Control Theory and Informatics
ISSN 2224-5774 (Paper) ISSN 2225-0492 (Online)
Vol.5, No.5, 2015
www.iiste.org

On a Packet-Wise Data Transfer Monitoring System

Brendan Ndifon F. U. Ogban
Department of Computer Science, University of Calabar, Calabar, Nigeria

Abstract
This work tends to propose a billing system that is measured by the quality of bits/bytes transfer. In order to determine the amount of network resources to be reserved, traffic and performance descriptors must be defined. Allocated resources are used only when customers send or receive traffic, whereas when customers are inactive, resources may remain unused. Network administrators clearly prefer to charge users in proportion to the reserved resources, that is to say in proportion to the *potential* use of the service. In packet-wise billing system, subscribers are bill based on the actual amount of data transferred as in terms of byte. This research was carried out at unical e-library because of their facility, the researcher designed a server which serves as the billing system, in the server which is ubuntu driven, the researcher install the radius server, PHP Admin and mysql. The reason being that the radius server will do the authentication, accounting and access control, then the researcher use the packet sniffer to retrieve packet from the network using mikrotik router to connect the server and the client computer. It was discovered that when a user tries to connect to the server, it will be requested to enter a username and password that will give him/her access to the server. With this a capture will display showing that the user was successfully logged in with it bandwidth detail on it instead of time. So with this, a user can freely enjoy the service of the internet
Keywords: reserved packets,, bandwidth, packet-wise billing system, processor clock timer, weighted fair queuing, Flat rate model.

1.0 Introduction

A cyber café is a place where internet service is provided for public use, usually for a fee. These businesses usually provide snacks and drinks, hence the café in the name. The fee for a computer is usually charged on a timer clock, whether or not any upload or download is involved. Currently, the billing system adopted by cyber cafes for internet services is based on time (processor clock timing) or induced counter timer. This timing process could be and is always a cheat to the user who may not do anything due to delays, time out, low memory, low processor speed etc and have his/her time out. Services from the net should have been measured by the volume of packets in bits/second or bytes per minutes. Since the bandwidth is a dependent factor on bytes transfer. This work tents propose a billing system that is measured by the quality of bits/bytes transfer. In order to determine the amount of network resources to be reserved, traffic and performance descriptors must be defined. Allocated resources are used only when customers send or receive traffic, whereas when customers are inactive, resources may remain unused. Network administrators clearly prefer to charge users in proportion to the reserved resources, that is to say in proportion to the *potential* use of the service. Thus, network administrators can protect themselves against unfair user behavior. On the other hand, the charge would be unfair for customers. At the same time, it is objectively difficult for users to predict their traffic rate process exactly, so that they consider it convenient to pay for the resources they actually use, rather than for estimated (and eventually overestimated) resources. Note that, in some cases, the bandwidth reserved and left unused can be re-assigned to other traffic, just as in the case of the best effort service, by means of intelligence link sharing mechanisms (e.g., the well-known Weighted Fair Queuing).

1.0.1 Background to Study

The first internet café started with the opening of the cyber café called café cyberia in London (UK) on September 1st 1994. Eva Pascoe is the founder of the internet café; she was working on her PHD at that time when she got the idea of mixing sipping coffee to surfing the web while she was sitting at one of the coffee shop near the city university in London. Café cyberia as it was formerly called started with half a dozen HP computers, connected to the internet through a dial- up modems that were to transfer data at 9.6 kilobits per second. Information and Communication Technology (ICT) development is rapidly coming up in developing countries. India for instance, has about 50,000 internet cafés and over 500,000 customers each month has compared to Nigeria. The World Wide Web (WWW) became available in Nigeria in 1996, while the full internet services became available in 1998, and the number of NCC (Nigerian Communication Commission) licensed internet services provider rose to over 150 by 2001 (Adomi, 2005). In late 2003, Nigeria had a total of 750,000 internet users and 60 users per 10,000 inhabitants representing 0.5 percent of the population (ITU, 2004). Nigeria had a total of 853,000 PCs and 0.71 PCs per 100 inhabitants as at 2003 (ITU, 2004).As a matter of fact, Adomi (2003) stated that the first cyber café in Delta state set up in 1999 and by 2001, there were nine (9) of them and by 2003, there were 18 of them. This number has increased tremendously all over Nigeria

