or a 0.
- **Byte** A *byte* is or 8 bits, depending on whether parity is used. (Henceforth a byte is 8 bits)
- **Octet** An octet, made up of 8 bits, is just an ordinary 8-bit binary number.
- **Network address** This is the designation used in routing to send packets to a remote network— for example, 10.0.0.0, 172.16.0.0, and 192.168.10.0.
- **Broadcast address** The address used by applications and hosts to send information to all nodes on a network is called the *broadcast address*. Examples include 255.255.255.255, which is all networks, all nodes; 172.16.255.255 [18].

2.6.3 The Hierarchical IP Addressing Scheme

An IP address consists of 32 bits of information. These bits are divided into four sections, referred to as *octets* or bytes, each containing 1 byte (8 bits). You can depict an IP address using one of three methods:

_ Dotted-decimal, as in 172.16.30.56

_ Binary, as in 10101100.00010000.00011110.00111000

_ Hexadecimal, as in AC.10.1E.38

All these examples truly represent the same IP address. Hexadecimal isn't used as often as dotted-decimal or binary when IP addressing is discussed, but you still might find an IP address stored in hexadecimal in some programs [18].

2.6.4 Network Addressing

The *network address* (which can also be called the network number) uniquely identifies each network. Every machine on the same network shares that network address as part of its IP address. In the IP address 172.16.30.56, for example, 172.16 is the network address. The *node address* is assigned to, and uniquely identifies, each machine on a network. This part of the address must be unique because it identifies a particular machine—an individual— as opposed to a network, which is a group. This number can also be referred to as a *host address*. In the sample IP address 172.16.30.56, the 30.56 is the node address [19].

The designers of the Internet decided to create classes of networks based on network size. For the small number of networks possessing a very large number of nodes, they created the rank *Class A network*. At the other extreme is the *Class C network*, which is reserved for the numerous networks with a small number of nodes. The class distinction for networks between very large and very small is predictably called the *Class B network* [18].

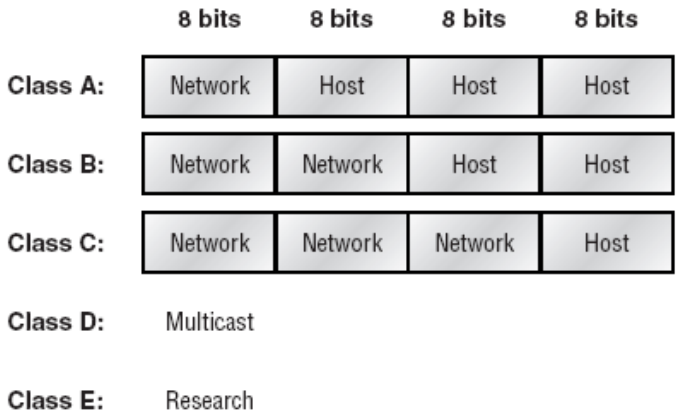


Figure 2.6 Three Classes of Networks

Table 2.1: Three classes of IP Addresses

Class	Leading Bit Pattern	Default Subnet Mask	Address Range	Number of Addresses per Network
A	0	255.0.0.0	1.0.0.0–126.255.255.255	16,777,214
B	10	255.255.0.0	128.0.0.0–191.255.255.255	65,534
C	110	255.255.255.0	192.0.0.0–223.255.255.255	254
D	1110	None	224.0.0.0–239.255.255.255	Multicast
E	1111	None	240.0.0.0–255.255.255.255	Experimental

2.6.5 Network Address Range: Class A

The designers of the IP address scheme said that the first bit of the first byte in a Class A network address must always be off, or 0. This means a Class A address must be between 0 and 127, inclusive. **0**xxxxxxx

If the other 7 bits are all turned off and then on, the Class A range of network addresses will be found to be:

00000000 = 0

01111111 = 127

So, a Class A network is defined in the first octet between 0 and 127, and it can not be less or more.

2.6.6 Network Address Range: Class B

In a Class B network, the RFCs state that the first bit of the first byte must always be turned on, but the second bit must always be turned off. If you turn the other 6 bits all off and then all on, you will find the range for a Class B network:

10000000 = 128

10111111 = 191

As you can see, a Class B network is defined when the first byte is configured from 128 to 191.

2.6.7 Network Address Range: Class C

For Class C networks, the RFCs define the first two (2) bits of the first octet as always turned on, but the third bit can never be on. Following the same process as the previous classes, the binary form is converted to decimal to find the range. The range for a Class C network is:

11000000 = 192

11011111 = 223

2.7 Bandwidth

In computer networks, bandwidth is often used as a synonym for data transfer rate - the amount of data that can be carried from one point to another in a given time period (usually a second). In recent years, the term bandwidth has been popularly used to refer to the ***capacity*** of a digital communications line, typically measured in some number of bits per second. It is usually expressed in bits (of data) per second (bps). Occasionally, it is expressed as bytes per second (Bps). In general, a link with a high bandwidth is one that may be able to carry enough information to sustain the succession of images in a video presentation[13].

• ***Throughput*** describes the actual amount of information flowing through a connection, disregarding protocol overhead. Like bandwidth, it is expressed in some number of bits per second. While a T1 may provide 1.544 Mbps between the endpoints, the protocol spoken on the physical line reduces the effective throughput to about 1.3 Mbps. When the additional overhead of Internet protocols is factored in, the available throughput is even less. When the actual usage of a connection is measured or a "speed test" performed on a line, it is the throughput measured[13].

• ***Latency*** refers to the amount of time it takes for a packet to travel from one point on a network to another. A closely related concept is ***Round Trip Time*** (***RTT***), which is the amount of time it takes for a packet to be acknowledged from the remote end of a connection. Latency is measured as some amount of time, usually in milliseconds. The latency of ethernet is about 0.3ms. A T1 connection has a latency of 2 to 5ms, while a VSAT connection requires at least 500ms before an acknowledgment can be received, due to the speed of light and the large distances involved. Some factors that contribute to latency are network congestion, over utilized servers, and the distance between the two points [13].

• ***Speed*** is an ambiguous term that refers to some combination of these other terms. An Internet connection may "feel slow" when using an interactive service (such as Voice over IP or gaming) on a line with high latency, even if there is sufficient bandwidth. Users will also complain when transferring large files on a connection with insufficient capacity, even if the latency is very low [13].

2.8 The University current Network Setup

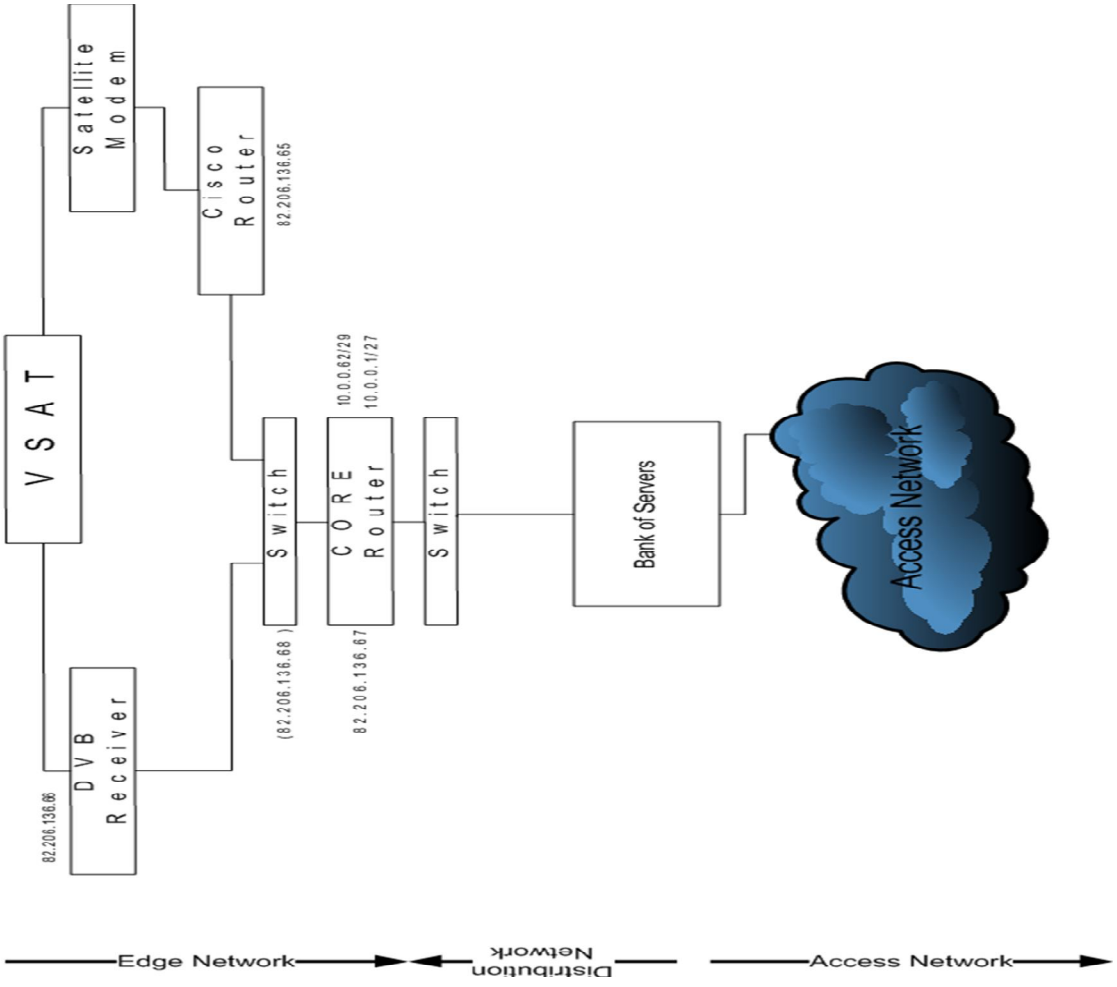


Fig 2.7 Schematic Diagram of the University's Current Network

The University currently connects to the internet via a Satellite network from Intelsat, with a Very Small Aperture Terminal (VSAT), terminating its receive path on the Digital Video Broadcast modem (DVB) and its transmit path on a satellite modem which connects to a Cisco router, the main server is called the core router and all other servers direct traffic through the core router as in Figure 2.7.

The core router has three (3) Ethernet interfaces with IP addresses shown below

Ether1-external: link to the edge network configured with IP address 82.206.X.X

Ether1-externel: link to the edge network configured with IP address 82.206.X.X

2.9 Detailed Configuration on the devices in the network

Ether2-internal: link to the Core network configured with IP address 10.X.X.X/27

Ether3-Library: link to the library configured with IP address 10.X.X.X/29

- Routes

The following are the static routes that were added to the Core router for the various segments of the network.

Dst-address=10.X.X.X/26 gateway=10.X.X.X for west sector access net

Dst-address=10.X.X.X/26 gateway=10.X.X.X for east sector access net

Dst-address=10.X.X.X/26 gateway=1.X.X.X for north sector access net

Dst-address=10.X.X.X/28 gateway=10.X.X.X for digital station access net

Dst-address=10.X.X.X/16 gateway=10.X.X.X for west sector distribution net

Dst-address=10.X.X.X/16 gateway=10.X.X.X for east sector distribution net

Dst-address=10.X.X.X/16 gateway=10.X.X.X for north sector distribution net

Dst-address=10.X.X.X/16 gateway=10.X.X.X for digital station distribution net

Dst-address=192.X.X.X/16 gateway=10.X.X.X for senate building distribution net

- Dynamic Routing Protocol

Open Shortest Path First (OSPF) was enabled on the ether2-internal interface of the core router.

- DNS Cache server

Domain Name System (DNS) cache server was enabled on the core router to serve as the default DNS server for the entire network; this will make name resolution faster.

- Firewall:

A list of well known virus port is added to the filter list of the core router.

- NAT at the edge

All outbound traffic from the 10.X.X.X/8 and 192..X.X.X/16 network through the ether1-external interface was source NAT to 82.X.X.X

The IP address 82.X.X.X was mapped to the IP address of the SUN server in the library on 10.X.X.X

- Transparent Web-proxy

Web-proxy was enabled on the core router with access control to allow only traffic from internal network. The proxy was activated on TCP port 3128.

A destination NAT rule was added to transparently redirect all traffic destine for TCP port 80 on servers that are not local to web proxy service on the core router on TCP port 3128. Content Filtering can be done through this web-proxy using the access list section.

From the configuration above, the main work done to reduce and control traffic is the configurations of firewall setting to block well known virus and other unwanted ports.

This has, however, proved not too efficient over time because issues of port masquerade and Denial of Service (DoS) to other applications using the same ports with some other unwanted services or application came up severally.

