**CHAPTER ONE**

**INTRODUCTION**

* 1. **PREAMBLE**

As the networking technology improves so are the demands of network users and their applications increasing. A wide variety of new applications are being invented daily. These applications have different demands. High bandwidth internet connectivity has become a basic requirement for efficient internet access, most often in academic environment. Wireless Local Area Networks (WLANs) has become one of the most promising and successful Technology in recent years. WLANs provide free wireless connectivity to end users, offering an easy and viable access to the network and its services in schools, office enterprises, public places and homes. Wireless networks are superior to wired networks with regard to issues such as ease of installation and flexibility. They do, however, suffer from lower bandwidth, higher delays, higher bit-error rates, and higher costs than wired networks. With the advent of Wireless Local Area Networks (WLANs), bandwidth has increased and prices have decreased on Wireless networking solutions. These factors have made WLANs a very popular Wireless networking solution.

This project is an effort at highlighting the problems (related to Quality of Service) encountered by the users of Campus Area Networks(CAN), taking in to cognisance The Ahmadu Bello University CAN.

Wireless networks are still an evolving technology and new standards are still being developed to increase bandwidth, enhance security and improve QoS delivery.

**1.2 PROBLEM DEFINITION**

High raw data rates (up to 11Mbps/54Mbps as per standards and twice that in proprietary ways) at physical layer have become possible in wireless communication. A key component in the development of single channel wireless networks is the medium access control (MAC) protocol with which nodes share a common radio channel.

A MAC protocol should provide an efficient use of the available bandwidth while satisfying the Quality of Service (QoS) requirements of both data and real-time applications. Real-time services such as streaming voice and video require a certain quality of service such as low packet loss and low delay to perform well. To provide QoS for such kind of applications, service differentiation is a must. Service differentiation means that different types of traffic have different requirements on the network. Various mechanisms have been developed to support quality of service but no effort has been made to implement the latest techniques in the Campus Networks.

The OPNET IT Guru Network Simulator is used to analyse them under some traffic conditions. This project analyses some QoS parameters (Bottleneck delay and throughput), their effect on single gateway Campus Networks and preparing recommendations for future development processes of QoS mechanisms in providing quality of service in WLANs. Here, unlike the real time network present (ABU hotspot), a virtual Intranet is considered where the campus own its servers. So, all users are tapping resources from those servers.

The main objectives of the Project are:

* The study of basic concepts and issues of Wireless network that causes delay in Wireless Campus Networks.
* Generation of efficient statistical data with regard to the QoS of WLAN by using OPNET IT Guru Network Simulator wireless module.
* Study the results obtained, and recommend the best possible access medium that can provide high QoS under respective network traffic conditions.
* To critically examine the constraints of the selected medium of transmission.
* Suggest some possible ways to minimise the rate of starvation of lower priority processes.

**1.3 LITERATURE REVIEW**

Wireless networking is an attractive networking solution due to its flexibility, mobility and ease of installation without damaging the furnishing of buildings (this factor play most important role in of situations where buildings are of higher heritage importance). In the earlier phases of its development, the wireless networks had low bandwidth, high bit-error rates and high prices which impeded their deployment. When WLANs were introduced in full fledge, a new era of wireless networking began.

The following texts were being consulted in the course of the project;

Ranjan Kaparti & Dan Likarish (2007) emphasized the importance of working with OPNET IT Guru Academic edition in Institutions of higher learning. The nature of the Networking technology itself is such that it is difficult to get “hands on” with it from the point of view making the technology available for classroom use. There is the issue of expense also. Many institutions for instance may not have the resources to build an appropriate lab with all relevant hardware and software. Furthermore real world networks may span not merely a lab or two but rather entire buildings or even multiple global locations. As such, the use of Network Simulators became inevitable for modelling and analysing network Performance [11].

Wheat, Jeffery et al (2001) hoped that the readers with no previous wireless or IP design experience to understand how wireless communication works, the physics behind it and its components. He cited the various technologies used today in deploying wireless networks with reference made to design case studies.

**1.4 PROJECT MOTIVATION**

I have always been excited hearing the phrase “Wireless Communication”, I wondered how it was possible to send letter or even communicate wirelessly, and having been very much used to NIPOST and NITEL i.e. the wired telephone.

Then came the time I dwell in a heterogeneous academic institution, the Ahmadu Bello University. Here I found many places to learn networking from fundamentals to a wider scope (CCNA).

I picked up interest in writing my project on this area, having recognised that students at the Samaru Campus are always complaining about how they suffer when trying to access the internet via the Campus hotspot. Hence the money they paid on ICT services seems useless.

With all these in mind, I decided to do my Project in analysing the QoS in a Campus network where all routers are connected to the gateway routerwirelessly under light of heavy client population.

**1.5 PROJECT OUTLINE**

The rest of the Project is organized as follows:

The whole work is divided in to five chapters, chapter one is the introduction: this introduction includes preamble, problem definition, literature review, thesis motivation and organisation of the project.

Chapter two explains technical overview; it explains the wireless technologies, standards, components, configurations, how it works and the factors halting their propagation.

Chapter three explains the quality of service parameters considered in the project (i.e. delay and throughput). It also explains IT Guru Academic Edition and how the wireless network topology of concern was created and configured.

Chapter four showed the processes followed to simulate the network and how the results were obtained. The results were also analysed using graphs.

Chapter five gives a summary of the network condition, the factors that contribute to those conditions and recommend some ways to improve the network performance.

**CHAPTER TWO**

**THEORETICAL BACKGROUND**

**2. 1 Wireless Media**

Wireless refers to the transmission of data and voice over radio waves. There for transmitting a signal using the typical 802.11 specification works a lot like it does with basic Ethernet. It allows its users to communicate with each other without requiring a physical connection to the network [2].

Wireless devices include anything that uses a wireless network to either send or receive data. Wireless communication has become the most widely used way to connect people. Cellular systems have experienced exponential growth over the last decade and there are currently around two billion users worldwide [2].

Wireless networks devices also called ‘wireless components’ works as networks that use a physical medium. Specifically, wireless nodes need transmitters and receivers, just like wired nodes. However, wireless components may take somewhat different forms and may turn up in unusual locations in wireless networks.

A network may use antennas located at strategic points to broadcast and capture signals across the network. In wireless communications, each node may have its own antenna, or a single antenna may serve a limited area. Antennas will generally be placed in open, unobstructed areas in order to avoid objects that can block incoming or outgoing signals.

**2.2 Wireless Local Area Network (WLAN)**

Wireless networks have expanded as its end users multiply geometrically in the world. As WLANs eliminate the need of wires for connecting end users, they provide a very easy, viable access to the network and its services.

A wireless LAN is a wireless local area network, which links two or more computers and other wireless components without using wires. WLAN utilizes spread-spectrum modulation technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network. Wireless has become popular due to ease of installation and mobility. To transport the data on a wireless network radio frequency, microwave and infrared are used as a transportation media [3].

* **The Radio Frequency Spectrum**

RF refers to frequencies of radio waves. RF is part of electromagnetic spectrum that ranges from 3 Hz - 300 GHz. Wireless technologies use electromagnetic waves to carry information between devices. An electromagnetic wave is the same medium that carries radio signals through the air. The electromagnetic spectrum includes such things as radio and television broadcast bands, visible light, x-rays and gamma-rays. Each of these has a specific range of wavelengths and associated energies as shown in the diagram.

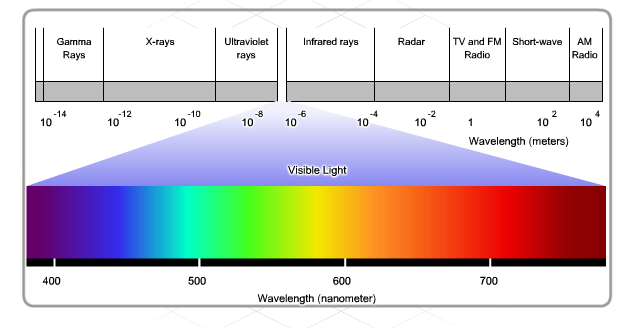


Fig. 2.1 Electromagnetic Spectrum [4]

Certain areas of the RF bands have been set aside for use by unlicensed devices such as wireless LANs, cordless phones and computer peripherals. This includes the 900 MHz, 2.4 GHz, and the 5 GHz frequency ranges. These ranges are known as the Industrial Scientific and Medical (ISM) bands and can be used with very few restrictions.

* **Bluetooth**

Bluetooth is a technology that makes use of the 2.4 GHz band. It is limited to low-speed, short-range communications, but has the advantage of communicating with many devices at the same time. This one-to-many communications has made Bluetooth technology the preferred method over IR for connecting computer peripherals such as mice, keyboards and printers.

Other technologies that make use of the 2.4 GHz and 5 GHz bands are the modern wireless LAN technologies that conform to the various IEEE 802.11 standards. They are unlike Bluetooth technology in that they transmit at a much higher power level, which gives them a greater range.

* **Infrared**

Infrared (IR) is a relatively low energy EM wave and cannot penetrate through walls or other obstacles. Infrared light is part of electromagnetic spectrum that is shorter than radio waves but longer than visible light. Its frequency range is between 300 GHz and 400 THz that corresponds to wavelength from 1mm to 750 nm [2].

However, IR is commonly used to connect and move data between devices such as Personal Digital Assistants (PDAs) and PCs. A specialized communication port known as an Infrared Direct Access (IrDA) port uses IR to exchange information between devices. IR only allows a one-to-one type of connection [3].

IR is also used for remote control devices, wireless mice, and wireless keyboards. It is generallyused for short-range, line-of-sight, communications. However, it is possible to reflect the IR signal off objects to extend the range. For greater ranges, higher frequencies of electromagnetic waves are required.

* **Microwave**

Microwave is the upper part of RF spectrum having frequencies above 1 GHz. Because of the availability of larger bandwidth in microwave spectrum, microwave is used in many applications such as wireless Personal Area Network (Bluetooth), Wi-Fi, broadband wireless access (BWA) or wireless Metropolitan Area Network (WiMAX), wireless WAN (2G-4G cellular networks), satellite communications and radar. But it became very famous in houses because of its use in microwave oven [4].

