International Journal of Inventive Engineering and Sciences (IJIES)
ISSN: 2319–9598, Volume-1 Issue-2, January 2013

Computer Network: "Analyzed Techniques for Measuring, Presenting and Interpreting the Different Properties for Remote Computer Network Administration"

Devajit Mahanta, Majidul Ahmed

Abstract: ***Computer networking is the connecting of two or more computers that allows them to share resources. It can be done between computers in a home, in a business, across a corporation, and even internationally. It can equally be defined as a method of connecting two or more computer systems together including printers and other devices. The benefits of networking are considerable, even on a network of only three systems. In computer networking there was never a truer statement than that this is a case of advantages experienced being far greater than the sum of the parts. Modern computer networks have gone from typically being a small local area network, to wide area networks, where users and servers are interconnected with each other from all over the world. This development has gradually expanded as bandwidth has become higher and cheaper. But when dealing with the network traffic, bandwidth is only one of the important properties. Delay, jitter and reliability are also important properties for the quality of network connection. This is because different applications has different needs, and therefore require different properties from the network. System administrators are in an increasing degree involved with the troubleshooting of solving network problems concerning the quality of service for the different applications. This study analyzed techniques for measuring, analyzing, presenting and interpreting the different properties for the administration of remote computer network. In this way system administrators can benefit from this thesis when administrating their remote computer networks.***

Keyword: ***Computer networking, bandwidth, System administrators, remote computer network, network traffic***.

I. INTRODUCTION

Communication systems are nowadays fundamental to support various applications, and this is especially true for computer networks as their utmost expression. Some examples include information interchange for critical operations, such as bank transfers or military data, as well as commonly used services such as the web, email, or streaming of multimedia contents. It is therefore essential to be able to ensure an uninterrupted and efficient operation of a computer network. The most used network architecture is the client-server architecture. In a client-server architecture the server passively waits for a request, until the client actively sends a request to the server.

Revised Version Manuscript Received on December 2013.

Mr. Devajit Mahanta, Department of Computer science, Nalbari College ,Assam (India), E-mail: devajitmahantah@sify.com

Dr. Majidul Ahmed, Department of Information Technology, Gauhati Commerce College,Assam (India), E-mail:- mjdahmd10@gmail.com ,

The server then executes the request and sends the reply back to the client. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. Computer transactions using the client/server model are very common. For example, to check your bank account from your computer, a client program in your computer forwards your request to a server program at the bank. That program may in turn forward the request to its own client program that sends a request to a database server at another bank computer to retrieve your account balance. The balance is returned back to the bank data client, which in turn serves it back to the client in your personal computer, which displays the information for you. The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. So does the Internet's main program, TCP/IP. In marketing, the term has been used to distinguish distributed computing by smaller dispersed computers from the "monolithic" centralized computing of mainframe computers. But this distinction has largely disappeared as mainframes and their applications have also turned to the client/server model and become part of network computing. In the usual client/server model, one server, sometimes called a daemon, is activated and awaits client requests. Typically, multiple client programs share the services of a common server program. Both client programs and server programs are often part of a larger program or application. Relative to the Internet, your Web browser is a client program that requests services (the sending of Web pages or files) from a Web server (which technically is called a Hypertext Transport Protocol or HTTP server) in another computer somewhere on the Internet. Similarly, your computer with TCP/IP installed allows you to make client requests for files from File Transfer Protocol (FTP) servers in other computers on the Internet. One of the first computer networks were isolated local area networks (LANs), with a client-server architecture. The clients were cheap terminals, attached to a screen and a keyboard. At the time, the clients required low network bandwidth. The only data transmitted was the keyboard activity sent to the server, and the screen updates sent back to the client. The terminals used in these networks are classified as thin clients. This is because most of the processing is done at the server, while the client typically process keyboard input and screen output. Some advantages with the thin client approach are: • A lower hardware costs, as there is usually no need for disk, a lot of memory, or a powerful processor.

This also creates a longer turnover time, because it takes a longer period of time before the equipment becomes obsolete.

• A lower administration cost, as the clients are almost completely managed from the server. All installations and upgrades are done on the servers, and not on each client.

• A higher client reliability, as the client hardware has less points of failure.

• Increased security, as no sensitive data ever resides on the client. The local environment is usually highly restricted, and the protection against malware is centralized on the servers.

The need to connection to other networks or clients from the existing network, created the next step for computer networks. The connection between the networks was typically created by leased lines or by dial-up connections. The new networks were called metropolitan area networks (MAN) or wide area networks (WAN) depending on the range of the networks. With the creation of these new networks, terminals could now connect to other servers in other networks, and process data in other computer environments. The personal computer (PC) was intended to conquer the private marked, but the corporate marked also showed great interest. And as time went by, the pc replaced the terminal as the preferred client. The pc can be a thick client, because it has a disk, memory and a powerful processor that allows the client to run its own operating system and programs. But even though the pc has the properties of a thick client, it can behave like a thin client. This all depends on the software that the pc is running. Applications like telnet and ssh emulates a thin client environment, because the applications connects to a remote server, and utilizes the resources which is provided by that server. Keyboard actions are sent to that server, and the server only replies with screen changes, just like in a thin client environment. Traditionally the server had processed both the client environment and the production environment. But with the arrival of the pc, user environment processing could be removed from the servers, and done on the clients own processor. This meant a more efficient usage of the processing servers. In situations where the data could be stored on the pc itself, the processing of the production data could be executed on the local processor. But this moved the bottleneck away from the production server processors, and to the network bandwidth.

Some advantages with the thick client approach are:

• Lower server requirements, as a thick client does most of the application processing itself.

• Lower user environment network bandwidth usage, because there is no keyboard or screen data that has to be sent to and from the server.

Working offline. Thick clients have advantages in that a constant connection to the central server is often not required.

Better multimedia performance. Thick clients have advantages in multimedia-rich applications that would be bandwidth intensive if fully served. For example, thick clients are well suited for video.

More flexibility. On some operating systems software products are designed for personal computers that have their own local resources. Running this software in a thin client environment can be difficult.Using existing infrastructure. As many people now have very fast local PCs, they already have the infrastructure to run thick clients at no extra cost.

Higher server capacity. The more work that is carried out by the client, the less the server needs to do, increasing the number of users each server can support. By the late 1980's, thousands of cooperating networks were participating in the Internet.

In 1991, the U.S. High Performance Computing Act established the NREN (National Research & Education Network). NREN's goal was to develop and maintain high-speed networks for research and education, and to investigate commercial uses for the Internet. The rest, as they say, is history in the making. The Internet has been improved through the developments of such services as Gopher and the World Wide Web. The internet started off as a few computer networks interconnected with each other. The connection speed, at that time, was only about 64 kilobits per second (kb/s), and the connection between the networks was within the United States of America. Since then, hundreds of millions of people, all around the world, has connected to the internet. The bandwidths available today typically range from 64 kilobits per second on dial-up connections, to gigabits per second on high performance broadband connections. The high bandwidth available on the internet today, enables new possibilities for network applications. But bandwidth is not the only property for a good internet connection. Properties like delay, jitter, and reliability have become the main focus area in the past years.Together these four properties make up the basis for quality of service (QoS). As the internet service providers improve their quality of service, this enables organizations and businesses to structure their computer networks in new ways. There is no longer the need for one location where both the user environment and the production environment are located. Examples of these new possibilities are:

• Employees may connect to the production environment from their home.

• The same production environment can be used for several remote user environments.

• Multiple remote production environments can be interconnected.

This allows the business to easier create new locations in other countries. But for the system administrators who are used to operate in a local area network environment, this creates new problem areas. This is because most programs are intended to run in a local area network with low delay, low jitter, high bandwidth, and high reliability. The new tasks that the system administrator has to adapt to are how to locate and remove bottlenecks in remote computer networks. To do this, the understanding of what these quality of service properties do, and how to overcome them.

II. COMPUTER NETWORKS

Computers a network is a way to connect computers together so that they can communicate, exchange information and pool resources

or a network is a communicating system connecting two or more computers [1].

2.1 Network classification

Networks are often classified by their physical or organizational extent or their purpose. Some of this are-

1. Personal area network:-A personal area network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles

2 Home network:-A Home network is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or Digital Subscriber Line (DSL) provider [4].

3. Campus network:-A campus network is a computer network made up of an interconnection of LANs within a limited geographical area.

4. Enterprise private network:-An enterprise private network (Figure 2.4) is a network built by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices, shops, in order to share computer resources.

5. Virtual private network:-A virtual private network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires **2.3.6. Local area network:-**A local area network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings [3].

7. **Metropolitan area network**:-A Metropolitan area network (MAN) is a large computer network that usually spans a city or a large campus. Example-Cable TV networks.

8. Wide area network:-A wide area network (WAN) is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves.

2.2 Computer Network Topology:- Topology of a network [5][6] refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations. Network topologies are categorized into the following basic types:

1. Bus Topology**:-**

Bus networks (figure 1) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector. A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message.

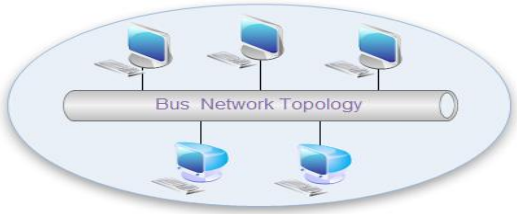

Figure 1:-Bus topology

2. Star Topology:-Many home networks use the star topology (figure 2). A star network features a central connection point called a "hub" that may be a hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.

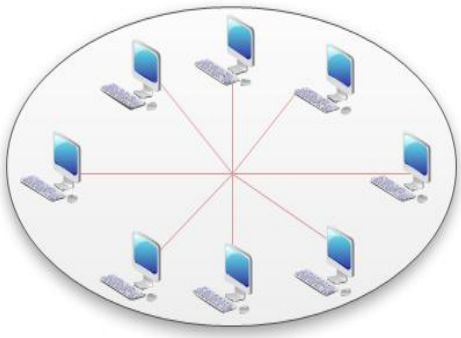

Fig 2:- Star Topology

3 Ring Topology:-In a Ring network (Figure 3), every device has exactly two neighbors for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or breaks the loop and can take down the entire network device..

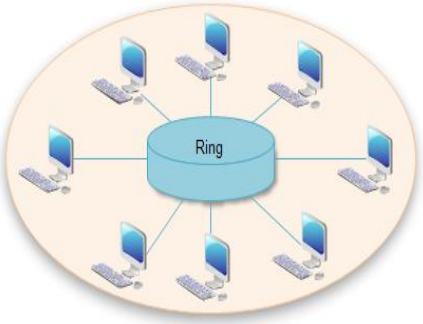

Figure 3:- Ring topology

4. Tree Topology:-Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices.

5. Mesh Topology:-Mesh Topology (Figure 4) involves the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. A mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.

