An Extensive Design and Implementation of a Campus Network Infrastructure Design

by

Md. Masum Billal
ID: CSE2001019146

Md. Mahbub Hasan
ID: CSE2001019119

Md. Azmal Ahmed
ID: CSE2001019121

Md. Nahid Hasan
ID: CSE2003021012

Supervised by
Md. Ashfakur Rahman

Submitted in partial fulfillment of the requirements for the degree of
Bachelor of Science in Computer Science and Engineering



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SONARGAON UNIVERSITY (SU)

May 2024

APPROVAL

The project titled "**Campus Network Infrastructure Design**" submitted by Md. Masum Billal (CSE2001019146), Md. Mahbub Hasan (CSE2001019119), Md. Azmal Ahmed (CSE2001019121) and Md. Nahid Hasan (CSE2003021012) to the Department of Computer Science and Engineering, Sonargaon University (SU), has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and approved as to its style and contents.

Board of Examiners

Md. Ashfakur Rahman — **Supervisor**
Lecturer
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 1**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 2**
Department of Computer Science and Engineering
Sonargaon University (SU)

(Examiner Name and Signature) — **Examiner 3**
Department of Computer Science and Engineering
Sonargaon University (SU)

DECLARATION

We, hereby, declare that the work presented in this report is the outcome of the investigation performed by us under the supervision of **Md. Ashfakur Rahman**, Lecturer**,** Department of Computer Science and Engineering, Sonargaon University, Dhaka, Bangladesh. We reaffirm that no part of this project has been or is being submitted elsewhere for the award of any degree or diploma.

Countersigned

(Md. Ashfakur Rahman)
Supervisor

Signature

Md. Masum Billal
ID: CSE2001019146

Md. Mahbub Hasan
ID: CSE2001019119

Md. Azmal Ahmed
ID: CSE2001019121

Md. Nahid Hasan
ID: CSE2003021012

ABSTRACT

In today's digital age, a robust and efficient network infrastructure is pivotal for the seamless operation of educational institutions. This thesis project explores the design, implementation, and optimization of a campus network tailored to meet the evolving connectivity needs while ensuring utmost security. The project aims to address the challenges associated with scalability, reliability, and security within the campus network environment. The efficacy of the proposed campus network design is evaluated through simulation studies and real-world experimentation. Performance metrics such as throughput, latency, and packet loss are analyzed to assess the network's reliability and efficiency. Additionally, security assessments and penetration testing are conducted to evaluate the resilience of the network against malicious attacks and vulnerabilities. The project begins with an analysis of existing campus network architectures, followed by the proposal of a novel framework integrating SDN, VLANs[1], and Wireless, LAN [1]. Scalability and seamless connectivity across campus departments are key focuses. Furthermore, the project delves into security measures to safeguard sensitive data and mitigate potential cyber threats. Implementation of access control policies, encryption protocols, and network segmentation techniques is explored to fortify the network perimeter and protect against unauthorized access and data breaches. The outcomes of this thesis project contribute to the advancement of campus network design methodologies, providing insights into best practices for enhancing connectivity and security in educational environments. The findings offer valuable recommendations for network administrators and stakeholders to optimize their campus network infrastructure, fostering a conducive environment for teaching, learning, and research endeavors.

ACKNOWLEDGMENT

At the very beginning, we would like to express my deepest gratitude to the Almighty Allah for giving us the ability and the strength to finish the task successfully within the schedule time.

We are auspicious that we had the kind association as well as supervision of **Md. Ashfakur Rahman**, Lecturer, Department of Computer Science and Engineering, Sonargaon University whose hearted and valuable support with best concern and direction acted as necessary recourse to carry out our project.

We would like to convey our special gratitude to **Prof. Bulbul Ahamed,** Head of the Department, Computer Science and Engineering and **Brig. Gen. (Retd) Prof. Habibur Rahman Kamal, NDC, PSC,** Dean, Faculty of Science and Engineering, Sonargaon University, for their kind concern and precious suggestions.

We are also thankful to all our teachers during our whole education, for exposing us to the beauty of learning.