# 2.2.1 Introduction to IEEE 802.11

In 1997 the IEEE adopted IEEE Std. 802.11-1997, the first wireless LAN (WLAN) standard. This standard defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless connectivity. It addresses local area networking where the connected devices communicate over the air to other devices that are within close proximity to each other.  
The standard is similar in most respects to the IEEE 802.3 Ethernet standard. Specifically, the 802.11 standard addresses:

* Functions required for an 802.11 compliant device to operate either in a peer-to-peer fashion or integrated with an existing wired LAN
* Operation of the 802.11 device within possibly overlapping 802.11 wireless LANs and the mobility of this device between multiple wireless LANs
* MAC level access control and data delivery services to allow upper layers of the 802.11 network
* Several physical layer signalling techniques and interfaces
* Privacy and security of user data being transferred over the wireless media

**2.2.2 Working of WLAN**

Wireless networks perform functions similar to their wired Ethernet. Networks perform the following functions to enable the transfer of information from source to destination [5];

* The medium provides a bit pipe (a path for data to flow) for the transmission of data.
* Medium access techniques facilitate the sharing of a common medium.
* Synchronization and error control mechanisms ensure that each link transfers the data intact.
* Routing mechanisms move the data from the originating source to the intended destination.
* Connectivity software interfaces an appliance, such as a pen-based computer or bar code scanner, to application software hosted on a server.

**2.2.3 Advantages of Wireless LAN**

***Flexibility***: within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls.

***Planning***: wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.

***Robustnes****s*: wireless networks can survive disasters; if the wireless devices survive people can still communicate

**2.2.4 Disadvantages of Wireless LAN**

***Connectivity***: There are no wires to connect to the Wi-Fi network but then the area of the hotspot is very limited and if the node gets out of the area it will be disconnected. This is perhaps the greatest disadvantages you have to be within 100-150 ft of the base station (indoors) and about 100-300 meters (outdoors) to get connected.

***Quality of Service (QoS)***: WLANs offer typically lower QoS. Lower bandwidth due to

Limitations in radio transmission and higher error rates due to interference.

***Safety and security***: using radio waves for data transmission might interfere with other high-tech equipment. The greatest challenge faced by Wi-Fi providers today is how to prevent outsiders from accessing the data.

**2.3 Logical Architecture of WLAN**

WLAN works in the lower two layers of OSI Reference model. First one is the physical layer which takes care of transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications. Second one is the data link layer which is sub-divided into two layers: logical link layer (LLC) and Medium Access Control layer (MAC) [5]. Only MAC layer is considered as the part of wireless LAN Functions.

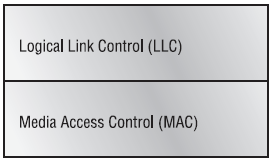


Fig. 2.2 the Divisions of Data Link Layer [15].

**2.3.1 Medium Access Control (MAC) Sub layer**

The primary function of a MAC protocol is to define a set of rules and give the stations a fair access to the channel for successful communication. Many MAC protocols provide the standardized medium access and physical layer protocols for WLANs and it is the most widely employed standard in wireless networks. Medium access control enables multiple wireless devices to share a common transmission medium via a carrier sense protocol similar to Ethernet. This protocol enables a group of wireless computers to share the same frequency and space. A wireless LAN Media Access Control protocol provides reliable delivery of data over somewhat error-prone wireless media.

**2.3.2 Physical Layer**

The Physical layer provides the transmission of bits through a communication channel by defining electrical, mechanical, and procedural specifications. Modulation, which is a Physical layer function, is a process in which the radio transceiver prepares the digital signal within the network interface card (NIC) for transmission over the air waves.

Spread spectrum “spreads” a signal’s power over a wider band of frequencies, sacrificing bandwidth in order to gain signal-to-noise performance [2]. This contradicts the desire to conserve frequency bandwidth, but the spreading process makes the data signal much less susceptible to electrical noise than conventional radio modulation techniques.

Other transmission and electrical noise, typically narrow in bandwidth, will interfere with only a small portion of the spread spectrum signal, resulting in much less interference and fewer errors when the receiver demodulates the signal. Spread spectrum modulators commonly use one of two methods to spread the signal over a wider area: frequency hopping or direct Sequence [2]. Main layer to be analyzed is MAC layer.

**2.4 Physical Architecture of WLAN**

There are two kinds of WLAN architectures:

* Ad-hoc (Infrastructure less) architecture or IBSS
* Infrastructure architecture

**2.4.1 Independent Basic Service Set (IBSS) Architecture**

It is the simplest WLAN configuration. It is an independent (or peer-to-peer) WLAN and is also known as an Ad-hoc network. It is a group of computers each equipped with a wireless LAN client adapter. In this configuration, no access point is necessary and the devices in the LAN configure themselves at the same radio channel to enable peer-to-peer communication. Independent network can be set up whenever two or more wireless adapters are within range of each other.

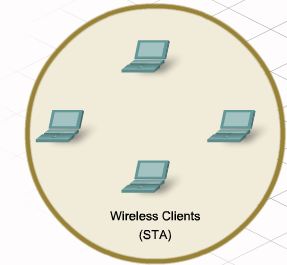


Fig. 2.3 Independent Basic Service Set [4].

**2.4.2 Infrastructured Architecture**

Infrastructured also called the Basic Service Set (BSS) WLAN consists of wireless stations and access points. Access Points are connected with a distribution system (such as Ethernet). Different access points create different cells having different locations and a confined communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called “handoff”



Fig. 2.4 Infrastructured Network [4]

**2.5 WLAN Components**

The basic advantage WLAN has over LAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the need of fitting cables through walls and ceilings. Basic components of a WLAN are access points (APs) and Network Interface Cards (NIC)/client adapters and these discussed as follows [6]:

**2.5.1 Access Points**

Access point (AP) is the wireless equivalent of a LAN hub. It is connected with the wired backbone through a standard Ethernet cable. It communicates with wireless devices with the use of antenna. An AP operates within a specific frequency spectrum. Most of the AP devices use the IEEE 802.11 standard, which enhances the interoperability. An AP also informs the wireless clients of its availability, authenticates and associates wireless clients to the wireless network.

**2.5.2 Wireless LAN Station**  
The *station* (STA) is the most basic component of the wireless network. A station is any device that contains the functionality of the 802.11 protocol, that being MAC, PHY, and a connection to the wireless media. Typically the 802.11 functions are implemented in the hardware and software of a network interface card (NIC)

**2.5.3 Network Interface Cards (NICs)**

Wireless client adapter connect PC or Workstation to a wireless network either in ad hoc (infrastructure less) peer-to-peer mode or in infrastructured mode with APs. It is available for two kinds of slots PCMCIA (Personal Computer Memory Card International Association) card and PCI (Peripheral Component Interconnect), it connects desktop and mobile computing devices wirelessly to the whole network. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. It comes with a software driver that couples it to the PC operating system.

(a) (b) (c) 

Fig. 2.5 (a)Wireless Access Point. (b) Network Interface Card (NIC). (c) Wireless PC.

.

**2.6 Wireless Technologies and Standards**

**2.6.1 Fixed Wireless Technologies**

A fixed wireless technology is any wireless technology where the transmitter and the receiver are at a fixed location such as home or office as opposed to mobile devices such as the cellular phones. Fixed wireless devises normally use utility main power supply (AC). The technologies under fixed wireless can be MDDS (Multichannel Multipoint Distribution Service) connectivity models, LMDS (Local Multipoint Distribution Service), encompassing WLL (Wireless Local Loop), point to point WLAN.

Fixed wireless technologies advantage to service providers in several areas. First, just by nature of the wireless technology, fixed wireless systems provide the ability to connect to remote users without installing costly copper cable over long distance. The service provider can display a fixed wireless access without having to use the local service provider’s last mile infrastructure. Also it can be deployed much quicker.

The disadvantages of fixed wireless vary, depending on which is being used, some of the issues include line-of-site and weather as well as interference from various sources and licensing issues.

**2.6.2 Point-to-point microwave (PTP)**

Point-to-point microwave is a line-of-site technology, which is affected by multipath and absorption much like MMDS and LMDS. PTP microwave falls into two categories: licensed and unlicensed, or spread spectrum. The regulatory agencies issue license for individuals to use specific frequencies for the licensed version which is used to link remote locations and extend link range.

The advantage of the PTP microwave is that the chance of interference or noise sources in the frequency range is remote; this is critical if the integrity of the traffic in that line need to be maintained. The drawback to licensed PTP microwave is that it may take a considerable amount for regulatory agencies to issue the licenses, and the fees associated with those licenses.

Since PTP microwave can span long distance, determined mostly power of the transmitter and the sensitivity of the receiver, as well as by traditional weather conditions, many different aspect need to be considered in designing a PTP microwave link. First, a site survey and path analysis needs to be considered. Obstruction and curvature of the earth determine the height of the towers or the building of the link in line of site environment.

**2.6.3 Mobile (Cellular) Wireless Technologies**

Cellular radio is a technique that was developed to increase the capability available for mobile radio-telephone service. Prior to the introduction of cellular radio, mobile radio-telephone service was only provided by a high power transmitter/receiver. A typical system will support about 25 channels with an effective radius of about 80km. The way to increase the capacity of the system is to use lower power system with shorter radius and to use numerous transmitters/receivers.

A geographic area is divided in to cells; the adjacent cells operate on operate at different frequencies to avoid interference; this is referred to as a frequency reuse. A lower power antenna is placed at a strategic place but it is not at the centre of the cell instead the transmitter is located at a common point between adjacent cells.

The common technologies in cellular networks are the Code Division Multiple Access (CDMA) and the Global System for Mobile Communication (GSM).

**2.6.4 Optical Wireless Technologies**

The basic definition of optical wireless system is a system that uses modulated light to transmit information in open space that use a high-powered beam in the optical spectrum. It is also known as the free space optics (FSO), open air photonics (OAP), or infrared broadband. FSO use low-powered infrared lasers and a series of lenses and mirrors to direct and focus different wavelengths of light towards an optical receiver. FSO is a line-to-sight technology and does not require spectrum licensing. Some FSO vendors claim data rates between 10mbps and 155mbps range with maximum distance of 3.7km as well as system in the 1.25Gbps range with a maximum distance of 350m.

**2.7 Factors Affecting Radio Signal Propagation**

In order for wireless communication to function, the signal must have a path from the transmitter and the receiver and arrive with enough power left in the signal for the receiver to comprehend what is being sent. Some of the factors that affect high frequency signals are as follows.