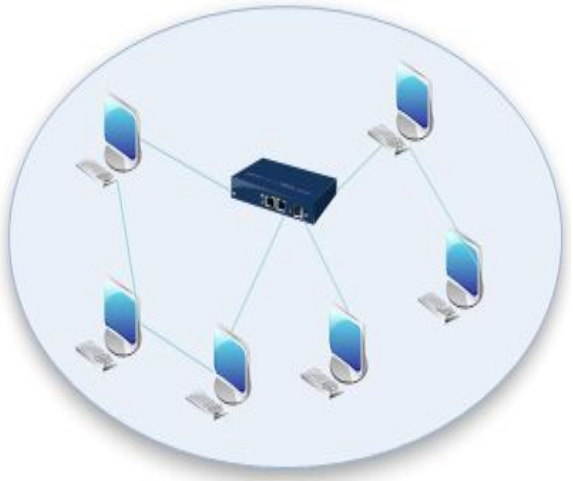

Figure 4:- Mesh Topology

6. Hybrid Topology:-A combination of any two or more network topologies called hybrid topology .It always accrues when two different basic network topologies are connected.

2.3 Computer Network Transmission Media

The means through which data is transformed from one place to another is called transmission or communication media. There are two categories of transmission media used in computer communications.

1. **Bounded media**:-Bounded media are the physical links through which signals are confined to narrow path. These are also called guide media. Bounded media are made up o a external conductor (Usually Copper) bounded by jacket material. Bounded media are great for LABS because they offer high speed, good security and low cast. However, some time they cannot be used due distance communication. Three common types of bounded media are used of the data transmission. These are- a) Coaxial cable b) Twisted Pair Cable c) Fiber Optics

2. Unguided or unbounded media:- Unguided media or wireless media doesn't use any physical connectors between the two devices Communicating. Usually the transmission is send through the atmosphere but sometimes it can be just across the rule. Wireless media is used when a physical obstruction or distance blocks are used with normal cable media.

a) Terrestrial microwave b) Antenna c) Satellite d) Cellular phone e) WI-FI

2.4 Computer Security

To create a secure computer system, three properties are necessary [22]:

a) Confidentiality b) Integrity c) Availability

2.5 Measurements

Measurements are conducted in four stages [23]:

1. Data collection

The first stage collects the raw data from the network or computer. This can be done by active measurement, which is tool that generates traffic on the network to conduct the measurements. Another name for active measurements are benchmarking. Another approach is passive measurements, which are contrary to active measurements in that they only monitor the network [23].

2. Analysis

In stage two, the raw data are processed in different ways to gather useful information about the measurements [23]. Interesting data can be: minimum value, maximum value, means value, median value, etc.

The Maximum

The maximum sample is the sample with the highest value [23].

The Minimum

The minimum sample is the sample with the lowest value [23].

The Median

The median of a set of samples is the sample for which there are an equal number of samples with a lesser value and an equal number with a greater value[23].

The Mean

The mean of a set of samples is the same as the average value, which can be found by the following formula[8]:

$$\langle V \rangle = \frac{V1+V2+\ldots\ldots..+Vn}{N} = (1/N)\sum_{i=1}^{n} Vi \quad \text{-------- (2.1)}$$

Where v1−N is the observation values and N is the number of observations.

The Standard Deviation

The standard deviation can be found by the following formula [8]:

$$\Delta = \sqrt{((1/n)\sum_{i=1}^{n} \Delta g_i^2} \quad \text{---------- (2.2)}$$

3. Presentation

In stage three, the raw and the processed data are visualized by creating graphs or charts. The visual aid, can help clarifying threads in the data [12][22].

Time series:-A time series diagram shows the x-axis in time and the y-axis as the measured values. Time series diagrams are useful for describing the measured data, and spotting trends.

III. LITERATURE SURVEY

3.1 Quality of Service

The stream of packet between two nodes in a network is called a flow. This flow will in a connection-oriented network follow the same route, but in a connectionless network, the packet may take different routes [1][12]. The problem with a connectionless network is that the routes may have different properties. The four main properties for network connections are [1] [12]:

1. Bandwidth 2. Delay 3. Jitter 4. Reliability

These four properties define the quality of service (QoS), that the flow requires. The QoS for the routes may not matter for some applications, but it may be crucial for others.

Table 1: How stringent the quality-of-service requirements are.

Application	Reliability	Delay	Jitter	Bandwidth
E-mail	High	Low	Low	Low
File transfer	High	Low	Low	Medium
Web access	High	Medium	Low	Medium
Remote login	High	Medium	Medium	Low
Audio on demand	Low	Low	High	Medium
Video on demand	Low	Low	High	High
Telephony	Low	High	High	Low
Videoconferencing	Low	High	High	High

From the table, the following interpretation can be made [1]:
• The four first applications require a high reliability. This means that all bits have to be transmitted correctly. This is usually achieved by check summing each packet and verifying that the checksum matches at both ends. If the packet is damaged, it will be retransmitted.
•The four last applications can tolerate errors, and will not require check summing or verification.
•Applications like telephony and videoconferencing require a low delay, and are therefore highly dependable on the delay. These are typical real-time applications, and real-time has strict delay requirements.
•Applications like e-mail and file transfer, are more delay tolerant, as these are typical "store and use" applications.
•Web access and remote login applications are interactive programs that require a relative low delay.
•For real-time applications like the last four applications, a low delay between the packages is important. A burst of packets may become very uncomfortable for these real-time applications.
•The other four applications are more immune for jitter, as buffers can be used to
Smooth the connection.
•Applications like e-mail, remote login or telephony requires a low bandwidth.
•Applications with graphical data and/or sound data requires a higher bandwidth.
By creating a service level agreement (SLA) with the internet service provider (ISP) about the property of the internet connection, the ISP can guarantee that the quality of service is good, as long as the customer obeys the agreement [1].

3.2 Bandwidth

Bandwidth represents the capacity of the connection. The greater the capacity, the more likely that greater performance will follow, though overall performance also depends on other factors, such as latency. In general, network bandwidth is a bit rate measure of available or consumed data communication resources expressed in bits/second or its multiples (kilobits/s, megabits/s etc.). Now a day's computer Networks are play very important role our various job they can transfer and received voice, data, images and video. But voice, data, images, and video have different requirements in terms of bandwidth, cell loss, delay, etc. In order to maximize the quality of service offered during the period of stress, as viewed by both the network provider and the customer, the following bandwidth challenges are to be considered:

a. Topology design and bandwidth allocation
b. Flow control and congestion avoidance.
c. Bandwidth allocation, the most critical challenge, is concerned with successful integration of link capacities through the different types of services. Given that a virtual path is a logical direct link composed of virtual circuits between any two nodes; and Bandwidth management given following benefit [6].
a. Faster applications b. Reduce bottlenecks c. Accelerate & compress traffic d. Better control over your network

Bandwidth management from Managed Communications enables our business to benefit by getting:
a) Get better information - we can better understand your bandwidth usage with comprehensive bandwidth management tools
b) Faster application speed - bandwidth management can allocate bandwidth to key critical applications enabling better performance
c) Reduce unwanted traffic - we can isolate P2P users or bandwidth hogs on your network so that you control the quality of performance seen across your data connections
d) More bandwidth - we can achieve up to 35 times the throughput with bandwidth management services.

In most cases we can count on doubling your throughput without a network upgrade. Without bandwidth management, an application or a user will not be able to control all available bandwidth and prevent other applications or users from using the networks. It will be impossible to differentiate between different types of network traffic, and it will also be difficult to control which users or applications have priority on the network. Applications which require specific quantity and quality of service may not be predicted in terms of available bandwidth, thus making some applications run poorly due to improper bandwidth allocation. Bandwidth management works by sorting outbound network traffic into classes by application and service type. There is an ever-increasing need for network bandwidth. Companies are growing, adding new offices and remote sites, using technologically advanced and powerful applications, and internet usage has exploded in the last decade. Local area networks (LANs) are in need of bandwidth. How much is required depending on individual company and user, and user's requirement can changed unexpectedly and sporadically. Bandwidth can be expensive, and when LANs begin to slow down because of heavier usage more bandwidth is often required. Corporate networks using intranets for information sharing and web navigation have an increased demand for bandwidth, but simply adding one more connection or larger connections does not address the bandwidth issues since availability is not always guaranteed.
Bandwidth is a term used to describe the capacity of a link. It is the transmission rate for the link. A link able to transmit at 100 Mbps, has a bandwidth of 100 Mbps [16]. Table 3.2 lists some of the typical bandwidths provided by the most common medium access control technologies. Table 3.3 lists categories of wide area network connections provided by internet service providers [1]. Even though bandwidth is what is provided by the internet service provider, it is the throughput of the connection that is of interest for the customer.

"Throughput is a measure of the amount of data that can be sent over a link in a given amount of Time [16]".
The throughput is determined by the formula:

$$\text{Throughput} = \frac{\text{Data Transferred}}{\text{Time}} \quad (3.1)$$

The throughput is expressed in bits per second or packets per second. But when expressed in bits per second, the more the typical expression is kilobits (103 bits), megabits (106 bits) or gigabits (109 bits) per second, depending on the connection throughput.
The difference between throughput and bandwidth is that throughput measurements may be affected by considerable overhead that is not included in bandwidth measurements. And therefore throughput is a more realistic estimator of the actual performance for the connection [16].

Table 2: Bandwidths provided in Local Area Networks

Description	Bits	Bytes
Ethernet (10base-X)	10 Mb/s	1,25 MB/s
Fast Ethernet (100base-X)	100 Mb/s	12,5 MB/s
FDDI	100 Mb/s	12,5 MB/s
Gigabit Ethernet (1000base-X)	1.000 Mb/s	125 MB/s

Data Collection
The two factors affecting the throughput are, the amount of data transferred, and the time it took to transfer that data.
Determining the throughput can be done in two ways:
1. Measuring the time it takes to transfer a predetermined amount of data.
2. Measuring the amount of data transferred in a predetermined amount of time.

1) Active Measurements:-
A simple method for actively measuring the throughput is to upload or download a file through ftp. This gives information about the file size and the time it took to transfer the file. The problem with this simple measurement approach is that the disk access needed to store or read the file, may interfere with the measurement [16].
Programs like nether, iperf [13] and ttcp[14] use methods so that no disk access is necessary. This is done by reading and writing the transmitted data into the RAM. All of these programs use the same functionality for measuring the throughput, but they differ in functionality [16].Of the three example programs here, iperf has the most functions. And can not only measure TCP throughput, but also UDP throughput, jitter and packet loss.

2) Passive Measurements:
Passive measurements do not add extra data to the network, but rather measures the current throughput, through a node. To capture the data flow, through the node, tools like tcpdump [20] must be used. These tools capture the data on a kernel level, and thus provide the raw data needed to perform analysis on the data. Other tools must then be used to analyze the data, and thus provide the throughput. Tools like tipster [21] can be used to analyze the data captured by tcpdump, but tcpstat can also capture the data itself. The advantage with tcpstat monitoring the bandwidth itself is that there is no need to store the captured data, which is the case with tcpdump[16]. Both tcpdump and tcpstat can be used with filters, which filter away unwanted data. This can be useful for monitoring only upload traffic, download traffic, http traffic, ftp traffic, etc.

3) Analysis:
The throughput measurements provide useful statistical information about the throughput of the node. If the node has used active measurements, the measurements show the throughput for the connection, while passive measurement tools show the utilization of the bandwidth. Trends are identified by presenting the measured data in a time series diagram, where the time is for a long duration
of time. The longer the duration, the easier the trend may be to recognize.

