STRUCTURED NETWORKING DESIGN AND PERFORMANCE ANALYSIS OF DIIT CAMPUS

BY

ABDULLAH AL ARIF
ID: 071-19-562

MASUD ALAM

ID: 071-19-597

AND

K.M. AZIMUL FARIZ

ID: 071-19-595

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering.

Supervised By

A. K. M. FAZLUL HAQUE
Assistant Professor
Department of ETE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

FEBRUARY 2011

APPROVAL

This Project titled **"Structured Networking Design and Performance Analysis of DIIT Campus**", submitted by Abdullah Al Arif, Md. Masud Alam and K. M. Azimul Fariz to the Department of Electronics and Telecommunication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation has been held on 27th February, 2011

BOARD OF EXAMINERS

____

Dr. Md. Golam Mowla Choudhury **Chairman**
Professor and Head
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

____

A. K. M. Fazlul Haque **Internal Examiner**
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

____

Mohammad Mirza Golam Rashed **Internal Examiner**
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

____

Dr. Subrata Kumar Aditya **External Examiner**
Professor and Chairman
Department of Applied Physics, Electronics and communication Engineering
University of Dhaka

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **A.K.M Fazlul Haque, Assistant Professor, Department of ETE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

____

A. K. M. Fazlul Haque
Assistant Professor
Department of ETE
Daffodil International University

Submitted by:

____

Abdullah Al Arif.
ID: - 071-19-562
Department of ETE
Daffodil International University

____

MD. Masud Alam
ID: - 071-19-597
Department of ETE
Daffodil International University

____

K. M. Azimul Fariz
ID: - 071-19-595
Department of ETE
Daffodil International University

ACKNOWLEDGEMENT

First we express our heartiest thanks and gratefulness to almighty Allah for His divine blessing makes us possible to complete this project successfully.

We fell grateful to and wish our profound our indebtedness to A.K.M Fazlul Haque, Assistant Professor, Department of ETE Daffodil International University, Dhaka. His Deep Knowledge and keen interest of our supervisor in the field of structured network design of a university campus influenced us to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Dr. Md. Golam Mowla Choudhury**,** Professor and Head, Department of ETE, for his kind help to finish our project and also to other faculty member and the staff of ETE department of Daffodil International University.

We are especially thankful to Md. Ruqunuzzaman, Assistant IT Officer and Library In charge and Md. Zillur Rahman , Senior IT Officer, DIIT for their assistance and technical support throughout the project period.

We would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

This project presents the Structured Networking Design and Performance Analysis, especially for DIIT Campus. This is a kind of network using MikroTik router, which helps a Network Administrator to build up bandwidth management and control over the total network using a MikroTik Server, DNS Server, DHCP server and wireless Access Point. It is found that the DIIT existing network not properly served in total campus area. So, it is needed to introduce a new project approach to support structured LAN and wireless mobile internet-working on a large university campus or similar environment for the purpose of supporting network access between its existing users (students, employee and its faculties). The combination provides simultaneously performance of LAN and wireless communication system with sufficient aggregate bandwidth to handle massive, synchronized movements of stand alone and remote computer & device users. In this project, the technical details of structured cabling have been introduced and the performance of proposed model and conventional system has also been analyzed.

TABLE OF CONTENTS

CONTENTS **PAGE**

LIST OF FIGURE

CHAPTER 8: PROPOSED NETWORK

LIST OF TABLE

TABLE **PAGE**

CHAPTER 1

INTRODUCTION

1.1 General Introduction

Campus networking is one of the most important issues at present to face rightly perceived in most colleges and universities. A campus network is far more than just a physical infrastructure, planning, and building for inter-networking. A campus network really means developing an entirely new information environment, which will have a profound impact on almost every aspect of campus life. To build a network, campuses are engaged in a change process, which is strategically essential to their very nature and existence. This paper offers some advice to administrators and faculty about entire networking, which engage in planning, building, and managing campus networks. Now a day computer networks have become extremely important and present demand. Current and future IT applications are using graphics, animations, images, voice and other multimedia streams, which use an incredible amount of traffic. Educational institutions depend on the proper functioning of their network for communication, administration, etc. The use of computers in classes, labs and faculty offices has led to complicated campus networks with an enormous amount of workstations.

1.2 Objective of the Project

The main goal of the project to restructuring the system, enhance the capacity of present network, ensuring total security, bandwidth management and to provide internet connection among the student along with mobile internet facilities. The approach supports optimal routing, bandwidth providing, campus network management, network security ensuring to each LAN and remote computer & remote user access with requiring modification of the structured Infrastructure network via adding Firewall, MikroTik server, DNS and DHCP server, and access point for the mobile computers, the existing Internet. This dissertation describes the design and implementation of structured network design for the purpose of emphasizes secured network and bandwidth management. Through a prototype implementation, we have shown that the approach is possible.

1.3 Organization of the Project:

Chapter 1 **–** "Introduction" describes General introduction and goal of the project.

Chapter 2 **–** "Network" describes what a network is and the different types of networks that exist and Topology describes the appearance or layout of a network and how data flows through the network.

Chapter 3 **–** "Campus Network" describes and why campus network.

Chapter 4 **–** "Campus Backbone Topology" focuses the Constructing a LAN within the confines of a building or campus.

Chapter 5 **–** "Existing Network of DIIT Campus" presents status of DIIT campus network system.

Chapter 6 **–** "Structured Cabling" what is structured cabling and how does it works.

Chapter 7 **–** "Wireless Networks" functions of wireless network and its implementation.

Chapter 8 **–** "Proposed Network" restructuring and enhance the capacity of present network.

CHAPTER 2

NETWORK

2.1 What is Network?

The generic term "**network**" refers to a group of entities (objects, people, etc.) which are connected to one another. A network, therefore, allows material or immaterial elements to be circulated among all of these entities, based on well-defined rules.[1]

Network: A group of computers and peripheral devices connected to each other. Note that the smallest possible network is two computers connected together.

Networking: Implementing tools and tasks for linking computers so that they can share resources over the network.[2]

2.2 Advantage of Network

A computer is a machine used to manipulate data. Humans, being communicative creatures, quickly understood why it would be useful to link computers to each other in order to exchange information.

A Computer Network can serve several distinct purposes:

- Sharing resources (files, applications or hardware, an Internet connection, etc.)
- Communication between people (email, live discussions, etc.)
- Communication between processes (such as between industrial computers)
- Guaranteeing full access to information for a specified group of people (networked databases)
- Lower costs, due to sharing data and peripherals
- Standardizing applications
- Providing timely access to data
- More efficient communication and organization.

Today, with the Internet, networks have become more unified. It is clear, then, that there are several reasons to install a network, whether for a business or an individual.

2.3 Networking

Next we look at how the basic elements of connections, communications, and services work together to make networks function properly:

- The connections must operate so that any computer can send or receive electrical signals (data) across the physical media that link them.
- Communications must function so that when one computer sends a message, the receiving computer can listen and understand the message.
- Computers on a network must either provide a service to other computers or make use of a service provided by other computers.

2.4 Types of Networks

Different types of (private) networks are distinguished based on their size (in terms of the number of machines), their data transfer speed, and their reach. Private networks are networks that belong to a single organization. There are usually said to be three categories of networks:

- LAN (local area network)
- MAN (metropolitan area network)
- WAN (wide area network)

2.4.1 Local Area Network (LAN)

A local area network (LAN) is usually privately owned and links the devices in single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer

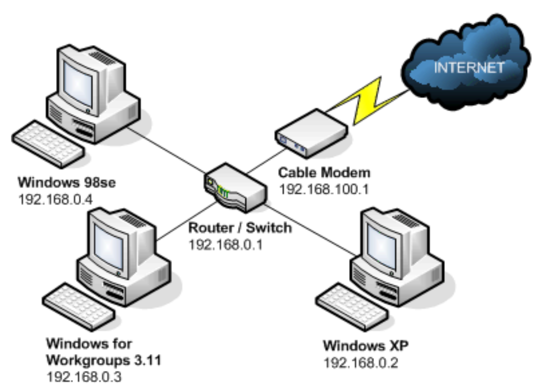

Figure 2.1: Local Area Network

in someone home office. Currently LAN size limited to a few kilometers. LANs are designed to allow resources to be shared between personal computers or workstations.

2.4.2 Metropolitan Area Network (MAN)

A Metropolitan Area Network is a network with a size between a LAN and a WAN. If normally covers the area inside a town or a city. It is designed for customers who need high speed connectivity, normally to the internet, and have end points speed over the city. A good example of a MAN is the part of the telephone company network that can provide a high speed DSL line to the customer.

A MAN is made from switches or routers connected to one another with high-speed links (usually fiber optic cables).

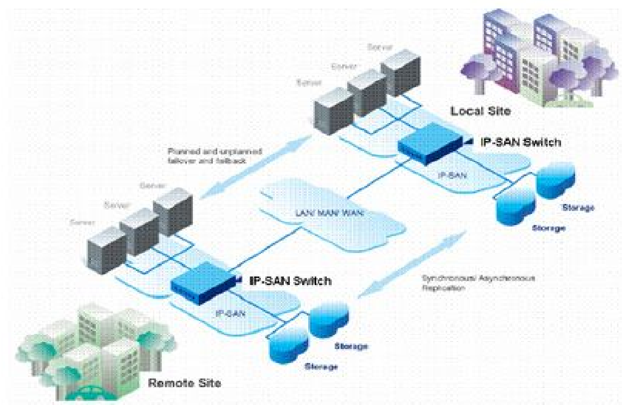

Figure 2.2: Metropolitan Area Network

2.4.3 Wide Area Network (WAN)

A wide area network provides long distance transmissions of data, image, audio and video information over large geographical areas that may comprise a country, a continent, or even the whole world. The speed available on a WAN varies depending on the cost of the connections (which increases with distance) and may be low.

WANs operate using routers, which can "choose" the most appropriate path for data to take to reach a network node.

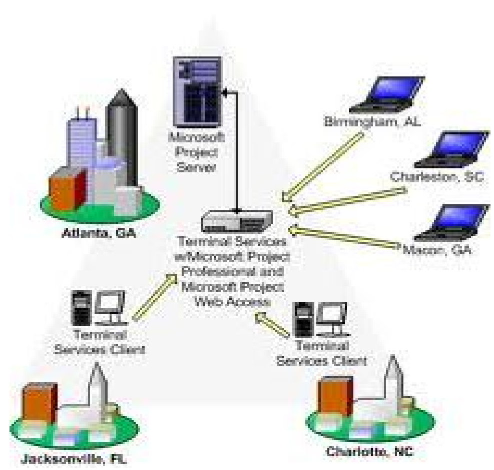

Figure 2.3: Wide Area Network

2.5 Network Topology

LAN design is called topology. Topology describes the appearance or layout of a network and how data flows through the network. There are four basic types of topologies: star, bus, ring, and mesh.[3]

2.5.1 Star Topology

In a star network (see Figure 2.4), all devices are connected to a central point called a hub/Switch. This hub/Switch collects and distributes the flow of data within the network. Signals from the sending computer go to the hub and are then transmitted to all computers on the network. Large networks can feature several hubs. A star network is easy to troubleshoot because all information goes through the hub, making it easier to isolate problems.