The history of internet accessibility and use in Nigeria started in 1991 when a few pioneering groups began to offer limited e-mail services (Eshekels Associates, 2001). The internet services at that time include e-mail, telnet, and gopher. Internet users had to pay for both the access and usages for sending and receiving e-mail messages, with the billing system being based on the length of the message sent. Most of the internet services providers (ISPs) then operated a store-forward messaging system using Unix-to-Unix copy protocol (UUCP) (Adomi, 2001).Charging for network resources can also assume an important role in controlling Congestion, due to the users' sensitivity to prices. At present, the most frequently used pricing model in the Internet is the flat-rate model. According to this model, users are charged a price which does not depend on the actual use of the network resources. Even if the simplicity of this approach is one of the reasons for the wide development of the Internet, it may soon become inadequate, since it cannot be adapted to the differentiated network support. Blefari-Melazzi; et al (2003) states that 'The introduction of Quality of services creates a strong impetus to move to usage-based tariffs, where the tariff is based on the level of use of the network's resources. This, in turn, generates a requirement to meter resource use…' The flat-rate pricing policy is the most common pricing policy used to charge Internet users. This policy makes subscribers pay for accessing the network (access charge) only, independent of the amount of traffic volume exchanged. By using this approach, it is possible to consider the following alternatives: free access, connection charge (e.g. a phone call), periodical subscription fee, and periodical subscription fee plus connection charge. The flat-rate model presents some advantages. First of all, it is very simple and does not need any additional accounting architecture. Users and network managers have an accurate idea of costs and revenues, respectively. The researcher is of the opinion that, if time process (i.e. The amount of time spent online) is the means of measuring the internet services delivered by cyber café owners, then the amount of data receives/transmitted during this period should be commensurate with the time spent irrespective of the café location, provided the following factors remain constant;

- **Backhand bandwidth**: the amount of data that can be passed along a communications channel in a given period of time.
- **Electrical power**: It the bulk transfer of electrical energy, from generating power plants to electrical substations located near demand centers. This is distinct from local wiring between high voltage substations and customers, which is typically referred to as Electrical power distribution.
- **Functional computer system**: The computer should provide automatic queuing of outgoing messages pending confirmation of transmission, and of incoming messages pending their review and dispositions.

For the users of computer systems, data transmission can impose an extra dimension of complexity. A user not only must keep track of transactions with the computer, but also must initiate and monitor data exchange with other people. Users will need extra information to control data transmission, perhaps including status information about other system, and the communication links with other systems. Users will need feedback when sending or receiving data. Users may need special computer assistance in composing, storing and retrieving messages, as well as in actual data transmission. And users will wish to control the disposition of received messages, perhaps renaming message and storing it with other related messages, and/or sending it on to other users.

This is not the case as the result of other silent factors, Hence bandwidth should be measured by the volume of packets received/transmitted per unit time.

2.0 LITERATURE REVIEW

Packet switching was first proposed for military uses in the early 1960s and implemented on small networks in 1968; it became one of the fundamental networking technologies behind the internet and most local area networks. The concept of switching small blocks of data was first explored independently by Paul Baran at the RAND Corporation in the US and Donald Davies at the National Physical Laboratory (NPL) in the UK in the early to mid-1960s (Abbate, Janet, 2000). Leonard kleinrock conducted early research in queuing theory which proved important in packet switching, and published a book in the related field of digital message switching (without the packets) in 1961; he also later played a leading role in building and management of the world's first packet-switched network, the ARPANET.

Baran developed the concept of message block switching during his research at the RAND Corporation for the US Air Force into survivable communications networks, first presented to the Air Force in the summer of 1961 as briefing B-265, (Stewart, Bill, 2000) then published as RAND paper P-2626 in 1962 and then including, and expanding somewhat within a series of eleven papers titled on distributed communications in 1964. Baran's P-2626 paper described a general architecture for a large-scale, distributed, survivable communications network. The paper focuses on three key ideas: first, use of a decentralized network with multiple paths between any two points; and second, dividing complete user messages into what he called *message blocks* (later called packets); then third, delivery of these messages by store and forward switching. Baran's study made its way to Robert Taylor and J.C.R.Licklider at the Information Processing Technology Office, both wide-area network evangelists, and it helped influence Lawrence Roberts to adopt the technology when Taylor put him in charge of