3.3 Delay
The delay is the time it takes to send a packet or frame from a source node to a destination node. Network delay is an important design and performance characteristic of a computer network or telecommunications network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes [9]. The delay is the product of three delays, these are called [2][8][15]:
a) Transmission delay: -Transmission delay is the amount of time it takes to put the signal onto the cable. This depends on the transmission rate (or interface speed) and the size of the frame [8].
b) Propagation delay:-Propagation delay is the amount of time it takes for the signal to travel across the cable [8]. This depends on the type of media used and the distance involved.
c) Queuing delay: - Queuing delay is the time it takes to process the packet or frame at intermediate devices such as routers and switches. It is called the queuing delay because most of time is spent in queues within the device [8].
The transmission delay and the propagation delay are quite predictable and stable delays, but queuing delays can introduce considerable variability [2][15].
The delay can be calculated by the following method:

$$d1 = t1 + p1 + q1$$
$$d2 = t2 + p2 + q2$$
$$dN = tN + pN + qN$$

Where d1−N is the delay for each node on the path, t1−N , is the transmission delay between each of the nodes on the path, p1−N is the propagation delay between each of the nodes on the path, and q1−N is the queuing delay for each node on the path. The total delay is then:

$$\text{Delay} = \sum_{i=1}^{N} di \quad (3.2)$$

Where d1−N is the delay for each node on the path, and N is the number of nodes on the path to the destination.
The delay is expressed in time, and since the delay usually is quite small, it is expressed in ms.

1) Data Collection
To measure the delay, it is necessary to send a packet to a destination node, and somehow measure the delay between the nodes. The ICMP are designed to handle these kinds of operations, but this may create an unreliable result as the ICMP packets are usually prioritized compared to the IP packets.
There are two methods for measuring the delay between two nodes:

A) One way delay B) Round trip delay

2) Analysis

The delay measurements can provide information as statistics of the connection that has been monitored. This can provide useful, when troubleshooting applications. By presenting the measurements in diagrams, the following information can be identified:

• Trends for the round trip time, for the measured connection. The trends can be viewed in a time series diagram.

• The distribution of the round trip time. This can be viewed in a histogram diagram.

• The congestion of the connection. Congestion is determined by a phase plot diagram.

Jitter

Jitter is the undesired deviation from true periodicity of an assumed periodic signal in electronics and telecommunications, often in relation to a reference clock source. Jitter may be observed in characteristics such as the frequency of successive pulses, the signal amplitude, or phase of periodic signals. Jitter is a significant, and usually undesired, factor in the design of almost all communications links (e.g., USB, PCI-e, SATA, OC-48). In clock recovery applications it is called timing jitter.[1]

Jitter can be quantified in the same terms as all time-varying signals, e.g., RMS, or peak-to-peak displacement. Also like other time-varying signals, jitter can be expressed in terms of spectral density (frequency content).

Jitter period is the interval between two times of maximum effect (or minimum effect) of a signal characteristic that varies regularly with time. Jitter frequency, the more commonly quoted figure, is its inverse. ITU-T G.810 classifies jitter frequencies below 10 Hz as wander and frequencies at or above 10 Hz as jitter.[19]

Jitter may be caused by electromagnetic interference (EMI) and crosstalk with carriers of other signals. Jitter can cause a display monitor to flicker, affect the performance of processors in personal computers, introduce clicks or other undesired effects in audio signals, and loss of transmitted data between network devices. The amount of tolerable jitter depends on the affected application.

Jitter is the variation in arrival times of successive packet from a source to a destination. And is determined by the difference experienced by subsequent packets, RTTI and RTTI+1[2][16][19]. The mathematical formula is:

Jitter $I = \sqrt{(½(RTT_1 - RTT_{I+1})}$ ---------- (3.3)

1) Data Collection

The jitter can be measured by monitoring the round trip time for packets between two nodes. This can be done by passive measurement tools like tcpdump that taps into the network and stores the relevant data. Other tools can then extract information from tcpdump which can then be analyzed.

Active measurement tools include all of those used to measure the round trip time.

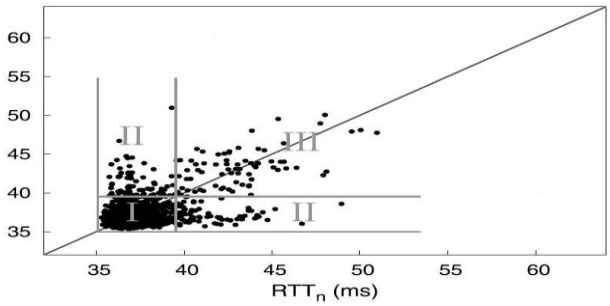

Figure 5: RTT in a phase plot diagram.

2) Analysis

Showing the jitter in a time series diagram, shows the jitter during that time period, but reveals little information about the jitter itself. More interesting information about the jitter comes from the distribution of the jitter. This can be viewed in a histogram chart. When the distribution of the jitter is mainly within a few seconds, the jitter can be qualified as low, but this depends on the requirement of the application. The desired distribution would be an exponential distribution. If the distribution is not within a few seconds, but rather spread across several second, the connection is unpredictable and has a high jitter value.

3.5 Reliability

Reliability is defined as "An attribute of any system that consistently produces the same results, preferably meeting or exceeding its specifications"[20]. A method to describe reliability is to use the failure rate, which describes how frequently something fails. A failure in network is when the packet does not reach its destination, before the time expire[20][21].The failure rate (λ) has been defined as "The total number of failures within an item population, divided by the total time expended by that population, during a particular measurement interval under stated conditions. (MacDiarmid, et al.)". It has also been defined mathematically as the probability that a failure per unit time occurs in a specified interval, which is often written in terms of the reliability function, R(t), as,

$\lambda = (R(t_2) - R(t_1))/(t_1 - t_2)\, R(t_1)$ ---------- 3.4

Where, t1 and t2 are the beginning and ending of a specified interval of time, and R (t) is the reliability function, i.e. probability of no failure before time t.

The failure rate data can be obtained in several ways. The most common methods are [1]:

• Historical data about the device or system under consideration.

• Government and commercial failure rate data.

• Testing.

Historical data can be provided by the companies that produce the device or system. This can be used to produce the failure rates. Another approach is to use failure rate data provided by government or commercial companies. The last approach is to monitor and test the devices or system to generate failure data [23].

When monitoring a network connection or a node, packet loss is a measurement for measuring the fraction of packets sent from a measurement node to a destination node for which the measurement node does not receive an acknowledgment from the destination node [23].

1) Data Collection:- The active measurement tools used for measuring the delay and jitter, are also suitable for measuring the failure rate.
2) Analysis:-The interesting information gathered from the raw data conserving the reliability, is how many error there where during the measurement period. This is known as the error rate. It shows the number of errors divided on the time interval.
To retrieve reliable failure rate data, the testing should be performed over a relative large period of time. This removes uncertainty in the result.

IV. METHOD

The state of a network link can be determined by measuring the throughput, the delay, the jitter and the packet loss. Following I given three case studies, methods for measuring these.

4.1 Case One: Network Traffic

4.1.1 Motivation

By monitoring the network traffic for a node, information about the state of that node can be determined. This may provide the network administrator, with enough information to optimize the system performance, by removing bottlenecks. The system can represent the node, a subnet, or the whole network. There are especially two locations that are of interest, when performing passive network measurements:
a) The state of a service host, that provides a network service. Examples of network services are the DNS, DHCP, HTTP, and FTP services.
b) The state of a network node, performing a routing or forwarding functions. Examples of such nodes are firewalls, virtual private networks (VPN), and routers.

4.1.2 Objective

By using a passive network measurement tool, two nodes are to be monitored for one day. The data gathered from these nodes are to be analyzed, and the state of the nodes is interest. Resources.In this experiment, the resources located in table 3 has been utilized

Table 3: The resources utilized in Case One.

Description	Node One	Node Two
Processor Model	Intel Pentium III	AMD Athlon(tm) XP
Processor Mhz	549,947Mhz	1852,314Mhz
Memory	640 MB	1024 MB
Network MAC	Fast Ethernet FD	Ethernet FD
Network Link	100 Mb/s	10 Mb/s
Internet Service Provider	BSNL Broad bands	Reliance Broad bands
IP Address	128.39.73.19	83.227.111.133

Description of Node One :- Node one is a host located in a test laboratory which located at CMJ University, in Shillong. Here I used operating system is GNU Linux Debian, where the version of Debian is "Sarge". The host is also running the following services: PostgreSQL, SMTP, HTTP, HTTPS, FTP, and SSH. The host is connected to a local area network, which shares a 155Mb/s internet connection with the rest of the school. But as the local area network, and the host network interface card only supports Fast Ethernet, the maximum network speed is about 100Mb/s.
Description of Node Two :-Node Two is a host serving as a firewall for a local area network, located in Shillong . The operating system is GNU Linux Debian, where the version of Debian is "Woody". The host serves the firewall, which protects a local area network with services like HTTP, FTP, and SSH. The host is connected to an Ethernet connection, providing 10 Mb/s internet connections.
Tools:-To perform the passive measurements, a program has to run on the node that is monitored. The SNMP service is an alternative method for collecting the measurements. But it may also generate traffic on the network, if the collecting node is located on the monitored network. Another approach would have been to log all network traffic, with the help of tcpdump or an equitant program, and then later process the saved data. But this generates a lot of data, requires a lot of disk space, and it lacks the function to measure the state of the node. A more suited program for the measurements conducted in this experiment, where tcpstat. tcpstat is a highly configurable program that measures some data, and may generate some statistics if wanted. Examples of the data that can be gathered are: bits per second, bytes since last measurement, ARP packets since last measurement, TCP packets since last measurement, ICMP packets since last measurement, etc.
The following command was executed on both nodes, and ran on the nodes for one day.
tcpstat -i eth0 \ -o "%S %A %C %V %I %T %U %a %d %b %p %n %N %l \n"
The explanation of logged data can be found in the result chapter.

4.1.5 Predictions

: -The predictions for the result are:
• Node One, will never fully utilize the available bandwidth, but will probably utilize 100% of the processing power.
• Node Two, will fully utilize the bandwidth, but will probably not utilize the processing power.
• For both nodes, IP will dominate the network layer protocols, and TCP will dominate the transport layer protocols.

4.2 Case Two: Throughput

4.2.1 Motivation

By performing active measurements from one node to another node with equal link speed, the state of the connection can be determined. If the link speed is not as expected, countermeasures can be taken to locate and remove the bottleneck.

4.2.2 Objective

By using a active measurement tool, the connection between two nodes are to be benchmarked and analyzed. The test should provide enough information to see trends in the network, and determine if the node manage to utilize the available bandwidth. To remove uncertainties in the results, benchmarking should be executed from one node, to two other nodes.

4.2.3 Resources

In this experiment, the resources located in table 4 have been utilized.
Description of Node One :- Node One is a host located in a test lab at CMJ University, in Meghalaya. The operating system is GNU Linux Debian, where the version of Debian is "Sarge". The host is also running the following services: PostgreSQL, SMTP, HTTP, HTTPS, FTP, and SSH. The host is connected to a local area network, which shares a 155Mb/s internet connection with the rest of the school. But as the local area network, and the host network interface card only supports Fast Ethernet, the maximum network speed is about 100Mb/s.