CHAPTER THREE

METHODOLOGY

3.0 Proposed Model and

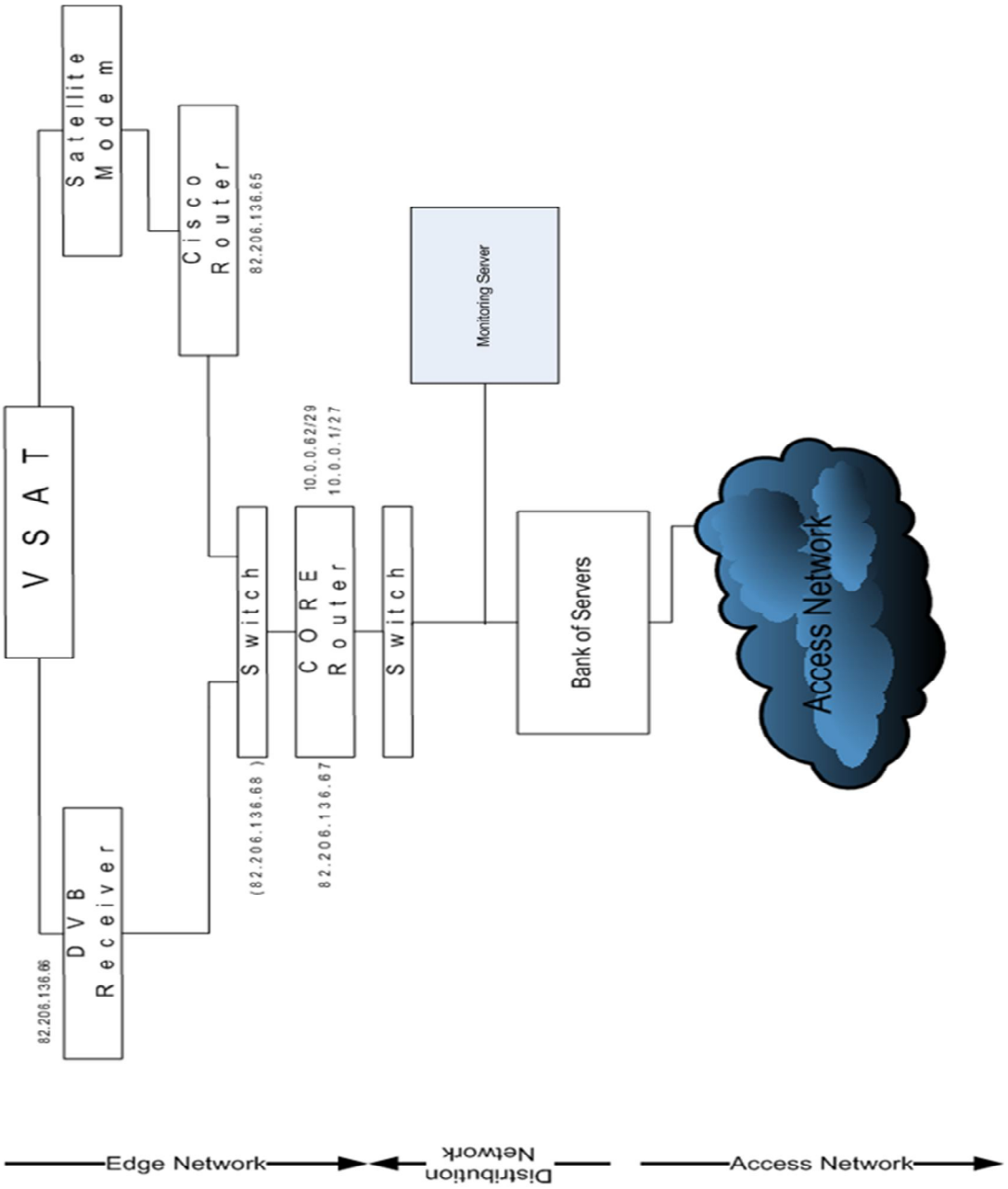


Figure 3.1 proposed Network Setup

In the proposed model, the initial configuration of the main router remains untouched however, the border router will have Netflow activated on it and the monitoring server

will be placed on the switch after the core router. This will not change the current setup but will only have the monitoring server added to it.

3.2 Installations and Configurations

ntop is an open-source web-based traffic measurement and monitoring application, and was originally written for tracking performance problems on campus backbone network. ***ntop*** however evolved into a more flexible, extensible and powerful tool as people over the Internet downloaded it and reported problems and suggestions. ***ntop*** is currently used for traffic measurement , monitoring and analysis [10].

Like most other Linux programs, ***ntop*** can be installed from software repositories of both Debian-based and RPM-based distributions and the sources can be downloaded and compiled by the user [9].

3.2.1 Installing *ntop* from Source

The operating system installed on the monitoring server is Ubuntu Server 8.04 with AMP [*Apache MySQL and php*] and *OpenSSH* servers pre-installed.

1. Download the ntop sources from **sourceforge.net**. It is usually a 'gzipped tarball' e.g. ntop-3.3.7.tar.gz.

2. Extract the contents of sources from the tarball by typing '***untar –xzvf ntop-3.3.7.tar.gz***'

3. Install all dependencies. [Although listed here as different commands, the same thing can be done with a single command by putting all the packages separated by a space after a single ***sudo apt-get*** install command.]

The dependencies required are listed in the Table 3.1 along with a brief description of what exactly they provide for ***ntop***.

Table 3.1 List of Dependencies Required by ***ntop*** [10]

Dependency	Description
glibc, glibc-devel, gcc, cpp	Required to compile almost any software from source
Awk	A utility for performing text-processing tasks.
libtool (1.4 or later)	Required to compile almost any software from source.
m4	Required to compile almost any software from source.
autoconf (2.53 or later)	Required to compile almost any software from source.
automake (1.6 or later)	Required to compile almost any software from source.
gdbm, gdbm-devl	Lightweight alternative to a full relational database. Enables storing and fast lookup with keys of arbitrary data
libpcap, libpcap-dev	Required to decode the packets that are fed to ntop
gd, gd-dev	Used to create .png picture files
libpng,libpng-dev	Used to create .png picture files
openssl,openssl-dev	Enables access to ntop web UI via https
zlib,zlib-dev	Used to compress HTML pages
rrdtool, librrd2, librrd2-dev	Used to create 'Round-Robin databases' which are used to store and graph historical data in a format that permits long duration retention without growing larger over time
graphviz	Used to construct the local traffic map [It provides the dot tool]

4. Change into the sources directory created when the source tarball is extracted ***(cd ntop-3.3.7)***

5. Compile and install the application by typing each of the following individually and waiting for it to complete without any errors.

/autogen.sh makes sudo make install

Look in the output of the commands for any error messages.

Error messages in the ***/autogen.sh*** command are most likely due to unmet dependencies.

The important thing to note is that the user to which ntop drops privileges must have appropriate rights in the location where ntop stores its databases (which is ***/usr/local/var/ntop*** by default).

To set the ownership and rights on that directory, type:

chown –R /usr/local/var/ntop

To set the administrator password, type:

sudo ntop –A5

then fill in and confirm the ***ntop*** administrator password.

ntop is run by typing

sudo ntop –d

Note: The ***–d*** option daemonizes ***ntop*** so it runs in the background.

To make it run at start-up and listen on the first network interface, insert

sudo /usr/local/bin/ntop -d in /etc/rc.local

3.2.2 Using *ntop* as a NetFlow Collector

To achieve this, the following three things are needed:

1. Prepare [configure] ***ntop*** to receive NetFlow information from a NetFlow probe.

2. Configure the NetFlow probe to send its flow information to ***ntop***.

3. Switch to the virtual NetFlow interface so that ***ntop*** analyzes traffic from NetFlow rather than from its local interfaces.

The procedures for each step are detailed in the following sections:

3.2.3 Configure *ntop* NetFlow Plugin to receive NetFlow Data

1. Click ***PluginsNetFlowActivate*** to activate the NetFlow plugin.

2. Click ***PluginsNetFlowView/Configure*** to see current NetFlow virtual interfaces and possible add more.

3. To set the port on which ***ntop*** listens for NetFlow information, go to AdminPreferences, look for the parameter called ***"netflow.2.netFlowInPort"*** and type in the desired port number and click Set. In the screenshot, it is set to 2055.

3.2.4. Configure the NetFlow Probe to export Data to *ntop*

The procedure on Cisco routers assuming the router's Internetwork Operating System (IOS) version is 12.2(T) or later, is as follows:

1. Configure the interface to capture flows into the NetFlow cache.

Router(config)# ip cef Router(config)# interface ethernet 1/0 .

Router(config-if)# ip flow ingress

2. Configure the router to export the NetFlow data to ***ntop***

Router(config)# ip flow-export version 9

Router(config)# ip flow-export destination a.b.c.d 2055

a.b.c.d is the IP address of the ***ntop*** server which has been configured to listen for NetFlow data on port 2055.

When using a Mikrotik RouterOS-based device, the procedure is as follows:

1. Enable traffic flow on the route:

[admin@MikroTik] **ip traffic-flow> set enabled=yes**

2. Specify the IP address of the ***ntop*** server and port on which it is listening for NetFlow data

[admin@MikroTik] ***ip traffic-flow target add address=192.x.x.x:2055 version=9***

3.2.5 Configure *ntop* to Analyze the NetFlow Data

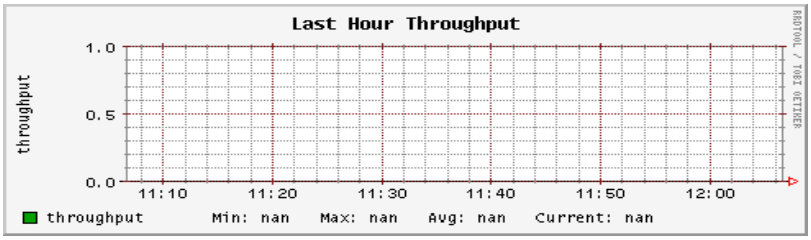
This just means switching the Interface from which ntop gets its data from. On the SummaryTraffic page, the row titled Network Interface(s) lists the available interface(s) from which ntop is getting data. If properly configured the NetFlow plugin, a NetFlow interface should be listed [NetFlow.interfaceX] The next table with heading Traffic Report for 'eth0' [switch] indicates that ***ntop*** is currently analyzing data that comes in through interface eth0. The switch link when clicked on goes to a dialog box (also accessed by clicking AdminSwitch Network Interface Cards (NICs)) that lists the various interfaces available on the system (both physical and virtual interfaces like NetFlow interfaces) and lets one choose which one ***ntop*** is to report traffic for. Simply select the NetFlow interface.

CHAPTER FOUR

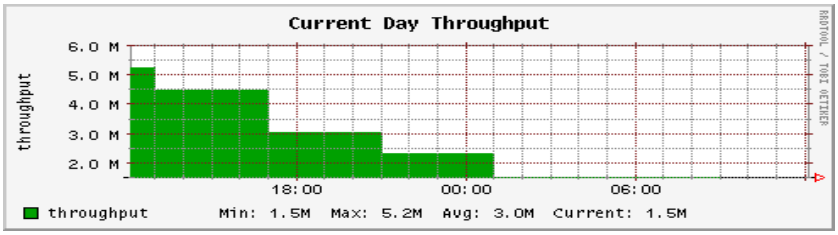
RESULTS AND ANALYSIS

4.0 Sample of Results and Data collected.

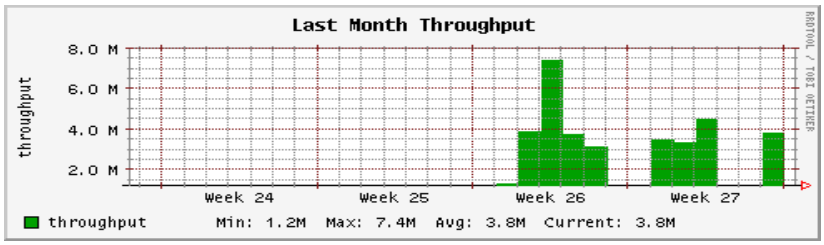
The monitoring system was initially installed on a small office network in order to test run it before installing it on the University network. The sample results are shown in Figures 4.1 and 4.2 and Tables 4.1 to 4.3 [11]



Time [Mon Jul 7 11:06:33 2008 to Mon Jul 7 12:06:33 2008]



Time [Sun Jul 6 12:06:33 2008 to Mon Jul 7 12:06:33 2008]



Time [Sat Jun 7 12:06:33 2008 to Mon Jul 7 12:06:33 2008]

Figure 4.1: Network Load Statistics (Test Data)

ntop

About Summary All Protocols IP Utils Plugins Admin

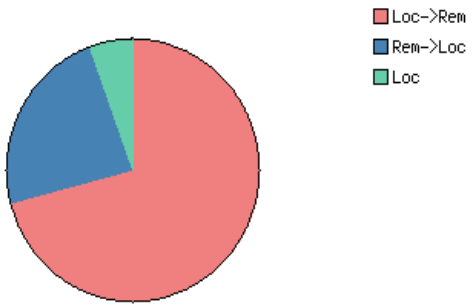


Figure 4.2 IP Protocol Distributions

Table 4.1: Local Traffic (Test Data)

,.IP Protocol	Data	Percentage
TCP vs. UDP	384.1 MB	TCP 45.8 % / UDP 54.2 %

TCP/UDP Protocol	Data	Percentage
FTP	595.2 KB	0%
PROXY	1.6 KB	0%
HTTP	67.1 MB	17.5%
DNS	173.9 MB	45.3%
Telnet	17.4 MB	4.5%
NBios-IP	2.9 MB	0%
Mail	2.1 MB	0%
SNMP	24.7 MB	6.4%
NEWS	12.6 KB	0%
DHCP-BOOTP	270.7 KB	0%
NFS	3.9 KB	0%
SSH	30.7 MB	8.0%
Gnutella	0.2 KB	0%
Kazaa	1.0 KB	0%
eDonkey	2.3 KB	0%
Messenger	3.2 KB	0%
Other TCP/UDP-based Protocols	64.3 MB	16.7%