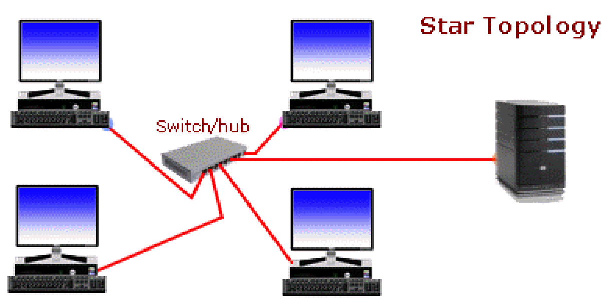

Figure 2.4: Star topology

2.5.2 Bus Topology

In a bus network (see Figure 2.5), all devices are connected to a single linear cable called a trunk (also known as a backbone or segment). Both ends of the cable must be terminated (like a SCSI bus) to stop the signal from bouncing. Because a bus network does not have a central point, it is more difficult to troubleshoot than a star network. A break or problem at any point along the bus can cause the entire network to go down.

Figure 2.5: Bus topology

NOTE: - A bus network is often referred to as an Ethernet network.

2.5.3 Ring Topology

In a ring network (see Figure 2.6), all workstations and servers are connected in a closed loop. There are no terminating ends; therefore, if one computer fails, the entire network will go down. Each computer in the network acts like a repeater and boosts the signal before sending it to the next station. This type of network transmits data by passing a "token" around the network. If the token is free of data, a computer waiting to send data grabs it, attaches the data and the electronic address to the token, and sends it on its way. When the token reaches its destination computer, the data is removed and the token sent on.

Figure 2.6: Ring topology

2.5.4 Mesh Topology

In a full mesh network, each network node connected to every other node in the network. Due to this arrangement of nodes, it becomes possible for a simultaneous transmission of signals from one node to several other nodes. In a partially connected mesh network, only some of the network nodes are connected to more than one node. This is beneficial over a fully connected mesh network require possessing some kind of routing logic so that the signals and the data traveling over the network take the shortest path during each of the transmissions.

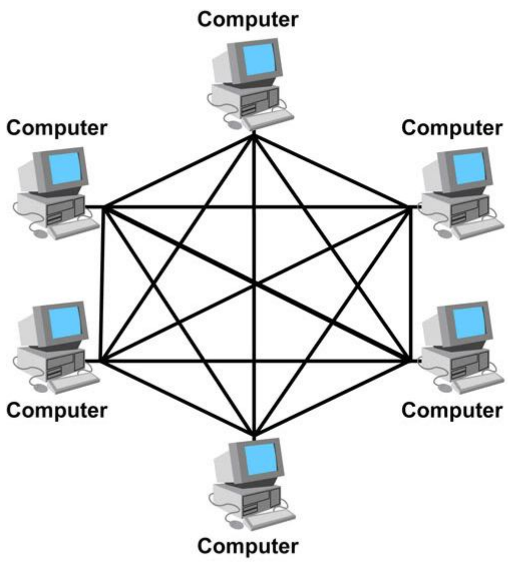

Figure 2.7: Mesh topology

CHAPTER 3

CAMPUS NETWORK

3.1 Campus network

A campus network is a computer network made up of an interconnection of local area networks (LANs) within a limited geographical area.[3][4]The networking equipment (switches, routers) and transmission media (optical fiber, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant / owner: an enterprise, university, government etc.)[4] [5]

In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including; academic departments, the university library and student residence halls.

Contents: 1. University campuses

2. Corporate campuses

3.1.1 University campuses

In the case of a college or university, its campus area network is likely to interconnect a variety of campus buildings, including administrative buildings, academic buildings, university libraries, campus or student centers, residence halls, gymnasiums, and other outlying structures, like conference centers, technology centers, and training institutes.

3.1.2 Corporate campuses

Much like a University campus network, a corporate campus network serves to connect buildings. Examples of such are the networks at DIU and DIIT campus. Campus networks are normally interconnected with high speed Ethernet links operating over optical fiber such as Gigabit Ethernet and 8 Gigabit Ethernet.

3.2 Designing Campus Networks

A campus network is a building or group of buildings all connected into one enterprise network that consists of many local-area networks (LANs). A campus is generally a portion of a company that is constrained to a fixed geographic area. [6]

The distinct characteristic of a campus environment is that the company that owns the campus network usually owns the physical wires deployed in the campus. The campus network topology is primarily LAN technology connecting all the end systems within the building. Campus networks generally use LAN technologies, such as Ethernet, Fiber Distributed Data Interface, Gigabit Ethernet, and Asynchronous Transfer Mode (ATM).[7]

Table 3.1: summarizes the various LAN technologies required to build successful campus networks. Cisco Systems offers product solutions in all these technologies.

LAN Technology	Typical Uses
Routing technologies	Routing is a key technology for connecting LANs in a campus network. It can be either Layer 3 switching or more traditional routing with Layer 3 switching and additional router features.
Gigabit Ethernet	Gigabit Ethernet builds on top of the Ethernet protocol but increases speed tenfold over Fast Ethernet to 800 Mbps, or 1 Gbps. Gigabit Ethernet provides high-bandwidth capacity for backbone designs while providing backward compatibility for installed media.
LAN switching technologies-Ethernet switching	Ethernet switching provides Layer 2 switching and offers dedicated Ethernet segments for each connection. This is the base fabric of the network.
LAN switching technologies-Token Ring switching	Token Ring switching offers the same functionality as Ethernet switching but uses Token Ring technology. You can use a Token Ring switch as either a transparent bridge or as a source-route bridge.
ATM switching technologies	ATM switching offers high-speed switching technology for voice, video, and data. Its operation is similar to LAN switching technologies for data operations. ATM, however, offers high-bandwidth capacity.

CHAPTER 4

CAMPUS BACKBONE TOPOLOGY

Campus networks can be extremely complex, with multiple protocols, various technologies and diverse configurations. A hierarchical model helps to design a scalable, reliable, cost-effective inter-network. Three logical layers with specific responsibilities are defined in this section.

4.1 Core Layer

The Core Layer is responsible for transporting large amounts of traffic both reliable and quick. Every single user can be affected by a failure in the Core. That is why fault tolerance at this layer is an issue. The Core is likely to see large volumes of traffic, so speed and latency are driving concerns here. Traffic passing the core shouldn’t be slowed down by packet filtering and access lists.

4.2 Distribution Layer

The Distribution Layer is the communication point between the Core and the Access Layer and it should provide redundant connections for reliability. It’s primary function is to provide routing and filtering. This is also the place to insert policies, add Access Control Lists, perform packet filtering, perform route summarization and define broadcast and multicast domains.

4.3 Access Layer

The Access Layer controls user access to the inter-network resources. Traffic for remote services is handled by the distribution layer. It provides access control and the creation of separate collisions domains. With this in mind, three topologies can be considered for University College of Antwerp. In the following sections each of these topologies is described.

4.4 Layer-3 Switch vs. Router

Layer-3 switching is a hybrid technology that combines the speed of a switch with the LAN segment analysis of a router to make packet forwarding decisions.

Characteristics	Lear-3 Switch	Router
Subnet Definition	Layer-2 Switch domain	**Port**
Forwarding Architecture	Hardware	**Software**
Price	Low	**High**
Forwarding Performance	High	**Low**
Policy Performance	High	**Low**
WAN Support	**No**	**Yes**

Table 4.1: Layer-3 Switch vs. Router.

4.5 Overview of IGP Routing Protocols

- **RIP** Routing Information Protocol is one of the longest lasting of all routing protocols and uses hop count to determine the shortest path to the destination. This isn't necessarily the fastest path to a destination. RIPv1 uses only classful routing, RIPv2 uses classless routing. As a distance-vector based algorithm, RIP works fine for small, stable, high-speed networks.
- **IGRP** Interior Gateway Routing Protocol is a distance vector routing protocol developed by Cisco specifically to address problems associated with routing in large network. IGRP uses a composite 24-bit metric that is calculated by factoring weighted values for internet work delay, bandwidth, reliability and load. By default, IGRP uses only bandwidth and delay to calculate their metric. Also IGRP uses only classful routing, has a much higher maximum hop-count limit than RIP to allow the network to scale and provides additional flexibility by permitting multi path routing. [8]

- **EIGRP** Enhanced Interior Gateway Routing Protocol is, like IGRP, a proprietary Cisco protocol. It is an advanced version of its predecessor IGRP and uses a 32-bit metric. It is a hybrid routing protocol. By integrating the capabilities of link-state protocols into distance vector protocols it can scale to thousands of routing nodes. But to ensure good performance in large internet works, EIGRP should be used only on networks with simple hierarchical topologies.
- **OSPF** Open Shortest Path First is a link-state routing protocol that sends link-state advertisements (LS As) to all other routers within the same hierarchical area.

OSPF was written to address the needs of large, scalable modern internet works and has the following advantages:

- **OSPF** is an open standard supported by many vendors.
- **OSPF** converges quickly.
- **OSPF** supports discontiguous subnets and VLSM.
- **OSPF** sends multicast frames, rather than broadcast frames, which reduces CPU utilization on LAN hosts (if the hosts have NICs capable of filtering multicasts).
- **OSPF** networks can be divided into hierarchical areas, which reduce memory and CPU requirements on routers.

- **OSPF** does not use a lot of bandwidth.

	Metrics Supported	Scalability	Convergence Time
RIP V1	Hop Count	15 Hops	Long if no load balancing
RIP V2	Hop Count	15 Hops	Long if no load balancing
IGRP	BW, delay, reliable, Load	255 Hops(Default 80)	Quick(triggered update)
EIGRP	BW, delay, reliable, Load	800s of routers	Very quick(Dual algorithm)
OSPF	Cost	8000s of routers	Quick (link-state adv.)

Table 4.2: Overview of IGP Routing Protocols.

CHAPTER 5

EXISTING NETWORK OF DIIT CAMPUS

5.1 Present Status

At present the DIIT campus networking system distributed scattered. It is very difficult to find fault, administrative security not properly work, lack of central antivirus solution, lot of time spent for trouble shooting and maintenance. There is no wireless connection so users are not comfort to use the network. There is no manageable software to manage bandwidth of the system for user as per their requirement. A key component is upgrading of the DIIT campus network in order to ensure a secure, managed, fully switched infrastructure that is sufficiently reliable, flexible and cost-effective to meet current demands and provide the platform and capacity for future growth.