Table 4: The resources utilized in Case Two.

Description	Node One	Node Two	Node Three
Processor Model	Intel P III	Intel P MMX	Intel P III
Processor Mhz	549,947Mhz	167,047Mhz	447,699Mhz
Memory	640 MB	96 MB	923 MB
Network MAC	Fast Ethernet FD	FastEthernet FD	Fast Ethernet FD
Network Link	100Mb/s	100Mb/s	100Mb/s
Internet Service Provider	BSNL	BSNL	BSNL
IP Address	128.39.73.19	158.38.88.147	128.39.74.16

Description of Node Two :- Node Two is a host located in the student housings at Shillong Engineering and Management College MEGHALAYA The operating system is GNU Linux Red Hat, where the version of Red Hat is "9.0". The host is connected to a local area network, which shares a 155Mb/s internet connection with the rest of the school. But as the local area network, and the host network interface card only supports Fast Ethernet, the maximum network speed is about 100Mb/s. The path from Node One to Node Two is shown in table 5.

Table 5: Path from Node One to Node Two.

Path ID	IP	Location
1	128.39.73.1	CMJ University,Meghalaya
2	158.36.84.21	CMJ University,Meghalaya
3	128.39.0.73	CMJ University,Meghalaya
4	128.39.46.249	CMJ University,Meghalaya
5	128.39.46.2	Gauhati University,Assam
6	128.39.46.102	Gauhati University,Assam
7	128.39.47.102	Gauhati University,Assam
8	128.39.47.130	Nalbari College,assam
9	158.38.0.66	Shillong Engineering and Management College ,MEGHALAYA
10	158.38.88.147	Shillong Engineering and Management College ,MEGHALAYA

Description of Node Three :- Node Three is a host located in the student network at CMJ University, in Meghalaya. The operating system is GNU Linux Debian, where the version of Debian is "Woody". The host is also running the following services: MYSQL, NTP, SMTP, HTTP, FTP, and SSH. The host is connected to a local area network, which shares a 155Mb/s internet connection with the rest of the school. But as the local area network, and the host network interface card only supports Fast Ethernet, the maximum network speed is about 100Mb/s.The path from Node One to node thee is shown in table 6.

Table 6: Path from Node One to Node Three.

Description	Node One
Processor Model	Intel Pentium III
Processor Mhz	549,947Mhz
Memory	640 MB
Network MAC	Fast Ethernet FD
Network Link	100 Mb/s
Internet Service Provider	UNINETT
IP Address	128.39.73.19

Table 7: The resources utilized in Case Three.

Path ID	IP	Location
01	128.39.73.1	CMJ University, in Meghalaya
02	128.39.74.16	CMJ University, in Meghalaya

Tools:-There are multiple tools that perform about the same function when performing active measurements. Known network throughput benchmarking tools are: netperf, iperf, ttcp, and ftp. The tool chosen to test the throughput is netperf. To execute the experiment, a server node and a client node has to be installed on each of the nodes.For the experiment, the server program was installed on Node Two and three, and the client software was installed on Node One. This setup was chosen, so that the process of benchmarking could be controlled from Node One. This minimizes the probability for interference from each measurement.

Predictions.The predictions for the result are as follows:

• As all nodes are attached to a over dimensioned network, the connection itself should not be a problem. And it should be possible to achieve full link utilization.

• Node Two could have a problem to achieve 100 Mb/s as the processing power is a bit low.

• All the nodes are connected to a school network. This will probably mean that the link has the highest load during the day. This is why there is a higher chance to achieve full link utilization during the night or weekends.

4.3 Case Three: Delay, Jitter and Packet Loss

4.3.1 Motivation

By using a active measurement tool that measures the delay between two nodes, the jitter and packet loss can be determined by using mathematical methods. The delay can be measured as the time it takes for one packet to be sent from a host, until it is received at the destination. But as this requires that the clocks are perfectly synchronized, an alternative method is mostly used. This is to measure the delay in form of the round trip time.

The round trip time is measured as the time it takes for one packet to be sent from a node to a destination node, until another packet is received from the destination node.

4.3.2 Objective

The previous cases showed methods for measuring the throughput for the link. In this last case study, the delay of a network link is to be measured, and based on those measurements, the jitter and packet loss is to be determined. The round trip time, from one node to three other nodes are to be measured for one week. This should provide enough information to make reasonable decisions about the link state.

4.3.3 Resources

In this experiment, the resources located in table 7 has been utilized.

In addition, the link and processing power of three remote nodes has been utilized. As the active measurements does not require any installation or configuration of the destination nodes, the hardware configuration of Node Three and four are not know.

Description of Node One :-Node One is a host located in a testlab at CMJ University, in Meghalaya. The operating system is GNU Linux Debian, where the version of Debian is "Sarge". The host is also running the following services: PostgreSQL, SMTP, HTTP, HTTPS, FTP, and SSH. The host is connected to a local area network, which shares a 155Mb/s internet connection with the rest of the school. But as the local area network, and the host network interface card only supports fast Ethernet, the maximum network speed is about 100Mb/s.

Description of Node Two :-Node Two is a host located in the student housings at Shillong Engineering andManagement College ,MEGHALAYA. The operating system is GNU Linux Red Hat, where the version of Red Hat is "9.0". The host is connected to a local area network, which shares a 155Mb/s internet connection with the rest of the school. But as the local area network, and the host network interface card only supports Fast Ethernet,

the maximum network speed is about 100Mb/s.

Description of Node Three:- Node Three is a node that is a part of a cluster.The path from Node One to Node Three can be view in table 8.

Table 8: Path from Node One to Node Three.

Path ID	IP	Location
1	128.39.73.1	CMJ University, in Meghalaya
2	158.36.84.21	CMJ University, in Meghalaya
3	128.39.0.73	CMJ University, in Meghalaya
4	193.156.120.3	CMJ University, in Meghalaya
5	193.75.3.6	CMJ University, in Meghalaya
6	193.75.3.1	CMJ University, in Meghalaya
7	193.69.165.11	CMJ University, in Meghalaya
8	193.69.165.11	CMJ University, in Meghalaya
		CMJ University, in Meghalaya
		CMJ University, in Meghalaya
		CMJ University, in Meghalaya
		CMJ University, in Meghalaya

Description of Node Four :-Node Four is a node that is a part of a cluster that serves the "www.kernel.org" domain. This domain belongs to the official GNU Linux kernel. The path from Node One to node four can be view in table 9.

IP	Location
128.39.73.1	CMJ University, in Meghalaya
158.36.84.21	CMJ University, in Meghalaya
128.39.0.73	CMJ University, in Meghalaya
128.39.46.249	CMJ University, in Meghalaya
193.10.68.101	CMJ University, in Meghalaya
193.10.68.29	Stockholm, Sweeden
213.242.69.21	Stockholm, Sweeden
213.242.68.201	Stockholm, Sweeden
212.187.128.25	London, England
4.68.128.106	New York, USA
64.159.1.130	San Jose, USA
4.68.114.158	San Jose, USA
209.245.146.251	San Jose, USA
192.5.4.233	San Jose, USA
204.152.191.5	San Jose, USA

Table 9: Path from Node One to Node Four.

4.3.4 Tools

There are multiple tools for measuring the round trip time, or one-way delays. The tools vary in methods for collecting and measuring the data. The biggest difference is what sort of packet which is used. The available packet formats can be ICMP, TCP or UDP. The tool used to measure the data, is a modified Perl script that utilized the ping command which is available for most operating systems. The Perl script is a part of the pinger measurement package, which is used to shows how the packets are distributed between the different network the load of the CPU usage, on the node. protocols. And it shows General statistical data from the measurements of Node One, can be viewed in table 10. measure round trip times from links all around the world. The modified Perl script together width other scripts are available in the appendix.

4.3.5 Predictions

The predictions for the result are as follows:

• Node Three has the least amount of hops, and is located in CMJ University, in Meghalaya
, this node will probably have the lowest delay, the lowest jitter, and the lowest packet loss.

• Node Two has the second least amount of hops, and it is located in Meghalaya, so this node will probably have a low delay, a predictable jitter, and a low packet loss.

• Node four is located in the United States of America. This will probably result in a high delay, with at times unpredictable jitter. The packet loss should however be relative low, with today's network link properties.

V. RESULTS

5.1 Case One: Network Traffic

Here I data collected from the two nodes by tcpstat program, consists of 17.280 lines, where each line represents one measurement. A sample from the measured data is located beneath.

Output 1 - 10 sample measurements from the tcpstat-node2.log le:

1115157729 0 0 0 117 116 1 687.73 546.39 128742.40 23.40 117 80464 0.01
1115157734 0 0 0 138 136 2 668.99 556.25 147712.00 27.60 138 92320 0.01
1115157739 0 0 0 130 122 8 674.28 540.56 140249.60 26.00 130 87656 0.01
1115157744 0 0 0 118 117 1 708.32 556.59 133731.20 23.60 118 83582 0.01
1115157749 0 0 0 126 124 2 674.03 543.12 135884.80 25.20 126 84928 0.01
1115157754 0 0 0 135 133 2 640.15 552.20 138272.00 27.00 135 86420 0.01
1115157759 0 0 0 125 121 4 701.07 545.80 140214.40 25.00 125 87634 0.01
1115157764 0 0 0 125 123 2 675.81 557.62 135161.60 25.00 125 84476 0.01
1115157769 2 0 0 120 118 2 650.70 541.93 127017.60 24.40 122 79386 0.01
1115157774 1 0 0 123 121 2 723.53 572.89 143548.80 24.80 124 89718 0.01

5.1.1 Analysis and Presentation

The tcpstat program extracts some data from the host node. These values are based on the data that has been measured since last measurement. The following values are processed by tcpstat itself, and can be viewed in the raw data log:

The average/mean packet size. The standard deviation of the size of each packet..The number of bits per second. The number of packets per second Here tcpstat program gathers information about the throughput,shown in packages and in bits per second. It

Table 10: Statistics for Node One.

Description	Bits per second	Packets per second
Minimum value	147, 20	0, 40
Maximum value	58.299.084, 80	28.406, 80
Mean value	1.266.042, 45	474, 57
Median value	7.160, 00	7, 40
Standard deviation value	6.114.076, 61	2.555, 20

Statistical data from these above measurements can be viewed in table 11.

Table 11: Statistics of Node One's Network Layer Protocol.

Description	ARP	ICMP	IPv6	IPv4
Minimum value	0	0	0	0
Maximum value	769	52	24	142.025
Mean value	3, 08	5, 94	0, 06	2367, 12
Median value	0, 00	0, 00	0, 00	33, 00
Standard deviation value	19, 15	13, 28	0, 33	12.775, 29
Sum packages	53.287	102.632	979	40.903.783
Distribution of packages	0, 13%	0, 25%	0, 00%	99, 62%

The tcpstat program also measures how many transport layer packets that has passed through the system since the last measurement and these measurements, can be viewed in table 12.
Table

Table 12: Statistics of Node One's Transport Layer Protocols

Description	TCP	UDP
Minimum value	0	0
Maximum value	142.022	75.583
Mean value	1.507, 92	850, 85
Median value	9, 00	14,00
Standard deviation value	10.417, 22	7.052, 29
Sum packages	26.056.907	14.702.654
Distribution of packages	63, 93%	36, 07%

The distribution of the transport layer protocols can be viewed in the pie chart In figure 6. The transport layer protocols are TCP and UDP, these protocols are encapsulated within the IP protocol.