development of the ARPANET. His work was similar to the research performed independently by Donald Davies at the National Physical Laboratory, UK. In 1965, Davies developed the concept of packet-switched networks and proposed development of a UK wide network. He gave a talk on the proposal in 1966, after which a person from the Ministry of Defence (MoD) told him about Baran's work. A member of Davies' team (Roger Scantlebury) met Lawrence Roberts at the 1967 ACM Symposium on Operating System Principles, bringing the two groups together. Scantlebury urged Roberts to use the highest speeds possible to reduce latency. Interestingly, Davies had chosen some of the same parameters for his original network design as Baran, such as a packet size of 1024 bits. In 1966 Davies proposed that a network should be built at the laboratory to serve the needs of NPL and prove the feasibility of packet switching. The NPL Data Communications Network entered service in 1970. Roberts and the ARPANET team took the name "packet switching" itself from Davies's work. The first computer network and packet switching network deployed for computer resource sharing was the Octopus Network at the Lawrence Livermore National Laboratory that began connecting four Control Data 6600 computers to several shared storage devices (including an IBM 2321 Data Cell in 1968 and an IBM Photo store in 1970) and to several hundred Teletype Model 33 ASR terminals for time sharing use starting in 1968 (Mendicino, Samuel, 1970). In 1973 Vint Cerf and Bob Kahn wrote the specifications for Transmission Control Protocol (TCP), an internetworking protocol for sharing resources using packet-switching among the nodes. A packet-switched network is an interconnected set of networks that are joined by routers. Each message is divided into smaller parts or packets which are routed separately using the address in their headers between nodes over data links shared with other traffic. Once all the packets forming a message arrive at the destination, they are merged together to form the original message. Unlike a circuit-switched network, which sets up a constant bit rate and constant delay connection between the two nodes for their exclusive use for the duration of the communication, a packet-switched network does not guarantee anything and packets are queued or buffered and in some cases dropped in different nodes resulting in variable delay. Packet-switched networks are also known as best-effort networks. When moving from one node to another using a data link in a packet-switched network, each packet uses the full link bandwidth. Hence it is not possible to physically divide the link between different data streams. Instead, statistical multiplexing technique, also known as dynamic bandwidth allocation method, is employed in routers to divide a physical communication channel in to an arbitrary number of logical variable bit-rate channels or data streams. There are some variants of packet-switched networks that use simple FIFO (First-In First-Out) order to advance packets through these streams. Packet switching can be categorized into datagram networks (also known as connection-less) such as Ethernet and IP networks (Internet) and virtual circuit switching (also known as connection-oriented) like ATM, X.25 and Frame relay. We will mainly consider the performance of routers in the first category i.e.in the Internet, as it is the biggest of all packet-switched networks.The simplicity of Frame Relay made it considerably faster and more cost effective than X.25 packet switching. Frame relay is a data link layer protocol, and does not provide logical addresses and routing. It is only used for "semi-permanent" connections, while X.25 connections also can be established for each communication session. Frame Relay was used to interconnect LANs or LAN segments, mainly in the 1990s by large companies that had a requirement to handle heavy telecommunications traffic across wide area network. Despite the benefits of frame relay packet switching, many international companies are staying with the X.25 standard (O'Brien, J.A & Marakas,G.M, 2009). In the United States, X.25 packet switching was used heavily in government and financial networks that use mainframe applications. Many companies did not intend to cross over to Frame Relay packet switching because it is more cost effective to use X.25 on slower networks. In certain parts of the world, particularly in Asia-Pacific and South America regions, X.25 was the only technology available (Girard. K, 1997).

2.0.1. Nomenclature

The throughput of communications links is measured in bits per second (bit/s), kilobits per second (Kbit/s), megabits per second (Mbit/s) and gigabits per second (Gbit/s). In this application, kilo, mega and giga are the standard S.I. prefixes indicating multiplication by 1,000 (kilo), 1,000,000 (mega), and 1,000,000,000 (giga).File sizes are typically measured in bytes— kilobytes, megabytes, and gigabytes being usual, where a byte is eight bits. In modern textbooks one kilobyte is defined as 1,000 byte, one megabyte as 1,000,000 byte, etc., in accordance with the 1998 International Electro technical Commission (IEC) standard. However, when Windows systems measure file size, the old computer science definition is still used, where 1 kilobyte is defined as 1,024 (or 2^{10}) bytes, which should be denoted 1 kibibyte according to IEC terminology. Similarly, a file size of 1 megabyte is 1,024 × 1,024 byte (should be called 1 mebibyte), and 1 gigabyte 1,024 × 1,024 × 1,024 byte (should be called one gibibyte). The result of all this is that a file that according to the operational system consists of 64 kilobyte data contains 64 × 1024 bytes, or 64 × 1024 × 8 bits.

2.0.2 Data Security in Packet Switching

The use of X.25 packet switching networks allows many channels to share one physical connection, and

dynamically allocates bandwidth according to the immediate demands of each channel, including call management, without denying access to other channels. The paper outlines the categories of threat to data in such corporate X.25 environments, and includes a brief statement of the major security requirements needed to meet those threats. It identifies where security mechanisms, in particular data encryption, are most effectively applied within the ISO network architecture model. An overview of one of the most complex security issues in X.25 security-the key management problem-is presented, and an implemented solution is described. Some of the future possibilities for development in this area are also examined.With traditional 'point-to-point' communications the desired security of user data can be obtained by using appropriate protection devices at either end of the communications channel. A protection device can be any 'black box' which provides the required level of user data security; it could employ, for example, hardware to scramble the bit order, a DES (Data Encryption Standard) chip or a military approved cryptographic device. Uunfortunately it is impractical to use the same type of security scheme between two hosts on a common carrier packet switched network, since each host sends and receives both user data and control information along a single network access link. If 'black box' protection devices are used on the host access links to the network then all the information flowing along these links will be transformed. Thus the nodes of the network will be unable to interpret the control information being sent to them from the hosts, and similarly, the hosts will be unable to interpret any control information received from the network. However, each individual link of a packet switched network can be secured with the aid of a pair of protection devices. Unfortunately it also means that all nodes of the network have to be secured since all data appears in its original form within them. Also this scheme provides no security against the effects of network nodes misrouting data. Thus all users of the network and all nodes of the network must be part of the same 'security partition', ie anyone within the 'security partition' may see anyone else's data. In the military environment, such a network is said to operate 'system high', ie all personnel with any access to the network (either at hosts or at node) must be cleared to the level of the highest classification of data carried by the network. It is impossible to use this type of security scheme to protect particular users' data on a common carrier packet switched network; a dedicated packet switched network is required for each security compartment. Packet switched network security can be provided by various combinations of four techniques,(Anderson, JP, 1973) depending upon the protection required. The Techniques are:

1. Encryption
2. Authentication
3. Access Control
4. Computer Security

The roles which can be played by each of these techniques can be considered separately.

Encryption: The principle purpose of encryption Is to transform information into a form which is unrecognizable except to its intended recipient. In order to be effective, end-to-end encryption has to be applied in conjunction with appropriate, and often very complex, key management techniques, to ensure that the required data security is actually achieved. However it must be recognised that such encryption cannot enforce security above the layer at which it is applied. Thus for certain security requirements it may be appropriate to apply end-to-end encryption techniques at more than one level of the 1S00S1 model.

Authentication: Before any security critical connection can be established, the communicating entities need to authenticate, ie uniquely identify, themselves to some trusted intermediary who is responsible for controlling who has access to whom (see access control). In addition it may be necessary to the communicating parties to mutually authenticate each other, prior to their transmission of any sensitive information. Taking a simple example, suppose a terminal user wishes to access a mainframe via a packet switched network. First the user will have to log-on to his terminal support host or PAD (Packet Assembler/ Disassembler), thus authenticating himself to that system. In some environments it may also be necessary for the terminal support host or PAD to authenticate itself to the user, eg via a reverse password. Upon the satisfactory completion of this operation, a connection will be established if this is permitted. Once the connection is established the user will have to log-on to the mainframe and may possibly also receive a reverse password from the mainframe in order to authenticate the machine to users. Thereafter, the user can proceed normally. Similar authentication schemes are required between all the elements of, and users attached to, secure multi-level networks.

Access Control: In reviewing the security requirements at each level of the ISO0S1 model, it should be remembered that these requirements are concerned with the security of the connection between communicating entitles at that level. In order that such a connection can be established in a security critical environment, some form of 'policing' the establishment and maintenance of all such connections must be provided. Such 'policing' must be trusted to uphold a security policy determining which users can talk to which other users and within which security compartment. Thus these trusted 'policing' mechanisms are providing a network access control function; such mechanisms could be centralised or distributed. The four distinct aspects of such an access control function are:

- Access request/authorisation for the connection

- Establishment and termination of the connection
- Maintenance of the connection
- Audit and surveillance of the Connection.

Computer Security: In any end-to-end security scheme, it is necessary to place some trust in the operation of computer systems. For example, it is necessary to trust computers to isolate the plain text data from the transformed data and to provide a mechanism for allowing some control information to bypass the transformation process.

2.0.3 Packet

A packet is one unit of binary data capable of being routed between an origin and a destination on the internet or any other packet switching network. To improve communication performance and reliability, each message sent between two network devices is often subdivided into packets by the underlying hardware and software as in figure 1.0. When any file (e-mail message, HTML file, Graphics interchange format file, Uniform Resource Locator request, and so forth) is sent from one place to another on the internet, the Transmission control protocol(TCP) layer of TCP/IP divides the file into 'chunks' of an efficient size for routing. Each of these packets is separately numbered and includes the internet address of the destination. The individual packets for a given file may travel different routes through the internet. When they have all arrived, they are reassembled into the original file (by the TCP layer at the receiving end).