Table 4.2: Remote to Local Traffic (Test Data)

IP Protocol	Data	Percentage
TCP vs. UDP	1.7 GB	TCP 91.7 % / UDP 8.3 %

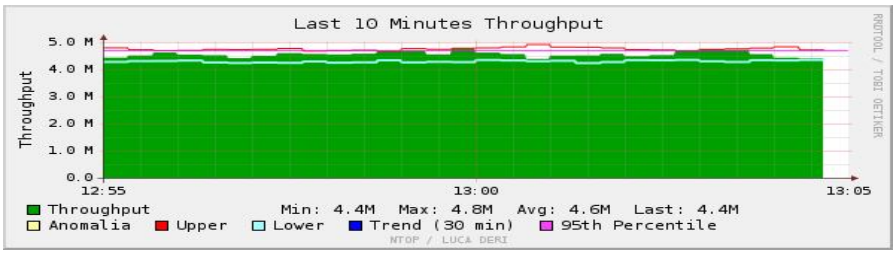
TCP/UDP Protocol	Data	Percentage
FTP	7.0 MB	0%
PROXY	17.6 MB	1.0%
HTTP	1.2 GB	72.3%
DNS	99.3 MB	5.8%
Telnet	1.3 MB	0%
NBios-IP	1.1 KB	0%
Mail	63.6 MB	3.7%
SNMP	1.7 MB	0%
NEWS	526.2 KB	0%
DHCP-BOOTP	2.4 MB	0%
NFS	83.9 KB	0%
X11	10.3 KB	0%
SSH	557.4 KB	0%
Gnutella	35.3 KB	0%
Kazaa	0.2 KB	0%
eDonkey	9.0 KB	0%
Messenger	3.2 MB	0%
Other TCP/UDP-based Protocols	277.5 MB	16.2%

Table 4.3 Local to Remote Traffic (Test Data)

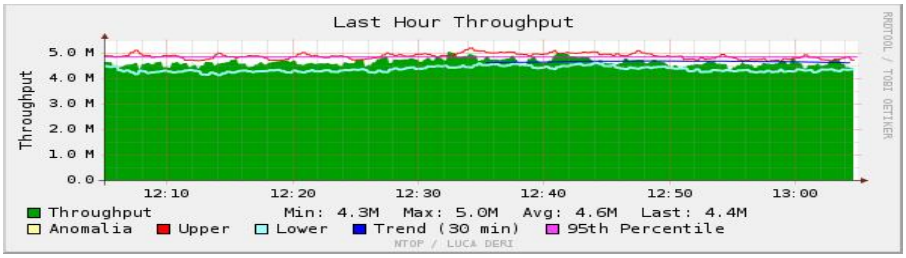
IP Protocol	Data	Percentage
TCP vs. UDP	5.0 GB	TCP 98.2 % UDP 1.8 %

TCP/UDP Protocol	Data	Percentage
FTP	822.8 KB	0%
PROXY	769.8 KB	0%
HTTP	1.2 GB	23.7%
DNS	53.8 MB	1.1%
Telnet	533.2 KB	0%
NBios-IP	2.9 KB	0%
Mail	50.7 MB	0%
SNMP	260.3 KB	0%
NEWS	275.1 KB	0%
DHCP-BOOTP	308.8 KB	0%
NFS	2.4 MB	0%
X11	75.7 KB	0%
SSH	33.1 KB	0%
Gnutella	48.7 KB	0%
Kazaa	1.5 MB	0%
WinMX	0.1 KB	0%
eDonkey	722.4 KB	0%
Messenger	2.0 MB	0%
Other IP-based Protocols	3.7 GB	74.1%

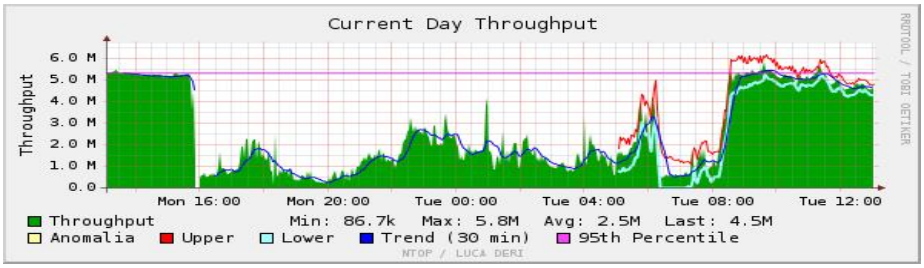
After a couple of weeks the system was then moved to the Network Operating Centre (NOC), the heart of the University network at the 7th Floor of the Senate building. Figure 4.3 and Tables 4.4 to 4.6 show some of the results obtained [12]



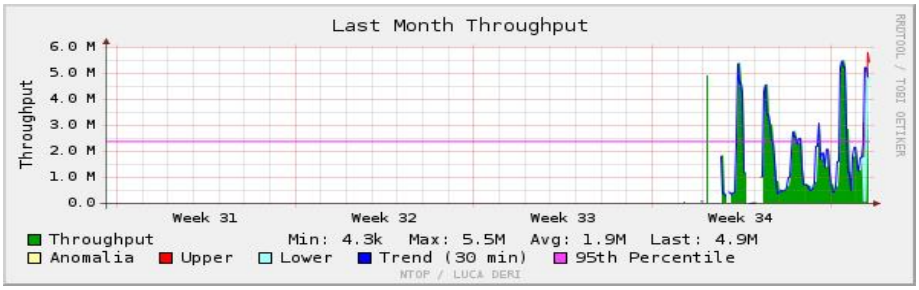
Time [Tue Aug 26 12:55:00 2008 toTue Aug 26 13:05:00 2008]



Time [Tue Aug 26 12:05:00 2008 to Tue Aug 26 13:05:00 2008]



Time [Mon Aug 25 13:05:00 2008 to Tue Aug 26 13:05:00 2008]



Time [Sun Jul 27 13:05:00 2008 to Tue Aug 26 13:05:00 2008]

Figure 4.3: Network Load Statistics(Live Data)

Table 4.4: IP Protocol Distribution(Live Data)

IP Protocol	Data	Percentage
TCP vs. UDP	9.4 GBytes	TCP 97.5 %  UDP 2.5 %

TCP/UDP Protocol	Data	Percentage
FTP	900.6 KBytes	0%
HTTP	8.5 GBytes	90.2%
DNS	125.7 MBytes	1.3%
Telnet	609.4 KBytes	0%
NBios-IP	1.4 MBytes	0%
Mail	33.4 MBytes	0%
DHCP-BOOTP	7.1 KBytes	0%
SNMP	11.8 MBytes	0%
NNTP	42.9 KBytes	0%
NFS/AFS	184.8 KBytes	0%
VoIP	942.1 KBytes	0%
X11	22.7 KBytes	0%
SSH	519.0 KBytes	0%
Gnutella	1.2 MBytes	0%
Kazaa	99.1 KBytes	0%
WinMX	1.0 KBytes	0%
eDonkey	358.1 KBytes	0%
BitTorrent	17.7 MBytes	0%
Messenger	1.2 MBytes	0%
Other TCP/UDP-based Protocols	744.6 MBytes	7.7%

Table 4.5:Remote to Local Traffic

IP Protocol	Data	Percentage
TCP vs. UDP	10.2 GBytes	TCP 99.2 % / UDP 0.8 % 

TCP/UDP Protocol	Data	Percentage
FTP	314.0 KBytes	0%
HTTP	8.9 GBytes	87.5%
DNS	7.2 MBytes	0%
Telnet	107.7 KBytes	0%
NBios-IP	44.6 KBytes	0%
Mail	3.4 MBytes	0%
DHCP-BOOTP	21.0 KBytes	0%
SNMP	971.3 KBytes	0%
NNTP	7.5 KBytes	0%
NFS/AFS	0.6 KBytes	0%
VoIP	57.6 KBytes	0%
X11	666.2 KBytes	0%
SSH	5.4 KBytes	0%
Gnutella	290.6 KBytes	0%
eDonkey	5.5 KBytes	0%
BitTorrent	64.5 MBytes	0%
Messenger	170.3 KBytes	0%
Other TCP/UDP-based Protocols	1.2 GBytes	11.8%

Table 4.6 Local to Remote Traffic

IP Protocol	Data	Percentage
TCP vs. UDP	565.6 MBytes	TCP 97.5 % / UDP 2.5 %

TCP/UDP Protocol	Data	Percentage
FTP	159.7 KBytes	0%
HTTP	480.6 MBytes	85.0%
DNS	3.0 MBytes	0%
Telnet	64.0 KBytes	0%
NBios-IP	2.8 KBytes	0%
Mail	7.7 MBytes	1.4%
SNMP	911.7 KBytes	0%
NNTP	8.9 KBytes	0%
NFS/AFS	1.5 KBytes	0%
VoIP	3.3 KBytes	0%
X11	25.7 KBytes	0%
SSH	12.9 KBytes	0%
Gnutella	449.8 KBytes	0%
Kazaa	0.6 KBytes	0%
WinMX	0.3 KBytes	0%
eDonkey	24.6 KBytes	0%
BitTorrent	1.1 MBytes	0%
Messenger	62.7 KBytes	0%
Other IP-based Protocols	71.6 MBytes	12.7%

4.2 Analysis of Sample data

The most relevant data for this work is the remote to local traffic. ***ntop*** recognizes data coming from the router into the University network as remote traffic so all traffic emanating from the router into the network are the traffic consuming the download bandwidth and causing congestion on the network. From Tables 4.4(12) and 4.5(12), Tables 4.7 and 4.8 and Figures 4.4 and 4.5 were developed:

Table 4.7 Summary Extract from Table 4.2 (Test Data)

Protocol	**Data (%)**
Http	72.3
Proxy	1.0
DNS	5.8
Mails	3.7
Other IP Protocols(OIP)	16.2
Others	1.0

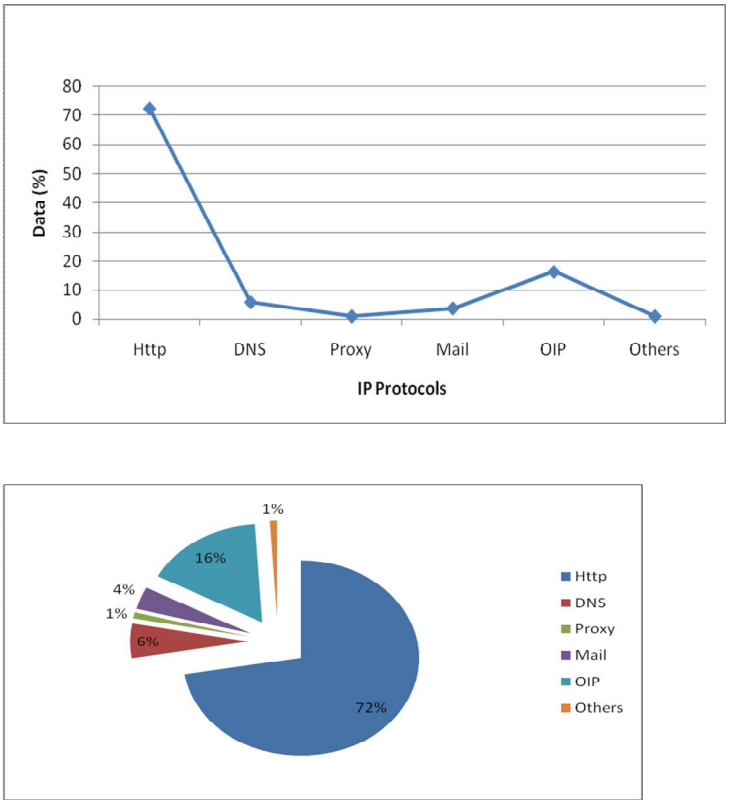
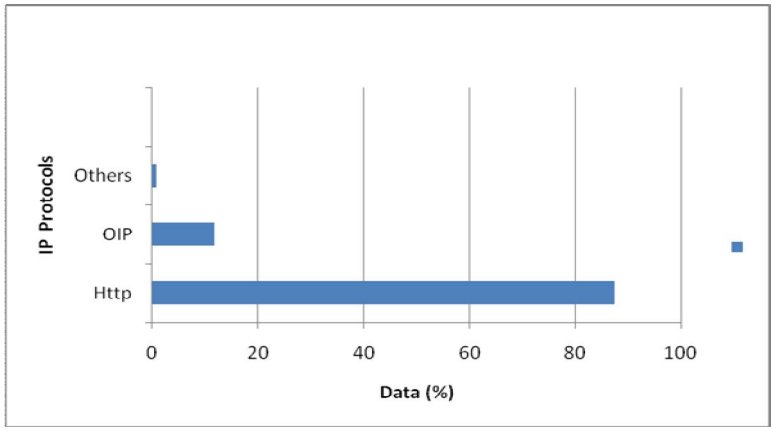


Figure 4.4 Remote to Local Traffic (Test Data)

Table 4.8: Summary Extracts from Table 4.5 (Live Data)

Protocol	Data (%)
Http	87.5
Other IP Protocols(OIP)	11.8
Others	0.7



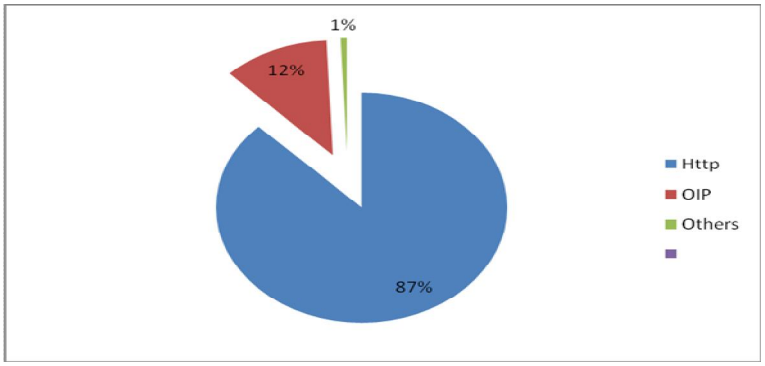


Figure 4.5 Remote to Local Traffic(Live data)

From the data collected, the following can be deduced

1. The load statistics shows that the community maximises the bandwidth of 5Mbps downlink (see Figure 4.3)
2. A comparison of Tables 4.5 and 4.6 shows clearly that there are some activities within the internal network that do not show clearly at the border gateway (router).