5.2 Used of the Existing Network Equipment

Table 5.1: DIIT Institute is used in this existing network in following device:

Name of the Equipment	**Description**	**Quantity**
Server	MikroTik Server use for only Gateway purpose	1
Switch	Managed Switch	No
	Unmanageable switch	8
Hub	Unmanageable Hub	2
UPS	Online UPS for server & Switch	No
	Offline UPS for server & Switch	2
Printer	Standalone Printer	1
	LAN/Share Printer	No
Scanner	Scanner	1
PC	Office use and Class Room	80
CCTV	CCTV Camera	7

Existing Network Diagram Figure

5.3 Simulation and Testing of Existing Network:

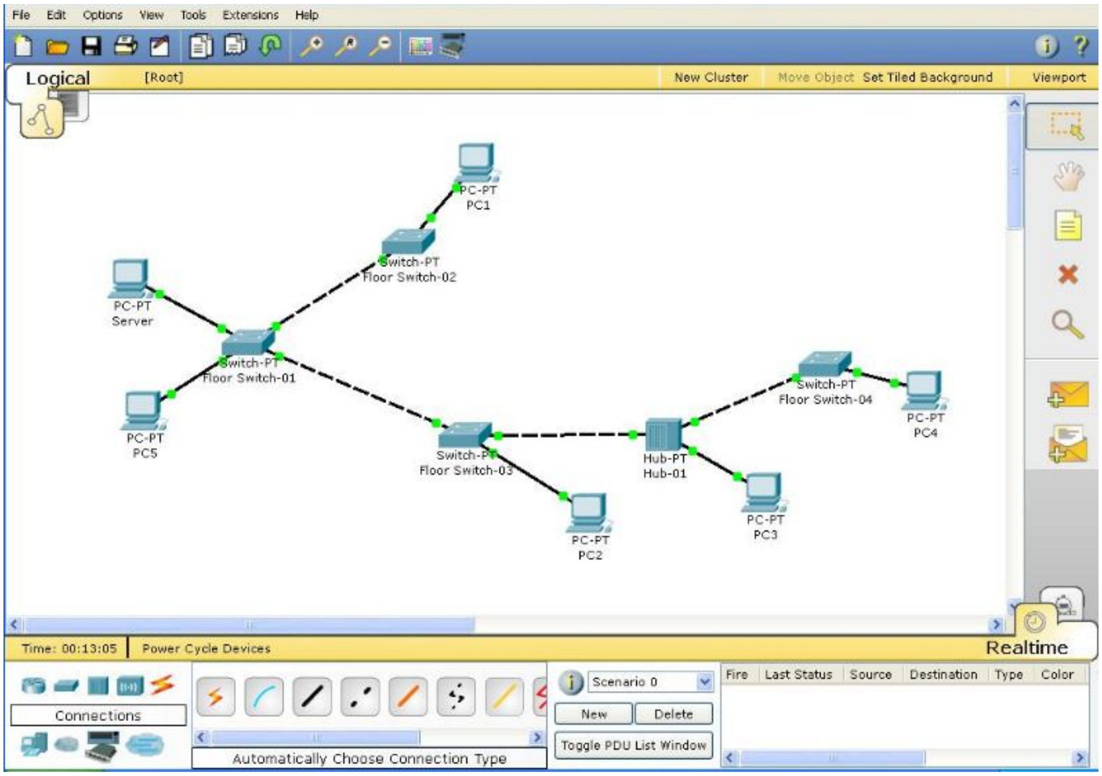

Figure 5.2_a: Simulated Existing Network Diagram.

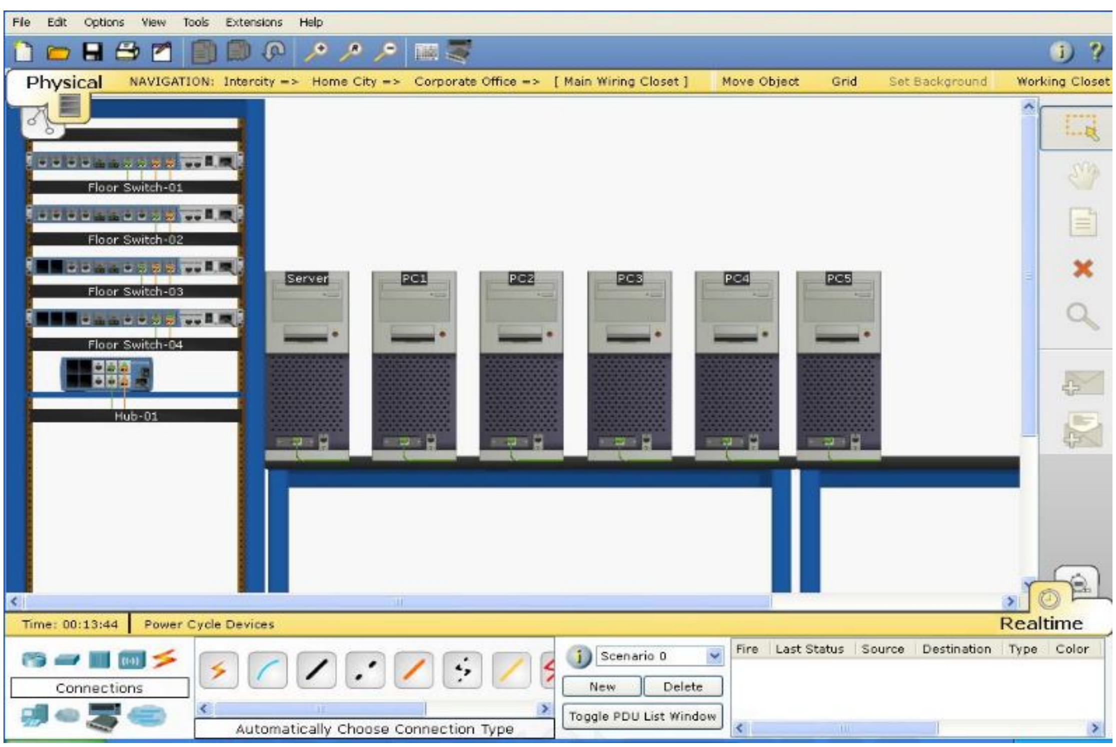

Figure 5.2_b: Existing Network Diagram.

The previous ratio of ping test from PC- 4 to Server PC is: minimum= 141ms, maximum: 265ms, Average: 176ms. (Figure- 5.3_a).

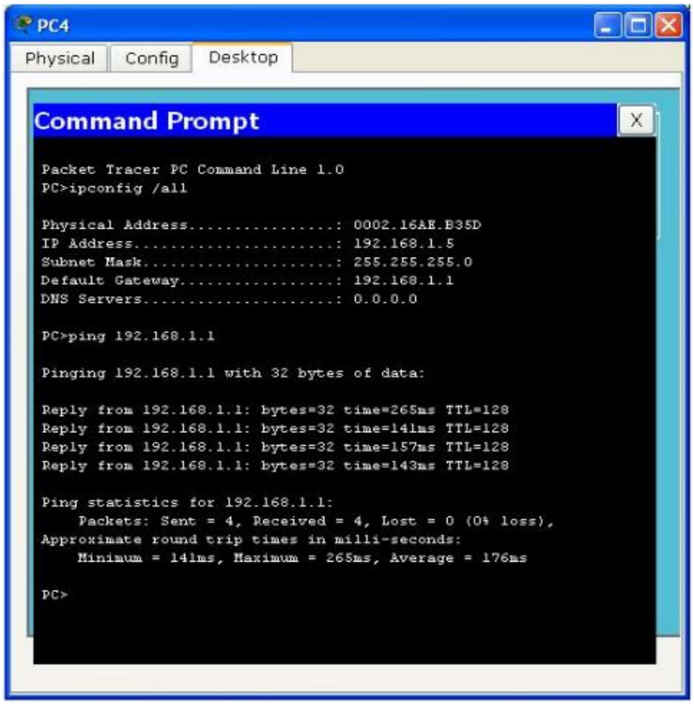

Figure 5.3_a: Ping test PC- 4 from Server Existing Cabling System.

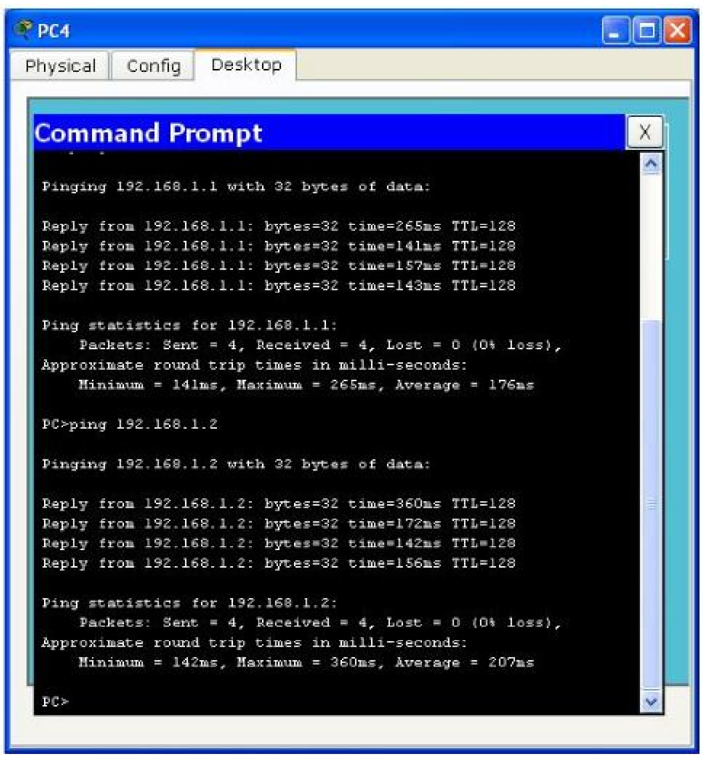

Figure 5.3_b: Ping test PC- 4 from PC- 1 Existing Cabling System.

5.4 The Deficiencies of the Current Network

Key deficiencies and risks associated with the current network are:

- It has become very difficult to manage the current network because it doesn't follow to a standards-based model.
- The jagged mix of technologies as well as the legacy connectivity.
- The cost to maintain the current network in terms of people is excessive as a result of it being unmanageable.
- A lot of time is spent in troubleshooting and maintaining the network resulting in reactive problem resolution due to the lack of pro-active network management.
- The existing infrastructure cannot cope with the rapid deployment of new services required by DIIT Faculties resulting in long delays in providing these services. This is a concern in today's fast moving ICT world since new technologies need to be exploited by educational institutions as and when they become available.
- The lack of structured security policies to run access to and from the network.
- Network security is of the highest importance today and the current network cannot manage with this requirement.
- The existing infrastructure does not have the capacity to provide for the security requirement as most of the devices are unmanaged switches and hubs.
- There is a lack of fault tolerance on the current network backbone as there is no redundancy in the existing environment.

CHAPTER 6

STRUCTURED CABLING

6.1 Introduction to Structured Cabling

With the technological advancements in the information technology field especially in the computer networking and data communications, there are a lot of communication mediums such as fiber optic cables and the structured cabling have evolved. Technology, business applications and the network cables are evolving rapidly. Structured cabling is the telecommunication infrastructure cable that consists of several parts and it is mostly used to connect the telecommunication networks. There are different standards that control the design, deployment and the setup of the structured cabling.[9] [10]

6.2 Network Cables

Cable is the medium through which information usually moves from one network device to another. There are several types of cable, which are commonly used with LANs. In some cases, a network will utilize only one type of cable; other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size.

6.3 Unshielded Twisted Pair (UTP)

UTP may vary from telephone-grade wire to extremely high-speed cable. This cable has four pairs inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. UTP can support telephone, 4 & 15 Mb/s Token Ring, Ethernet, 80 Mb/s Ethernet, and Copper 155 Mb/s ATM. UTP cable is rated by the EIA/TIA standards into categories. UTP cable is generally wired in the star topology due to the troubleshooting advantages associated with stars.

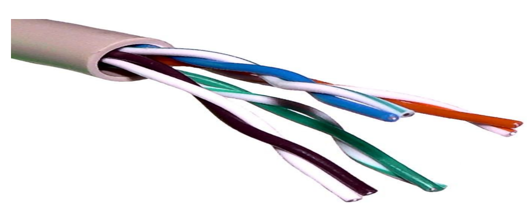

Figure 6.1: Unshielded Twisted Pair (UTP) cable

6.4 Shielded Twisted Pair (STP)

A disadvantage of the UTP is that it is susceptible to radio and electrical frequency interference. Shielded twisted pair (STP) is suitable for environments with electrical interference; however the shielding can make the cables quite bulky. Shielded twisted pair is often used on networks using Token Ring topology.

6.5 Fiber-Optic Cable

Fiber Optic cabling consists of a center glass core surrounded by several layers of protective materials. Fiber optic cable offers up the possibility of very high bandwidth and perfect immunity to noise [11] [12]. It transmits light rather than electronic signals, eliminating the problem of electrical interference. This makes it ideal for environments with large amount electrical interference and it has also been made a standard for connecting networks between buildings, due to its immunity to the effects of moisture and lightning. [13]

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. However, it costs significantly more to purchase fiber optic cable, connectors, patch panels, jumper cables, tools and network interface cards. It is also difficult to install and modify.