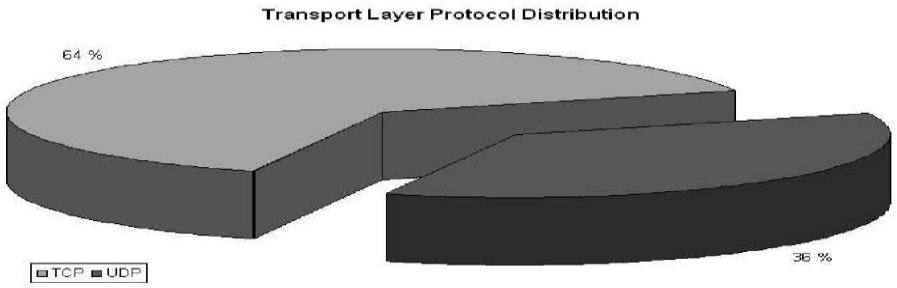

Figure 6 .:- Distribution of the transport layer protocols pie chart

The two first figures show the throughput, in megabits per second, for Node One. Figure 7 shows the measurement in a time series diagram, and figure 8 .shows the distribution of the measurements, in a histogram diagram.

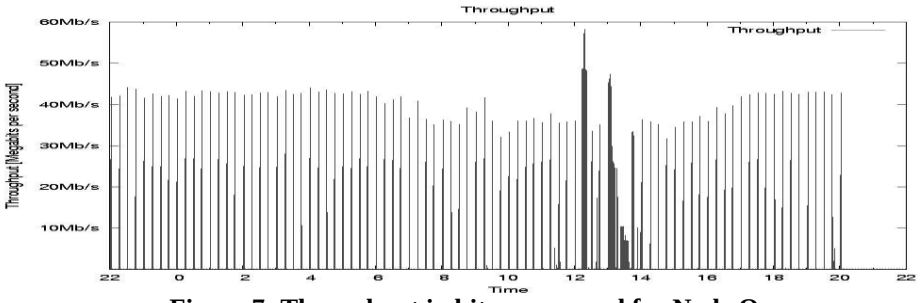

Figure 7: Throughput in bits per second for Node One.

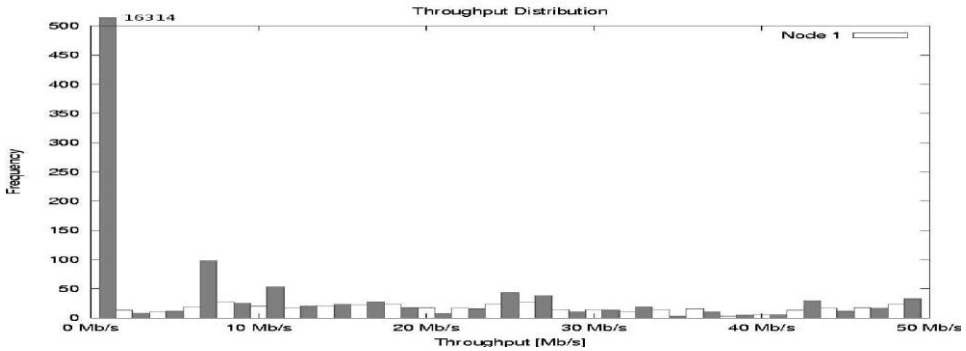

Figure 8:- Distribution of the throughput (bps) for Node One.

The Figure 9 and figure 10 show the throughput, in packets per second, for Node One.

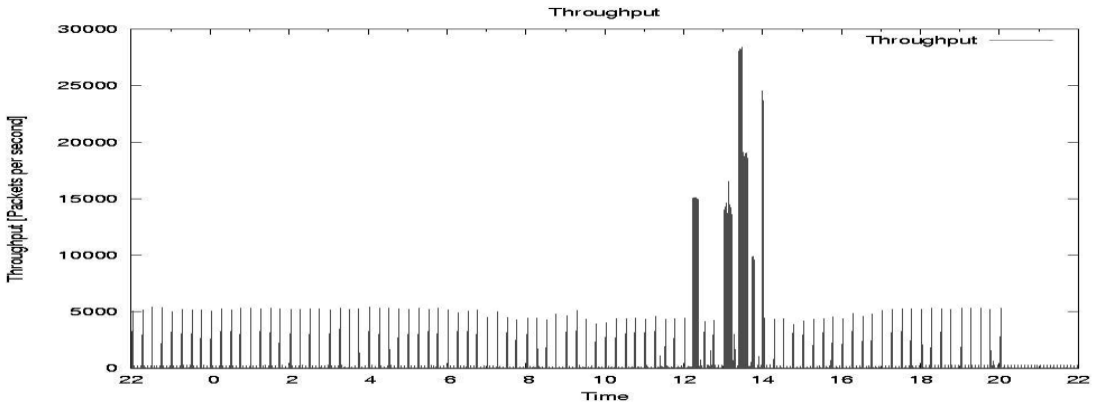

Figure 8: Throughput in packets per second for Node One.

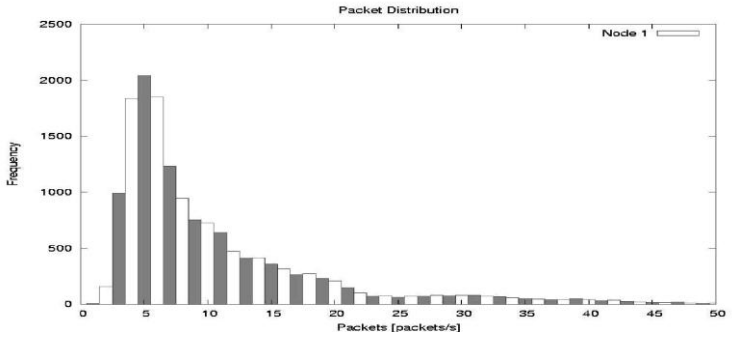

Figure 9: Distribution of the throughput (pps) for Node One.

Table 13: Statistics for Node Two.

Description	Bits per second	Packets per second
Minimum value	76, 80	0, 20
Maximum value	14.849.148, 80	2.002, 40
Mean value	564.568, 72	86, 81
Median value	5.704, 00	3, 20
Standard deviation value	1.832.270, 03	256, 26

Table 14: Statistics of Node Two's Network Layer Protocols.

Description	ARP	ICMP	IPv6	IPv4
Minimum value	0	0	0	1
Maximum value	16	14	0	10.012
Mean value	0, 53	0, 70	0, 00	433, 51
Median value	0, 00	0, 00	0, 00	15, 00
Standard deviation value	0, 94	2, 58	0, 00	1.281, 29
Sum packages	9.227	12.035, 00	0	7.490.984
Distribution of packages	0, 12%	0, 16%	0, 00%	99, 72%

Table 15: Statistics of Node Two's Transport Layer Protocol

Description	TCP	UDP
Minimum value	0	1
Maximum value	10.011	2.777
Mean value	429, 33	3, 46
Median value	7, 00	2, 00
Standard deviation value	1.279, 95	28, 26
Sum packages	7.418.787	59.865, 00
Distribution of packages	99, 20%	0, 80%

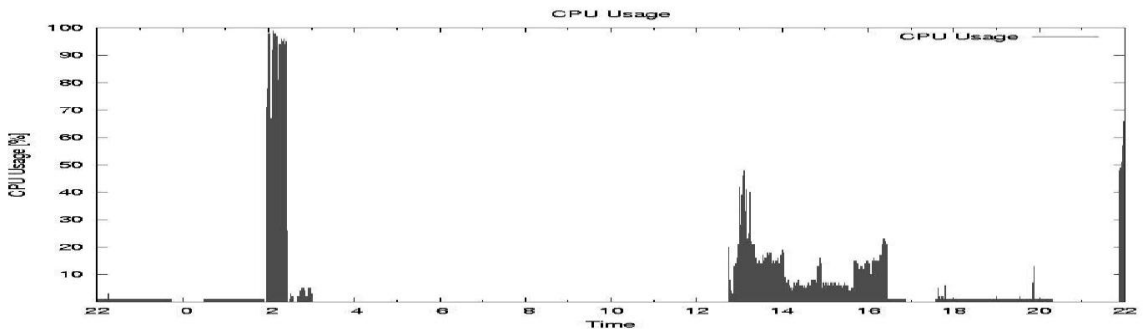

Figure 10:- CPU usage for Node Two.

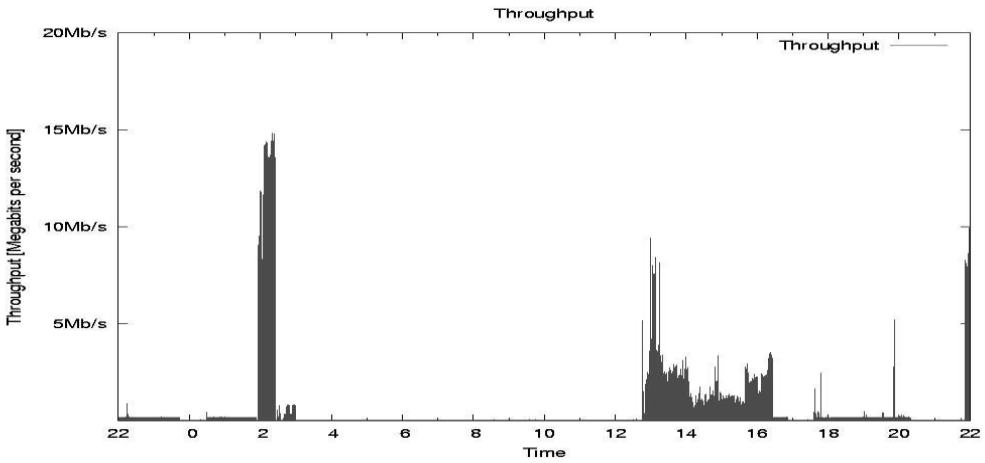

Figure 11: Throughput in bits per second for Node Two.