Finally, our deepest gratitude and love to my parents for their support, encouragement, and endless love.

LIST OF ABBREVIATIONS

ISP	Internet Service Provider
WAN	Wide Area Network
LAN	Local Area Network
MAN	Metropolitan Area Network
PAN	Personal Area Network
CAN	Campus Area Network
WWAN	Wireless Wide Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPAN	Wireless Personal Area Network
VLAN	Virtual Local Area Networks
MAC	Media Access Controller
QoS	Quality of Service
NAT	Network Address Translation
DHCP	Dynamic Host Configuration Protocol
ACL	Access Control Lists

TABLE OF CONTENTS

Title		Page No.
DECLARATION ……..…….		**i**
ABSTRACT ……...……		**ii**
ACKNOWLEDGEMENT ……..……		**iii**
LIST OF ABBREVIATION ……..……		**iv**
CHAPTER 1		1 – 3
INTRODUCTION TO CAMPUS NETWORK INFRASTRUCTURE DESIGN		
1.1	Introduction ……..…….....	1 – 2
1.2	Security……..…….	2
1.3	Capacity ……...……...	2
1.4	Proposed Solution ……..……..……..…….....	2
1.5	User friendliness …….	2
1.6	Manageability …….	2 – 3
CHAPTER 2		4 – 9
RELATED WORK		4
2.1	IEEE 802.11 Standards ……..…….……....	4
2.1.1	IEEE 802.11 Legacy ……...	4
2.1.2	IEEE 802.11 a …….	4
2.1.3	IEEE 802.11 b …….	4
2.1.4	IEEE 802.11 g …….	4
2.1.5	IEEE 802.11 n …….	5
2.2	The Categories of Wireless Networks…….	5
2.2.1	WLAN (Wireless Local Area Networks)…….	5
2.2.2	WMAN (Wireless Metropolitan Area Networks)…….....	5
2.2.3	WWAN (Wireless Wide Area Networks)……	6
2.2.4	WPAN (Wireless Personal Area Networks)……	6
2.3	Technologies Used In Wireless Securtiy……...……..	7
2.3.1	WPA (Wi-Fi Protected Access)……...	8
2.3.2	WPA2 (Wi-Fi Protected Access Version 2)…….	8 – 9

CHAPTER 3 10 – 15

ARCHITECTURE OF THE CAMPUS WIRELESS NETWORK …….. 10 – 11

WIRELESS NETWORK INFRASTRUCTURE FOR ADMINISTRATIVE AND ACADEMIC STAFF ……...…… 12

3.1 802.1X …… 12 – 14

3.2 HOTSPOT (CAPTIVE PORTAL)…….. 14 – 15

CHAPTER 4 16 – 19

PERFORMANCE TESTS 16

4.1 DOWNLOAD SPEED TEST FOR WIRELESS LINKS……. 16 – 18

4.2 PERFORMANCE TESTS OF LOGIN PAGES…….. 18 – 19

CHAPTER 5 20 – 21

CONCLUSION……..... 20 – 21

REFERENCES ……..……... 22 – 23

APPENDIX ……. 24 – 25

LIST OF TABLES

Figure No.	Title	Page No.
Table 2.1	Comparison of the 802.11 Wireless Standards……..	13
Table 2.2	Comparison of Cryptographic Techniques in Wireless Networks……	17
Table 4.1	Download Results of Dormitories……..	26
Table 4.2	Comparison of Access Points…….	27

LIST OF FIGURES

Figure No.	Title	Page No.
Figure 2.1	Comparison of Wireless Technologies……	14
Figure 3.1	University Network Infrastructure…….....	18
Figure 3.2	Access Point Controller…….....	19
Figure 3.3	802.1x Technical Overview…….....	21
Figure 3.4	Hotspot Login Page…….	22
Figure 3.5	Hotspot Technical Overview……...	23
Figure 4.1	Fiber Infrastructure Links Between Core Switch and Dormitories……..	25
Figure 4.2	Dormitory D and Core Switch Connection …….	27
Figure 4.3	Dormitory B and Core Switch Connection …….	27