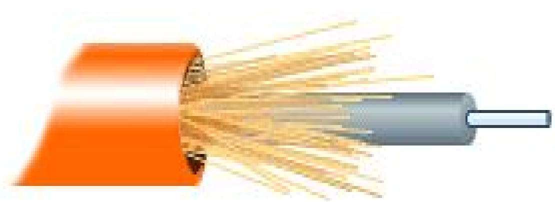

Figure 5.2: Fiber Optic Cable

6.6 Currently existing categories

The Table below shows supported protocols, maximum transmission rates, and recommended use for all categories.

	Cat 3	Cat 4	Cat 5	Cat 5E	Cat 5	Cat 5A	Cat 6	Cat 6A
Supported Protocols	Analog, Voice, ISDN, 8BaseT	IBM Token Ring	80BaseT and Lower	800BaseT and Lower	800BaseTX and Lower	8GBaseT and Lower	8GBaseT and Lower	8GBaseT and Lower
Bandwidth	15 MHz	20 MHZ	80 MHZ	80 MHZ	200 MHZ/250 MHZ	500 MHz	500 MHZ/ 650 MHZ	800 MHz
Maximum Transmission Rate	8 Mbps	15 Mbps	80 Mbps (Fast Ethernet)	1,000 Mbps (Gigabit Ethernet)	1,000 Mbps (Gigabit Ethernet)	8 Gbps	8 Gbps	8 Gbps
Usability	Predominantly telephone distribution systems	No longer installed	No longer installed	Regular data and voice traffic	Higher data traffic (Multimedia, streaming)	High data traffic, backbone distribution systems, SAN	High data traffic, backbone distribution systems, SAN	High data traffic, backbone distribution systems, SAN

Table-6.1: Shows supported protocols, maximum transmission rates, and recommended use for all categories.

Ethernet Cable Summary

Specification	Cable Type
10BaseT	Unshielded Twisted Pair
10Base2	Thin Coaxial
10Base5	Thick Coaxial
100BaseT	Unshielded Twisted Pair
100BaseFX	Fiber Optic
100BaseBX	Single mode Fiber
100BaseSX	Multimode Fiber
1000BaseT	Unshielded Twisted Pair
1000BaseFX	Fiber Optic
1000BaseBX	Single mode Fiber
1000BaseSX	Multimode Fiber

Table 6.2: Summary of Ethernet Cable.

6.7 Installing Cable - Some Guidelines

When running cable, it is best to follow a few simple rules:

- Always use more cable than you need. Leave plenty of slack.
- Test every part of a network as you install it. Even if it is brand new, it may have problems that will be difficult to isolate later.
- Stay at least 3 feet away from fluorescent light boxes and other sources of electrical interference.
- If it is necessary to run cable across the floor, cover the cable with cable protectors.
- Label both ends of each cable.
- Use cable ties (not tape) to keep cables in the same location together.

6.8 What is structured Cabling?

Structured cabling is a universal system [13]

- that supports digital as well as analog signal transmissions,
- in which the telecommunication outlets are installed even in locations where they are not needed at the moment of installation,
- that use data cables with four twisted pairs and fiber cables,
- in which long technical and also moral service life is expected,
- whose correct functionality is as important for a company as the functioning of the electrical distribution system or any other system in company's infrastructure.

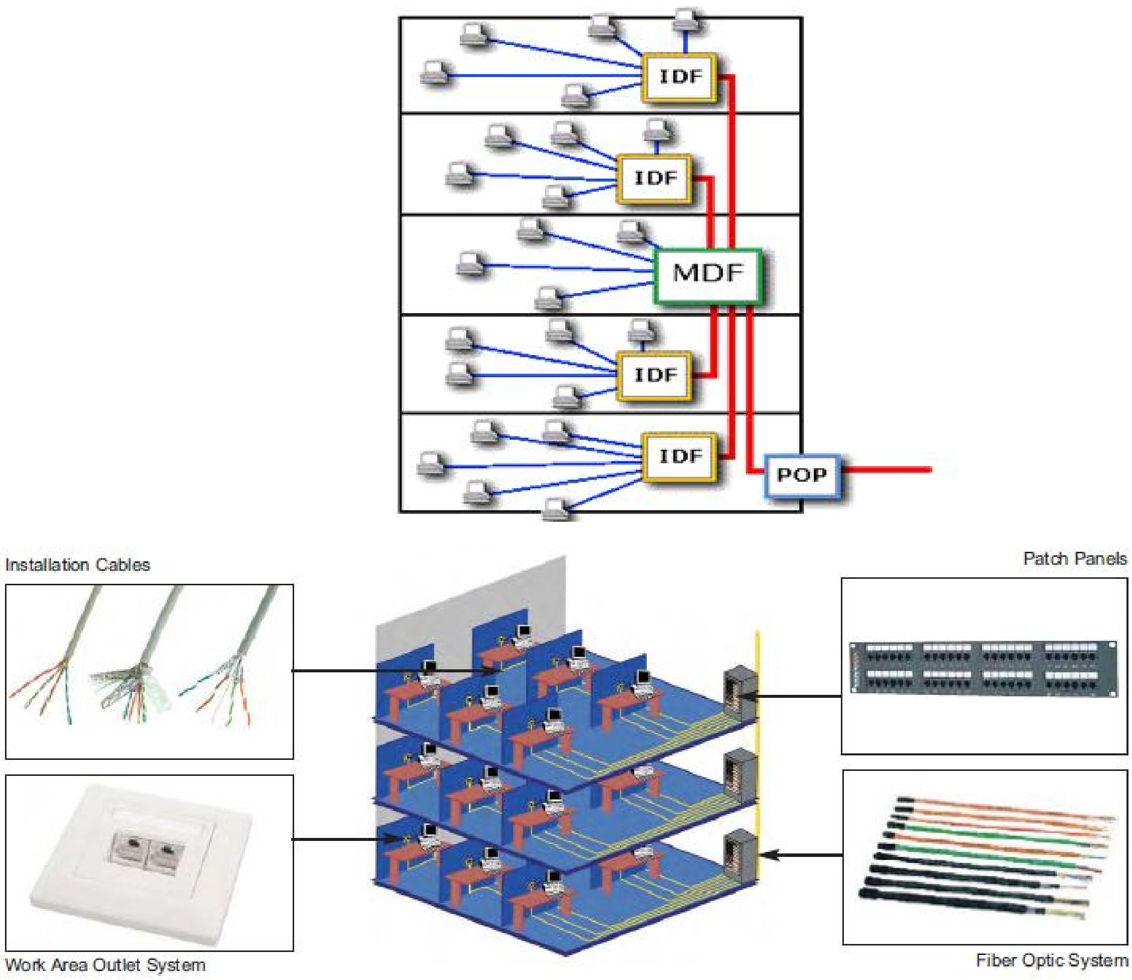

Figure 6.3: Extended Star Topology in a Multi-Story Building.

CHAPTER 7

WIRELESS NETWORKS

7.1 Introduction

A wireless network, as its name suggests, is a network in which two or more terminals (such as laptop computers, PDAs, etc.) can communicate without a hard-wired link. With wireless networking, a user can stay connected even when moving around within a given geographic area and this is why the word "mobility" is sometimes used when discussing them.[15] Wireless networks are based on a link using electromagnetic radiation (radio and infrared) instead of normal cables. There are several different technologies, which differ by the broadcast frequency they use and the range and speed of their transmissions. Wireless networks are used to make linking remote devices easier over distances from a dozen meters to a few kilometers away. This has caused the technology to attain widespread use.

Normally, wireless networks are classified into one of several categories, depending on the geographic area within which a user may connect to the network (called the coverage area):

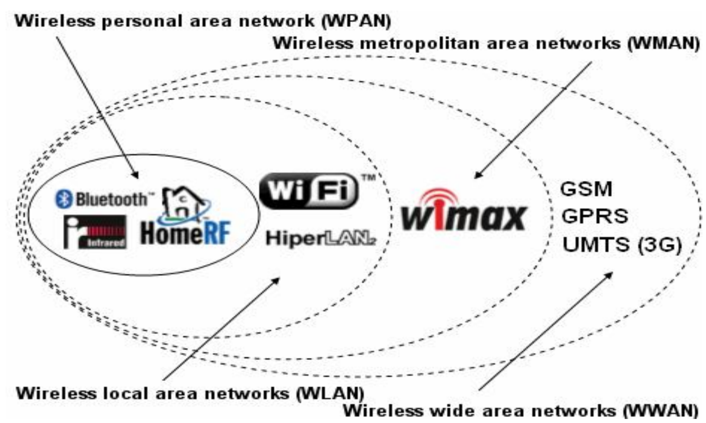

Figure 7.1: Geographically Wireless Network Coverage Area

7.2 Wireless Personal Area Networks (WPAN)

A wireless personal area network (WPAN for short) is a low-range wireless network which covers an area of only a few dozen meters. This sort of network is generally used for linking peripheral devices (like printers, cell phones, and home appliances) or a personal assistant (PDA) to a computer, or just two nearby computers, without using a hard-wired connection. There are several kinds of technology used for WPANs:

7.2.1 Bluetooth:

The main WPAN technology is Bluetooth, launched by Ericsson in 1994, which offers a maximum throughput of 1 Mbps over a maximum range of about thirty meters.

7.2.2 HomeRF:

HomeRF (for Home Radio Frequency), launched in 1997 by HomeRF Working Group (which includes the manufacturers Compaq, HP, Intel, Siemens, Motorola and Microsoft, among others) has a maximum throughput of 8 Mbps with a range of about 50 to 80 meters without an amplifier.

7.2.3 ZigBee:

The technology **ZigBee** (also known as IEEE 702.15.4) can be used to connect devices wirelessly at a very low cost and with little energy consumption. Zigbee, which operates on the frequency band of 2.4 GHz and on 16 channels, can reach transfer speeds of up to 250 Kbps with a maximum range of about 80 meters.

7.2.4 Infrared:

Finally, Infrared connections can be used to create wireless connections over a few meters, with speeds than can reach a few megabits per second. This technology is widely used in home electronics (like remote controls), but light waves can interfere with the signal. IrDA (Infrared Data Association), formed in 1995, has more than 150 members.

7.3 Wireless local area networks (WLAN)

A wireless local area network (WLAN for short) is a network covering an area equivalent to that of a business's local network, about a hundred meters in range. It allows terminals within the area of coverage to be linked to one another. There are several different technologies for this:

7.3.1 Wi-Fi:

Wi-Fi (or IEEE 702.9), supported by WECA (Wireless Ethernet Compatibility Alliance) offers a maximum throughput of 54 Mbps over a distance of several hundred meters.

7.3.2 HiperLAN2:

HiperLAN2 (High Performance Radio LAN 2.0) is a European standard developed by ETSI. HiperLAN2 lets users reach speeds of up to 54 Mbps over an area of about a hundred meters, and broadcasts in the frequency range between 5150 and 5300 MHz.

7.4 Wireless Metropolitan Area Networks (WMAN)

A Wireless Metropolitan Area Network (**WMAN**) is also known as a Wireless Local Loop (WLL). WMANs are based on the IEEE 702.16 standard. Wireless local loop can reach effective transfer speeds of 1 to 8 Mbps within a range of 4 to 8 kilometers, which makes it useful mainly for telecommunications companies.