**2.7.1 Refraction**

Refraction is a property that affects the path of propagation; Refraction is the bending of a wave. Just as the lens of an eyeglass bends the light waves, suspended particles in a water droplet in the atmosphere can bend radio waves. A signal can refract and bend with the curve of the earth, to a certain extent.

**2.7.2 Attenuation**

Attenuation is the weakening of a signal as it travels from a source to a destination, beside when a signal passes through objects like walls, trees and rain it gets weaker.

**2.7.3 Bouncing**

The ability of Electromagnetic waves to waves to pass through some objects is limited, for some objects it gets reflected. This is also called signal scattering.

Bouncing can degrade the performance of some systems and enhance the performance of others. For example, AM broadcast radio signals can be bounced off of the upper layer of the earth’s atmosphere and increase its range.

On the other hand, a type of bouncing that affects mobile communications is called multipath scattering. Multipath scattering is where a signal reaches a receiver from multiple paths due to part of the signal bouncing off of various objects which may amplify or cancel received signal or cause echoing.

**2.7.4 Line of Sight (LOS)**

The straight clear path from the transmitter to the receiver is called the Line of Sight. All signals propagate best when they have a line of sight, but as a general rule, high frequency sight requires a line of sight signal more than low frequency signals. Infrared transmission particularly sensitive to obstructions in line of sight.

**2.8 Wireless LAN Standards**

Prior to the adoption of wireless LAN standards, wireless data-networking vendors made equipment that was based on proprietary technology. Wary of being locked in to relationship with specific vendor, potential wireless customers instead turned to more standard based wireless technologies.

The only way wireless LANs would be generally accepted would be if the wireless hardware involved had a low cost and had become commodity items like routers and switches.

The European Telecommunications Standards Institute (ETSI) and the Institute of Electrical and Electronics Engineers (IEEE) which are standards making bodies have come up with wireless LAN standards. HiperLAN is a WLAN standards developed by ETSI and 802.11 is a WLAN standard developed by the IEEE

**2.8.1 High Performance LAN (HiperLAN)**

HiperLAN is the European Equivalent of the 802.11 standard. It is sub-divided in to two, HiperLAN type 1, supports 20Mbps of bandwidth in the 5GHz spectrum. HiperLAN type 2(HiperLAN2) also operate in the 5GHz band but offers up to 54Mbps bandwidth, it offers many more QoS feature and thus currently supports many more multimedia applications than 802.11a counterpart. HiperLAN 2 is also a connection-oriented technology, which combined with its QoS and bandwidth, gives applications outside the normal enterprise networks [13].

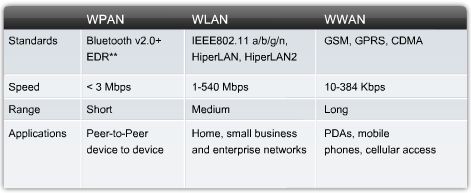


Fig. 2.6 Data rate of HiperLAN [4]

**2.9 IEEE 802 Architecture**

The architecture of a LAN is best described in terms of layering in protocols that organise the basic functions of a LAN. The IEEE802 committee developed the IEEE 802 architecture relating the protocols of LAN standards to the OSI reference model.

In OSI terms, higher-layer protocols (layer 3 and above) are independent of network architecture and are applicable to LANs, CANs and WANs thus the scope of IEEE 802 Standards is from the datalink to the lowest layer.

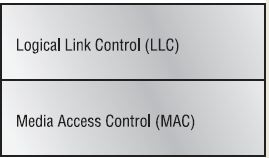
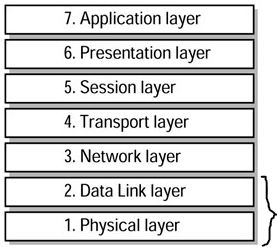


Fig. 2.7 Protocol Layers Compared to OSI Model [15]

Working from the bottom up, the lowest layer of the IEEE 802 reference model corresponds to the physical layer of the OSI model and includes such functions as;

* Encoding/Decoding of signals
* Preamble generation/removal (for synchronisation)
* Bit transmission Reception

Above the physical layer, that is the data link layer, are functions associated with providing service to LAN user. These include the following.

* On transmission, assemble data in to a frame with address and error detection fields.
* On reception, disassemble frame, and perform address recognition and error detection.
* Govern access to the LAN transmission medium.
* Provide an interface to higher layers and performs flow and error control.

**2.9.1 Medium Access Control (MAC) Functions**

IEEE 802.11 MAC layer covers three functional areas: reliable data delivery, access control and security.

* **Reliable Data Delivery**

As with any wireless network, a wireless LAN using the IEEE 802.11 physical and MAC layer is subject to noise, interference and other propagation effects which results in the loss of a significant number of frames.

The basic access mechanism for 802.11 is Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) with binary exponential back-off. This is very similar to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) when dealing with 802.3 (Ethernet), but with a couple of major difference.

Unlike Ethernet, which send out a signal until a collision is detected, CSMA/CD takes great care to not transmit unless it has the attention of the receiving unit, and so no other unit is talking to it.

* **Access Control**

The 802.11 working group considered two types of proposals for a MAC algorithm: distributed access protocols, which like Ethernet, distribute the decision to transmit over the entire node using a carrier-sense mechanism; and centralised access protocols, which involve regulation of transmission by a centralised decision maker.

A distributed Access protocol makes sense for an *ad hoc* network of peer workstations and may also be attractive other wireless LAN configuration that consist primarily of large traffic. A centralised access protocols is natural for configurations in which a number of wireless stations are interconnected with each other to a base station that attaches to a backbone wired LAN.

The end result for 802.11 is a MAC algorithm called DFWMAC (Distribution Foundation Wireless MAC) that provides a distribution access control mechanism with an optional centralised control built on top of that.

* **Security**

Security a wireless LAN, eavesdropping is a major concern because the ease of capturing transmission. IEEE802.11 provides both security and authentication mechanisms of which are the wired equivalent privacy (WEP), Pre-Shared Key (PSK) etc.

**2.10 IEEE 802.11 Standards**

The IEEE 802.11 standards are developed with modifications as new ones are launched over the years; some of the ones available today are 802.11a, 802.11b, 802.11g and 802.11n.

**2.10.1 IEEE802.11a (Wi-Fi 5)**

Due to the overwhelming demand for more bandwidth and the growing number of technologies operating at the 2.4 GHz band, the 802.11 standard was created for wireless LANs. This standard makes use of the 5 GHz spectrum to solve the problem of interference from 2.4 GHz spectrum. It provides a significant bandwidth improvement than the 802.11 b, it also abandons completely the spread spectrum techniques and uses OFDM. The possible data rates for IEEE 802.11a are 6, 9, 12, 18, 24, 36, 48 and 54 Mbps using 52 subcarriers that are modulated using BPSK, QPSK, 16-QAM or 64-QAM, depending on the rate required.

The major drawback of this standard is that because it is using a higher frequency its range is reduced when compared to 802.11b. It is mostly used in corporate environments where bandwidth demand is high in a clustered area.

**2.10.2 IEEE 802.11b (Wi-Fi 11)**

This was the first version of 802.11 to hit the market in the year 1999. It makes use of the 2.4GHz band and provides data rates of 5.5 and 11Mbps which most of the devices used in this project are based on. It uses the DSSS Complementary Code Keying (CCK) scheme. 802.11b has a significant deployment form of hotspots in airports, hotels and coffee shops. It has a typical indoor range of 100-150feet but is susceptible to interference from devices that make use of the 2.4GHz spectrum like cell Phones, microwave ovens and Bluetooth devices.

**2.10.3 IEEE 802.11g (Wi-Fi 54)**

This standard takes the advantage of both 802.11a and 802.11b which are range and bandwidth respectively, because it operates in the 2.4GHz spectrum and provide a bandwidth of 54Mbps. The modulation technique used is OFDM and CCK and the standard is backward compatible with 802.11b [14].

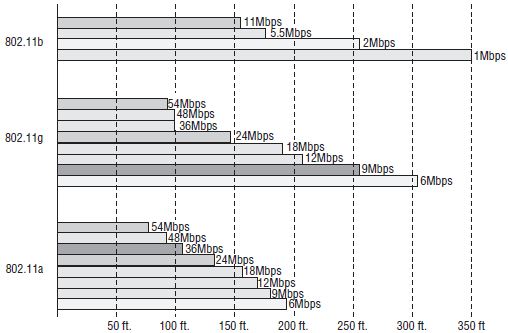


Figure 2.8 Ranges of 802.11 Spectrums. [15]

**2.11 Developing WLANs through the 802.11 Architecture**

The 802.11 architecture can best be described as a series of interconnected cells, and consists of the following the wireless device or station, the access point (AP), the wireless medium, the distribution system (DS), the basic service set (BSS), the extended service set (ESS), and station and distribution services. All of these working together providing a seamless mesh give wireless devices the ability to roam around the WLAN looking for all intents and purposes like a wired device.

**2.11.1 The Basic Service Set (BSS)**

The core of the IEEE802.11 standard is the BSS. The BSS is made up of the Access Point and devices that communicate via the Access point in a single radio cell. If there are no connections back to a wired network, it is called an independent basic service set.

When a BSS has a connection to the wired network via an AP, it is called infrastructure BSS, the AP bridges the gap between the wireless device and the wired network.

**2.11.2 The Extended Services Set (ESS)**

The compelling force behind WLAN deployment is the fact that with 802.11, users are free to move about without having to worry switching network connections manually. If we were operating with a single infrastructure BSS, this moving about would be limited to the single range of one AP. Through the ESS, the AP’s talk amongst themselves forwarding traffic from one BSS to another. They do this using a medium called the distribution system (DS). The DS forms the spine of the WLAN which could be a switch, a wired network or a wireless medium making the decisions whether to forward traffic from one BSS to the wired network or back out to another AP or BSS.

**2.11.3 *Ad-hoc* Network**

If there is no access point in the wireless network, it is referred to as an ad-hoc network. This means that all wireless communications is transmitted directly between the members of the *ad-hoc* network.

**CHAPTER 3**

**METHODOLOGY OF THE ANALYSIS**

This chapter elaborates more on wireless technologies since it is the main concern of the project. Then considered quality of service, taking in to cognisance Delay and Throughput, then features OPNET IT guru academic edition and then the modelled network.