CHAPTER 1

INTRODUCTION TO CAMPUS NETWORK INFRASTRUCTURE DESIGN

1.1 Introduction

The wireless networks have become a part of the rapidly evolving technology. Currently the wireless networks can be seen everywhere such as airports, shopping malls, schools and most areas of social life. Nowadays, the wireless networks are a must and indispensable for people. People expect wireless internet access in work and living places. Because of people's habits, the fast access to social media and information has a significant impact over their life style and work. According to a report issued by IDC (Information Data Corporation) in the last quarter of 2013, 1.5 billion people use smartphone in the world. When the number of devices with wireless access such as tablets, PDAs and notebooks are added, this amount increases dramatically [1].

The first term coming to mind about wireless Internet access will probably be the ease of using it. For instance, if you will make a presentation at work and you need to use the internet in some part of the presentation, but there is no wired internet access in the meeting room. In such a case, if there is wireless Internet in that room, you can easily setup your portable computer's wireless network configuration and connect to the nearest wireless Access Point.

In a report dated 2013, the New York City Municipal has planned to supply the world's largest and free wireless internet usage service as a social responsibility project. It is expected that 95 cities and nearly 80,000 people will benefit from the free wireless internet [2-4]. In addition, Google donated some funding to San Francisco to provide free wireless Internet service to public in San Francisco parks, recreational centers and plazas [4]. Google also started to provide free wireless internet service in the southwest Chelsea neighborhood of New York City [5]. According to Google, this initiative will provide free Internet access to hundreds of thousands of people each year.

In order to assess the cost of wireless networks, many parameters need to be considered. For Example, If you are a home user, your cost of wireless network may be low because more than one person may benefit from wireless internet by using only one modem, but the same thing cannot be said for campus networks because a serious cost may be created according to the models and number of access points. Moreover, if the box solutions, which is called the controller and the central of access point is able to manage from a single location, is added to this cost, it can increase significantly.

In the large corporate networks like universities, many users with different needs demand using the wireless internet service at the same time. Campus networks that connect different local networks located in a limited geographical area is a large computer network. There are many types of users with different internet access needs in the Campus networks (academics, administrative staff, students, guest users). This complicates the network structure significantly. In addition, all Internet service providers have some legal obligations under the law of 5651 in Turkey. Designed campus wireless network infrastructure needs to provide the required mechanisms to comply with this law [6].

In the thesis, the purpose is to design a wireless network infrastructure for a university campus. We have determined the following criteria for the Campus wide wireless network services:

- Security
- Capacity
- Performance
- User-friendliness
- Manageability

1.2 Security

The designed system should be secure against hacking with conventional attacking methods. For instance, an attacker who listens to the wireless network with some sniffing tools should not be able to access people's passwords as clear text. In addition, the network should be resilient against man-in-the-middle attacks by introducing rogue access points. Moreover, MAC addresses of computers can easily be copied and the system should be designed to handle this kind of misuse.

1.3 Capacity

The wireless network is designed for a campus with approximately 4,000 students and 300 employees. In addition, the campus has many buildings. There are some buildings with classrooms, some other buildings for social life such as dormitories and cafeterias, and some buildings for administrative divisions. Wireless internet access should be provided in all buildings to all kinds of users.

1.4 Performance

Performance of the wireless Internet is very important. When we consider the performance of the wireless network, it has many aspects. First of all, the login speed of users to the wireless network should be as fast as possible. Second, download and upload speed of users should be as fast as possible. Third, the university has a connection bandwidth of 200Mb/s to the national Internet backbone for universities. This bandwidth should be divided among the users fairly. While some heavy users are getting good download speeds, other users should not be starved of the bandwidth. In addition, selection of access point devices is very important. Since many students may concurrently connect to the same access points, it is very important that the proper access point devices be deployed.

1.5 User friendliness

The wireless network should be easy to use for all kinds of users. Students, academics, administrative staff and guests should be able to access the wireless Internet with minimum overhead. In addition, new users should be able to join the network with ease. New user addition mechanisms for all kinds of users should be determined. Login methods to wireless network for all kinds of users should be specified.