TCP segment format

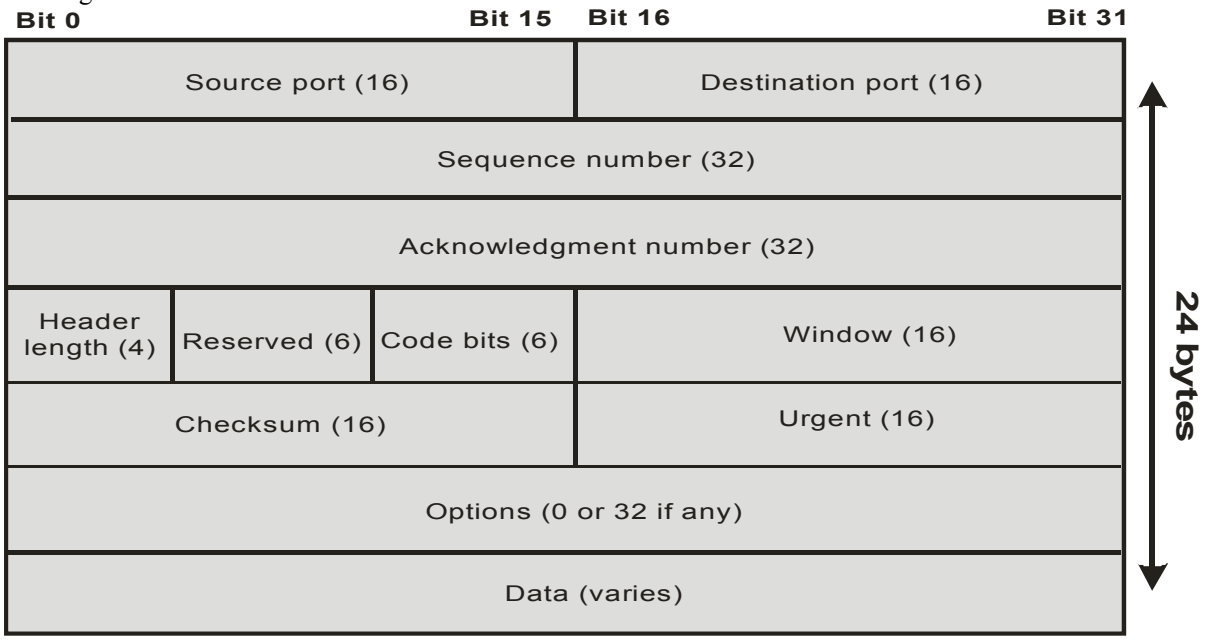

Fig.1.0 TCP segment format for packets.

The TCP header is 20 bytes long, or up to 24 bytes with options. You need to understand what each field in the TCP segment is:

Source port: the port number of the application on the host sending the data.
Destination port: The port number of the application requested on the destination host.
Sequence number: A number used by TCP that puts the data back in the correct order or
Retransmits missing or damaged data, a process called *sequencing*.
Acknowledgment number: The TCP octet that is expected next.
Header length: the number of 32-bit words in the TCP header. This indicates where the data begins. The TCP header (even one including options) is an integral number of 32 bits in length.
Reserved: Always set to zero.
Code bits: Control functions used to set up and terminate a session.
Window: The window size the sender is willing to accept, in octets.
Checksum: The cyclic redundancy checks (CRC), because TCP doesn't trust the lower layers and checks everything. The CRC checks the header and data fields.
Urgent: A valid field only if the Urgent pointer in the code bits is set. If so, this value indicates the offset from the current sequence number, in octets, where the first segment of non-urgent data begins.
Options: Maybe 0 or a multiple of 32 bits, if any. What this means is that no options have to be present (option

size of 0). However, if any options are used that do not cause the option field to total a multiple of 32 bits, padding of 0s must be used to make sure the data begins on
a 32-bit boundary.
Data Handed down to the TCP protocol at the Transport layer, which includes the upper layer headers.
Let's take a look at a TCP segment copied from a network analyzer:

TCP - Transport Control Protocol
Source Port: 5973
Destination Port: 23
Sequence Number: 1456389907
Ack Number: 1242056456
Offset: 5
Reserved: %000000
Code: %011000
Ack is valid
Push Request
Window: 61320
Checksum: 0x61a6
Urgent Pointer: 0
No TCP Options
TCP Data Area:
vL.5.+.5.+.5.+.5 76 4c 19 35 11 2b 19 35 11 2b 19 35 11
2b 19 35 +. 11 2b 19
Frame Check Sequence: 0x0d00000f

Did you notice that everything I talked about earlier is in the segment? As you can see from the number of fields in the header, TCP creates a lot of overhead. Application developers may opt for efficiency over reliability to save overhead, so User Datagram Protocol was also defined at the Transport layer as an alternative.

3.0 ANALYSIS AND DESIGN.
Before packet-wise billing system can be deployed into the department of math's / statistic and computer science there are few considerations you must first address, a mikrotic router, a Linux box (radius server) and a good battery backup solution to protect you from power failures.
The key requirements are:

- Complete system with Ubuntu operating system installed with MySQL, myPHPadmin, Daloradius
- Mikrotic router box
- Internet connection

We have tree topology network architecture in d department of math's/statistics and computer science whereby lectures are connected together in an unmanaged switch. We create a gateway; in the gateway we put a layer 3 device that will send all packet to the radius server. We first of all update the radius server; we then install my php admin and mysql which will do the accounting, authentication and access control. Mysql is for the database while PhP is for administrators. Packet sniffer or packet tracer is used to spy data from the network. The sniffer captures each packet and if, needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications as illustrated in the logic diagram of figure 2.0. Packet capture is the process of interpreting and logging traffic. It is also used to analyze network problems, Filter suspect content from network traffic, Debug client/ server communications. The researcher designs the interfaces using HTMLThere is no form of billing system in the department's intranet. Since the network wasn't built as a profit venture, the departments of maths/stat & computer science setup this network for academic research purpose.With this kind of setup, there is bound to be some levels of abuse in terms of: Unauthorized access: Students/Staff members with the technological know-how on cyber hacking will find such a network as 'a field of play'. With access into the network, via a friendly staff member who allows non-staff into his/her office, the intruder can have access into staff members systems and/or the internet.