**3.1 Quality of Service (QoS)**

QoS is defined as the ability of the network to provide a service at an assured service level [7].

Quality of Service (QoS) is the ability to provide a level of assurance for data delivery over the network. For example, traffic of different classes or traffic with different requirements receives different levels of QoS assurance.

Therefore, the term QoS support mechanism to refer to any mechanism that is equipped by any kind of QoS support. The term QoS guarantee will be referred to a mechanism that can provide guaranteed support. The objectives of QoS provision can be categorized into:

1. prioritized QoS support and
2. Parameterized QoS support.

Prioritized QoS support aims at providing different level of QoS support for different classes of traffic, e.g., high priority traffic receives better throughput and delay than low priority class traffic. Prioritized QoS support is also known as differentiated QoS support. Parameterized QoS support aims at providing a specific level of QoS support, e.g., at least 64 Kbps and delay less than 30 ms, on average. Parameterized QoS support is also known as specific QoS support.

Under prioritized QoS support, scheduling mechanisms classify packets into different priority classes. Under parameterized QoS support, scheduling mechanisms consider the requirement of a particular packet and provide the appropriate treatment. The wireless communication was originally developed for military use, because of its ease of mobility, installation and flexibility; later on it was made available to civilian use also. With the increasing demand and penetration of wireless services, users of wireless network now expect quality of service and performance comparable to what is available from fixed networks. Some of factors that influence QoS of Wireless Network include:

**3.1.1 Queuing Mechanisms**

The queuing mechanism is categorised in to

* Weighted fair queuing
* Custom queuing

**3.1.2 Quality of Service in WLANs**

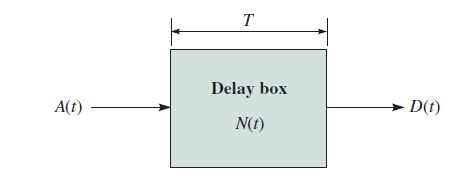
When WLANs were introduced in full fledge, a new era of wireless networking began. Now, solutions based on WLANs provide a bandwidth close to that of wired networks at a competitive price. Because of this, wireless LANs are deployed at many places today. In the earlier phases its development the wireless networks had low bandwidth, high bit-error rates and high prices which impeded their deployment [10].

We take in to consideration the only elements of Quality of Service featured in the project topic i.e. Delay and Throughput.

**3.1.2.1 Delay**

The delay of a packet in a network is the time it takes the packet to reach the destination after it leaves the source [8].

*Little’s Formula* relates the average occupancy in the system to the average time spent in the system. This formula is powerful in obtaining average delay performance in complex systems.

**

We begin by introducing several key system variables and some of their averages. Let

* A(*t*) Number of arrivals at a server in the interval between 0 and time *t*
* B(*t*) Number of Blocked clients by the servers
* D(*t*) Number of Client departures in the same interval (0 to *t*)

The number of clients in the system at time *t* is given by

Because the number of clients that have entered in time *t* is A(*t*) – B(*t*) and because D(*t*) of these clients have departed at time *t.* The rate of active sessions in the system is given by *λ*

Then we relate the average time spent in a session to the rate of active sessions λ and the average number of clients in a session using the relation

Delay is of many types, some of which are;

* Serialisation delay
* Propagation delay
* Forwarding/Processing delay
* Queuing delay
* Shaping delay
* Codec delay
* Compression delay
* Network delay

The queuing delay is the point of concern in our network design. Queuing is frequently called congestion management or scheduling. Queuing is also subdivided in to many categories, they are; Priority queuing, custom queuing, weighted fair queuing, class-based weighted fair queuing and low latency queuing.

**3.1.2.2 Throughput**

In wireless networks, such as Ethernet or packet radio, throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot [9].

The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network. The throughput can be analyzed mathematically by means of queuing theory, where the load in packets per time unit is denoted arrival rate λ, and the throughput in packets per time unit is denoted departure rate μ. Throughput is essentially synonymous to digital bandwidth consumption [9].

The throughput of a network is given by

Maximum throughput is essentially synonymous to digital bandwidth capacity.

Four different values have meaning in the context of "maximum throughput", used in comparing the 'upper limit' conceptual performance of multiple systems. They are 'maximum theoretical throughput', 'maximum achievable throughput', and 'peak measured throughput' and 'maximum sustained throughput'. These represent different quantities and care must be taken that the same definitions are used when comparing different 'maximum throughput' values. Comparing throughput values is also dependent on each bit carrying the same amount of information. Data compression can significantly skew throughput calculations, including generating values greater than 100%. If the communication is mediated by several links in series with different bit rates, the maximum throughput of the overall link is lower than or equal to the lowest bit rate.

The lowest value link in the series is referred to as the bottleneck

* **Maximum theoretical throughput**

This number is closely related to the channel capacity of the system, and is the maximum possible quantity of data that can be transmitted under ideal circumstances. In some cases this number is reported as equal to the channel capacity, though this can be deceptive, as only non-packetized systems (asynchronous) technologies can achieve this without data compression. Maximum theoretical throughput is more accurately reported to take into account format and specification overhead with best case assumptions.

* **Peak measured throughput**

Peak measured throughput is throughput measured by a real, implemented system, or a simulated system. The value is the throughput measured over a short period of time; mathematically, this is the limit taken with respect to throughput as time approaches zero. This term is synonymous with "instantaneous throughput". This number is useful for systems that rely on burst data transmission; however, for systems with a high duty cycle this is less likely to be a useful measure of system performance.

* **Maximum sustained throughput**

This value is the throughput averaged or integrated over a long time (sometimes considered infinity). For high duty cycle networks this is likely to be the most accurate indicator of system performance. The maximum throughput is defined as the asymptotic throughput when the load (the amount of incoming data) is very large. The maximum throughput may be defined as the minimum load in bit/s that causes the delivery time (the latency) to become unstable and increase towards infinity. This value can also be used deceptively in relation to peak measured throughput to conceal packet shaping.

* **Channel utilization - normalized throughput**

Throughput is sometimes normalized and measured in percentage, but normalization may cause confusion regarding what the percentage is related to. Channel utilization and packet drop rate in percentage are less ambiguous terms.

The channel utilization, also known as bandwidth utilization efficiency, in percentage is the achieved throughput related to the net bit rate in bit/s of a digital communication channel). For example, if the throughput is 70 Mbit/s in a 100 Mbit/s Ethernet connection, the channel utilization is 70%. In a point-to-point or point-to-multipoint communication link, where only one terminal is transmitting, the maximum throughput is often equivalent to or very near the physical data rate (the channel capacity), since the channel utilization can be almost 100% in such a network, except for a small inter-frame gap [9].

**3.2 Introduction to OPNET IT Guru Academic Edition**

OPNET IT Guru is used to design and study communication networks, devices, protocols and applications. It provides a graphical editor interface to build models for various network entities from physical layer modulator to application processes.

OPNET Modeller features: creating and configuring a network topology, adding traffic to this topology, using the custom task, setting up custom applications and profiles, interpreting the Simulation Log, getting and analyzing simulation results etc.

**3.2.1 OPNET IT Guru Operations**

OPNET supports model specification with a number of tools, called editors. These

Editors handle the required modelling information in a manner that is similar to the Structure of real network systems. Therefore, the model-specification editors are organized hierarchically. Model specifications performed in the Project Editor rely on Elements specified in the Node Editor.

The rest of the editors are used to define various data models, new links and nodes.



Fig. 3.1 OPNET Software

**3.2.1.1 IT Guru Workflow**

The sequence of executing a project in OPNET is shown in figure 3.2.



Fig. 3.2 Workflow model [12]

**3.2.1.2 Creating Network Model**

The first step is to create the networks models. It is necessary to generate the network to simulate in any of the following three ways:

* Placing individual nodes from the object palette into the workspace.
* Using the rapid configuration tool.
* And/or importing the network from an external data.

Furthermore, you have to introduce the traffic you want to run through the network.

There is two main ways of putting traffic in the model:

a) Importing

b) Manually specifying

**3.2.1.3 Choose Individual Statistics**

Afterwards and before running a simulation, it is necessary to choose the statistics we want to collect. OPNET does not automatically collect all statistics in the System because there are so many available that you may not have enough disk space to store them. Specifying statistics is a straightforward task which is performed through the GUI.

**3.2.1.4 Run Simulation**

The third thing to set is configuring the parameters of the simulation and Running them. Running simulations is typically thought of as the next-to-last step in the simulation and modelling process, the last step being results analysis. However, simulation is typically done many times in the modelling process to check the rightness of the generated network. There are different kinds of analysis that can be done in OPNET MODELER.

* Discrete Event Simulation
* Flow Analysis
* Failure Impact Analysis
* NetDoctor Validation

Discrete event simulation (Which is used to analyse the project) provides the most detailed results but has the longest running times. This is because it does a more thorough analysis than the others, handling explicit traffic, conversation pair traffic, and link loads. The other types answer specific types of questions and generate results much faster than a discrete event simulation. A flow analysis, for example, handles only conversation pair traffic (flows) and a NetDoctor validation does not consider traffic at all.

**3.2.1.5 View and Analyze Results**

It is the last step of simulation. The results can be watched from the Project Editor or from the Analysis Tool. The Analysis Tool provides the capability to extract data from simulation output files, and to manipulate and display it according to various plotting methods. Data can be manipulated through built-in operations in a different way to get wanted information. Hence, the final workflow of a project could be as follows:

* Create project
* Create baseline scenario
* Import or create topology
* Import or create traffic
* Choose results and reports to be collected
* View results and analyze them

Iterate by duplicating the scenario and changing parameters OPNET uses a project and scenario approach to model networks. Project is a collection of related network scenarios in which each explores a different aspect of network design. A project contains at least one scenario and a scenario is a single instance of a network containing all the information. It is possible to run all the scenarios of the network at the same time and compare the results of each one. This allows the scenarios to check if a server will support and increment of the traffic, the effect of the increment of the traffic in a link in the response of a service, etc

**3.2.2 Project Editor**

Project Editor is used to develop network models. Network models are made up of subnets and node models. This editor also includes basic simulation and analysis capabilities. The Project Editor is the main staging area for creating a network simulation. From this editor, you can build a network model using models from the standard library, choose statistics about the network, run a simulation and view the results. It is also possible to create node and process models, build packet formats, and create filters and parameters, using specialized editors that you can access from the Project Editor. In Figure 3.3 is an example of the project editor view of a Wireless network is shown.