3. Tables 4.5 and 4.6 also show clearly that the amount of DNS request done remotely is minimal. This translates to the fact that the border router takes care of the DNS traffic.

4. It also indicates that there is less traffic that can be attributed to virus attack, shown clearly by the ratio of TCP to UDP traffic.

5. HTTP (Hyper-Text Terminal Protocol) is always the topmost unequalled traffic, which confirms the fact that port blocking will not solve the current congestion on the network.

6. The second constant topmost is called other IP-based Protocol. It is important that more work be done to ascertain exactly what this traffic is all about. This is because it takes a significant bit of the traffic constantly.

4.3 Additional configuration of ntop

Based on the results above it was concluded that further work needed to be done to be able to ascertain the composition of the HTTP traffic and also the components of the item termed 'other IP protocols'. Hence the following additional configurations were done on the ***ntop*** server.

1. To have a record of all sites visited on the university network, the traffic and activity module was enabled for all protocols from the configuration terminal of ntop.
2. More dependencies were installed in order to be able to activate a packet filtering module.

It should however be noted that the module enabled in step 1 cannot be kept on the

monitoring server for a long time due to the amount of data generated and the overhead on both the monitoring server and the storage space on the server.

4.4 Results obtained with the additional configuration

This Section describes results obtained from the ***ntop*** server showing the network traffic by all protocols on the University network. Table 4.9 represents only 12.5% of the total traffic on the University network at the time it was captured.

Table 4.9 Summary of Network Traffic (extracts from Table A1)[1]

S/N	Site URL	Frequency	%	Significance	Priority
1	www.avast.com	75	2.86259542	Antivirus download and update	Medium
2	www.microsoft .com	392	14.96183206	Patches and service packs + mail + instant messenger	Medium
3	www.google.com	431	16.45038168	Search engine	High
4	www.yahoo.com	812	30.99236641	Mail + search engine +Instant Messenger	
5	www.facebook.com	289	11.03053435	Online social interactions	Low
6	www.amazone.com	82	3.129770992	Online purchase	Medium
7	www.bbc.com	67	2.557251908	Online news, sports	Medium
8	www.mit.edu	45	1.717557252	Online edu courseware	High
9	www.Kapersky.com	34	1.297709924	Virus download and upgrade	Medium
10	www.grisoft.com	98	3.740458015	Virus download and upgrade	Medium
11	www.macafee.com	24	0.916030534	Virus download and upgrade	Medium
12	www.ingenta.com	45	1.717557252	Online database	High
13	www.adobe.com	15	0.572519084	Productivity Software	Medium
14	www.ebscohost.com	65	2.480916031	Research database	High
15	www.youtube.com	70	2.671755725	Video Streaming	Low
16	www.abu.edu.ng	35	1.335877863	University information + Mail	High
17	Others	41	1.564885496	Various	Medium
	Total	**2620**	100		

$$\text{Frequency} = \frac{\text{No of times site was visited}}{\text{14 days}}$$

$$\text{Percentage (\%)} = \frac{frequency}{total} \; x \; 100$$

[1] Source : Table 4.9 is an extract from Table A1 in Appendix A.

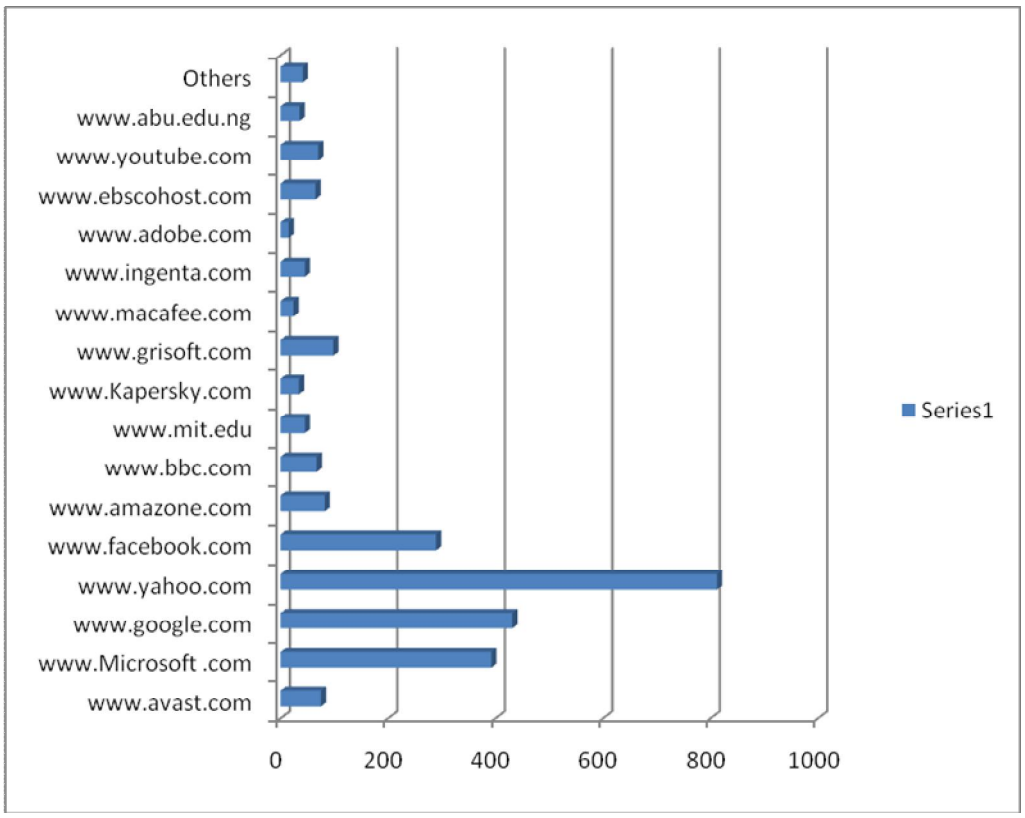


Figure 4.6 Summary of Network Traffic.

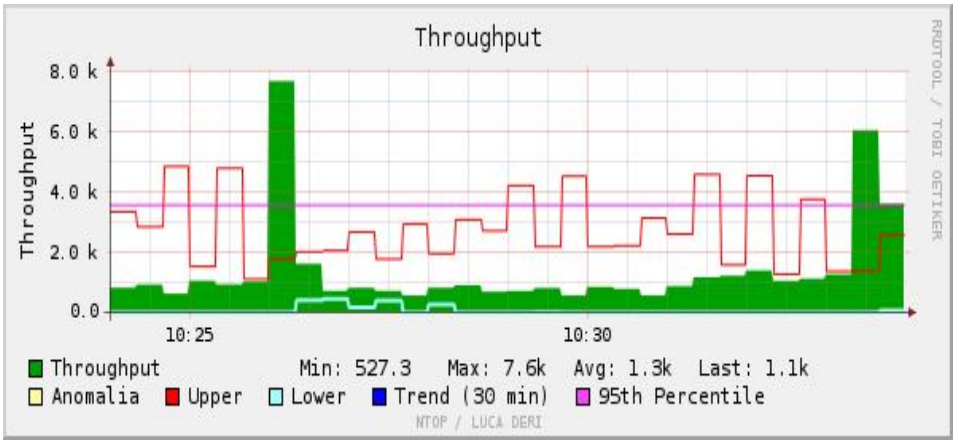
4.5 Deduction from Results of Data Analysis

- Some sites are visited very regularly on the University network
- Most http traffic generated are not of high priority for academic purposes
- A very large percentage of the University community run Windows operating systems which need daily updates of both the operating system and the antivirus software on them
- Very few notable academic activities can be seen on the University network
- A bit of traffic is generated by online social interactions (e.g. Facebook, Yahoo and Instant Messengers, etc).

4.6 Experimental solution.

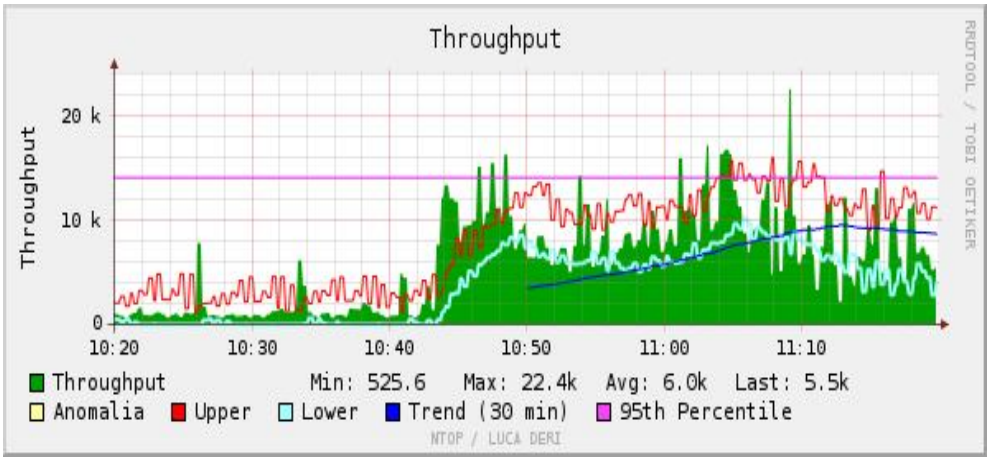
Further to the summary of result in Table 4.9, a trial experiment was done on the University core router by blocking all Internet mails (Yahoo, Hotmail, Gmail etc) on the University network. This is in order to determine the impact of the Internet mails. Figure 4.7 and Table 4.10 show the outcome of the experiment.

Last 10 Minutes



Time [Wed Jan 14 10:20:18 2009 to Wed Jan 14 10:30:18 2009]

Last 1 Hour



Time [Wed Jan 14 10:20:18 2009 to Wed Jan 14 11:20:18 2009]

Figure 4.7: Network Load Statistics (Experimental)

Table 4.10 Remote to Local Traffic (Experimental)

IP Protocol	Data	Percentage
TCP vs. UDP	44.4 GB	TCP 96.2 % / UDP 3.8 %

TCP/UDP Protocol	Data	Percentage
FTP	43.4 MB	0%
PROXY	30.2 MB	0%
HTTP	11.1 GB	25.0%
DNS	612.6 MB	1.3%
Telnet	14.2 MB	0%
NBios-IP	5.4 KB	0%
Mail	35.6 MB	0%
SNMP	6.9 MB	0%
NEWS	112.4 KB	0%
DHCP-BOOTP	131.7 KB	0%
NFS	8.9 MB	0%
X11	2.2 MB	0%
SSH	32.0 KB	0%
Gnutella	13.4 MB	0%
Kazaa	7.6 MB	0%
WinMX	2.9 KB	0%
eDonkey	30.9 MB	0%
Messenger	36.0 MB	0%
Other IP-based Protocols	32.5 GB	73.1%

4.7 Observations

From Table 4.10 and Figure 4.7, it was observed that:

1. By denying access to Internet mails and other facilities on those sites alone, bandwidth usage on the network dropped considerably which definitely translates into faster browsing speed.

2. The percentage of the HTTP traffic also dropped drastically to 25%. This also confirms that most of the HTTP traffic generated on the network are either

3. When the Denial of Service (DoS) was removed the bandwidth consumption on the network rose to about 95% within a few minutes.

4.8 Summary of results and Suggestions

The data collected from ntop clearly indicated two major IP traffic on the university network, the HTTP traffic and another termed 'other IP protocol' a closer look on the whole network traffic shows that the constituents of the two major IP traffic are mostly not relevant to academic and research purposes. A random hourly experiment was then carried out blocking all internet mail sites including the instant messengers on those sites. These showed a sharp decline in the traffic and bandwidth consumption on the network.

It is suggested access to free email sites be blocked during work hours, the official university email should be used during this period. An FTP server should be deployed on the network and all download request should be redirected to the ftp server. Provision should be made to have all a network antivirus and Microsoft update servers such that all individual system update can be done through the update servers, while the servers will be configured to download updates in the night.

CHAPTER FIVE

RECOMMENDATIONS AND CONCLUSION

5.0 Introduction

The installation, configuration and analysis of IP traffic on the University network is very crucial to help in making informed decisions and proper management of the university network, such that the expensive and limited bandwidth can be used maximally for the majorly academic purposes.