3.0.1 Network Diagram

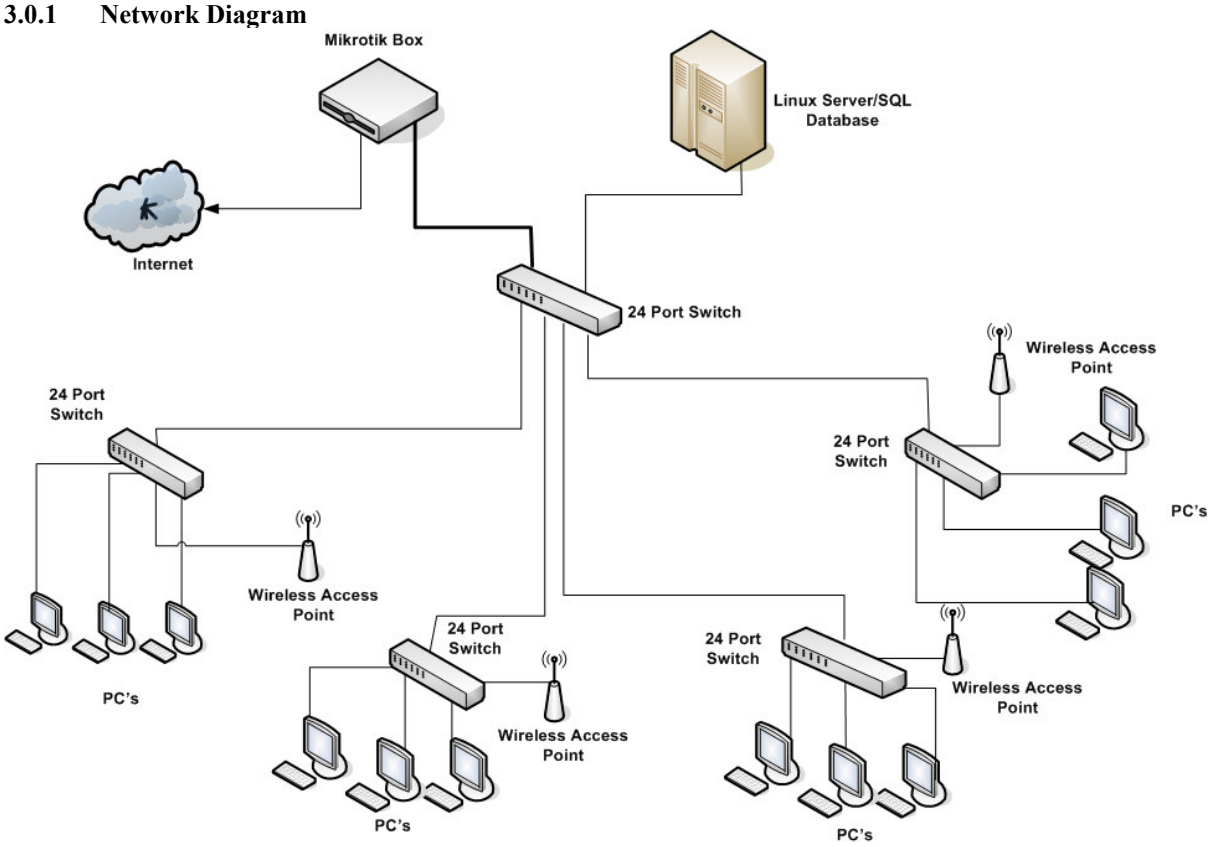

Fig 2.0 Logical Design of the system

Logical design explains the logic between the input and output design.

- The user of the network request for access to the internet, the mikrotik router supplies a captive portal for the user's username/password
- After supplying the username/password, the mikrotik router verifies with the radius server which in turns verifies from the database
- If all the information supplied is correct, the mikrotik router gives access to the user using a user profile accounting for the bandwidth utilization.

4.0 Findings /Results

1. **User requesting for internet access:** Here, the user may be interested in the direct access to the internet without recourse to the resources expected for a smooth flow of data in and out of his or her domain. But the window of figure 3.0 pops up. An authentication is then expected of the user to ease a direct monitoring of the flow of packets.