Fig. 3.3 a Project Editor.

**3.2.3 Object Palette**

The object palette consist of all networking components, be it wired or wireless, LAN or WAN, which support different networking technologies and routing protocols. Different types of connections used in LANs and WANs like 1000BaseX, 10BaseT, FDDI, DSL, ADSL, ISDN and Token Ring are also embedded in the Object Palette.

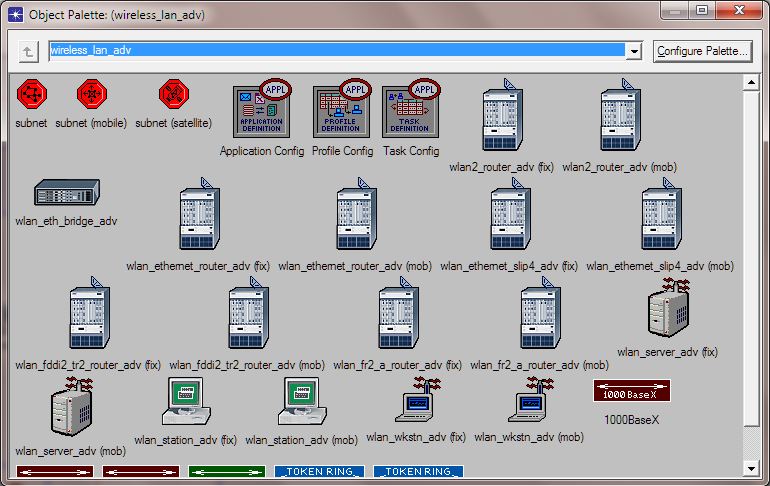


Fig. 3.4 Object Palette.

**3.2.4 Node Editor**

Node Editor is used to develop node models. Node models are objects in a network model. They are made up of modules with process models. The Node Editor lets you define the behaviour of each network object. Behaviour is defined using different modules, each of which models some internal aspect of node behaviour such as data creation, data storage, etc. A network object is typically made up of multiple modules that define its behaviour. In the Figure 3.5, there are some parts of wireless properties.

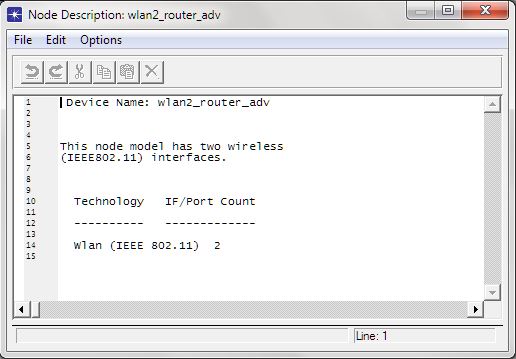
 

Fig 3.5 Router and its Description

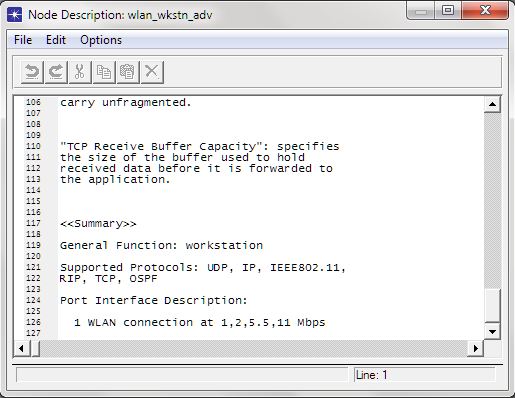
 

Fig. 3.6 Mobile workstation and its features

**3.2.5 Applications and Profile Configuration**

* **Application Configuration toolbox**

The "Application Configuration" node can be used for the following specifications:

**1. "ACE Tier Information":**

Specifies the different tier names used in the network model. This attribute will be automatically populated when the model is created using the "Network->Import Topology->Create from ACE..." option. The tier name and the corresponding ports at which the tier listens to incoming traffic is cross-referenced by different nodes in the network.

**2. "Application Specification":**

Specifies applications using available application types. You can specify a name and the corresponding description in the process of creating new applications. For example, "Web Browsing (Heavy HTTP 1.1)" indicates a web application performing heavy browsing using HTTP 1.1. The specified application name will be used while creating user profiles on the "Profile Configuration" object.

**3. "Voice Encoder Schemes":**

Specifies encoder Parameters for each of the encoder schemes used for generating

Voice traffic in the network.



Fig. 3.7 The Application Configuration toolbox.

* **Profile Configuration toolbox**

The "Profile Config" node can be used to create user profiles. These user profiles can then be specified on different nodes in the network to generate application layer traffic. The application defined in the “Application Config” objects is used by this object to configure profiles. Therefore, applications must be created using the "Application Config" object before using this object. Traffic patterns can be specified followed by the applications as well as the configured profiles on this object.



Fig. 3.8 Profile Configuration Toolbox.

**3.3 Structure of the Modelled Network**

This project considered a network similar to that of the ABU Samaru Campus Network in which network users mostly students roam. It features an ICT Router which is the gateway router via which all wireless clients access the servers.

The network also features three independent Servers i.e. Http Server, The Database Server and the ftp Server.

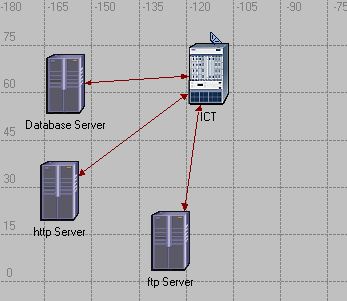


Fig. 3.9 The ICT Router Connected with three LAN Servers.

Application Definition and Profile Definition must also be present in any network, without which the network cannot be simulated. They represented with boxes obtained from the object palette.

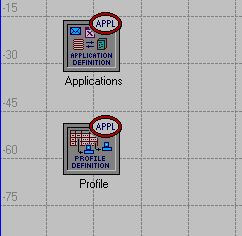


Fig. 3.10 the toolboxes the houses the network applications and user Profiles.

Subnets are represented with red octagons; here I featured ten faculties which are; Arts, Science, Education, Social Science, Environmental Design, Engineering, Medicine, Pharmacy, Veterinary Medicine and Agriculture.

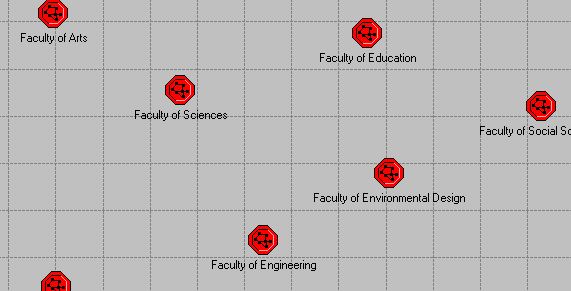


Fig. 3.11 Cross section of the Faculties.

Inside each subnet are the mobile workstations that access the network, a router, an application configuration tool and a profile configuration tool. Figure 3.12 and 3.13 show the topology of the Faculties of Engineering and Pharmaceutical Sciences.

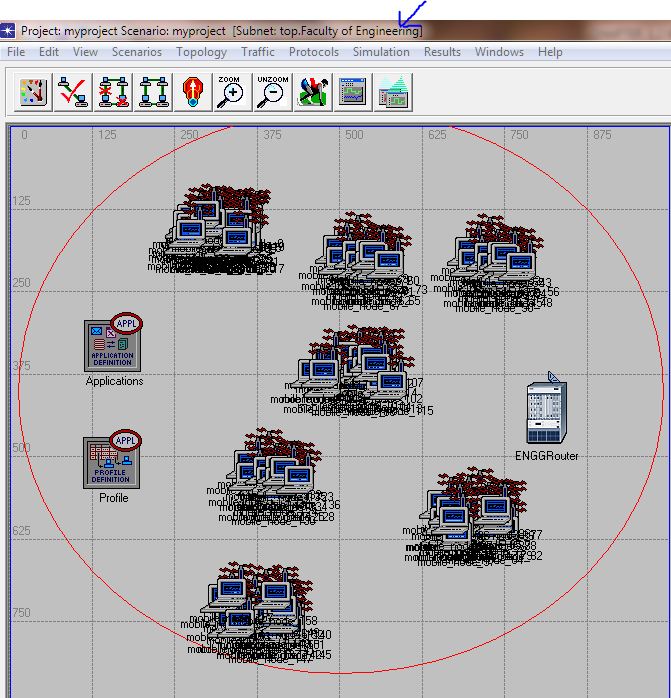


Fig. 3.12 Engineering Subnet, showing clusters of workstations in various Departments.

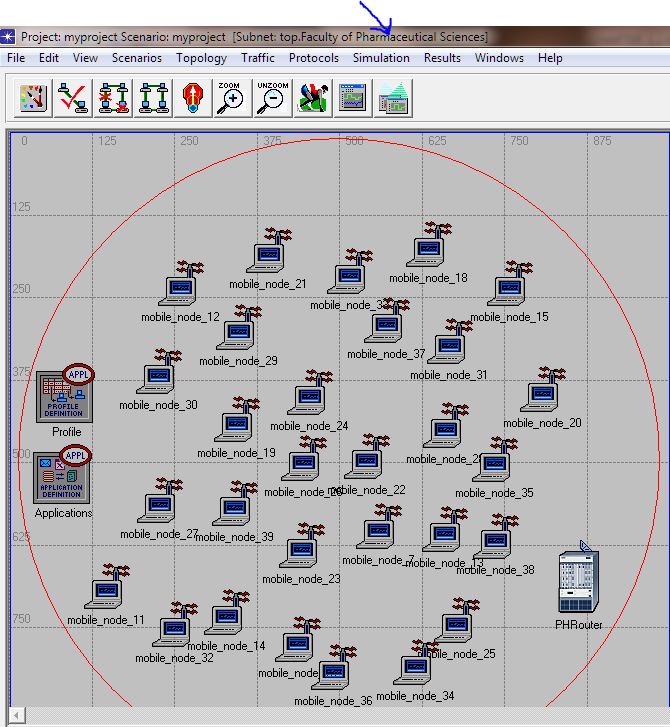


Fig 3.13, Pharmaceutical Sciences Subnet.