1.6 Manageability

Management of wireless networks is very important in university campuses. Since there are many buildings in the campus and many access points in every building, monitoring of the healthy operations of wireless access points is very important by network administrators. In addition, network administrators should be able to manage the access points remotely for

speedy handling of problems. Network administrators should also be able determine the needs for additional access points and deploy new

ones when needed. Moreover, network administrators should be able to detect unauthorized login attempts and improper network usage.
These criteria are very important in order to design a good university campus wireless network. The purpose of this thesis is to design a wireless network infrastructure for a university campus that is stable and have its problems minimized by regarding the criteria mentioned in the previous section.

In the second chapter of the thesis, we will put forward the related standards of the wireless networks and technologies that are used. In addition, the security models for wireless networks will be explained.

In the third chapter of the thesis, the general network architecture will be given. The buildings and the campus plan are provided. The wireless network model is explained and the technologies that are used discussed. In addition, the expectations from the wireless network are delivered.

In the fourth chapter of the thesis, we provide the performance measurement results for access points and the network infrastructure.

In the last chapter of the thesis, conclusions are provided.

CHAPTER 2

RELATED WORK

In this chapter, we first explain the historical developments and the standards of wireless network structures and then the categories of wireless network technologies. After that, we will explain the security scenarios that are widely used in wireless networks.

2.1 IEEE 802.11 Standards

Due to some problems experienced in wireless networks, in 1997, 802.11 standard group was established by the Institute of Electrical and Electronics Engineers (IEEE) (international non-governmental organization). Through this group, by being come a sequence of letters to end of the form of 802.11x…., some new standards were tried to build on these structures. Along with every new change, the safety and coverage distance of 802.11-communication standard is gradually increased. [7]

We explain the main standards about wireless network with the chronological order:

2.1.1 IEEE 802.11 Legacy

The first version of the 802.11 communication-rules was launched in 1997. This version is called "legacy". Legacy data speed was max. 2 Mbit / s. As a frequency band it was broadcasted over 2.4 Ghz. This version used the technology of Carrier Sense Multiple Collision Avoidance (CSM / CA). Although this technology is very successful in respect of reliable data transfer, it leads to a large workload over the data transfer volume. While there is no clear information about the shooting distance of Legacy 802.11 in the standard off the field, in the open field, this value is approximately 75m. [7][8]

2.1.2 IEEE 802.11 a

The second of 802.11 series was implemented together with problems experienced in legacy and was launched in 1999. While Legacy is using 2.4GHz frequency, 802.11a is broadcasting in the 5 GHz frequency band. Of course, according to the legacy, the 802.11a series increased access distance and data transfer speed like each standard developed. The maximum data transfer speed 802.11a standard is 23 Mbit/s and its shooting distance in the open field about is 100m, in the closed field about is 13m respectively [7].

2.1.3 IEEE 802.11 b

Like 802.11a series, it was launched in October 1999. It is broadcasting over the 2.4 GHz as a frequency band. Its maximum data speed is 54 Mbit/s and its access area is approximately 35m in the interior [7][9].

2.1.4 IEEE 802.11 g

802.11g series was launched in 2003, it’s the data transfer speed while the 2.4 GHz frequency band is being used is again 54 Mbit/s. When it is compared with 802.11a, it can be said that it has got lower path-loss and is cheaper. Access area in the interior is about 35m like 802.11b [7][9].

2.1.5 IEEE 802.11 n

802.11n series was published in 2008, it is broadcasting in two different frequency bands (2.4 GHz for n pre-broadcasting, 5 Ghz for the n standard). Currently, it is the most commonly used standard. The maximum limit for data transfer speed is 600 Mbit/s [7][10].

The comparison of the 802.11 wireless standards :

802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac (Draft)
Year Released	1999	1999	2003	2009	2011 (Draft)
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	>1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	TBD
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	TBD

Table 2.1 : Comparison of the 802.11 Wireless Standards

Using 5GHz frequency has several disadvantages. As it is known, if the frequency of the carrier signal increases, this frequency undergoes to the damping more quickly in the environment. In addition, due to the fact that the frequency is absorbed by walls and other objects found in the environment, the distance increase at 5GHz- communication is harder than at 2.4GHz [11].