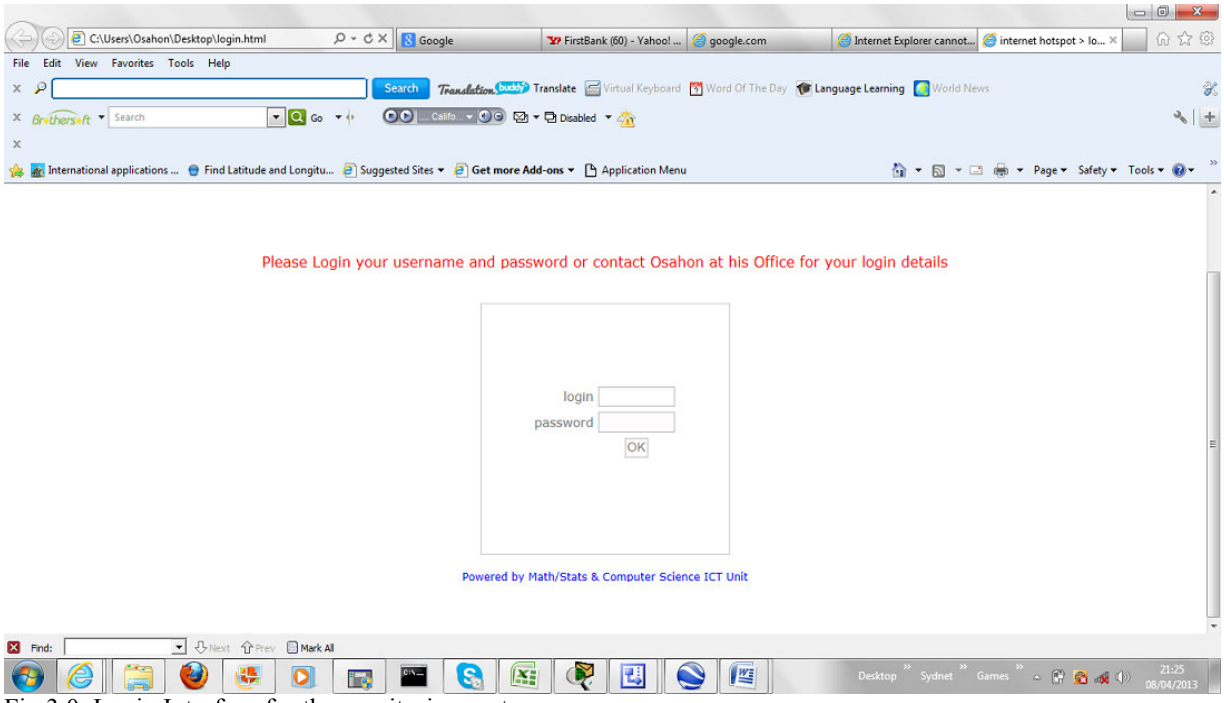

Fig 3.0. Login Interface for the monitoring system

A successful log in would produce a welcom screen of figure 4.0 where the details on the transaction are shown. Parameters such as the IP address, the connection status, the quantity of data up-loaded and or downloaded are all displayed.