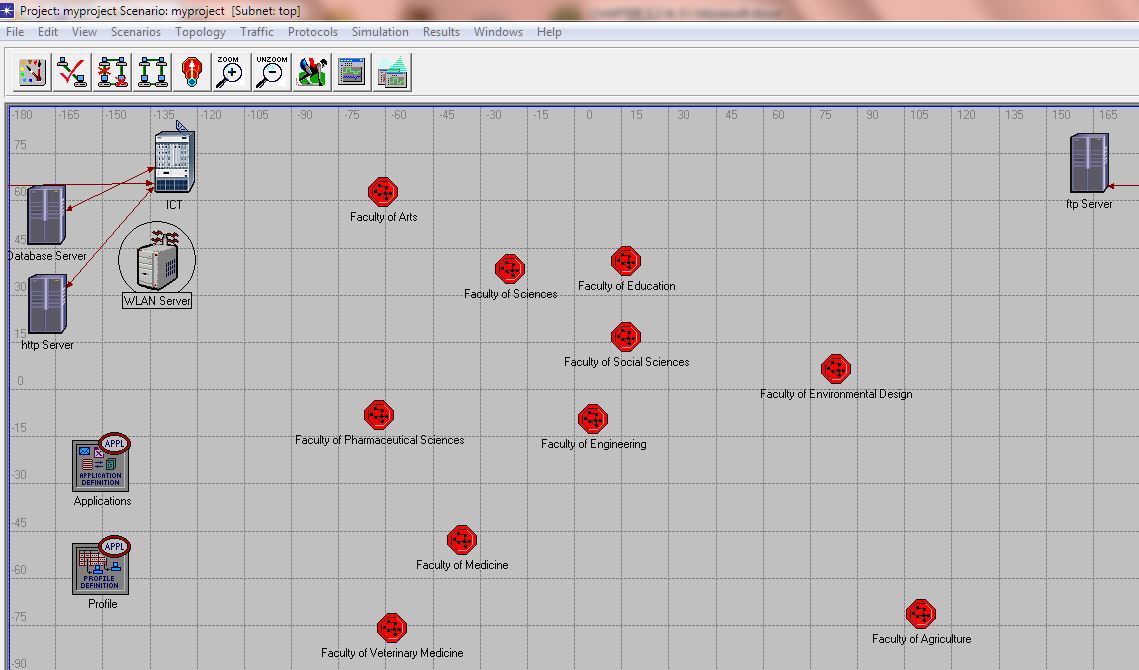


Fig. 3.14 the Campus Network.

**3.4 The Network Configurations**

In this chapter, I demonstrate the configuration of every node used in the network. The nodes are classified in to groups as many are used in each category.

* **Workstation configurations**

Workstations are configured with required properties by selecting similar nodes after right clicking on a single workstation. By doing this, all computers of the network will be configured at the same time.

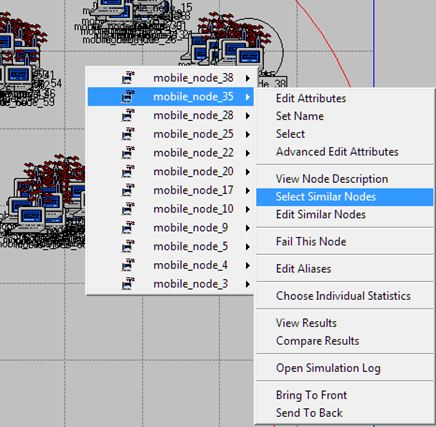


Fig. 3.15 Selecting Similar Nodes

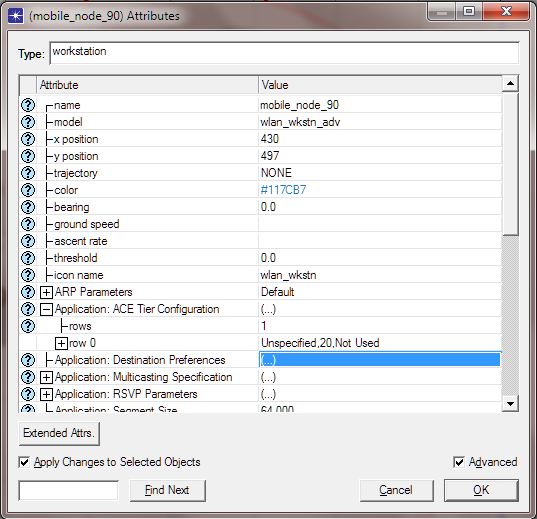


Fig. 3.16 Selecting Application: Destination Preference

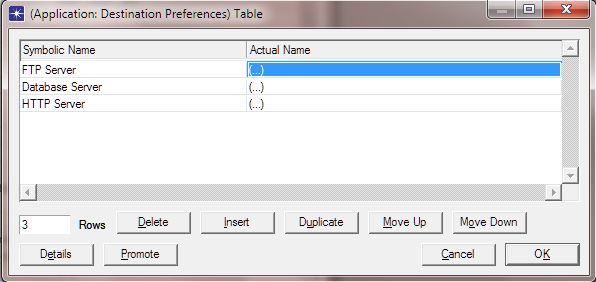


Fig. 3.17 Supported Applications

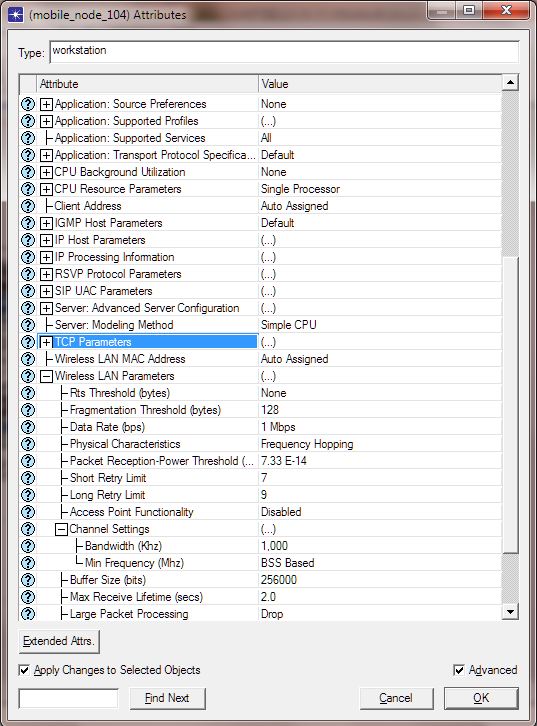


Fig. 3.18 Wireless Properties of the mobile WSs.

* **Applications Configurations**

The application definition log holds all the applications supported by the network, there for, all simulation environments must contain the Application log. Which stores the application configuration.

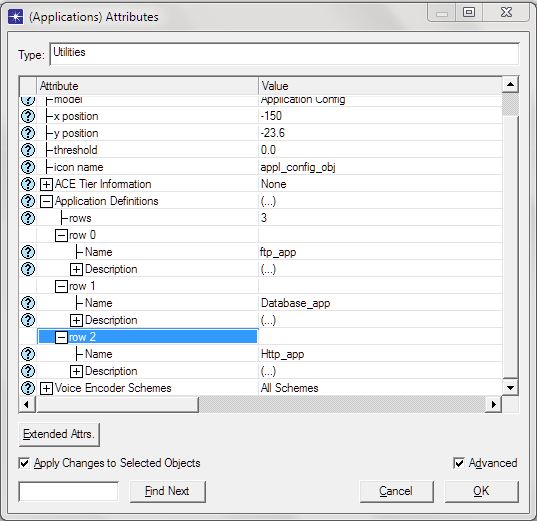


Fig. 3.19 Application Configurations

* **Profile Configurations**

The Profile configuration log saves the user profiles of every wireless client streaming on the network. For our network users are only configured to have http, database and ftp profiles.

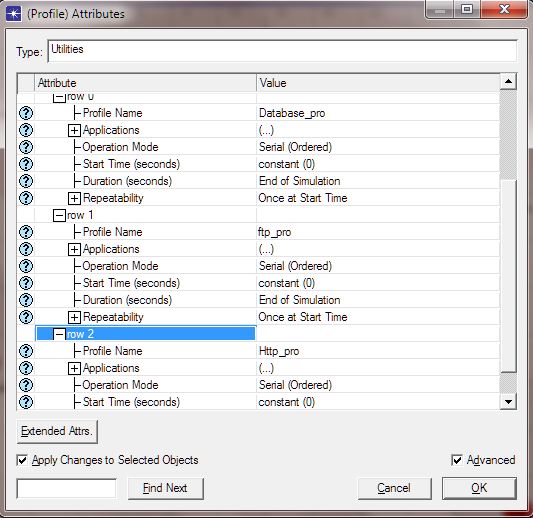


Fig. 3.20 Profile Configuration dialog box

* **Router Configurations**

Routers are configured to provide the most efficient signal for clients in the network. Figure 3.21 shows the configurations of the router.

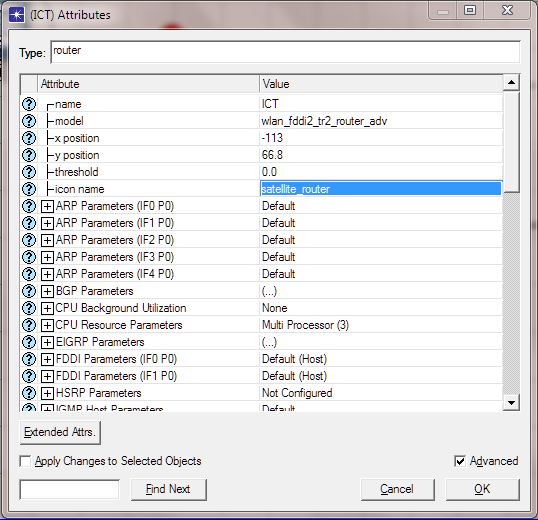


Fig. 3.21 Router Configuration dialog box

* **Sever Configurations**

The three servers used in the network are configured to support single application each. The http server is configured to receive only http traffic and subsequently load web pages for wireless users. The ftp server serves as a store of educational resources where students download lecture materials; likewise the database server receives queries from clients trying to access their personal data.