5.1 Limitations

Due to cost of software license and durability, open source software was chosen to carry out this research, this However, it requires a lot of understanding and support to be able to install and configure the monitoring server

The Software (ntop) could not store data for a long period and most often data is reset whenever the system shuts down. This requires that data be taken and stored elsewhere on daily basis.

The server was configured on a university live network , this limits the period of time the experimental configuration of DoS could be allowed on the network.

5.2. Conclusion

To be able to achieve the desired goal of paying a large sum of money for bandwidth by the university management which is mainly for academic and research purposes some measures need to be put in place to check unwanted traffic on the network. It should however be noted that while such denials are put in place some (though very few) activities may also be affected but can always be resolved when they are noticed.

Some sites that are not of high priority for academic activities are recommended to be allowed on the university network between 5pm and 9am. Access to such sites like yahoo, Microsoft, Avast, grisoft should be denied during the hours of 9am and 4pm.

The university mail should be the official e-mail for all university community members. This will reduce the use of free mail boxes like yahoo, hotmail, gmail etc.

Software download should be denied on the university site except on special request, alternative arrangement can be made to have an ftp server where regularly downloaded software can be kept for download on the university network.

A Microsoft update server may be installed on the university network where all Microsoft update traffic will be redirected for updates.

The university management may also need to adopt a good and light weight antivirus to be used on the university network; this will allow the university to make an arrangement for a network update of such antivirus.

5.3 Suggestion for Further Work

It is suggested that a further research may be carried out on how to compress ntop data automatically so that the data can be stored for a long period.
This will further help to make informed decision when trying to put in place measures to manage a campus network and reduce congestion.

References

1. "Bandwidth Management" http://en.wikipedia.org/wiki/Bandwidth_management
2. Greaves, D.(2008), "Making Strategic Decisions about Bandwidth", e/Merger 2008 South Africa
3. "Info Vista(April 2008) Intelsat monitoring system Itsdvb.fus.idr.14 inbound 2008
4. "ntop Man page" http://www.ntop.org
5. "History of the Internet" http://www.walthowe.com/navnet/history.html
6. Hunt, C. (2002), TCP/IP Network Administration, 3. ed, O'Reilly Inc
7. Ziwicky, E.D (2000), Building Internet Firewalls, 2. ed O'Reilly Inc 2000
8. E.E. Mohamed, H. Abdel-Wahab, I. Salama, "Multicast address management in the Internet: a study of the port blocking problem," *aiccsa*, pp. 74-I, ACS/IEEE 2005
9. "Ntop Network Monitoring Guide" Mukom Akong Tamon http://Techowto.wordpress.com
10. Luca D et.al(2000) " Improving Network Security using Ntop", RAID 2000 Toulouse, France
11. Report created on Mon Jul 7 12:07:56 2008[ntop uptime:3:07:21] Generated by ntop v.3.2 [i686-pc-linux-gnu]
12. Report created on Tue Aug 26 13:06:06 2008 [ntop uptime: 21:05:16] Generated by ntop v.3.3.7 [i686-pc-linux-gnu]
13. Flickenger, R et.al (2006), How to Accelerate your Internet.
14. Report created on Mon Jan 12 11:29:33 2009 [ntop uptime: 2 days 20:21:27] Generated by ntop v.3.3.7 [i686-pc-linux-gnu]

15. Report created on Wed Jan 14 14:06:25 2009 [ntop uptime: 2 days 4:54:04] Generated by ntop v.3.3.7 [i686-pc-linux-gnu]
16. Cisco Router Documentation (1998), Cisco press.
17. Wade Edwards, et.al (2005) CCNP complete Study Guide. Sybex Inc.
18. Todd Lammle (2005) CCNA Study guide 5.ed Sybex Inc.
19. 3 COM Corporation (2001)Understanding IP Addressing
20. Teare, Diane (July 1999) Designing Cisco Networking. Cisco Press.
21. Ravi Kumar Paluri, http://www.buzzle.com/editorials/8-24-2004-58325.asp
22. (http://www.livinginternet.com/i/ii_summary.htm)
23. Internetworking Technology Handbook
24. F.Saffre, C.Holie & M.Shackleton ,Bandwidth Management for the people, BT Technology Journal Vol23 No 2 April 2005
25. A.M.G Soto, S.S Macias , Bandwidth Growth Forecasting , Internet and Information Technology November 2003
26. Mirkalkak ,M. Scult,N, Thomson D ,Dynamic Bandwidth Management and Adaptive applications ,Selected Areas in Communications, IEE Journal Vol19,Issue 10 October 2001.
27. Devi, B.B.; Differential Availability & Bandwidth Management**,** Military Communications Conference, 2006. MILCOM 2006 ,23-25 Oct. 2006
28. Cidon, I.; Gopal, I.; Guerin, R.; Bandwidth management and congestion control in planet Communications Magazine, IEEE Volume 29, Issue 10, Oct. 1991
29. Irvin, D.R.; The role of customer-premises bandwidth management Network, IEEE Volume 8, Issue 3, May-June 1994
30. D. Sarkar, U.K. Sarkar, and G. Peng , Bandwidth Requirement of Links in Hierarchical caching network. International Journal of computers and applications , Vol 29 2007

31. Bateman, P.(2005), “Bandwidth Connectivity & Management” Frontiers of Knowledge, University Leaders’ forum, Cape town South African(Nov 19-21)
32. Gwynne, S(2006),”The Importance of Bandwidth management and Optimization in research and education institutions “International Network for Availability of Scientific Publications (INASP), IAP Workshop, Dakar Senegal(30-31 Jan 2006).
33. Cheah, K.L.; Cheng, T.H.; Oh, S.H.;Improving the performance of a dynamic bandwidth management scheme Teletraffic. 11th. Performance Engineering in Telecommunications Networks. IEE Eleventh UK 23-25 Mar 1994
34. Wilson, B.J.; Doverspike, R.D.;A network control architecture for bandwidth management.Communications, 1992. ICC 92, Conference record, SUPERCOMM/ICC '92, discovering a New World of Communications. IEEE International Conference 14-18 June 1992

Appendix A.

Table A1: Network Traffic [All Protocols]: Remote Hosts - Data Sent



Hosts: [All] [Local Only] [**Remote Only**]

Data: [All] [**Sent Only**] [Received Only]

Host	Domain	Data		TCP	UDP	ICMP	ICMPv6	DLC	IPX	Decnet	(R)ARP
00146cffc8b3.cpe.persona.ca		215	0.0 %	152	63	0	0	0	0	0	0
058177252096.ctinets.com		458	0.0 %	0	458	0	0	0	0	0	0
084202202129.customer.alfanett.no		8.1 KB	0.0 %	8.1 KB	0	0	0	0	0	0	0
089-100-018014.ntlworld.ie		1.4 KB	0.0 %	0	1.4 KB	0	0	0	0	0	0
0x50c4ef91.odnxx3.dynamic.dsl.tele.dk		4.6 KB	0.0 %	4.6 KB	0	0	0	0	0	0	0
115.102.189.72.cfl.res.rr.com		3.5 KB	0.0 %	3.5 KB	0	0	0	0	0	0	0
12-215-255-168.client.mchsi.com		215	0.0 %	152	63	0	0	0	0	0	0
121.243.252.248.static-bangalore.vsnl.net.in		100	0.0 %	100	0	0	0	0	0	0	0
122-116-113-219.hinet-ip.hinet.net		884	0.0 %	884	0	0	0	0	0	0	0
122-57-7-136.jetstream.xtra.co.nz		1.1 KB	0.0 %	1.1 KB	0	0	0	0	0	0	0
122.54.163.161.pldt.net		100	0.0 %	100	0	0	0	0	0	0	0
123.167.189.72.cfl.res.rr.com		12.6 KB	0.0 %	11.1 KB	1.5 KB	0	0	0	0	0	0
125.24.189.245.adsl.dynamic.totbb.net		152.0 KB	0.0 %	152.0 KB	0	0	0	0	0	0	0
125.25.60.96.adsl.dynamic.totbb.net		780	0.0 %	780	0	0	0	0	0	0	0
131-180.96-97.tampabay.res.rr.com		1.0 KB	0.0 %	1.0 KB	0	0	0	0	0	0	0
158-8-41-200.elsitio.com		2.1 KB	0.0 %	2.1 KB	0	0	0	0	0	0	0
162.red-83-55-3.dynamicip.rima-tde.net		2.5 KB	0.0 %	2.5 KB	0	0	0	0	0	0	0
169.40.189.72.cfl.res.rr.com		9.9 KB	0.0 %	5.1 KB	4.8 KB	0	0	0	0	0	0
170-136.207-68.elmore.res.rr.com		40	0.0 %	0	40	0	0	0	0	0	0
173-16-1-59.client.mchsi.com		92	0.0 %	0	92	0	0	0	0	0	0
173-23-255-178.client.mchsi.com		152	0.0 %	152	0	0	0	0	0	0	0
173-25-1-207.client.mchsi.com		129	0.0 %	0	129	0	0	0	0	0	0
174-151-98-1.pools.spcsdns.net		1.4 KB	0.0 %	1.4 KB	0	0	0	0	0	0	0
189-18-132-206.dsl.telesp.net.br		131	0.0 %	0	131	0	0	0	0	0	0
189-95-58-92.3g.claro.net.br		624	0.0 %	624	0	0	0	0	0	0	0

189250311125.user.veloxzone.com.br		4.6 KB	0.0 %	4.6 KB	0	0	0	0	0	0	0
189250942l0.user.veloxzone.com.br		205	0.0 %	0	205	0	0	0	0	0	0
190-174-215-177.speedy.com.ar		80	0.0 %	0	80	0	0	0	0	0	0
190-82-43-18.adsl.tie.cl		117.1 KB	0.0 %	116.0 KB	1.0 KB	0	0	0	0	0	0
196-200-123.accelonafrica.com		33.3 KB	0.0 %	33.3 KB	0	0	0	0	0	0	0
201-048-002-017.static.ctbctelecom.com.br		25.9 KB	0.0 %	21.4 KB	4.5 KB	0	0	0	0	0	0
201008052226.user.veloxzone.com.br		252	0.0 %	0	252	0	0	0	0	0	0
20129015232.user.veloxzone.com.br		29.4 KB	0.0 %	29.3 KB	40	0	0	0	0	0	0
208-117-60-128.block5.gvtc.com		612	0.0 %	0	612	0	0	0	0	0	0
209-59-108-070.candw.ag		1.1 KB	0.0 %	1.1 KB	0	0	0	0	0	0	0
210-210.amazon.com		727	0.0 %	727	0	0	0	0	0	0	0
210.91.233.72.static.reverse.ltdomains.com		65.7 KB	0.0 %	65.7 KB	0	0	0	0	0	0	0
216-15-66-65.c3-0.smt-ubr2.atw-smt.pa.cable.rcn.com		9.0 KB	0.0 %	8.9 KB	40	0	0	0	0	0	0
220-128-108-241.hinet-ip.hinet.net		2.1 KB	0.0 %	0	2.1 KB	0	0	0	0	0	0
229-152.186-72.tampabay.res.rr.com		101	0.0 %	0	101	0	0	0	0	0	0
232.red-79-146-4.staticip.rima-tde.net		131	0.0 %	0	131	0	0	0	0	0	0
24-158-228-37.dhcp.leds.al.charter.com		2.1 KB	0.0 %	2.1 KB	0	0	0	0	0	0	0
24-216-176-120.dhcp.stls.mo.charter.com		124	0.0 %	0	124	0	0	0	0	0	0
24.red-88-17-54.dynamicip.rima-tde.net		137	0.0 %	0	137	0	0	0	0	0	0
242.74.32.216.static.reverse.ltdomains.com		40.5 KB	0.0 %	40.5 KB	0	0	0	0	0	0	0
242694hfc227.tampabay.res.rr.com		215	0.0 %	152	63	0	0	0	0	0	0
252m08.oasis.mediatti.net		126	0.0 %	0	126	0	0	0	0	0	0
32.82.344a.static.theplanet.com		1.8 KB	0.0 %	1.8 KB	0	0	0	0	0	0	0
38-216.104-92.cust.bluewin.ch		232	0.0 %	232	0	0	0	0	0	0	0
42.223.118.66.brainstorminternet.net		142.4 KB	0.0 %	0	142.4 KB	0	0	0	0	0	0
46-89.62-81.cust.bluewin.ch		109.0 KB	0.0 %	109.0 KB	0	0	0	0	0	0	0
48-245.127-70.tampabay.res.rr.com		63	0.0 %	0	63	0	0	0	0	0	0
53511c22.cable.casema.nl		17.5 KB	0.0 %	17.5 KB	0	0	0	0	0	0	0
58.69.103.101.pldt.net		152	0.0 %	152	0	0	0	0	0	0	0
59-158.96-97.tampabay.res.rr.com		3.0 KB	0.0 %	2.6 KB	402	0	0	0	0	0	0
5ac23ee8.bb.sky.com		3.7 KB	0.0 %	3.7 KB	0	0	0	0	0	0	0
5ad25689.bb.sky.com		1.6 KB	0.0 %	0	1.6 KB	0	0	0	0	0	0
60-242-255-173.static.tpgi.com.au		131	0.0 %	0	131	0	0	0	0	0	0
62-50-226-41.client.stsn.net		143	0.0 %	143	0	0	0	0	0	0	0
63-226-5-2.dia.static.qwest.net		255.7 KB	0.0 %	255.7 KB	0	0	0	0	0	0	0
63-226-5-3.dia.static.qwest.net		522.5 KB	0.0 %	522.5 KB	0	0	0	0	0	0	0
64-130-216-50.static-ip.ravand.ca		1.8 KB	0.0 %	1.8 KB	0	0	0	0	0	0	0
66-168-87-182.dhcp.kgpt.tn.charter.com		101	0.0 %	0	101	0	0	0	0	0	0