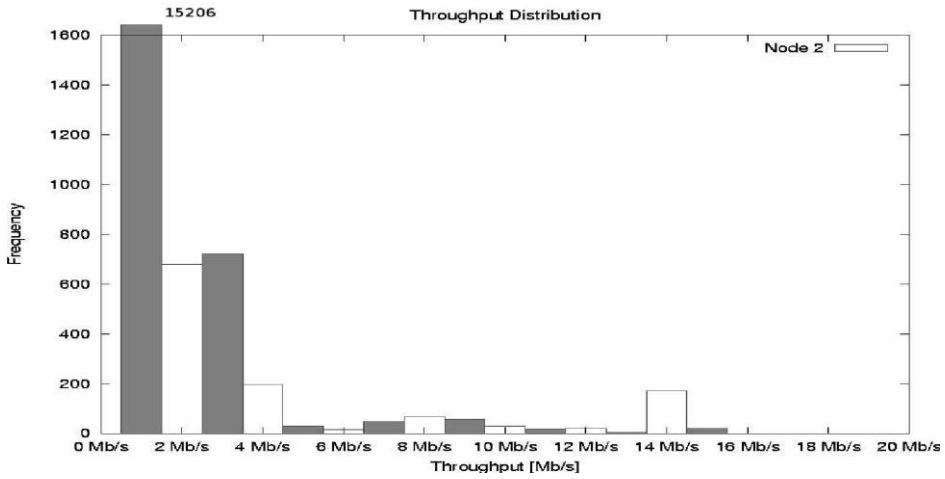

Figure 12: Distribution of the throughput (bps) for Node Two.

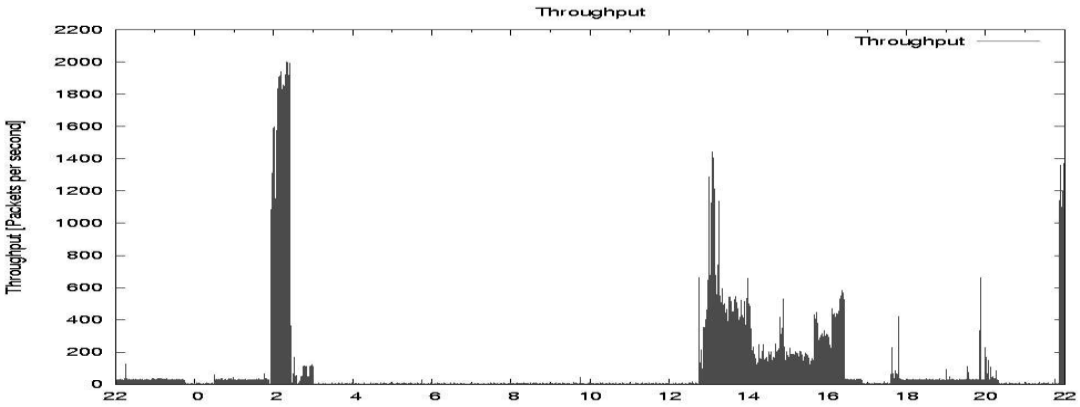

Figure 13: Throughput in packets per second for Node Two.

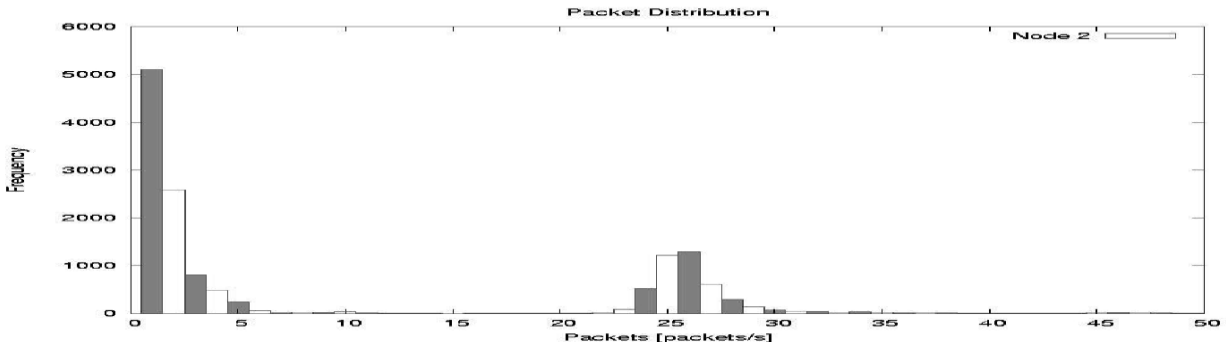

Figure 14: Distribution of the throughput (pps) for Node Two.

5.1.2
Interpretation

Node One:-From the raw data, the analysis, and the presentations, the following information can be interpreted about the state of Node One's network traffic. The general statistics shows that during the 24 hours that the node was monitored, it reached a max throughput of 58 Mb/s, which is a network utilization of 29%, as this is a 100 Mb/s full-duplex connection. The mean throughput was 1Mb/s, which gives a mean network utilization of 0,5%. The general statistics also show that the standard deviation is 6 Mb/s, which would indicate that the traffic was retrieved and/or sent in bursts. In the statistics created by the data from the network layer, one can see that IPv4 dominates the network layer, with a 99,62% margin. But there were over 100.000 ICMP packets sent and/or received during the 24 hours measurements, which means that more then one ICMP packet was sent and/or received every second during that measurement period. As the data show similarities with the data gathered in Case Two, this could lead to the assumption that the active measurements conducted in Case Two has been captured by the passive measurements conducted by tcpstat in this case. The monitored traffic is quite periodic, except between 12:00 and 14:00 where the figure shows shorter bursts of downloads or uploads, with a peak at about 60Mb/s. This is in itself interesting, if there is a correlation between these measurements and the measurements done in Case Two, as that measurement show a top throughput at about 40-45Mb/s, while at least 60Mb/s is a possible throughput. This is about six times higher, compared with the burst peaks at 5000 packets per second. The high packet count between 12:00 and 14:00 could indicate some sort of denial of service attempt or more plausible, the usage of a bit torrent client. This is a plausible assumption, as bit torrent is used on this node to download GNU Linux distributions, which is distributed through the bit torrent network.Figure also varies the observation from figure, about the halt of bursts at 20:00.Figure presents the distribution of the measured throughput data, in packets per second. The figure shows that most of the time, only 3-15 packets per second are passed through the node. This varies the claim that the connection is mostly idle, as 3-15 packets per second in most situations would be considered as an idle connection, at least for a 100Mb/s full-duplex internet connection.Figure presents the CPU usage of the node, during the network traffic measurements. The figure shows a definite correlation between the throughput and the CPU usage. The figure also indicates that 60Mb/s could be the throughput limit, as the CPU reaches 100% utilization at that point. But higher throughput may be possible if the software creating the throughput is requiring much processing power. Lower CPU intensive software may get a higher throughput.**Node Two:-** From the raw data, the analysis, and the presentations, the following information can be interpreted about the state of Node Two's network traffic.The general statistics shows that during the 24 hours that the node was monitored, it reached a max throughput of 15 Mb/s, which is a network utilization of 29%, as this is a 10 Mb/s full-duplex connection. The mean throughput was 500Kb/s, which gives a mean network utilization of 5%. The general statistics also show that the standard deviation is 1,8 Mb/s, which would indicate that the traffic was retrieved and/or sent in bursts. In the statistics created by the data from the network layer, one can see that IPv4 dominates the network layer, with a 99,72% margin. The transport layer statistics show that of the IP traffic, 99% is TCP traffic, and 1% is UDP traffic, this is illustrated in figure 5.7.Interpretations of the other vary figures are as follows: Figure 5.9 presents the throughput measurements, in bits per second, for one day. The figure shows a relative idle connection, with some exceptions when something has been downloaded or uploaded. Around 2:00 the graph passed 10 Mb/s which means that there has to be both upload and downloads, as it is a 10 Mb/s full-duplex internet connection Figure 5.10 presents the distribution of the measured throughput data, in bits per second. It shows that the connection is mostly idle, as the throughput between and 1 Mb/s is dominating in frequency. The usual throughput is 2-3 Mb/s, but also 4 Mb/s and 14 Mb/s occurs quite often Figure presents the throughput measurements, in packets per second, for one day. The graph corresponds with the graph from figure. This graph has a normal amount of packets per second, compared to the throughput. Figure presents the distribution of the measured throughput data, in packets per second. The figure shows that there are either 0-5 packets per second, or 24-28 packets per second.Figure 5.8 presents the CPU usage of the node, during the network traffic measurements. The figure shows that on this node there is also a definite correlation between the throughput and the CPU usage, as with the previous node. The figure also indicates that 15Mb/s could be the throughput limit, as the CPU reaches 100% utilization at that point. But this is a bit strange since this has a considerable better performance then the previous Node.

Case Two: Throughput

The data measured between the two nodes by the netperf program, consists of 650 lines where each line represents one measurement. A sample from the measured data are located beneath.

Output 2 - 15 sample measurements from the netperf-128.39.74.16.log le:

```
...

1114651931  87380  16384  16384  10.01  41.11
1114652771  87380  16384  16384  10.00  40.63
1114653732  87380  16384  16384  10.00  41.26
1114654632  87380  16384  16384  10.01  40.93
1114655532  87380  16384  16384  10.01  40.97
1114656371  87380  16384  16384  10.01  40.95
1114657332  87380  16384  16384  10.01  40.55
1114658232  87380  16384  16384  10.01  40.69
1114659132  87380  16384  16384  10.00  41.46
1114659971  87380  16384  16384  10.01  40.83
1114660931  87380  16384  16384  10.00  41.24
1114661831  87380  16384  16384  10.01  41.21
1114662731  87380  16384  16384  10.02  28.60
1114663571  87380  16384  16384  10.01  31.03
1114664532  87380  16384  16384  10.01  40.89
```

Table 16: Description of the raw data.

.

Column	Description
Column 01	Timestamp in UNIX time.
Column 02	The buffer socket size for the recieving host.
Column 03	The buffer socket size for the sending host.
Column 04	The send size for the message.
Column 05	Elapsed time, in seconds.
Column 06	The throughput expressed in 10^6 bits per second.

The throughput of the measurements is included in the data logs, and is shown in the last column as megabits per second.Node One to Node Two Statistical data from the measurements between Node One and Node Two, can be viewed in table 16.

Table 17: Statistical data between Node One and Node Two.

Description	Value
Minimum value	0, 00 Mb/s
Maximum value	25, 70 Mb/s
Mean value	20, 20 Mb/s
Median value	22, 10 Mb/s

.

Table 18: Throughput Distribution between Node One and Node Two.

Throughput	In Frequency	In Percentage
00 Mb/s - 05 Mb/s	22	3%
05 Mb/s - 10 Mb/s	19	3%
10 Mb/s - 15 Mb/s	34	5%
15 Mb/s - 20 Mb/s	140	21%
20 Mb/s - 25 Mb/s	353	53%

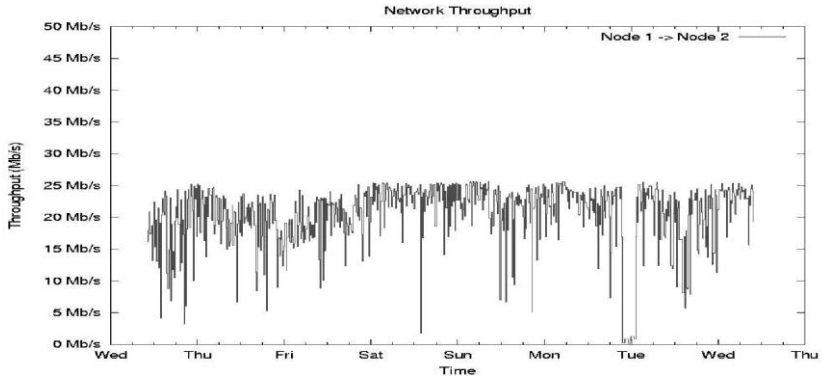

Figure 15: The figure shows a Throughput between Node One and Node Two.