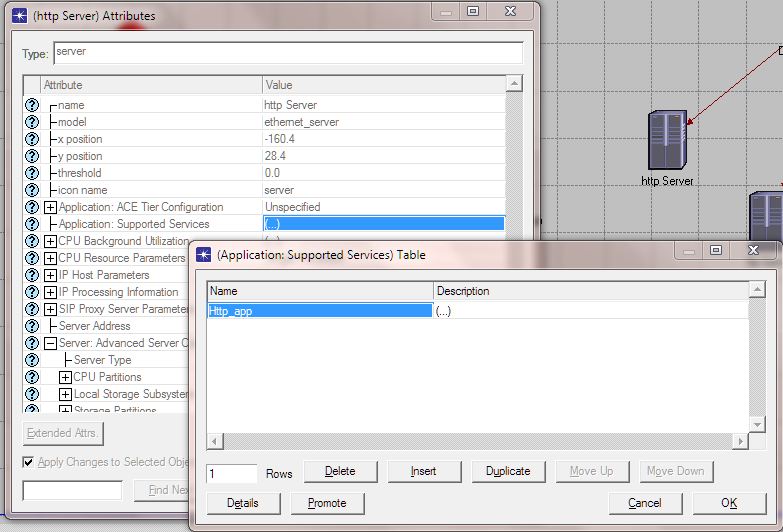


Fig. 3.22 http Server Configuration

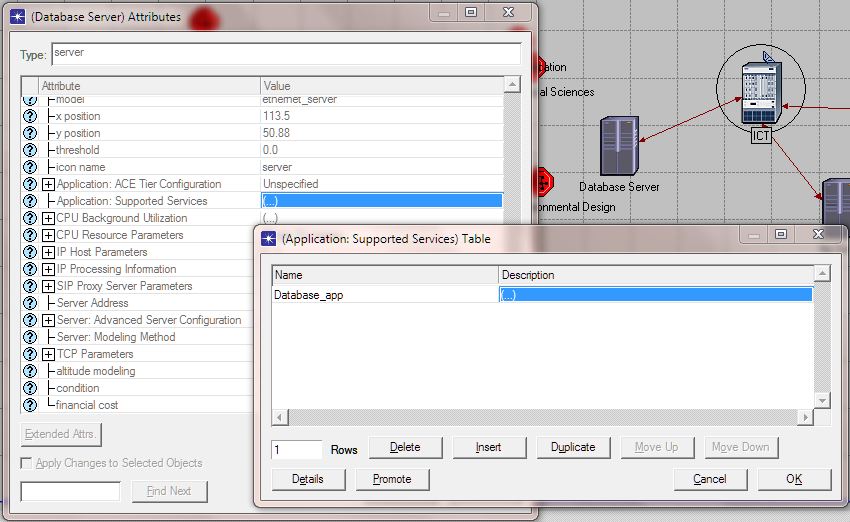


Fig. 3.23 Database Server Configuration

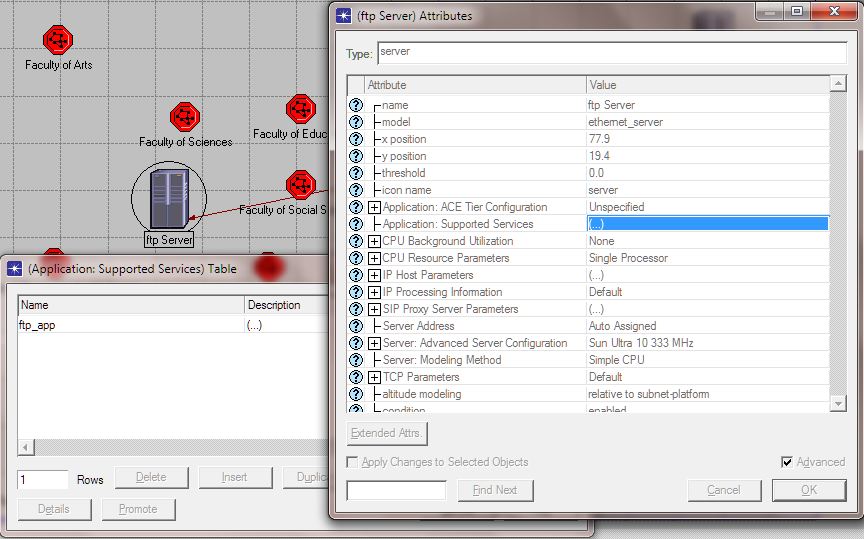


Fig. 3.24 ftp Server Configuration

**CHAPTER FOUR**

**SIMULATION AND RESULTS ANALYSIS**

**4.1 Introduction**

In this chapter, the ABU Hotspot wireless backbone was modelled using OPNET Modeller to simulate and analyse the behaviour of the signal strength.

The project considered Delay and throughput QoS parameters in the analysis. Delay and throughput traffic simulation and result analysis will be presented.

**4.2 Modelled Network Configurations**

In OPNET, the Individual statistics dialog box is used to specify the parameters that are required to be collated during simulation. Figure 4.1 shows the parameters selected for the project.

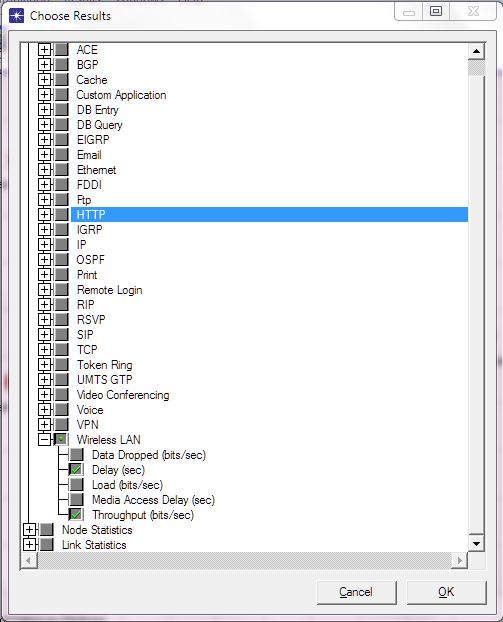


Fig. 4.1 Parameters Selected

**4.3 Simulation configurations**

Before simulating the network, certain settings need to be made in the simulation log, such attributes include total simulation time, specifying the right environmental file, enabling reports and configure the common attributes. Figure 4.2 shows the simulation log

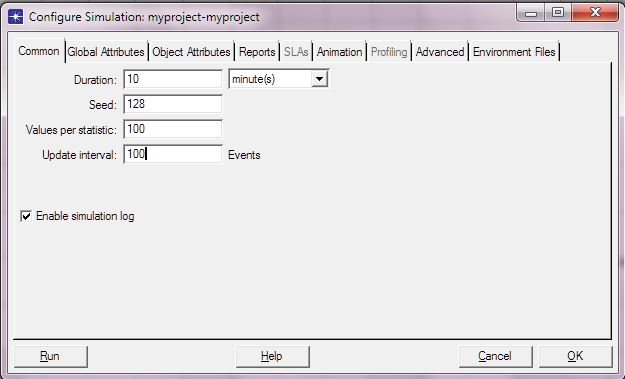


Fig. 4.2 Simulation Log

* During Off-peak period, the traffic generated is very small. In this case delay will be lower and the network will present an appreciable throughput.

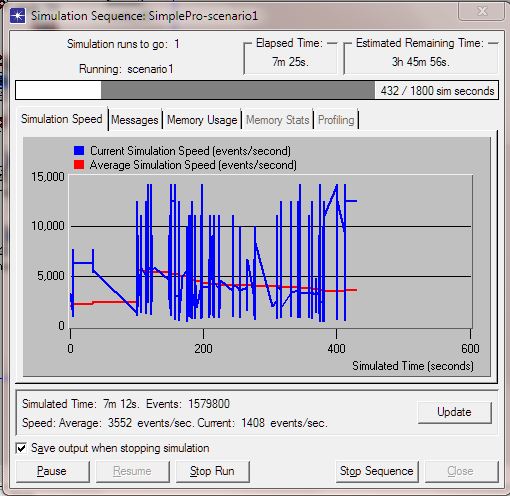


Figure 4.3 Off-peak period Simulation process.

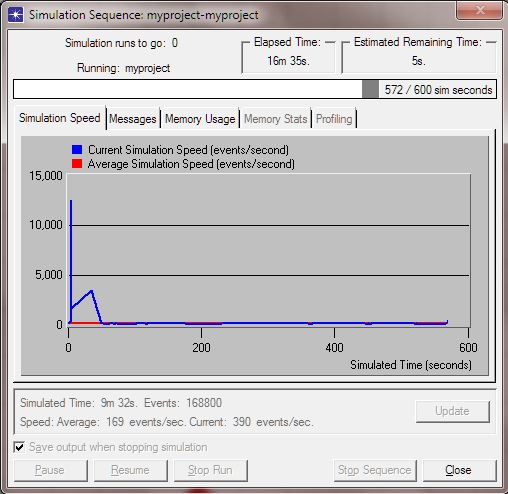


Fig. 4.4 Peak Period Simulation process.

**4.4 Results Obtained**

**4.4.1 Mobile node Statistics**

The performance of mobile node 7 during off-peak period and node 106 in the faculty of engineering trying to access the ABU web Server during peak period was examined. Figure 4.6 shows the graph of the wireless client

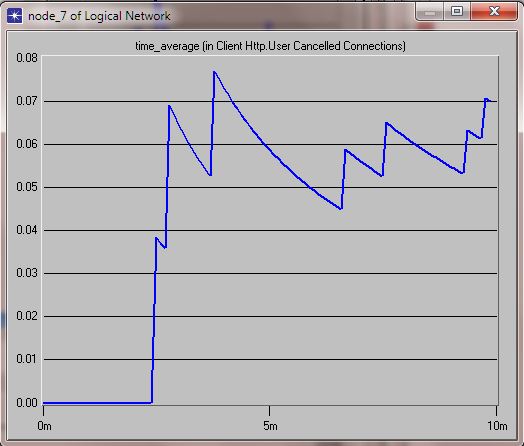


Fig. 4.6 Client 7 http cancelled connections graph.



Fig. 4.7 Node 106 Cancelled connections graph.