66-199-250-170.reverse.ezzi.net		37.0 KB	0.0 %	36.3 KB	714	0	0	0	0	0	0
66-214-108-208.dhcp.nlto.ca.charter.com		215	0.0 %	152	63	0	0	0	0	0	0
69.59.152.188.servepath.com		226	0.0 %	226	0	0	0	0	0	0	0
69.59.163.42.servepath.com		263.2 KB	0.0 %	263.2 KB	0	0	0	0	0	0	0
71-83-196-38.dhcp.snbr.ca.charter.com		2.6 KB	0.0 %	1.5 KB	1.1 KB	0	0	0	0	0	0
72-53-119-216.g-net.net		3.6 KB	0.0 %	3.6 KB	0	0	0	0	0	0	0
74-138-43-140.dhcp.insightbb.com		1.3 KB	0.0 %	0	1.3 KB	0	0	0	0	0	0
75-107-223-208.cust.wildblue.net		323.9 KB	0.0 %	323.9 KB	0	0	0	0	0	0	0
75-128-199-120.dhcp.fdul.wi.charter.com		14.3 KB	0.0 %	14.3 KB	0	0	0	0	0	0	0
75-39-184-199.lightspeed.dllstx.sbcglobal.net		35.5 KB	0.0 %	35.4 KB	70	0	0	0	0	0	0
76-241-41-38.lightspeed.ltrkar.sbcglobal.net		624	0.0 %	624	0	0	0	0	0	0	0
77-101-173-2.cable.ubr05.camd.blueyonder.co.uk		71.5 KB	0.0 %	71.5 KB	67	0	0	0	0	0	0
77-103-89-100.cable.ubr18.live.blueyonder.co.uk		152	0.0 %	152	0	0	0	0	0	0	0
77-232-85-174.static.servage.net		17.5 KB	0.0 %	17.5 KB	0	0	0	0	0	0	0
77-96-138-46.cable.ubr11.pres.blueyonder.co.uk		100	0.0 %	100	0	0	0	0	0	0	0
78-21-216-155.access.telenet.be		4.9 KB	0.0 %	4.9 KB	0	0	0	0	0	0	0
78-21-90-249.access.telenet.be		95.4 KB	0.0 %	94.6 KB	774	0	0	0	0	0	0
79-117-127-198.rdsnet.ro		7.7 KB	0.0 %	7.7 KB	0	0	0	0	0	0	0
79-126-30-140.dynamic.mts-nn.ru		571	0.0 %	0	571	0	0	0	0	0	0
80-239-200-102.customer.teliacarrier.com		782	0.0 %	0	782	0	0	0	0	0	0
80-239-200-103.customer.teliacarrier.com		68	0.0 %	0	68	0	0	0	0	0	0
80-239-200-104.customer.teliacarrier.com		340	0.0 %	0	340	0	0	0	0	0	0
80-239-200-105.customer.teliacarrier.com		102	0.0 %	0	102	0	0	0	0	0	0
80-239-200-106.customer.teliacarrier.com		442	0.0 %	0	442	0	0	0	0	0	0
82-135-158-21.ip.ignet.lt		77.0 KB	0.0 %	76.3 KB	707	0	0	0	0	0	0
82-141-153-194.netra.hu		593	0.0 %	0	593	0	0	0	0	0	0
82-46-184-123.cable.ubr03.perr.blueyonder.co.uk		163	0.0 %	100	63	0	0	0	0	0	0
82.131.219.8.pool.invitel.hu		44.5 KB	0.0 %	43.8 KB	703	0	0	0	0	0	0
85-132-208-131-eth2-gwfm4-user.802.cz		205	0.0 %	0	205	0	0	0	0	0	0
85-92-200-253.bis-internet.co.uk		539	0.0 %	539	0	0	0	0	0	0	0
85.131.96.66.static.eigbox.net		349.0 KB	0.0 %	349.0 KB	0	0	0	0	0	0	0
86-122-241-13.rdsnet.ro		131	0.0 %	0	131	0	0	0	0	0	0
86-44-105-103-dynamic.b-ras2.bbh.dublin.eircom.net		1.1 KB	0.0 %	1.1 KB	0	0	0	0	0	0	0
88-107-170-18.dynamic.dsl.as9105.com		278	0.0 %	152	126	0	0	0	0	0	0
89-178-29-52.broadband.corbina.ru		676	0.0 %	676	0	0	0	0	0	0	0
89.46.72.125.broad.xn.gh.dynamic.163data.com.cn		580	0.0 %	0	580	0	0	0	0	0	0
90.85-87-138.dynamic.clientes.euskaltel.es		6.1 KB	0.0 %	6.1 KB	0	0	0	0	0	0	0
91-67-96-49-dynip.superkabel.de		1.1 KB	0.0 %	1.1 KB	0	0	0	0	0	0	0

92-108-10-42.dynamic.upc.nl		125.0 KB	0.0 %	124.9 KB	67	0	0	0	0	0	0
97-113-93-130.tukw.qwest.net		14.9 KB	0.0 %	12.2 KB	2.7 KB	0	0	0	0	0	0
97-120-59-154.ptld.qwest.net		945	0.0 %	945	0	0	0	0	0	0	0
97-86-38-13.dhcp.stpt.wi.charter.com		5.9 KB	0.0 %	0	5.9 KB	0	0	0	0	0	0
a.tribalfusion.com		18.0 KB	0.0 %	18.0 KB	0	0	0	0	0	0	0
a.tribalfusion.com		103.8 KB	0.0 %	103.8 KB	0	0	0	0	0	0	0
a.tribalfusion.com		134.6 KB	0.0 %	134.6 KB	0	0	0	0	0	0	0
a.www.eset.sk		89.4 KB	0.0 %	89.4 KB	0	0	0	0	0	0	0
a17-112-152-32.apple.com		9.2 KB	0.0 %	9.2 KB	0	0	0	0	0	0	0
a638sm.avast.com		159	0.0 %	0	0	159	0	0	0	0	0
a645sm.avast.com		8.8 KB	0.0 %	0	0	8.8 KB	0	0	0	0	0
a646sm.avast.com		962	0.0 %	0	0	962	0	0	0	0	0
a88-112-251-79.elisa-laajakaista.fi		4.9 KB	0.0 %	4.9 KB	0	0	0	0	0	0	0
a88-114-41-170.elisa-laajakaista.fi		9.9 KB	0.0 %	9.8 KB	52	0	0	0	0	0	0
a903sm.avast.com		24.9 KB	0.0 %	24.9 KB	0	0	0	0	0	0	0
a909sm.avast.com		35.3 KB	0.0 %	35.3 KB	0	0	0	0	0	0	0
a921sl.avast.com		172	0.0 %	0	0	172	0	0	0	0	0
a923sl.avast.com		654	0.0 %	654	0	0	0	0	0	0	0
a934sm.avast.com		6.3 KB	0.0 %	6.3 KB	0	0	0	0	0	0	0
a936sm.avast.com		1.2 KB	0.0 %	1.2 KB	0	0	0	0	0	0	0
a938sm.avast.com		5.9 KB	0.0 %	5.9 KB	0	0	0	0	0	0	0
a940sm.avast.com		304	0.0 %	0	0	304	0	0	0	0	0
a955sl.avast.com		160	0.0 %	0	0	160	0	0	0	0	0
a96-6-150-212.deploy.akamaitechnologies.com		1.5 KB	0.0 %	1.5 KB	0	0	0	0	0	0	0
a96-6-178-10.deploy.akamaitechnologies.com		30.4 KB	0.0 %	30.4 KB	0	0	0	0	0	0	0
a96-6-178-151.deploy.akamaitechnologies.com		134.8 KB	0.0 %	134.8 KB	0	0	0	0	0	0	0
a96-6-178-199.deploy.akamaitechnologies.com		920	0.0 %	920	0	0	0	0	0	0	0
a96-6-178-70.deploy.akamaitechnologies.com		75.6 KB	0.0 %	75.6 KB	0	0	0	0	0	0	0
a96-6-179-91.deploy.akamaitechnologies.com		4.6 KB	0.0 %	4.6 KB	0	0	0	0	0	0	0
a963sl.avast.com		70.2 KB	0.0 %	70.2 KB	0	0	0	0	0	0	0
a973sm.avast.com		5.1 KB	0.0 %	5.1 KB	0	0	0	0	0	0	0
a977sm.avast.com		366	0.0 %	366	0	0	0	0	0	0	0
a980sm.avast.com		129	0.0 %	0	0	129	0	0	0	0	0
aaqj155.neoplus.adsl.tpnet.pl		888	0.0 %	0	888	0	0	0	0	0	0
ac81ce60.ipt.aol.com		421	0.0 %	421	0	0	0	0	0	0	0
ad1.rtm-1.vip.rm.ac4.yahoo.com		2.3 MB	0.0 %	2.3 MB	0	0	0	0	0	0	0
ad2.rtm-1.vip.rm.ac4.yahoo.com		329.4 KB	0.0 %	329.4 KB	0	0	0	0	0	0	0
ad3.rtm-1.vip.rm.ac4.yahoo.com		1.0 MB	0.0 %	1.0 MB	0	0	0	0	0	0	0

address2.pim.vip.mud.yahoo.com		528.9 KB	0.0 %	528.9 KB	0	0	0	0	0	0	0
adfarm.mediaplex.com		5.9 KB	0.0 %	5.9 KB	0	0	0	0	0	0	0
ads.gsmarena.com		146.3 KB	0.0 %	146.3 KB	0	0	0	0	0	0	0
ads.nyx.adbrite.com		12.4 KB	0.0 %	12.4 KB	0	0	0	0	0	0	0
ads.valueclick.net		5.0 KB	0.0 %	5.0 KB	0	0	0	0	0	0	0
adserver2.adtech.de		1.6 KB	0.0 %	1.6 KB	0	0	0	0	0	0	0
adsl-17-227-139.jax.bellsouth.net		10.2 KB	0.0 %	10.2 KB	0	0	0	0	0	0	0
adsl-65-65-223-222.dsl.rcsntx.swbell.net		910	0.0 %	0	910	0	0	0	0	0	0
adsl-69-105-56-87.dsl.irvnca.pacbell.net		367	0.0 %	304	63	0	0	0	0	0	0
adsl-69-221-113-244.dsl.akrnoh.ameritech.net		124	0.0 %	0	124	0	0	0	0	0	0
adsl-69-224-37-29.dsl.irvnca.pacbell.net		101	0.0 %	0	101	0	0	0	0	0	0
adsl-dyn26.91-127-116.t-com.sk		13.2 KB	0.0 %	13.2 KB	0	0	0	0	0	0	0
afontenayssb-152-1-5-80.w82-121.abo.wanadoo.fr		128.5 KB	0.0 %	128.4 KB	60	0	0	0	0	0	0
blackcollegereunion.org		1.0 KB	0.0 %	1.0 KB	0	0	0	0	0	0	0
blk-215-90-188.eastlink.ca		152	0.0 %	152	0	0	0	0	0	0	0
bnc.82110clan.de		144	0.0 %	144	0	0	0	0	0	0	0
bs1.ads.vip.ac4.yahoo.com		32.6 KB	0.0 %	32.6 KB	0	0	0	0	0	0	0
bs1b1.ads.vip.re2.yahoo.com		2.2 MB	0.0 %	2.2 MB	0	0	0	0	0	0	0
btv89201100236.btv.lv		295	0.0 %	0	295	0	0	0	0	0	0
by1msg2275507.phx.gbl		8.1 KB	0.0 %	8.1 KB	0	0	0	0	0	0	0
bzq-82-80-230-133.cablep.bezeqint.net		191.9 KB	0.0 %	191.9 KB	0	0	0	0	0	0	0
c-67-182-99-12.hsd1.ca.comcast.net		3.0 KB	0.0 %	0	3.0 KB	0	0	0	0	0	0
c-68-49-171-181.hsd1.va.comcast.net		136.1 KB	0.0 %	134.6 KB	1.5 KB	0	0	0	0	0	0
c-68-58-24-246.hsd1.in.comcast.net		101.2 KB	0.0 %	95.9 KB	5.3 KB	0	0	0	0	0	0
c-68-58-250-133.hsd1.sc.comcast.net		152	0.0 %	152	0	0	0	0	0	0	0
c-68-61-206-193.hsd1.mi.comcast.net		1.8 KB	0.0 %	1.8 KB	0	0	0	0	0	0	0
c-68-82-160-176.hsd1.nj.comcast.net		215	0.0 %	152	63	0	0	0	0	0	0

Note: These counters do not include broadcasts and will not equal the 'Global Protocol Distribution'

[1 / 8]

NOTE: Click here for more information about host and domain sorting.

Report created on Mon Jan 12 11:29:33 2009 [ntop uptime: 2 days 20:21:27]

Generated by ntop v.3.2 SourceForge .tgz [i686-pc-linux-gnu]

© 1998-2005 by Luca Deri, built: May 21 2007 17:35:55.