7.5 Wireless Wide Area Networks (WWAN)

Wireless Wide Area Networks (WWAN) is the most common of all wireless networks, because all mobile phones are connected to a wireless wide area network. The main technologies are:

- GSM (Global System for Mobile Communication)
- GPRS (General Packet Radio Service)
- UMTS (Universal Mobile Telecommunication System)

Summary table of Wireless WAN

Standard	**Generation**	**Frequency band**	**Throughput**	
GSM	2G	Allows transfer of voice or low-volume digital data.	9.6 kbps	9.6 kbps

GPRS	2.5G	Allows transfer of voice or moderate-volume digital data.	21.4-171.2 kbps	47 kbps
EDGE	2.75G	Allows simultaneous transfer of voice and digital data.	43.2-345.6 kbps	171 kbps
UMTS	3G	Allows simultaneous transfer of voice and high-speed digital data.	0.144-2 Mbps	374 kbps

Table 7.1: Summery table of Wireless wide area networks

7.6 Properties of media

The weakening of signal strength is largely due to the properties of the medium that the wave is passing through. Here is a table showing attenuation levels for various materials:

Materials	**Degree of Attenuation**	**Examples**
Air	None	Open space, inner courtyard
Wood	Low	Door, floor, partition
Plastic	Low	Partition
Glass	Low	Untainted windows
Tinted glass	Medium	Tinted windows
Water	Medium	Aquarium, fountain
Living creatures	Medium	Crowds, animals, people, plants
Bricks	Medium	Walls
Plaster	Medium	Partitions
Ceramic	High	Tiles
Paper	High	Rolls of paper
Concrete	High	Load-bearing walls, floors, pillars
Bulletproof glass	High	Bulletproof windows
Metal	Very high	Reinforced concrete, mirrors, metal cabinet, elevator cage

Table 7.2: Attenuation levels for different materials.

CHAPTER 8

PROPOSED NETWORK

As finding the disadvantage of the existing network, we like to propose the following well-structured campus network solution as well as advantages.

8.1 The Proposed Network

- The campuses will be serviced by a fully switched network infrastructure that will be centrally managed. A switched network will provide for enhanced performance and throughput by giving each user a dedicated connection to the switch.
- The two main building blocks of the network will be the Core, Distribution and Access layers. The user workstations connect to an Access layer switch which in turn connects to a Distribution layer switch which acts as an aggregation point.
- The Core will be formed between Sobhanbag Campus and Kolabagan Campus.
- Maintenance will be substantially enhanced with the deployment of a single vendor product set.
- Provision has been made for wireless hotspots (approximately 15) on all campuses. These hotspots will enable users to connect via wireless technology to the network.

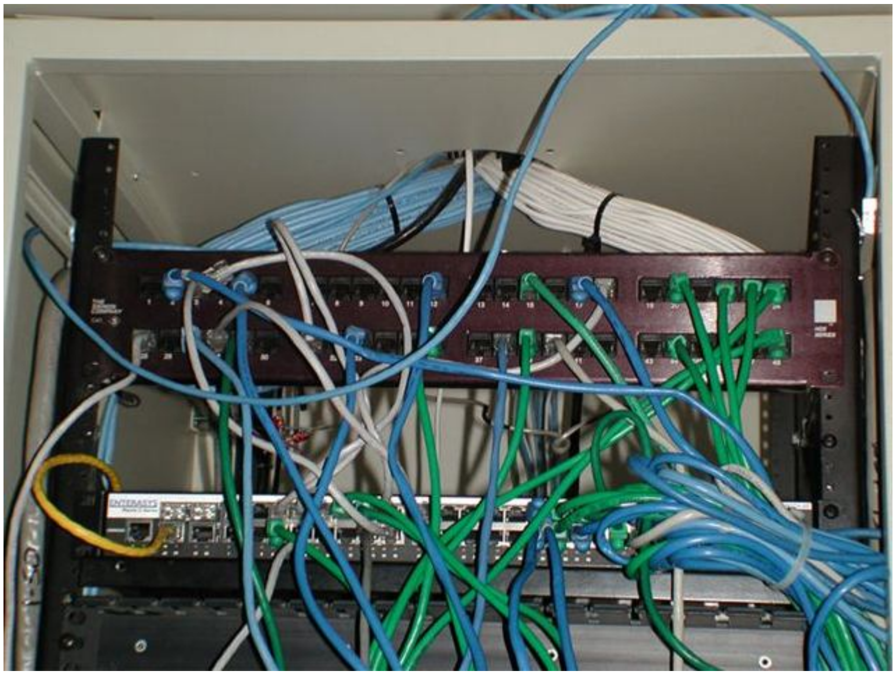

Figure 8.1: Unmanaged Cable plug in Patch panel to Switch.

Figure 8.2: Managed Cable plug in Patch panel to Switch.

Proposed Network Diagram

8.2 Simulation and Testing of Proposed Network: we are showing simulation of proposed network in DIIT Campus.

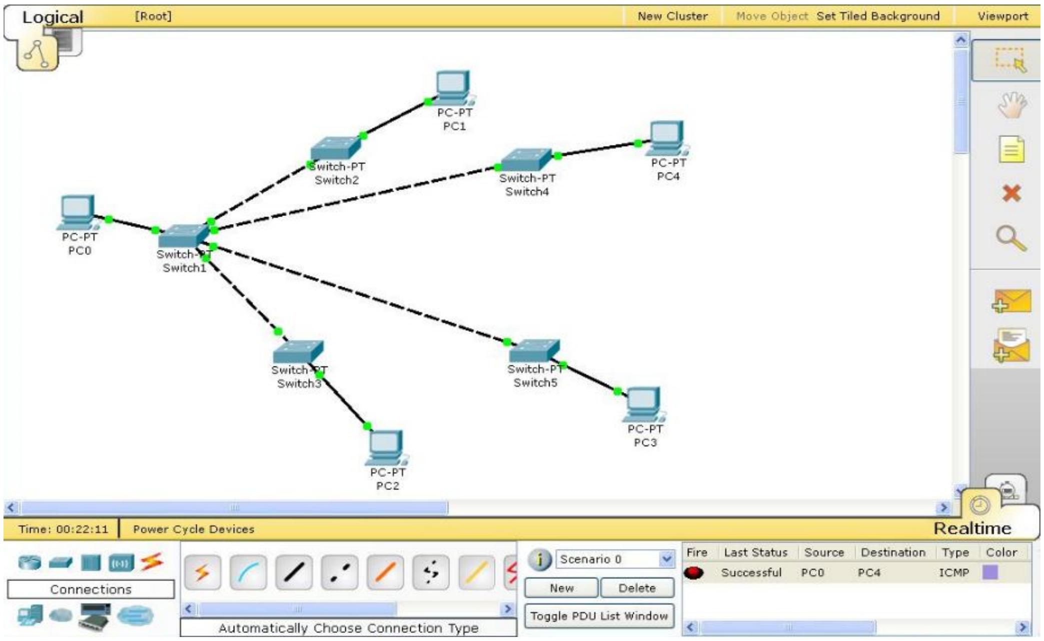

Figure 8.4_a: Simulated Proposed Network Diagram.

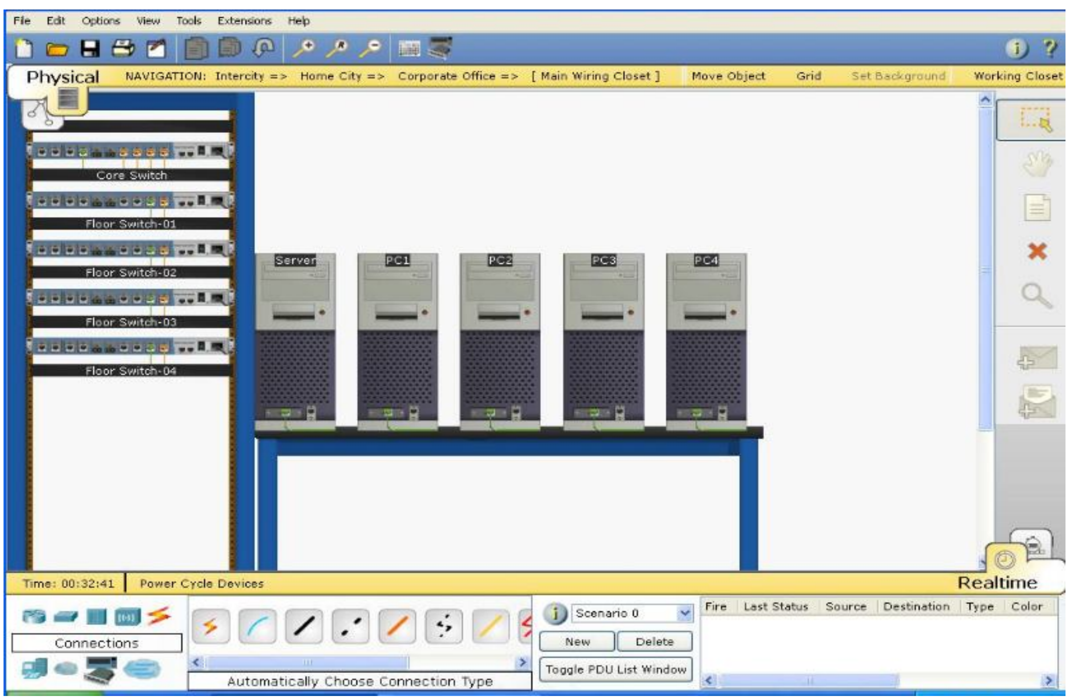

Figure 8.4_b: Simulated Proposed Network Diagram.

After introduce the propose project it has been found the ratio of ping test: from PC- 3 to Server PC is: minimum= 62ms, Maximum: 94ms, Average: 85ms. (See Figure- 8.5_b).

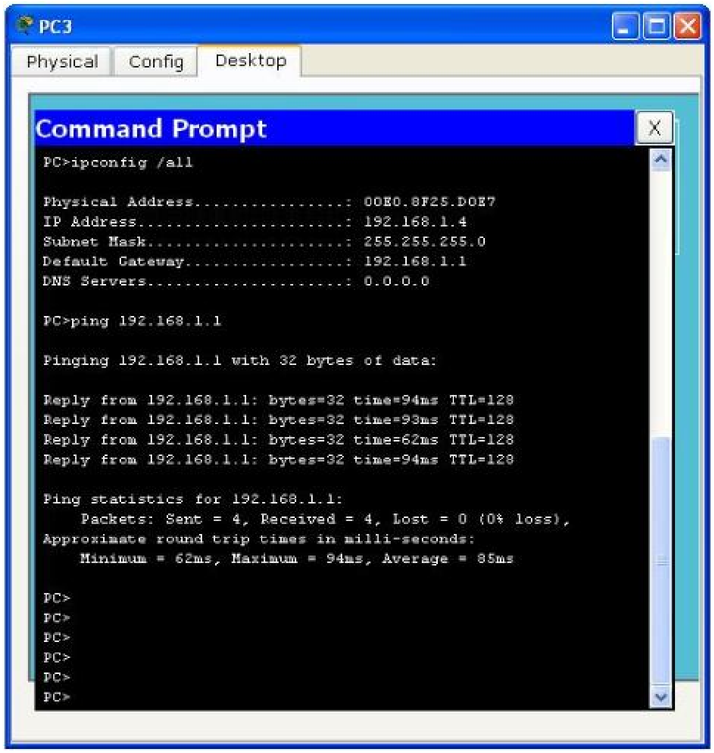

Figure 8.5_a: Ping test PC- 3 from Server in Proposed Cabling System.