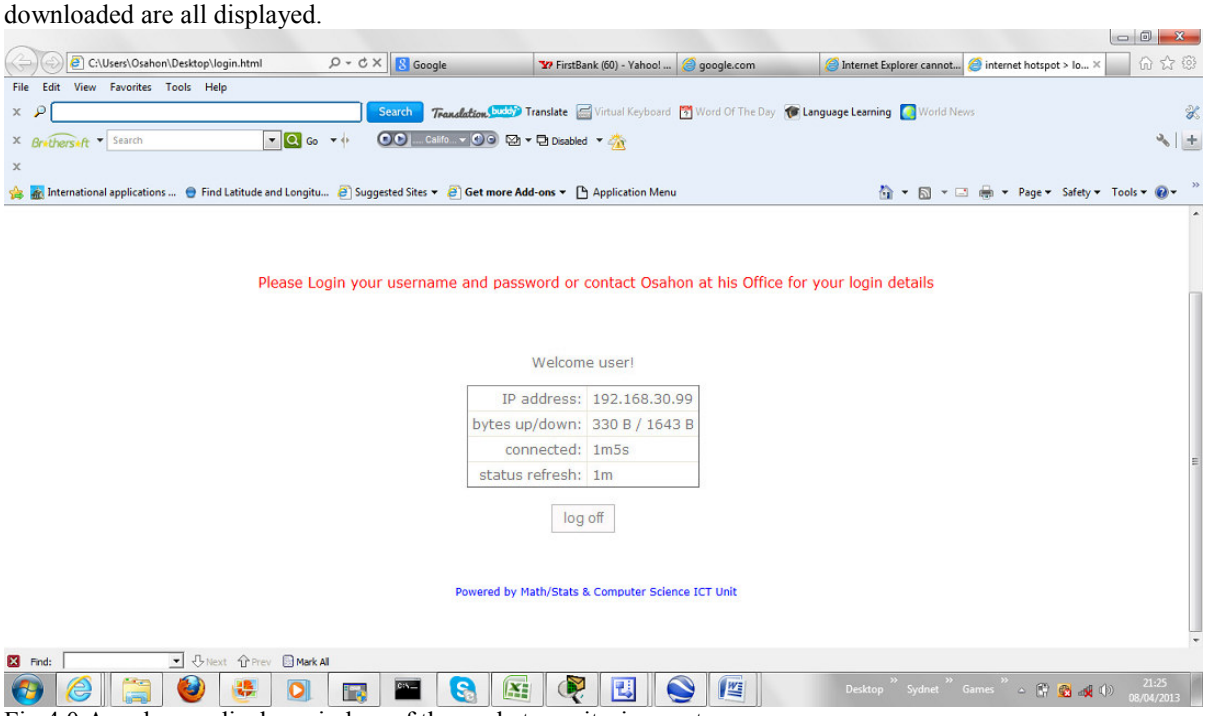

Fig 4.0 A welcome display window of the packet monitoring system

With this, a user can freely enjoy the services of the internet whether the network is down or not.

5.0 CONCLUSION

This research was carried out at unical e-library because of their facility, the researcher designed a server which serves as the billing system, in the server which is ubuntu, the researcher install the radius server, PHP Admin and mysql. The reason being that the radius server will do the authentication, accounting and access control, then the researcher use the packet sniffer to retrieve packet from the network using mikrotik router to connect the server and the client computer. It was discovered that when a user tries to connect to the server, it will be requested to enter a username and password that will give him/her access to the server. With this a capture will

display showing that the user was successfully logged in with it bandwidth detail on it instead of time. So with this, a user can freely enjoy the service of the internet

The university should adopt this method of billing the lectures and students in it e-library such that a user of the e-library can be given a bandwidth (megabytes) for a day or a lecture or staff can open an account in the e-library so that the server can be program to allocate like 1mb or 2gb as the case maybe for a day to each user register in the university intranet.

An appeal should be made to organization, ISP, and even the business centre (cyber cafe) to adopt the packet-wise billing system instead of induced counter timer to bill it staff or customers. For with this, even if the server is down or any other internal factors should affect the internet, the users are sure of being charged by the actual bandwidth uses instead of time spent surfing the internet.

References

Abbate, J. (2000), Inventing the internet, MIT press, ISBN 9780262511155 Retrieved 2014-03-06

Adomi, E.E (2005). Internet Development and Connectivity. Program: Electronic Library and information systems. 39(3), 257-268

Adomi, E.E ,Okiy, R.B and Ruteyan, J.o. (2003),survey of cyber cafes in Delta states, Nigeria. the electronic library in Nigeria.2(5), 487-495

Anderson, J.P., 1973, "Computer Security Technology Planning Study", Volumes 1 and 2, ESD-TR-73 51, October 1973.

Blefari-Melazzi. N, D. Di Sorte, G. Reali. (2003)"Accounting and Pricing: a Forecast of the Scenario of the Next Generation Internet Retrieved 5feburary, 2014 from {blefari,disorte,reali}@diei.unipg.it

C. Rigney, S. Willens, A. Rubens, W. Simpson,(2000) "Remote Authentication Dial In User Service (RADIUS)", IETF RFC 2865,June 2000. Retrieved from http://en.wikipedia.org/wiki/AAA_protocol

Captive portal retrieved on the 14 November 2013 from http://en.wikipedia.org/wiki/Captive portal

Cyber Café management systems Retrieved 28 October,2013 from Umpire.ump.edu.my/2621/1/MOHD-KHAZRO'IE-BIN-JAAFAR.pdf

Eshekels Associates (2001).Trends in internet usage in Nigeria. Lagos: informsation and communication technologies (ICTs) Resource and Research centre

Girard, K.(1997, January).X.25 users remaining loyal despite frame-relay hype.computerworld.31(4).16.Retrieved January 2014-04-04 from ABI/INFORM GLOBAL database (Document ID: 10946641)

International Standards Organisation draft proposal 7498, 1982, "Information Processing Systems Open Systems Interconnection – Basic Reference Model", February 1982.

International Telecommunication Union (ITU, 2004).internets indicators: hosts, user and number of PCs. Retrieved 28 October, 2013 from www.Hu.In/ITU-d/ict/statistics/at-glance/internet.

Kurose, James F. & Ross, Keith W. (2007), "Computer Networking: A Top-Down Approach" ISBN 0-321-49770-8

Mendicino, Samuel (1970-11-30). "Octopus: The Lawrence Radiation laboratory Network". Retrieved 2014-03-06

Method and apparatus for changing codec to reproduce video and/or audio data streams encoded by different codecs within a channel - Patent EP1827030

Robert H'obbes' Zakon. "Hobbes' Internet Timeline v10.1". Retrieved November 14, 2011. Also published as Robert H. Zakon from http://en.wikipedia.org/wiki/Internet_service_provider

Stewart, Bill (2000-01-07). "Paul Baran Invents Packet Switching". *Living Internet*.Retrieved 2014-02-020.

The IBM 2321 Data Cell Drive, Columbia University Computing History