2.2 The Categories of Wireless Networks

2.2.1 WLAN (Wireless Local Area Networks)

WLAN is a wireless LAN with the short description. In other words, WLAN have all the features of which a wired local area networks have. Along with WLAN, many facilities are provided to users such as access to programs on the server (with internet access with broadband), electronic mail and file sharing service. The range of WLAN systems is approximately 100 meters. [12]

2.2.2 WMAN (Wireless Metropolitan Area Networks)

The networks, which have been formed by the computer connection in a city sized areas and in places far from each other, are called WMAN. In today's technology, the connection is provided by Fiber optic connection. Geographically, WMAN include structures which is larger than the LAN and smaller than WAN. Approximately their capture field varies between 4 km and 10 km. Although WMAN are cheaper and more flexible structure than a wired networks, WMAN have so much weakness in terms of the healthy working. WiMAX applications are being developed in this field. [13]

2.2.3 WWAN (Wireless Wide Area Networks)

According to WLAN, WWAN have been developed for the wide coverage fields and they can cover an area the size of a country. They are widely used in technology which is well known such as GSM (Global System for Mobile Communications) and GPRS (General Packet Radio Service). All the mobile phones are connected to these networks. [13]

2.2.4 WPAN (Wireless Personal Area Networks)

WPAN wirelessly connect electronic devices which are close in terms of distance. Generally, they are able to work between a few meters away and max. 10 m away (approximately). According to other networks, WPAN have lower data speeds. WPAN are heavily used in Bluetooth, HomeRF and UWB technology. [14]

The comparison of Wireless Technologies :

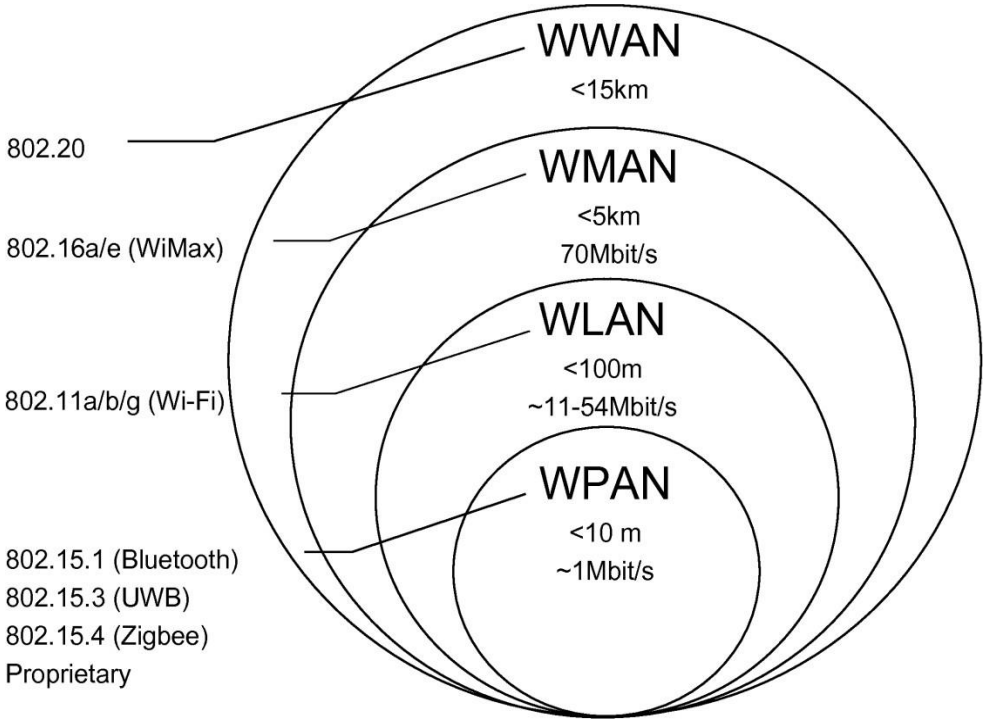


Figure 2.1 : Comparison of Wireless Technologies

2.3 TECHNOLOGIES USED IN WIRELESS SECURTIY

The widespread use of wireless networks resulted in some security problems. Although a technology that facilitates our lives, of course it may have some negative sides. The biggest problem in wireless networks is shuffling of data in the air. Unlike that is not a problem for the computers which do not have access to key devices connected to us in the wired networks, in the wireless networks each computer that can receive the broadcast is enough to create a security risk for wireless network users. [15] In this regard, we will talk about a number of measures.