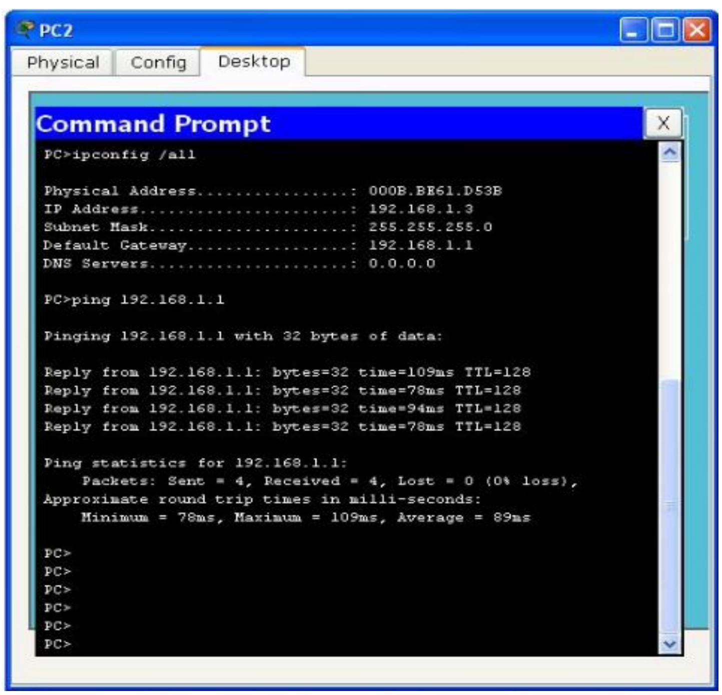

Figure 8.5_b: Ping test PC- 2 from Server in Proposed Cabling System.

8.3 Bandwidth Manage with MikroTik Server:

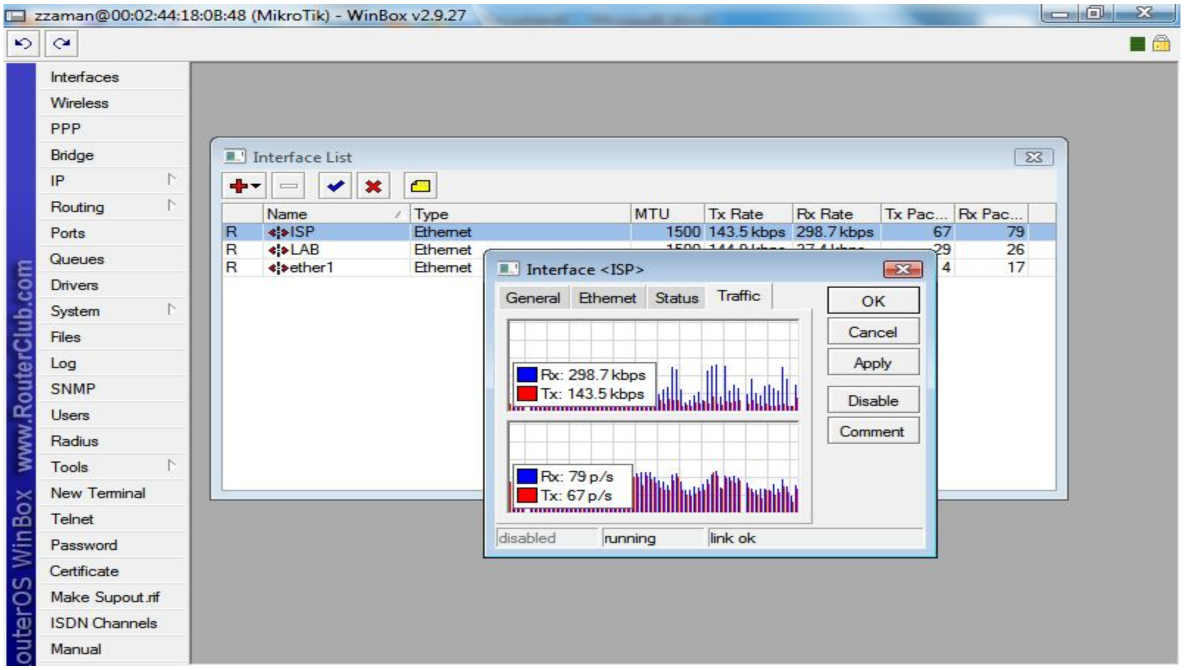

Figure 8.6_a: Showing the Interface in ISP by using the Bandwidth Graph.

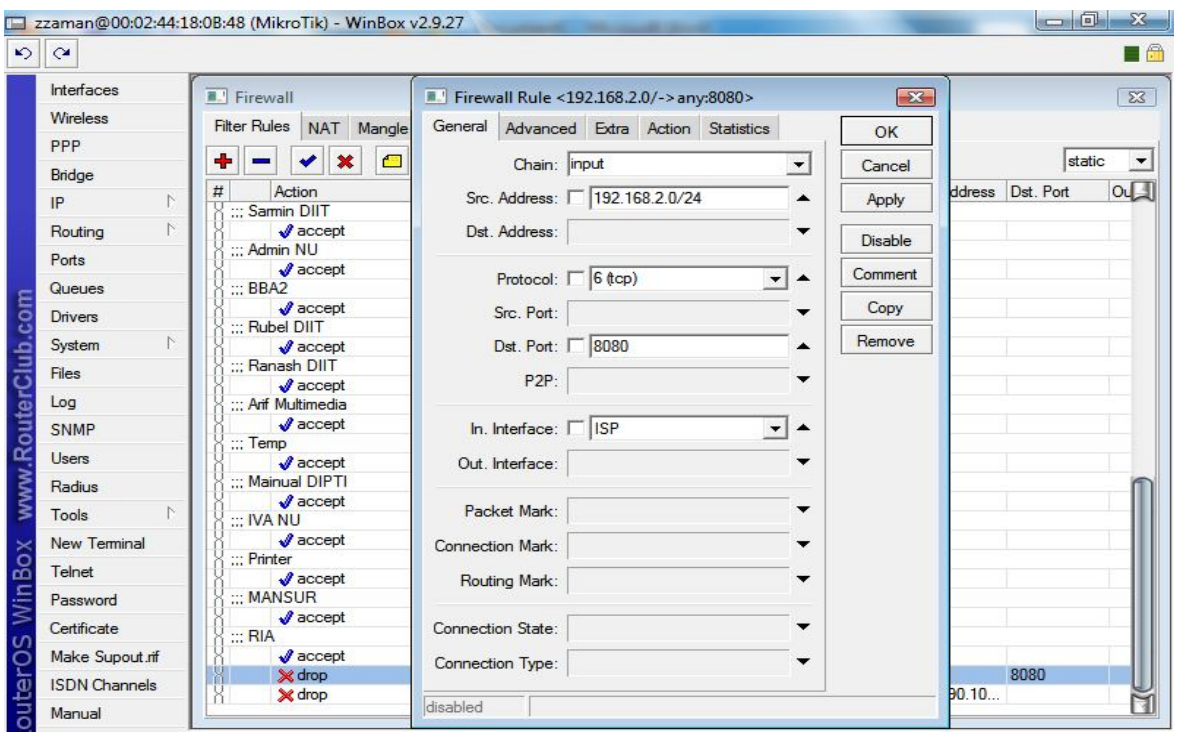

Figure 8.6_b: Firewall configure in MikroTik Server.

The above figure is showing the accepted user who might be access the internet connection and not able to access in internet below the drop button. See figure 8.6_b.

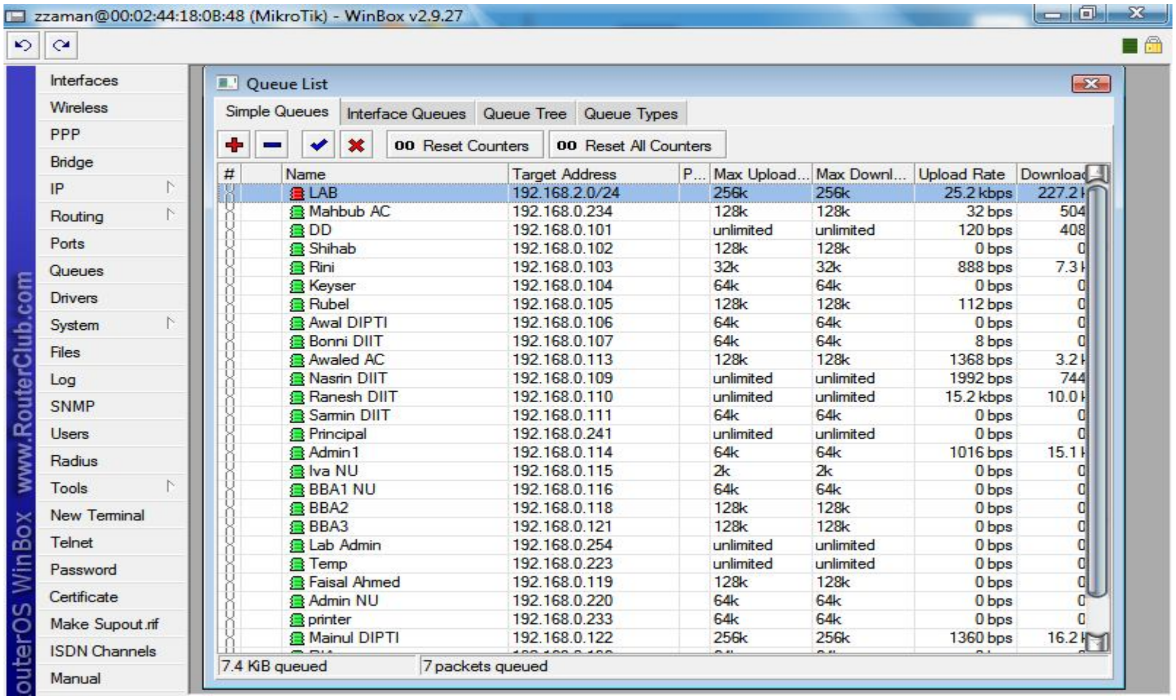

Figure 8.6_c: Showing the Interface in LAB by using the Bandwidth Graph.

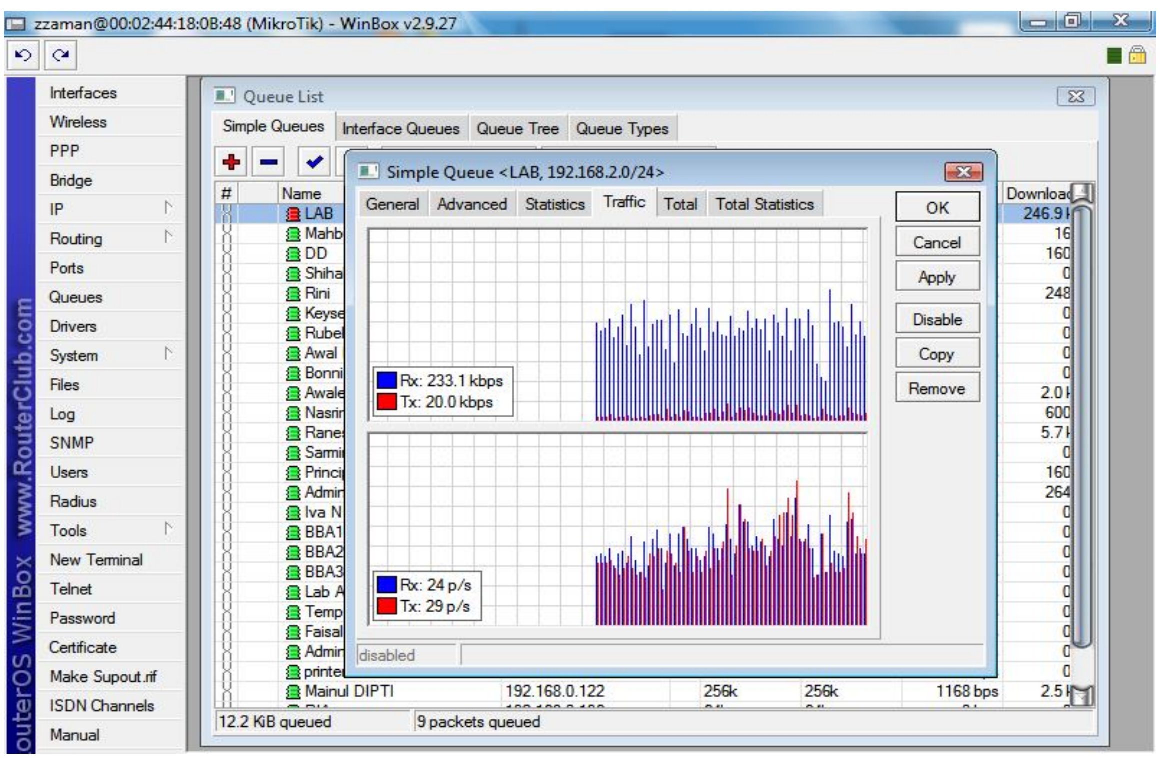

Figure 8.6_d: Bandwidth manages for Computer LAB with MikroTik Server.