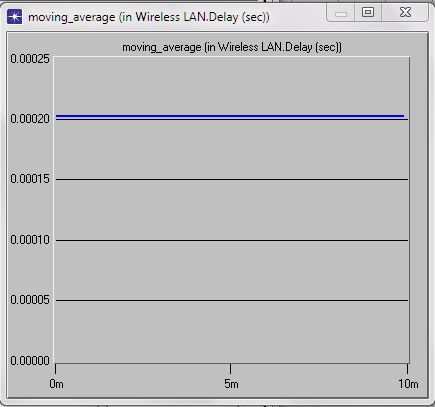


Fig. 4.8 Graph of delay in the off-peak period.

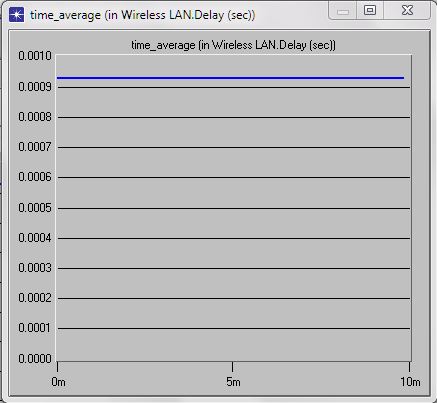


Fig. 4.9 Graph of delay in peak period.

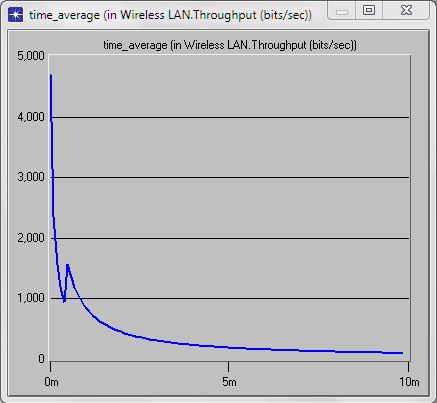


Fig. 4.10 Graph of throughput during off-peak period.

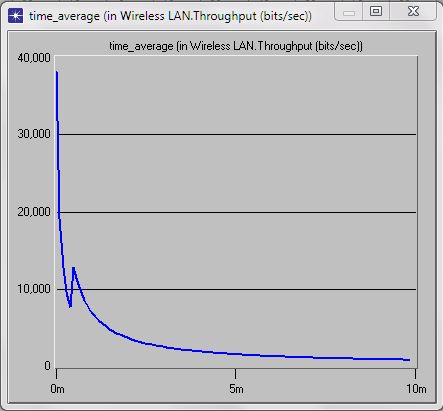


Fig. 4.11 Graph of throughput during peak period.

**4.5 Results Analysis**

**4.6.1 Delay Analysis**

Table 4.1 shows the data collection at off-peak period from the raw data of the simulation and figure 4.12 show the nature of the delay for the off-peak period. Table 4.2 shows the table of data collected at peak period of the network utilization and figure 4.13 shows the graph of the delay in peak period.

Table 4.1 Delay data for off-peak period

|  |  |  |  |
| --- | --- | --- | --- |
| Delay | | | |
| S/N | X(bytes) | Y(min) | Y(sec) |
| 1 | 0.00021 | 1 | 60 |
| 2 | 0.00021 | 2 | 120 |
| 3 | 0.00021 | 3 | 180 |
| 4 | 0.00021 | 4 | 240 |
| 5 | 0.00021 | 5 | 300 |
| 6 | 0.00021 | 6 | 360 |
| 7 | 0.00021 | 7 | 420 |
| 8 | 0.00021 | 7.5 | 450 |
| 9 | 0.00021 | 7.7 | 462 |
| 10 | 0.00021 | 9 | 540 |
| 11 | 0.00021 | 10 | 600 |

Fig. 4.12 Delay graph for off-peak period

Table 4.2 Delay data for peak period.

|  |  |  |  |
| --- | --- | --- | --- |
| Delay | | | |
| S/N | X(bytes) | Y(min) | Y(sec) |
| 1 | 0.00094 | 1 | 60 |
| 2 | 0.00094 | 2 | 120 |
| 3 | 0.00094 | 3 | 180 |
| 4 | 0.00094 | 4 | 240 |
| 5 | 0.00094 | 5 | 300 |
| 6 | 0.00094 | 6 | 360 |
| 7 | 0.00094 | 7 | 420 |
| 8 | 0.00094 | 8 | 480 |
| 9 | 0.00094 | 9 | 540 |
| 10 | 0.00094 | 10 | 600 |

Fig. 4.13 Delay (bytes/sec) for peak period

From the results we can see that wireless LAN delay in the off-peak period amounts to 0.0002 bytes of data delayed per second. The nature of the constant delay just presumes the delay at 10 minutes of the simulation. Where as in the peak period, a constant delay of 0.0009 bytes per second was experienced from the beginning to the end of the simulation time. This means the maximum number of users always occupies the network, and for that reason new connections are hardly launched in to the network.

The result analysis shows that at peak period, we experience constant delay which leads to the loss of service due to high demand of the network resources.

* + 1. **Throughput Analysis**

Table 4.3 shows the data collected at off-peak period from the raw data of the simulation, and figure 4.14 shows the data of throughput at off-peak period. Table 4.4 show the data collected at peak period of the network resource utilization, while figure 4.15 shows the result analysis

Table 4.3 Throughput data at off-peak period

|  |  |  |  |
| --- | --- | --- | --- |
| Data Throughput(off-peak) | | | |
| S/N | X(Kbits) | Y(min) | Y(sec) |
| 1 | 4.8 | 0.2 | 12 |
| 2 | 3 | 0.3 | 18 |
| 3 | 1.5 | 0.5 | 30 |
| 4 | 1 | 1 | 60 |
| 5 | 1.5 | 1.5 | 90 |
| 6 | 1 | 2 | 120 |
| 7 | 0.3 | 3 | 180 |
| 8 | 0.2 | 5 | 300 |
| 9 | 0.1 | 7 | 420 |
| 10 | 0.05 | 10 | 600 |

Fig. 4.14 Throughput graph at off-peak period

Table 4.4 Throughput data at peak period.

|  |  |  |  |
| --- | --- | --- | --- |
| Data Throughput(peak) | | | |
| S/N | X(Kbits) | Y(min) | Y(sec) |
| 1 | 38 | 0.2 | 12 |
| 2 | 25 | 0.3 | 18 |
| 3 | 9 | 0.5 | 30 |
| 4 | 12 | 1 | 60 |
| 5 | 8 | 1.5 | 90 |
| 6 | 5 | 2 | 120 |
| 7 | 4 | 3 | 180 |
| 8 | 1 | 5 | 300 |
| 9 | 0.5 | 7 | 420 |
| 10 | 0.2 | 10 | 600 |

Fig. 4.15 Throughput graph at peak period.

During the off-peak period, only about 49 clients are running web sessions. From the results obtained, throughput performance of the backbone during the off-peak period is considerably good compared to the number of clients on session, as it starts from 4.8Kbps down to 0.05Kbps at the end of simulation time.

There for, the average Throughput per client at off-peak period is 48.5 bits per second.

But during the peak period of the network resources utilisation, when the number of clients in the network is around 1200, the throughput went from 38 kilo bits per second to 0.2 Kbps at the end of the simulation time.

This shows the average throughput per client at the peak period as 15.8 bits per second.

.

**CHAPTER FIVE**

**CONCLUSIONS AND RECOMMENDATIONS**

**5.1 CONCLUSIONS**

From the results analysed, it is very clear that ABU hotspot having a large number of users experiences high delays and low data throughput. This delay and low throughput is caused by numerous unavoidable natural and artificial phenomena.

The ABU hotspot experience poor network performance due to;

* Wireless Backbone has very small bandwidth when compared with the high demand from Staff and Students.
* Heavy traffic can also affect network performance. In this network of about a thousand clients, traffic is one of the major constrains. Heavy traffic or bandwidth-intensive activity slows down data transmission in the network.

**5.2 LIMITATIONS**

* The software is not capable of showing all simulation graphs because it is an Academic Edition.
* The software does not provide environmental conditions that may affect radio signals.

**5.3 RECOMMENDATIONS**

The wireless backbone should be replaced with high speed backbone, like fibre optic cables. This will eliminate the problem of interference, obstructions, signal attenuation due to distance and intensive bandwidth usage.

* There is also need for quality of service both in the LAN and the backbone network.
* Proper bandwidth management
* Proper deployment of QoS at all level of the network
* Standard corporate security policy to reduce the risk of network downtime.

**REFERENCES**

1. M.M. Siddiq and A. Congen, *WLAN lab Opnet tutorial*. Bremen: Universitat Bremen Press, 2008.
2. I. Stajmenovic, *Handbook of Wireless Networking and Mobile Computing*. India: Wiley Publication, 2002.
3. Conniq.com. (2011, May). Networking Guide: Physical Media-Radio (RF), Microwave Infrared. [Online] Available: <http://conniq.com/networking_media5.htm>
4. Cisco Discovery 4.0. *Networking for Homes and Small Businesses*. Cisco Systems, Inc, 2007.
5. J. Schiller, *Mobile Communication*, 2nd Edition. Pearson.Edu, 2007.
6. C.P. Brian et al., “IEEE 802.11 Wireless Local Area Networks,” *IEEE Commun Mag*, may1997.
7. A. Lindgren et al., “Quality of Service Schemes for IEEE 802.11,” *IEEE Commun Mag*, Vol. 39, no. 2, may 2001.
8. P. Gupta and P.R. Kumar, “The Capacity of Wireless Networks,” *IEEE Trans on Information Theory*, 2000, Vol. 46, no. 2, pp. 388-404.
9. Wikipedia. (2011, April). Throughput. [Online]. Available: <http://en.wikipedia.org/wiki/throughput.htm>
10. J. Theunis et al., *Simulation of a Campus Backbone Network*. OPNETWORKS, 2002.
11. K. Ranjan and L. Dan, “Opnet IT Guru: A tool for Networking Education,” *MSCIT Practicum Paper*. Colorado: Regis University, 2008, pp. 5-8.
12. A. Farhid, *OPNET Tutorial*, 2002.
13. J. Wheat et al., *Designing a Wireless Network*. USA: Syngress, 2001.
14. V. Pierre, *Wireless Networks*. Quantum Mobile Communications Handbook, 2002.
15. T. Lammle, *CCNA: Cisco Certified Network Associate*. Indiana, USA: Wiley Publishing, Inc, 2007.