Listening on [eth0,NetFlow-device.2] for all packets (i.e. without a filtering expression)

Web reports include only interface "NetFlow-device.2"

Table A2: TCP/UDP: Local Protocol Usage

Reporting on actual traffic for 2620 host(s) on 49 service port(s)

Service		Clients	Servers
0	0	• 10.0.0.71	• 10.0.0.71
tcpmux	1	• 10.0.0.81	• 10.0.0.81
3	3	• 10.0.0.13	• 10.0.0.13
5	5	• 10.5.7.249	• 10.5.7.249
12	12	• 10.0.0.81	• 10.0.0.81
daytime	13	• 192.168.7.55 • 10.0.0.141	• 192.168.7.55 • 10.0.0.141
netstat	15	• 10.0.0.81	• 10.0.0.81
ftp-data	20	• 10.2.0.20 • 10.0.0.71 • 10.0.0.81 • 10.0.0.193 • 10.3.75.181	• 10.2.0.20 • 10.0.0.71 • 10.0.0.81 • 10.0.0.193 • 10.3.75.181
ftp	21	• 192.168.4.85 • 10.0.0.13 • 10.2.0.20 • 10.0.0.81 • 10.0.0.193 • 10.2.38.61 • 10.3.40.13	• 192.168.4.85 • 10.0.0.13 • 10.2.0.20 • 10.0.0.81 • 10.0.0.193 • 10.2.38.61 • 10.3.40.13
ssh	22	• 10.0.0.81	• 10.0.0.81
telnet	23	• 192.168.7.29 • 10.0.0.141 • 10.0.0.193 • 10.5.13.27 • 10.2.38.53	• 192.168.7.29 • 10.0.0.141 • 10.0.0.193 • 10.5.13.27 • 10.2.38.53

		• 10.2.94.206	• 10.2.94.206
smtp	25	• 10.2.0.20 • 10.0.0.71 • 10.0.0.81 • 10.0.0.141 • 10.0.0.193 • 10.5.13.26 • 10.2.38.53 • 10.2.38.61	• 10.2.0.20 • 10.0.0.71 • 10.0.0.81 • 10.0.0.141 • 10.0.0.193 • 10.5.13.26 • 10.2.38.53 • 10.2.38.61
time	37	• 192.168.8.16 • 192.168.8.220 • 10.5.4.250 • 10.5.7.27 • 10.5.7.23 • 10.5.7.249 • 10.2.0.20 • 10.0.0.81 • 10.0.0.141 • 10.0.0.193 • 10.5.11.30 • 10.2.54.98 • 10.3.75.249 • 10.10.100.18 • 10.10.100.15	• 192.168.8.16 • 192.168.8.220 • 10.5.4.250 • 10.5.7.27 • 10.5.7.23 • 10.5.7.249 • 10.2.0.20 • 10.0.0.81 • 10.0.0.141 • 10.0.0.193 • 10.5.11.30 • 10.2.54.98 • 10.3.75.249 • 10.10.100.18 • 10.10.100.15
47	47	• 10.0.0.13	• 10.0.0.13
domain	53	• 10.2.23.250 • 192.168.5.30 • 192.168.7.47 • 192.168.8.17 • 192.168.8.22 • 192.168.8.220 • 192.168.8.195 • 10.5.4.250 • 10.5.5.14 • 10.5.5.4 • 10.5.7.27 • 10.5.7.23	• 10.2.23.250 • 192.168.5.30 • 192.168.7.47 • 192.168.8.17 • 192.168.8.22 • 192.168.8.220 • 192.168.8.195 • 10.5.4.250 • 10.5.5.14 • 10.5.5.4 • 10.5.7.27 • 10.5.7.23

		• 10.5.7.21 • 10.5.7.36 • 10.5.7.249 • 10.0.0.1 • 10.0.0.13 • 10.0.0.15 • bigbrother • ftp • nis-portal • 10.0.0.29 • 10.0.0.43 • 10.0.0.71 • 10.0.0.74 • 10.0.0.81 • 10.0.0.129 • 10.0.0.138 • 10.0.0.141 • 10.0.0.147 • 10.0.0.193 • 10.5.12.35 • 10.5.12.32 • 10.5.12.252 • 10.5.13.26 • 10.5.13.27 • 10.5.13.30 • 10.5.13.32 • 10.5.13.38 • 10.5.13.37 • 10.5.13.51 • 10.3.13.250 • 10.2.14.65 • 10.3.14.151 • 10.5.11.30 • 10.2.54.51 • 10.2.54.56 • 10.2.54.79 • 10.2.54.98 • 10.3.40.14 • 10.3.40.13 • 10.3.40.22 • 10.3.40.17 • 10.3.40.36	• 10.5.7.21 • 10.5.7.36 • 10.5.7.249 • 10.0.0.1 • 10.0.0.13 • 10.0.0.15 • bigbrother • ftp • nis-portal • 10.0.0.29 • 10.0.0.43 • 10.0.0.71 • 10.0.0.74 • 10.0.0.81 • 10.0.0.129 • 10.0.0.138 • 10.0.0.141 • 10.0.0.147 • 10.0.0.193 • 10.5.12.35 • 10.5.12.32 • 10.5.12.252 • 10.5.13.26 • 10.5.13.27 • 10.5.13.30 • 10.5.13.32 • 10.5.13.38 • 10.5.13.37 • 10.5.13.51 • 10.3.13.250 • 10.2.14.65 • 10.3.14.151 • 10.5.11.30 • 10.2.54.51 • 10.2.54.56 • 10.2.54.79 • 10.2.54.98 • 10.3.40.14 • 10.3.40.13 • 10.3.40.22 • 10.3.40.17 • 10.3.40.36

		• 10.3.40.51 • 10.3.40.65 • 10.3.40.74 • 10.3.40.87 • 10.3.40.90 • 10.3.40.91 • 10.3.40.89 • 10.3.40.102 • 10.3.40.99 • 10.3.40.97 • 10.3.40.114 • 10.2.94.15 • 10.2.94.11 • 10.2.94.206 • 10.2.95.111 • 10.2.89.245 • 10.3.67.235	• 10.3.40.51 • 10.3.40.65 • 10.3.40.74 • 10.3.40.87 • 10.3.40.90 • 10.3.40.91 • 10.3.40.89 • 10.3.40.102 • 10.3.40.99 • 10.3.40.97 • 10.3.40.114 • 10.2.94.15 • 10.2.94.11 • 10.2.94.206 • 10.2.95.111 • 10.2.89.245 • 10.3.67.235
mtp	57	• 10.0.0.81 • 10.2.54.98 • 10.3.40.97	• 10.0.0.81 • 10.2.54.98 • 10.3.40.97
bootpc	68	• 10.0.0.193	• 10.0.0.193
www	80	• 10.2.23.250 • 192.168.5.18 • 192.168.5.30 • 192.168.4.85 • 192.168.4.88 • 192.168.4.18 • 192.168.7.87 • 192.168.7.21 • 192.168.7.24 • 192.168.7.29 • 192.168.7.14 • 192.168.7.15 • 192.168.7.50 • 192.168.7.52 • 192.168.7.55 • 192.168.7.33 • 192.168.7.39	• 10.2.23.250 • 192.168.5.18 • 192.168.5.30 • 192.168.4.85 • 192.168.4.88 • 192.168.4.18 • 192.168.7.87 • 192.168.7.21 • 192.168.7.24 • 192.168.7.29 • 192.168.7.14 • 192.168.7.15 • 192.168.7.50 • 192.168.7.52 • 192.168.7.55 • 192.168.7.33 • 192.168.7.39

		• 192.168.7.40 • 192.168.7.43 • 192.168.7.47 • 192.168.8.16 • 192.168.8.17 • 192.168.8.18 • 192.168.8.22 • 192.168.8.11 • 192.168.8.220 • 192.168.8.195 • 192.168.8.224 • 10.5.4.250 • 10.5.5.14 • 10.5.5.4 • 10.5.7.27 • 10.5.7.23 • 10.5.7.21 • 10.5.7.36 • 10.5.7.249 • 10.0.0.13 • 10.0.0.15 • bigbrother • 10.0.0.71 • 10.0.0.74 • 10.0.0.81 • 10.0.0.129 • 10.0.0.138 • 10.0.0.141 • 10.0.0.193 • 10.5.12.35 • 10.5.12.32 • 10.5.12.252 • 10.5.13.26 • 10.5.13.27 • 10.5.13.30 • 10.5.13.32 • 10.5.13.38 • 10.5.13.37 • 10.5.13.51 • 10.3.13.250 • 10.2.14.65 • 10.3.14.151	• 192.168.7.40 • 192.168.7.43 • 192.168.7.47 • 192.168.8.16 • 192.168.8.17 • 192.168.8.18 • 192.168.8.22 • 192.168.8.11 • 192.168.8.220 • 192.168.8.195 • 192.168.8.224 • 10.5.4.250 • 10.5.5.14 • 10.5.5.4 • 10.5.7.27 • 10.5.7.23 • 10.5.7.21 • 10.5.7.36 • 10.5.7.249 • 10.0.0.13 • 10.0.0.15 • bigbrother • 10.0.0.71 • 10.0.0.74 • 10.0.0.81 • 10.0.0.129 • 10.0.0.138 • 10.0.0.141 • 10.0.0.193 • 10.5.12.35 • 10.5.12.32 • 10.5.12.252 • 10.5.13.26 • 10.5.13.27 • 10.5.13.30 • 10.5.13.32 • 10.5.13.38 • 10.5.13.37 • 10.5.13.51 • 10.3.13.250 • 10.2.14.65 • 10.3.14.151

		• 10.10.10.28 • 10.10.10.29 • 10.5.10.7 • 10.5.10.42 • 10.5.10.36 • 10.5.11.30 • 10.2.11.251 • 10.2.54.51 • 10.2.54.56 • 10.2.54.79 • 10.2.54.98 • 10.3.60.2 • 10.3.40.14 • 10.3.40.13 • 10.3.40.22 • 10.3.40.17 • 10.3.40.36 • 10.3.40.51 • 10.3.40.65 • 10.3.40.74 • 10.3.40.86 • 10.3.40.87 • 10.3.40.90 • 10.3.40.91 • 10.3.40.89 • 10.3.40.102 • 10.3.40.99 • 10.3.40.97 • 10.3.40.114 • 10.2.94.15 • 10.2.94.11 • 10.2.94.206 • 10.2.95.111 • 10.2.89.116 • 10.2.89.132 • 10.2.89.245 • 10.2.91.130 • 10.3.67.235 • 10.3.75.181 • 10.3.75.201 • 10.3.75.229 • 10.3.75.251	• 10.10.10.28 • 10.10.10.29 • 10.5.10.7 • 10.5.10.42 • 10.5.10.36 • 10.5.11.30 • 10.2.11.251 • 10.2.54.51 • 10.2.54.56 • 10.2.54.79 • 10.2.54.98 • 10.3.60.2 • 10.3.40.14 • 10.3.40.13 • 10.3.40.22 • 10.3.40.17 • 10.3.40.36 • 10.3.40.51 • 10.3.40.65 • 10.3.40.74 • 10.3.40.86 • 10.3.40.87 • 10.3.40.90 • 10.3.40.91 • 10.3.40.89 • 10.3.40.102 • 10.3.40.99 • 10.3.40.97 • 10.3.40.114 • 10.2.94.15 • 10.2.94.11 • 10.2.94.206 • 10.2.95.111 • 10.2.89.116 • 10.2.89.132 • 10.2.89.245 • 10.2.91.130 • 10.3.67.235 • 10.3.75.181 • 10.3.75.201 • 10.3.75.229 • 10.3.75.251

		• 10.3.75.249 • 10.10.100.20 • 10.10.100.21 • 10.10.100.17 • 10.10.100.18 • 10.10.100.19 • 10.10.100.12 • 10.10.100.14 • 10.10.100.15	• 10.3.75.249 • 10.10.100.20 • 10.10.100.21 • 10.10.100.17 • 10.10.100.18 • 10.10.100.19 • 10.10.100.12 • 10.10.100.14 • 10.10.100.15
81	81	• 10.0.0.81	• 10.0.0.81
85	85	• 10.0.0.81	• 10.0.0.81
kerberos	88	• 10.10.100.17	• 10.10.100.17
90	90	• 10.0.0.81	• 10.0.0.81
supdup	95	• 10.0.0.81	• 10.0.0.81
pop3	110	• 192.168.7.43 • 10.0.0.13 • 10.0.0.71 • 10.0.0.81 • 10.5.10.42 • 10.3.75.251	• 192.168.7.43 • 10.0.0.13 • 10.0.0.71 • 10.0.0.81 • 10.5.10.42 • 10.3.75.251
auth	113	• 10.0.0.81	• 10.0.0.81
nntp	119	• 10.2.0.20 • 10.0.0.81 • 10.0.0.193 • 10.2.38.53 • 10.3.40.87	• 10.2.0.20 • 10.0.0.81 • 10.0.0.193 • 10.2.38.53 • 10.3.40.87
ntp	123	• 192.168.7.87 • 192.168.7.52 • 192.168.7.39 • 10.5.4.250 • 10.5.5.14 • 10.5.7.23	• 192.168.7.87 • 192.168.7.52 • 192.168.7.39 • 10.5.4.250 • 10.5.5.14 • 10.5.7.23