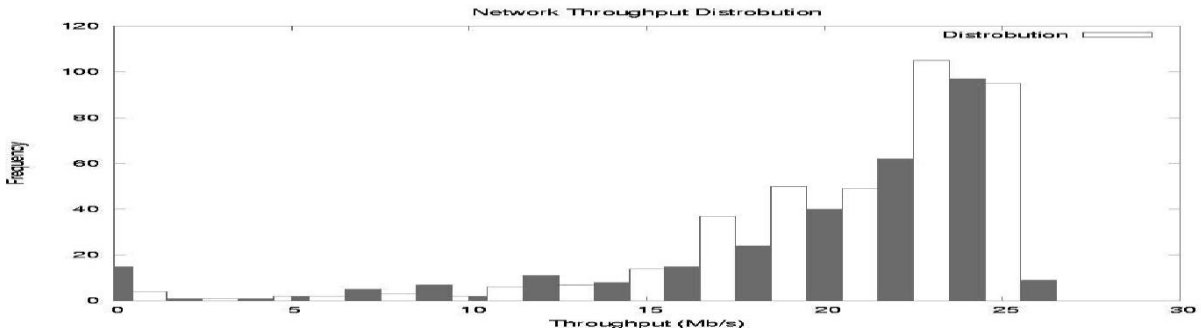

Figure 16: The figure shows the distribution of the throughput between Node One and Node Two.

A summery of the distribution of the throughput data, can be viewed in table 19.

Table 19: Throughput distribution between Node One and

Throughput	in Frequency	in Percentage
00 Mb/s – 05 Mb/s	16	2%
05 Mb/s – 10 Mb/s	0	0%
10 Mb/s – 15 Mb/s	1	0%
15 Mb/s – 20 Mb/s	12	2%
20 Mb/s – 25 Mb/s	40	6%
25 Mb/s – 30 Mb/s	62	9%
30 Mb/s – 35 Mb/s	102	15%
35 Mb/s – 40 Mb/s	138	21%
40 Mb/s – 45 Mb/s	301	45%
45 Mb/s – 50 Mb/s	0	0%

A time series graph, and a histogram graph of the data are presented in figure 16, and in figure 17

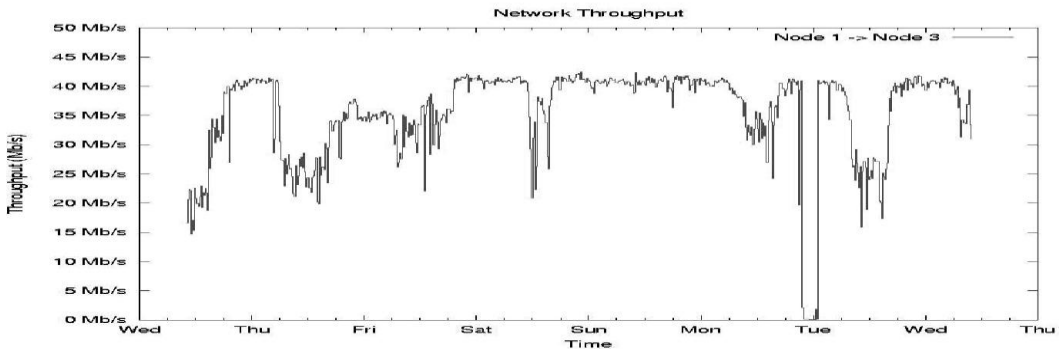

Figure 17: the figure shows a Throughput between Node One and Node Three.

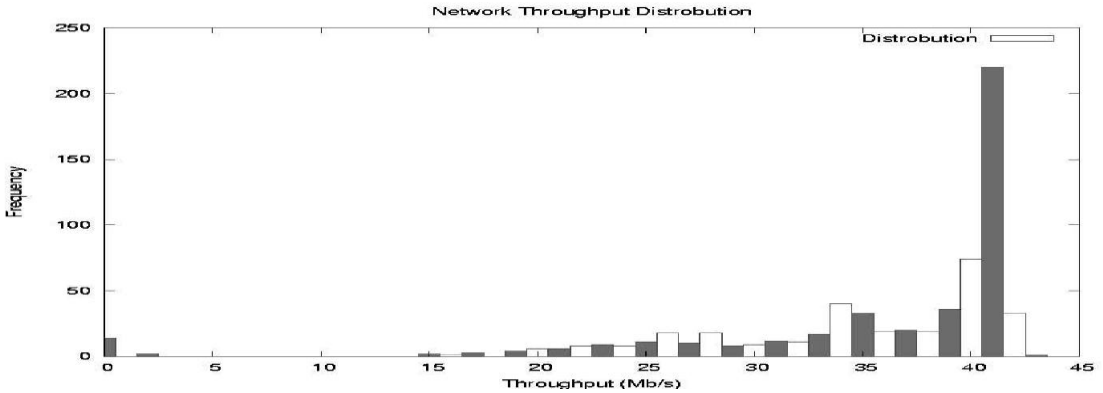

Figure 18: The figure shows the distribution of the throughput between Node One and Node Three .

5.2.2 Interpretation:

Node One to Node Two :- The statistics show a mean throughput value of 22,20 Mb/s, which is a 22,2 utilization of the network bandwidth. But it reached a maximum throughput of 25,70 Mb/s, which is a25,7% utilization of the network bandwidth.

5.3 Case Three: Delay, Jitter and Packet Loss

The data collected from the three nodes by the pinger script, consists of 2.000 lines, where each line represents one measurement. A sample from the measured data is located beneath.

5.3.1 Analysis and Presentation:-The pinger script extracts data gathered from the active measurements, it also pro-vides some processed data based on the measured data. The following values are processed from the ten round trip time values measured for that measurement:The minimum RTT of the ten packages sent in that measurement

The mean RTT for the ten packages sent in that measurement.

The maximum RTT of the ten packages sent in that measurement.

Node One to Node Two:- Statistical data from the measurements between Node One and Node Two, can be viewed in table 20.

Table 20: Statistical data between Node One and Node Two.

Description	Value
Minimum value	16, 80 ms
Maximum value	199, 80 ms
Mean value	23, 10 ms
Median value	18, 30 ms
Standard deviation value	16, 60 ms

The packet loss rate between Node One and Node Two, was 809/20160 as there where 602 error, and a total of 20160 packets.

Node One to Node Three:-Statistical data from the measurements between Node One and Node Thre can be viewed in table 21.

Table 21:- measurements between Node One and Node Three

Description	Value
Minimum value	1, 00 ms
Maximum value	635, 30 ms
Mean value	8, 70 ms
Median value	1,60 ms
Standard deviation value	25, 25 ms

The packet loss rate between Node One and Node Three, was 594/20160.

Node One to Node Four:- Statistical data from the measurements between Node One and Node Three, can be viewed in table 22.

Table 22 : Statistical data between Node One and node four.

Description	Value
Minimum value	184, 70 ms
Maximum value	310, 30 ms
Mean value	188, 50 ms
Median value	187, 60 ms

Standard deviation value	37, 40 ms

Table 23: Round Trip Time (RTT) between Node One and Node Four.

Round Trip Time	in Frequency	in Percentage
-> 0ms	0	0%
185 ms	22	0,10%
186 ms	6041	31,20%
187 ms	2716	14,00%
188 ms	4015	20,80%
189 ms	2683	13,90%
190 ms	813	4,20%
191 ms	954	4,90%
192 ms ->	2107	10,90%

Table 24: Jitter between Node One and Node Four.

Jitter	in Frequency	in Percentage
0 ms	1430	7,10%
1 ms	7295	36,20%
2 ms	6178	30,70%
3 ms	1548	7,70%
4 ms	970	4,80%
5 ms ->	2738	13,60%

The packet loss rate between Node One and node four was 809 error, and a total of 20160 packets. To present then measured and analyzed data, the following figures are used:

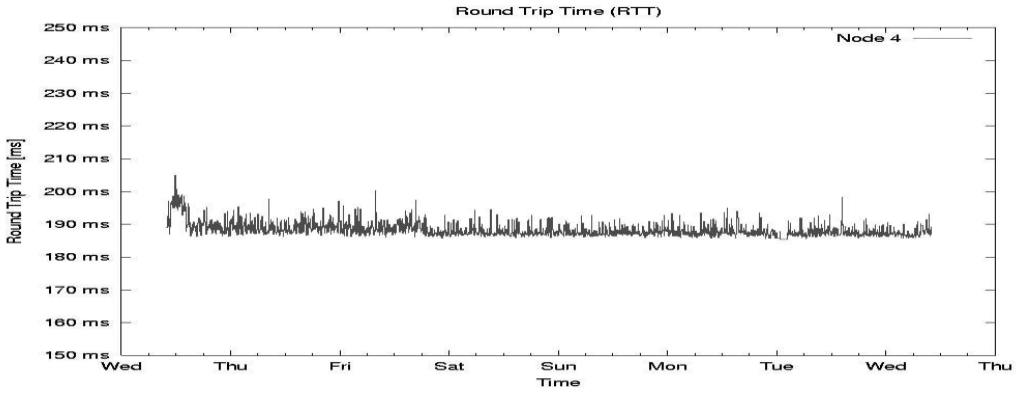

Figure 19: Delay between Node One & Node Four.

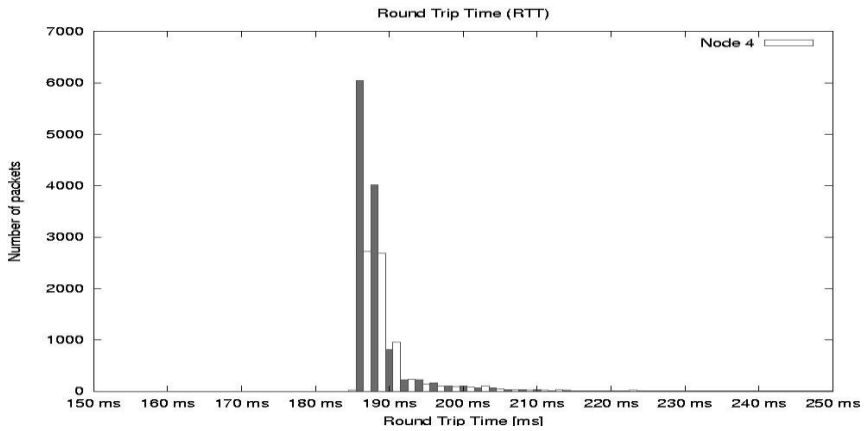

Figure 20: Histogram of Node One & Node Four.