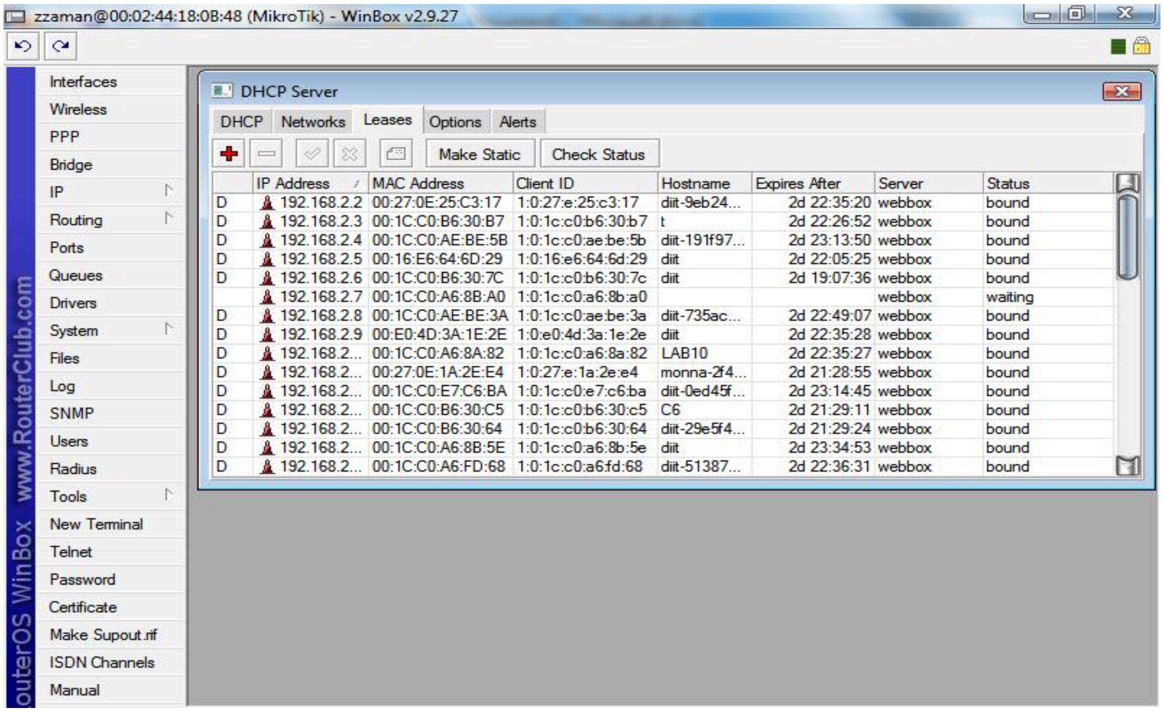

Figure 8.6_e: IP Leases in DHCP with MikroTik Server in DIIT campus.

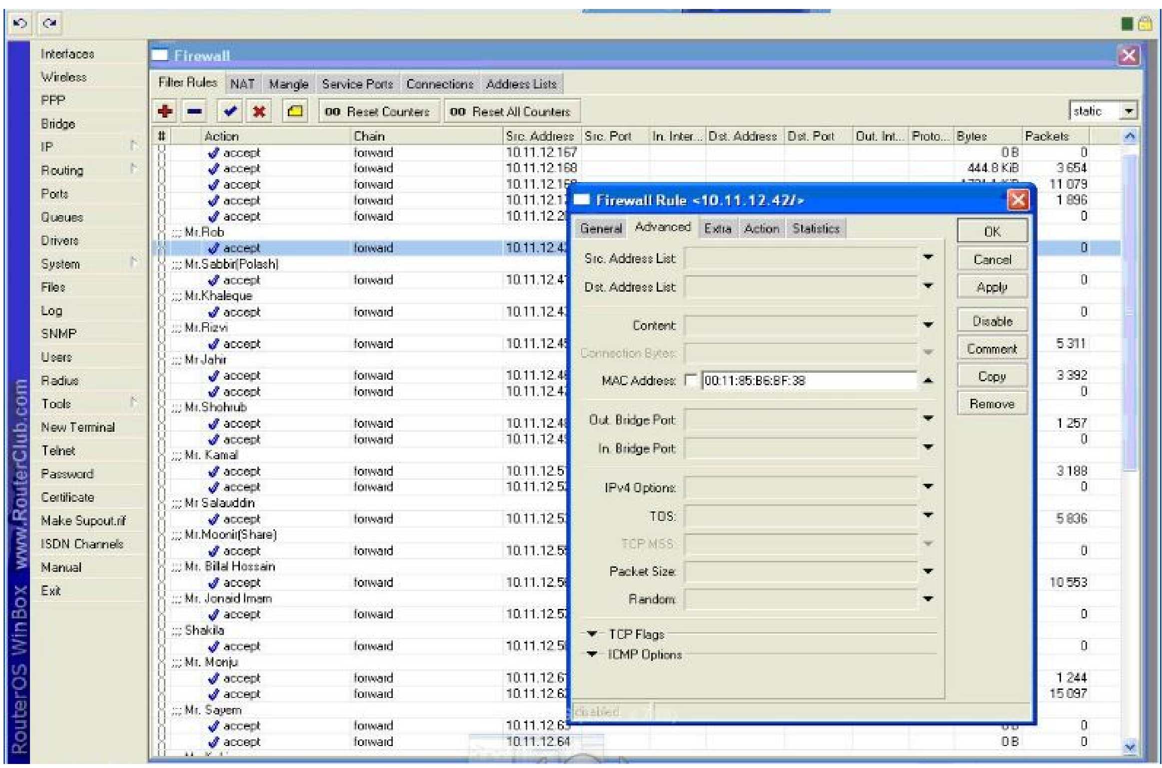

Figure 8.6_f: showing the bandwidth management system of user by using MikroTik Server.

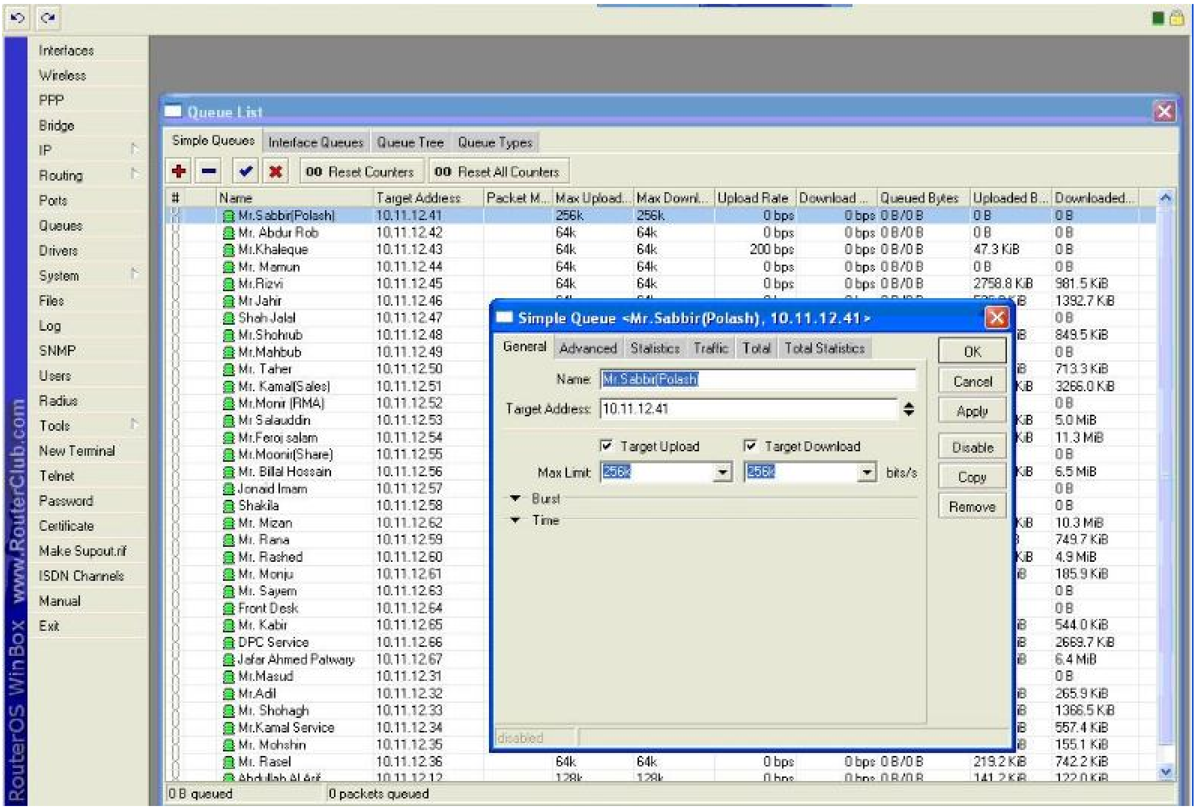

Figure 8.6_g: showing the bandwidth management system of user (Limit 256k) by using MikroTik Server.