		• 10.5.7.36 • 10.5.7.249 • 10.0.0.1 • 10.0.0.13 • bigbrother • ftp • 10.0.0.71 • 10.0.0.81 • 10.0.0.141 • 10.0.0.193 • 10.5.13.27 • 10.5.13.51 • 10.5.11.30 • 10.2.38.61 • 10.3.40.13 • 10.3.40.17 • 10.3.40.90 • 10.3.40.114 • 10.3.75.181 • 10.10.100.20	• 10.5.7.36 • 10.5.7.249 • 10.0.0.1 • 10.0.0.13 • bigbrother • ftp • 10.0.0.71 • 10.0.0.81 • 10.0.0.141 • 10.0.0.193 • 10.5.13.27 • 10.5.13.51 • 10.5.11.30 • 10.2.38.61 • 10.3.40.13 • 10.3.40.17 • 10.3.40.90 • 10.3.40.114 • 10.3.75.181 • 10.10.100.20
netbios-ns	137	• 10.5.7.36 • 10.0.0.1 • 10.0.0.13 • 10.2.54.51	• 10.5.7.36 • 10.0.0.1 • 10.0.0.13 • 10.2.54.51
412	412	• 192.168.8.16	• 192.168.8.16
shell	514	• 192.168.7.39 • 10.5.5.14 • 10.5.7.23	• 192.168.7.39 • 10.5.5.14 • 10.5.7.23
555	555	• 10.0.0.13	• 10.0.0.13
600	600	• 10.0.0.81	• 10.0.0.81
672	672	• 10.0.0.81	• 10.0.0.81
843	843	• 10.0.0.193 • 10.5.13.38	• 10.0.0.193 • 10.5.13.38

		• 10.3.36.11	• 10.3.36.11
888	888	• 10.0.0.81	• 10.0.0.81
988	988	• 10.0.0.81	• 10.0.0.81
pop3s	995	• 10.0.0.13 • 10.0.0.81 • 10.2.94.206	• 10.0.0.13 • 10.0.0.81 • 10.2.94.206
997	997	• 10.0.0.13	• 10.0.0.13
1000	1000	• 10.0.0.81	• 10.0.0.81
customs	1001	• 10.0.0.13	• 10.0.0.13
1002	1002	• 10.0.0.81	• 10.0.0.81

The color of the host link indicates how recently the host was FIRST seen

0 to 5 minutes 5 to 15 minutes 15 to 30 minutes 30 to 60 minutes 60+ minutes

---

Report created on Mon Jan 12 11:29:33 2009 [ntop uptime: 2 days 20:21:27]

Generated by ntop v.3.2 SourceForge .tgz [i686-pc-linux-gnu]

© 1998-2005 by Luca Deri, built: May 21 2007 17:35:55.

Listening on [eth0,NetFlow-device.2] for all packets (i.e. without a filtering expression)

Web reports include only interface "NetFlow-device.2"

Table A3: Last Contacted Peers

Sent To	IP Address	Received From	IP Address
64.86.71.41	64.86.71.41	64.86.71.41	64.86.71.41
www.04.05.sf2p.facebook.com	69.63.176.140	208.67.217.230	208.67.217.230
www-g.facebook.com	69.63.176.12	www.04.05.sf2p.facebook.com	69.63.176.140
www.04.07.facebook.com	69.63.180.13	64.86.71.26	64.86.71.26
208.67.217.230	208.67.217.230	www-g.facebook.com	69.63.176.12
64.86.71.64	64.86.71.64	www.04.07.facebook.com	69.63.180.13
64.86.71.26	64.86.71.26	64.86.71.64	64.86.71.64
64.86.71.43	64.86.71.43	64.86.71.43	64.86.71.43
Total Contacts	66283	**Total Contacts**	66684

Table A4: TCP/UDP Service/Port Usage

IP Service	Port	# Client Sess.	Last Client Peer	# Server Sess.	Last Server Peer
tcpmux	1	6/10.7 KB	77.166.185.12	2/280	77.166.185.12
12	12	2/4.7 KB	host97-195-dynamic.4-87-r.retail.telecomitalia.it	1/66	host97-195-dynamic.4-87-r.retail.telecomitalia.it
netstat	15	25/38.0 KB	lns-bzn-48f-62-147-150-116.adsl.proxad.net	9/943	lns-bzn-48f-62-147-150-116.adsl.proxad.net
ftp-data	20	1/52	scsb.msg.yahoo.com	1/52	scsb.msg.yahoo.com
ftp	21	78/388.5 KB	pc-221-66-86-200.cm.vtr.net	28/114.1 KB	pc-221-66-86-200.cm.vtr.net
ssh	22	164/284.2 KB	124-170-162-109.dyn.iinet.net.au	58/15.6 KB	124-170-162-109.dyn.iinet.net.au
smtp	25	306/2.2 MB	cs109.msg.mud.yahoo.com	108/12.1 KB	cs109.msg.mud.yahoo.com
time	37	11/1.4 KB	cs105.msg.mud.yahoo.com	6/624	cs105.msg.mud.yahoo.com
domain	53	8406/23.1 MB	10.0.0.1	4285/715.6 KB	10.0.0.1
mtp	57	228/854.8 KB	219.232.241.91	78/2.6 KB	219.232.241.91
www	80	1447/269.0 MB	64.86.71.64	23022/32.7 MB	64.86.71.64
81	81	71/80.2 KB	139.red-83-59-254.dynamicip.rima-tde.net	24/8.3 KB	139.red-83-59-254.dynamicip.rima-tde.net
85	85	795/1.8 MB	193.153.136.252	280/86.7 KB	193.153.136.252
90	90	82/165.2 KB	dsl212-235-34-81.bb.netvision.net.il	28/8.8 KB	dsl212-235-34-81.bb.netvision.net.il
supdup	95	3/903	85.54.239.66	1/63	85.54.239.66
pop3	110	61/132.7 KB	wc40-main.medialogik.com	21/2.1 KB	wc40-main.medialogik.com
auth	113	135/886.0 KB	32.127.191.90.dyn.estpak.ee	47/324.3 KB	32.127.191.90.dyn.estpak.ee
nntp	119	9/3.3 KB	cs127.msg.mud.yahoo.com	3/344	cs127.msg.mud.yahoo.com
ntp	123	14/13.5 KB	207.46.197.32	10/1.9 KB	207.46.197.32
154	154	3/304	85.155.237.130	1/119	85.155.237.130
snmp-trap	162	3/627	host80-57-dynamic.8-79-r.retail.telecomitalia.it	1/63	host80-57-dynamic.8-79-r.retail.telecomitalia.it

z3950	210	25/12.3 KB	188.pool85-54-37.dynamic.orange.es	9/3.0 KB	188.pool85-54-37.dynamic.orange.es
https	443	5449/21.7 MB	65.54.165.136	1855/1.8 MB	65.54.165.136
546	546	5/2.1 KB	86.52.135.103	2/182	86.52.135.103
rtsp	554	5/123.4 KB	ds87-230-83-44.dedicated.hosteurope.de	2/105	ds87-230-83-44.dedicated.hosteurope.de
600	600	3/246	83.39.51.15	1/63	83.39.51.15
672	672	2/118	77.253.122.188	1/63	77.253.122.188
888	888	4/922	84.188.100.50	2/126	84.188.100.50
988	988	3/2.0 KB	cla34-1-88-160-214-47.fbx.proxad.net	1/63	cla34-1-88-160-214-47.fbx.proxad.net
pop3s	995	72/83.3 KB	bl7-39-226.dsl.telepac.pt	25/7.2 KB	bl7-39-226.dsl.telepac.pt
1000	1000	98/183.9 KB	dsl85-106-36289.ttnet.net.tr	36/10.6 KB	dsl85-106-36289.ttnet.net.tr
1002	1002	25/14.1 KB	85.103.156.21	9/3.6 KB	85.103.156.21

Table A5: TCP/UDP - Traffic on Other Ports

Client Port	Server Port
• 43107 • 54641 • 60069 • 54643 • 54637	• 4536 • 1683 • 1684 • 4743 • 2676

Table A6: TCP/UDP Recently Used Ports

Client Port	Server Port
• 54643 • 54637 • www • 60069 • 54641	• 54637 • 54641 • 60069 • 54643 • 54770

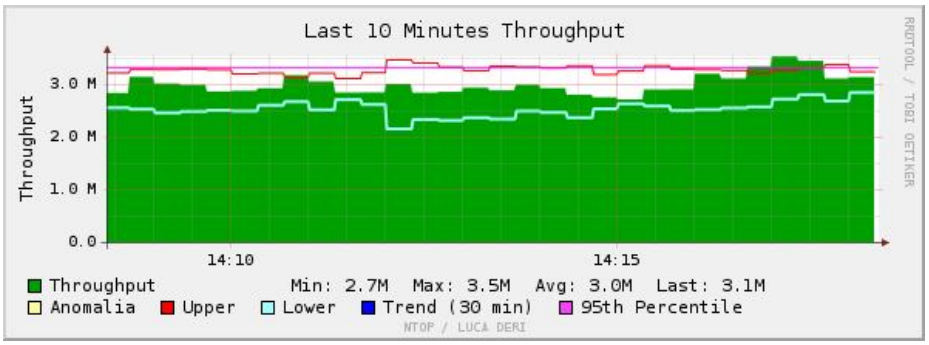
Report created on Fri Jan 9 12:34:28 2009 [ntop uptime: 12:26:23]

Generated by ntop v.3.2 SourceForge .tgz [i686-pc-linux-gnu]

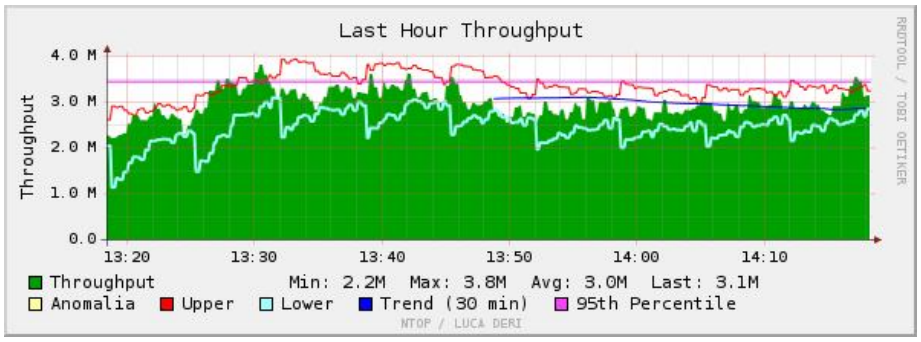
© 1998-2005 by Luca Deri, built: May 21 2007 17:35:55.

Listening on [eth0,NetFlow-device.2] for all packets (i.e. without a filtering expression)

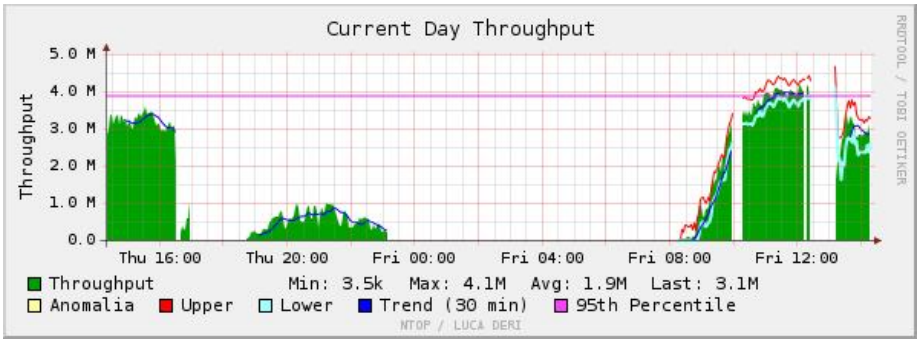
Web reports include only interface "NetFlow-device.2"



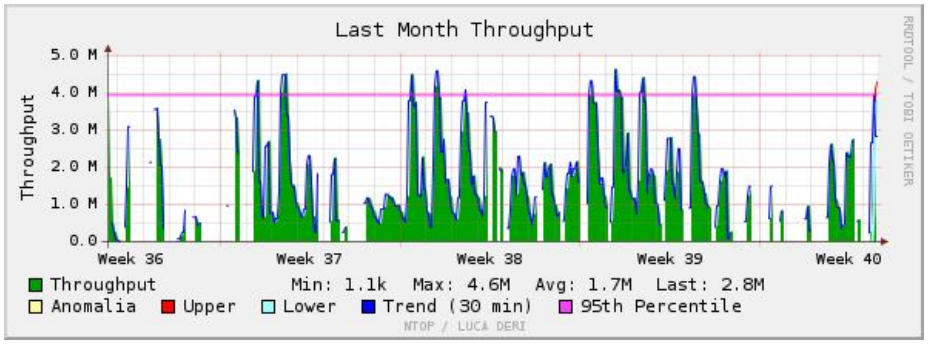
Time [Fri Oct 3 14:08:23 2008 to Fri Oct 3 14:18:23 2008]



Time [Fri Oct 3 13:18:23 2008 to Fri Oct 3 14:18:23 2008]



Time [Thu Oct 2 14:18:23 2008 to Fri Oct 3 14:18:23 2008]



Time [Wed Sep 3 14:18:23 2008 to Fri Oct 3 14:18:23 2008]

Figure A1: Network Load Statistics