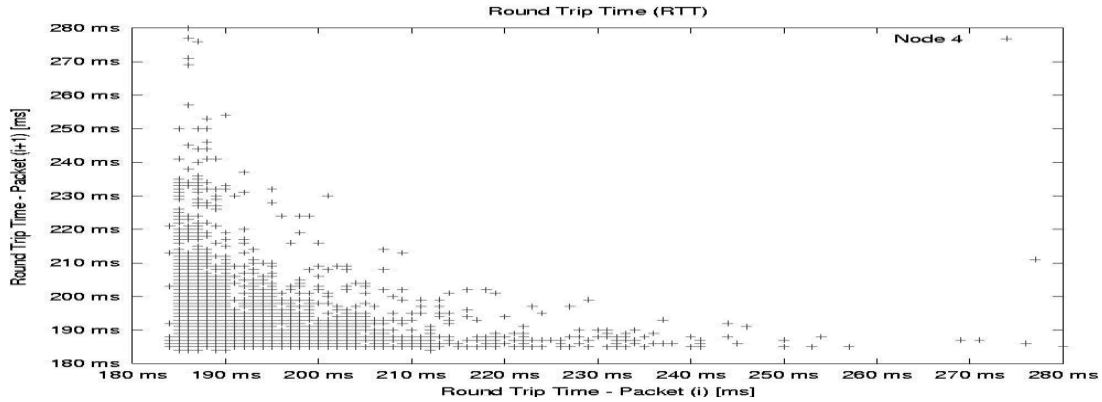

Figure 21: Phase plot of Node One & Node Four.

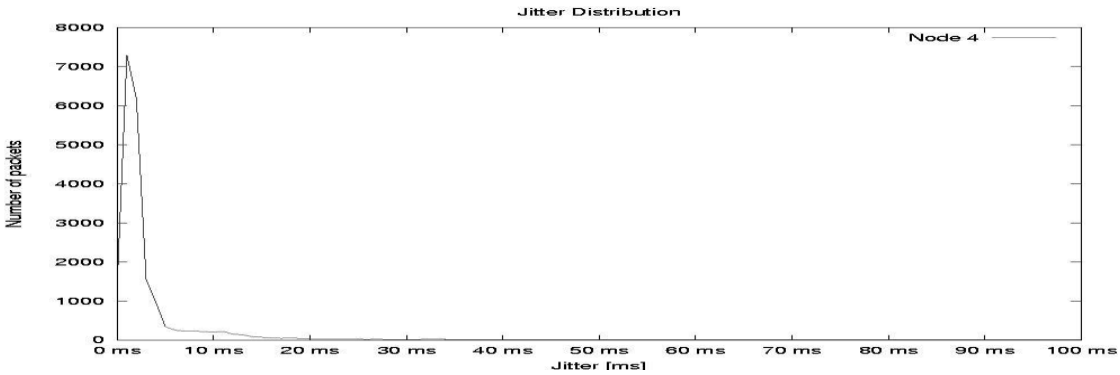

Figure 22: Distribution of jitter between Node One & node four.

Node One to Node Three:-The measurements show that there where 594 errors out of a total of 20160 packets.Of the packets that where received, the minimal round trip time was 1,00 ms, the maximum round trip time was 635,30 ms, and the mean round trip time was 8,70 ms. Figure presents the mean value, for the ten samples sent in each measurement, in a time series diagram. The Figure has a relative predictable pattern, where the transmission delay and the propagation delay represents the predictable 1-2 ms minimum delay, and the queuing delay represents the random delay. The pattern shows bursts of data from about 5 ms, to about 40 ms, and occasionally bursts up to 160 ms, but the bursts occur at executed periods of the day, indicating periods of high load.

Node One to Node Four:-The measurements show that there where 809 errors out of a total of 20160 packets. Of the packets that where received, the minimal round trip time was 184,70 ms, the maximum round trip time was 310,30 ms, and the mean round trip time was 188,50 ms. Figure has a very predictable pattern, where the transmission delay and the propagation delay represents the predictable 185 ms minimum delay, and the queuing delay represents the random delay, but the delay is only about 10 ms. The standard deviation of 37,40 ms seems not to correspond with Figure presents the distribution of the measured round trip times, in a histogram. The Figure shows that most of the packets arrive within the range of 184 ms to 191 ms, which is a relative large delay. Figure present the RTTi and RTTi+1 packets in a phase plot diagram. The Figure show that most samples are in region I (bottom left corner), which suggests a low congestion. The Figure also shows that there are some transition delays, where one of the packets are queued, while the other packets pass right through, but these transitions does not occur often. Figure presents a distribution of the jitter, in a histogram. From the Figure it becomes clear that the majority of the packets arrive within 6 ms, and the rest of the packets arrive within 20 ms. The Figure show that the delays are medium, the jitter is low, and the packet loss is also low. This shows that the internet connection between Node One and four are of good quality, but with a medium delay. This delay is probably caused by the propagation delay, from the United States of Americas west coast to Europe, through the Atlantic Ocean. But because of the lack of bursts, this connection probably supports quality of service, by the use of some sort of traffic shaping method.

VI. CONCLUSION

The objective with this study was to assist network and system administrators in administration of remote computer networks. This was primary done by identifying the properties for securing the remote computer networks, and the properties that are important for the quality of the services. The properties provide quality of service for the connection between the remote computer networks. Secondary, some simple methods for analyzing and presenting the measured data was identified. These methods simplify the interpretation part of the administration of remote computer networks. The three case studies were created to demonstrate the functionality for some of the tools used to measure the four properties in quality of service.

In Case One, the objective was to make use of passive throughput measurement tools, to monitor the traffic on two different nodes for one day. The tcpstat tool successfully measured the data on both nodes, and provided enough information to create a good understanding of what had happened on the network for the last 24 hours. The only mistake in these two experiments was that the alter functionality in tcpstat should had been used to alter input and output traffic. But as the objective was demonstrate, the experiments can still be classified as successful.

In Case Two, the objective was to make use of active throughput measurement tools, to benchmark the network connection between two different nodes for one week. The netperf tool successfully measured the throughput from one node, to two other nodes situated at different computer networks. In this case, the results did not match the predictions, and this had probably something to do with limited hardware resources at the nodes. It would have been interesting to remove that bottleneck, and have really tested the network throughput between two high performance nodes, or at least include the CPU of the measurement nodes during the measurement. But again the objective was to demonstrate the active throughput tools, and since netperf performed as expected, the experiment can still be classified as successful.

In Case three, the objective was to make use of active delay measurement tools, to benchmark the network connection between three different nodes for one week. The round trip time measurement that was done in the experiment can be used to found both the delay and the jitter of a connection. The packet loss data can be used to figure out the reliability of the connection. These three properties provide important information bout the quality of service for the connection. And with the available information relative important assumptions could be done to describe the quality of service for these network connections. This helps the system administrator in designing the network for services that require different quality of service properties. This experiment can definitely be classified as successful.

The three case studies together demonstrated all aspects of quality of service measurements, and together with the analysis and presentation methods described in this thesis, the network and system administrators should be able to administrate remote computer networks.

REFERENCE

1. Andrew S.Tanenbaum. Computer Networks, Fourth Edition. Prentice Hall, 2003, revised 2011.
2. http://en.wikipedia.org/wiki/Computer_network
3. http://www.google.co.in/search?q=computer+network+lan&hl=en&tbo=d&source=lnms&tbm=isch&sa=X&ei=4mfsUPKRJIeOkgXh44GQBQ&ved=0CAcQ_AUoAA&biw=1024&bih=456
4. http://www.google.co.in/imgres?q=Home+network&um=1&hl=en&sa=N&tbo=d&biw=1024&bih=456&tbm=isch&tbnid=C8iIAueiW8IqM:&imgrefurl=http://www.arronsupport.co.uk/networking.php&docid=BzSP0MTfLadgnM&imgurl=http://www.arronsupport.co.uk/PC_Support/image/network2l.jpg&w=518&h=674&ei=i2jsUMajLoeClAXFqYCIDg&zoom=1&iact=hc&vpx=12&vpy=95&dur=476&hovh=141&hovw=108&tx=85&ty=174&sig=110711043523376603863&page=1&tbnh=141&tbnw=108&start=0&ndsp=10&ved=1t:429,r:0,s:0,i:102
5. Annabel Z. Dodd. The Essential Guide to Telecommunications, Second Edition.Prentice Hall PTR, 1999.
6. Sergio Verdú. Wireless bandwidth in the making. IEEE, 2000.
7. Kevin Hamilton Kennedy Clark. Cisco LAN Switching (CCIE Professional Development).Cisco Press, 1999.
8. Mark Burgess. Analytical Network And System Administration. Wiley, 2004.
9. http://en.wikipedia.org/wiki/Network_delay/2012
10. Matt Bishop. Computer Security, Art and Science. Addison-Wesley, 2002.
11. Mahbub Hassan and Raj Jain. High Performance TCP/IP Networking. Pearson.
12. Bruce S. Davie Larry L. Peterson. Computer Networks - A System Approach,.-2008
13. The Board of Trustees of the University of Illinois. The iperf website.
14. http://dast.nlanr.net/Projects/Iperf/, May 2005.
15. The ttcp website. http://www.pcausa.com/Utilities/pcattcp.htm, May 2005.ond Edition. Morgan Kaufmann, 2000.Prentice Hall, 2004,2012.
16. Sugih Jamin Amgad Zeitoun, Zhiheng Wang. Rttometer: Measuring path minimum rtt with con_dence. Technical report, The University of Michigan, Ann Arbor, 2003.
17. Joseph D. Sloan. Network Troubleshooting Tools. O'Reilly, 2001.
18. Rick Jones. The netperf website. http://www.netperf.org/, May 2005.
19. http://blog.level3.com/data-center-networking/improve-your-day-with-less-round-trip-delay/ of 2012 by admin
20. Kevin Mills and Christopher Dabrowski. Adaptive Jitter Control for UPnP M-Search,2012
21. Dictionary.com. Dictionary.com's website. http://dictionary.com/, May 2011.
22. Muriel M´edard.Network Reliability and Fault Tolerance 2010
23. Mahbub Hassan and Raj Jain. High Performance TCP/IP Networking. Pearson Prentice Hall, 2011.
24. Cross-Industry Working Team. Internet service performance: Data analysis and visualization. Technical report, The Cross-Industry Working Team (XIWT),2000,2009
25. PING 127.0.0.1 Computer Services. The ping website. http://www.ping127001.com/pingpage.htm, 2005,2009.
26. Zhiheng Wang Amgad Zeitoun. The rttometer website.
27. http://idmaps.eecs.umich.edu/rttometer/, 2005.

AUTHORS – BIBLIOGRAPHY

[1] Mr. Devajit Mahanta, MSc (Computer Science) , MCA ,M.Phil

He received his MSc (Computer Science) degree from the Sikkim Manipal University,Gangtok in 2007 and MCA degree from the Punjab Technical University,Punjab in 2008 and M.Phil(Computer Science) from CMJ University,Meghalaya,India in 2011 .He is a Assistant professor in the department of Computer Science in the Nalbari college(under Gauhati University)for the past 5yrs. At the moment he is a PhD student in the department of Computer Science in the Faculty of computer Science of CMJ University, Meghalaya,India.
devajitmahantah@sify.com
+91-9864147912
+91-8876664921

[2]Dr. Majidul Ahmed**, PhD**

He did his PhD at Gauhati University,Guwahati,Assam. He worked as a Assistant professor and HOD, Department of Information Technology, Gauhati Commerce College (under Gauhati University), Guwahati Assam (India) for the past 9yrs.
E-mail:- mjdahmd10@gmail.com