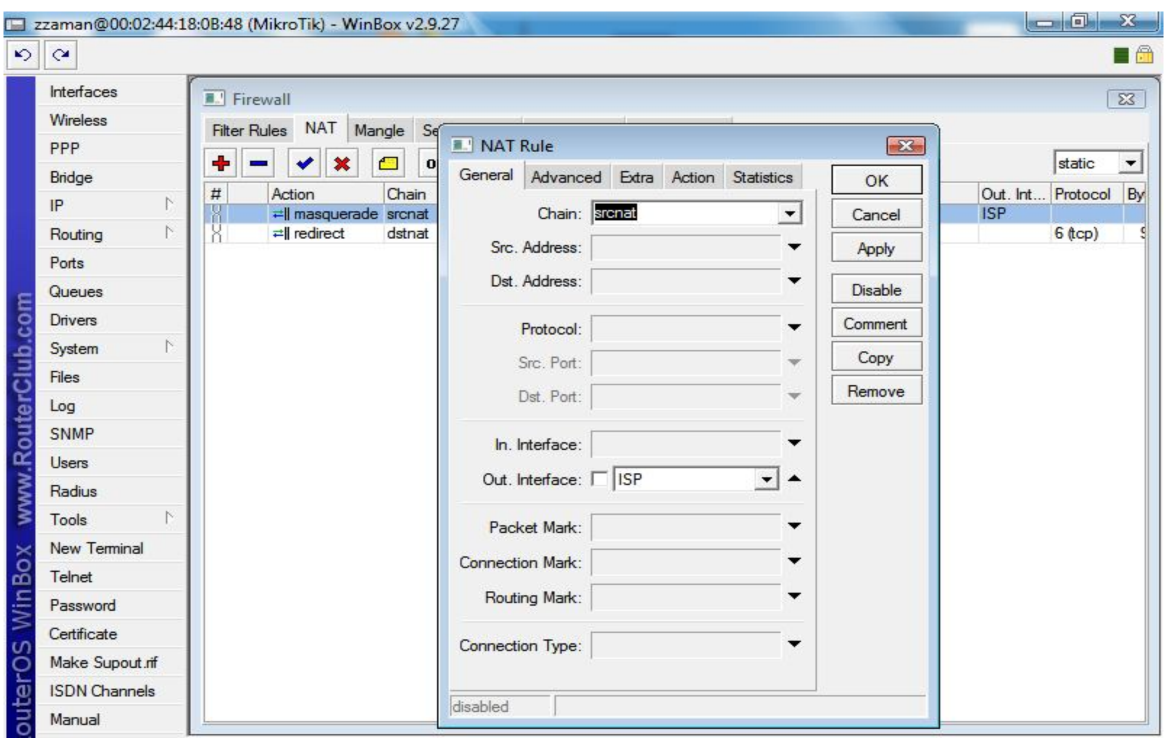

Figure 8.6_h: NAT Configure with MikroTik Server

8.4 Advantage of the Proposed Network

The proposed network design offers a number of advantages. The new design:

- Ensures a strategically positioned network infrastructure.
- Puts in place network infrastructure that is sufficiently reliable, flexible and cost effective to meet current demands.
- Provides a network platform and capacity for future growth.
- Provides a network which supports the Endeavour’s of DIIT's research community, facilitates innovative approaches to teaching and learning, and meets the communications, administrative and support service requirements of the University.
- Supports consistent service-level improvements in networking services across campus.
- Ensures a level of strength required by the DIIT user community.
- Increased speed to the desktop thus improving user productivity.
- Fewer users per switch mean that there will be no more bottlenecks in the network.
- Improved reliability and availability through managed network components and degrees of redundancy. By managing the network pro-actively, DIIT network staff will be able to identify and resolve problems and eliminate costly downtimes on the network.
- Convenience of wireless hot spots in strategic locations.
- Investment protection with regards to future technologies.
- A structured design (core, distribution and access) which will contain network traffic within necessary segments.
- Centralized management through appropriate and standards-compliant tools.
- Embracement of network security, user group segmentation and access port level authentication.
- Scalability in speed, scalability in numbers of network users and in future technology functionality.

8.5 Network Security

Network security measures on the DIIT network are primarily designed to:

- Protect the network from virus and other disruptive traffic from the Internet.
- Control access to and from the Computer Lab and open Campus.
- Force certain types of traffic (HTTP, FTP and SMTP) through proxies for security and bandwidth management purposes.
- All traffic to and from the Internet passes through DIIT's central firewall, and MikroTik server.

The policy in effect on most firewalls is an open one. Authentication is the primary security mechanism in use within the network.

8.6 Maintaining and Troubleshooting in DIIT's Network

Maintaining and troubleshooting networks differ according to the operating system. Therefore, we will need to refer to the operating systems' manuals for detailed troubleshooting procedures.

Situation	Probable Cause
Reduced bandwidth	Called a bottleneck, this occurs when the network doesn't handle as much data as usual. A bottleneck is some constraint that limits the rate at which a task can be completed. If a task uses the processor, network, and disk resources, and spends more of its time transferring data to and from the disk, you could have a memory bottleneck. A memory bottleneck might require additional RAM.
Loss of data	If data transfers are incomplete or inaccurate, check to ensure that all network cabling and connectors are intact.
Slow loading of programs	Fragmentation occurs when the operating system saves, deletes, and moves information. You must defragment the drive. If slow loading

and files	persists even after defragment, check for memory bottlenecks.
Unauthorized software	Network administrator must manage software distribution to ensure that users are not loading unlicensed software and computer viruses on the network. One way is to load only software from a centralized location or server and then remotely copy it to local hard disk drives.
Traffic overloads	A hardware or software failure can bring a LAN to a halt, or the failure can result in more data traffic than the network is designed to handle. You might receive an error message or you might not see any signs other than poor network performance. You must have a system in place that can monitor and manage network traffic. To resolve this problem, you will need to reduce the traffic on the LAN or expand its capabilities.
Common mode failures	Some LAN-component failures affect other components. This is known as a common mode failure. For example, the on-board logic of a NIC might jumble the data format. The NIC will hand the result to the network operating system, which might not detect the error. If the network operating system puts that data into a file, the file will become corrupt.
Network-security violations	Entire books address the subject of network security alone. Every operating system is different, and every customer requires a different level of security. First determine the customer's needs, and then find and read the appropriate documentation.

Table 8.1: DIIT Network maintaining and troubleshooting procedure.

CONCLUSION

The status of this research is that structured network design appears to be a suitable technique for high performance. In this report, all necessary steps of structured network have been designed and implemented. By gathering strong knowledge and compared the proposed structured network system, it is found that the proposed system is more effective and efficiency than existing network system. The campuses will be a serviced by a fully switched network infrastructure that can be centrally managed. A central switched network will provide for improved performance, ensures a strategically positioned network infrastructure, puts in place network infrastructure that is sufficiently reliable flexible and cost effective to meet current demands, provide a network which supports the endeavor's of DIIT's research community, facilitates innovative approaches to teaching and learning and meets the communications administrative and support service requirements of the University. In this project, at the NOC (Network Operation Center), DIIT's network team have monitored DIIT campus's whole network system, and problem identification, initial support to its existing users (students, employee and its faculties) over phone or physically and update to the responsible supervisor time to time. After implementing the whole functions of the proposed network, the system is tested in different stages and it works successfully as a prototype. We have faced some problem, error arises in simulation but we solved it successfully. We have tested the simulation by "Packet Tracer" version 5.0. Measure the overall things we see that the switching system, data management, controlling, traffic and security are more intelligent in well-structured network designing of Campus Network. Therefore, we are proposing this type of network system to implement in such area, which can be properly meet the total campus network requirement. Finally, the bandwidth management of the system is controlled and observed by the MikroTik software.

REFERENCE

1. Website http://en.kioskea.net/contents/networking/

2. Features of "Cabling: The complete Guide of Network Wiring", by david Groth, Jim McBee.

3. Edwards, Wade. CCNP Complete Study Guide (642-801, 642-811, 642-821, 642-831). Sybex.© 2005.

4. Gary A. Donahue (2007-06). Network Warrior. O'Reilly. p. 5.

5. http://en.wikipedia.org/wiki/Campus_network - cite_note-0

6. http://www.ciscopress.com/articles/article.asp?p=25259

7. http://www.ciscopress.com/articles/article.asp?p=25259&seqNum=3

8. Features of "MCSE: Network Essentials (Study Guide)" Chapter 4, 5 and 6.

9. website http://en.kioskea.net/contents/networking/

10. Features of "Cabling: The complete Guide of Network Wiring", by david Groth, Jim McBee.

11. Cisco networking website http://cisco.netacad.net

12. Cisco Campus networking website http://www.cisco.com

13. Features of Optical Fiber from Optical Network Magazine Volume 4, Number 6 from www.springerlink.com

14. Website www.signamax.eu

15. Website http://www.webopedia.com/quick_ref/WLANStandards.asp

ANNEX – I

Structured cabling standards:

The group, which sets standards, for structured cabling system is the Electronic Industry Association/Telecommunication Industry Association, or EIA/TIA. The EIA/TIA 568A standard defines multiple categories or upgrading of structure cabling system performance, with the category 5 designations as the highest currently standardized. The EIA/TIA 568A category 5 specifications are the basis to which many of the new high-speed LAN technologies are targeted. In October of 1995, EIA/TIA published a baseline standard for field-testing installed category 5 structured cabling.

The following are the published standards:

- **EIA/TIA-568-A:** Commercial Building Telecommunications Cabling/wiring Standards.

- **EIA/TIA-569-A:** Telecommunications Pathways & Spaces.

- **EIA/TIA TSB-36:** Additional UTP Specifications.

- **EIA/TIA TSB-40A:** Additional UTP Connecting Hardware Specifications.

- **EIA/TIA TSB-53:** Additional STP Connecting Hardware Specifications.

- **EIA/TIA TSB-67:** Field Testing Bulletin for TIA 568-A.

- **EIA/TIA TSB-95:** Field Testing Bulletin for TIA 568-A.

- **EIA/TIA-606:** Building Infrastructure Administration Standard.

- **EIA/TIA-607:** Grounding and Bonding Requirements.

- **EIA/TIA TSB-72:** Centralized Optical Fiber Cabling Guidelines.

- **EIA/TIA 526-14(OFSTP-14):** Optical Power Loss Measurement of Installed Multimode Fiber Cable Plant.

- **EIA/TIA 526-7(OFSTP-7):** Measurement of Optical Power Loss of Installed Single-Mode fiber Cable Plant.

ANNEX-II

Wireless Networking Standards

Use this chart to get some quick information to help you differentiate between the available wireless networking standards and choose which standard might be the right fit for our business. See the links below the chart for further information on wireless networking standards.

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons & More Info
IEEE802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP&WPA	This specification has been extended into 802.11b.
IEEE802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	OFDM	WEP&WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE802.11	Up to	DSSS with	WEP&WP	Products that adhere to this standard

b (Wi-Fi)	11Mbps in the 2.4GHz band	CCK	A	are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE802.11 g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP&WP A	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.16 (Wi-MAX)	Specifie s Wi-MAX in the 10 to 66 GHz range	OFDM	DES3 and AES	Commonly referred to as Wi-MAX or less commonly as Wireless MAN or the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs)
IEEE 802.16a	Added support	OFDM	DES3 and AES	Commonly referred to as Wi-MAX or less commonly as Wireless

(Wi-MAX)	for the 2 to 11 GHz range.			MANor the Air Interface Standard, IEEE 802.16 is a specification for fixed broadband wireless metropolitan access networks (MANs)
Bluetooth	Up to 2Mbps in the 2.45GHz band	FHSS	PPTP, SSL or VPN	No native support for IP, so it does not support TCP/IP and wireless LAN applications well. Not originally created to support wireless LANs. Best suited for connecting PDAs, cell phones and PCs in short intervals.
HomeRF	Up to 10Mbps in the 2.4GHZ band	FHSS	Independent network IP addresses for each network. Data is sent with a 56-bit encryption algorithm.	Note: HomeRF is no longer being supported by any vendors or working groups. Intended for use in homes, not enterprises. Range is only 150 feet from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Responds well to interference because of frequency-hopping modulation.
Hiper LAN/1 (Europe)	Up to 20Mbps in the 5GHz band	CSMA/CA	Per-session encryption and individual authenticati	Only in Europe. Hiper LAN is totally ad-hoc, requiring no configuration and no central controller. Doesn't provide real isochronous services. Relatively

			on.	expensive to operate and maintain. No guarantee of bandwidth.
HiperLAN/2 (Europe)	Up to 54Mbps in the 5GHz band	OFDM	Strong security features with support for individual authentication and per-session encryption keys.	Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth.
Open Air	Pre-802.11 protocol, using Frequency Hopping and 0.8 and 1.6 Mb/s bit rate	CSMA/CA with MAC retransmissions	OpenAir doesn't implement any encryption at the MAC layer, but generates Network ID based on a password (Security ID)	OpenAir is the proprietary protocol from Proxim. All OpenAir products are based on Proxim's module.