1. Access Point (AP) settings- their default settings to be changed:

   As a result of many research done, especially most of home users is using their wireless internet distributor device with the default settings. This means that everyone can easily access or reach their wireless network user names and passwords. These

   adjustments must be carried out firstly, otherwise someone who knows your device's user name and password is able to use your network as he or she wants. [15]

2. The SSID broadcast in Access Point (AP) to be hidden:

   This security method is basic and very simple measures. Our SSID information is declared anywhere the network broadcast reaches at certain periods. If the SSID is hidden, then we'll be able to eliminate this declaration. In this way, the machines which call the wireless networks cannot see the SSID which we hide. Therefore, only computers which have SSID information or the devices which use the wireless network will have an access. When the network broadcasts without any password, because of being a very simple security measure, a user with basic technical knowledge is able to learn the SSID information we hide by using a 3rd party-software.[15]

3. Access Point (AP) the MAC-based network makes possible to provide access:

   One other safety measure is that only defined users should provide access to the network by defining the MAC-information of users wanting to enter the network to the system. Therefore, a device with the MAC address not defined will not be able to enter the network. But assuming that all the information is flying in the air, learning a valid MAC address will be very easy by using simple environment listening software. Afterwards, the last step is that the valid MAC address change with the MAC address of the device you want to enter the network by using just one command line. With this way, another device instead of the device allowed to connect to the network can use network resources.

Nowadays, listening to wireless networks and reaching a set of datas are very easy by analyzing the network. All items listed above are only some of the basic security measures. Unfortunately, we cannot say that we are completely sure about the security of the network even if all of these security applications are applied because of all of the datas are at the vacuum of space. In summary, to establish a secure wireless network, certainly, the connection should be encrypted [15].

2.3.1 WPA (Wi-Fi Protected Access)

(802.11i) was launched as a new security protocol by Wi-Fi Alliance in 2003 in order to solve serious security weaknesses in WEP (802.11) [16]. The data encryption together with WPA is being converted more complex and difficult structure against the

breaking. The encryption is reinforced by using variable key structure instead of the static key in WEP. Along with WPA, Temporal Key Integrity Protocol (TKIP) and 802.1x mechanism is discussed. Together with the two new features, the dynamic key encryption and mutual authentication is becoming realized. All these features have been developed to eliminate weaknesses in the security of 802.11.
While the data in WPA are encrypting with RC4, 128-bit key and 48 -bit length initialization vector (IV) are used. Additionally, in WPA, MIC (message integrity check) was developed. This feature was developed to prevent take overing the packages in the wireless network from hackers, so it replaced the CRC in WEP. WPA uses the Message Integrity Check Algorithm (named Michael) to ensure data integrity. According to CRC in WEP, Michael is much stronger [17]. There are two different versions of its, personal and enterprise.

2.3.2 WPA2 (Wi-Fi Protected Access Version 2)

WPA2 is the improved version of WPA and was announced by the Wi-Fi Alliance in September 2004. Along with WPA2, AES which is a encryption techniques more powerful than TKIP was developed. AES use the key 128-bit in encryption but in WPA2 variable key is used like WPA. In addition to this, particularly, CCMP (Cipher Blocking Chain Message Authentication) encryption protocol was added for using in wifimax technology. Even though CCMP mostly uses the same key for encryption and authentication, it uses a different initial vector (IV). Along with WPA2 security level has improved considerably.

While WEP passwords can be cracked in a few minutes by hackers, the breaking passwords has been very difficult situation for hackers via the WPA and WPA2 even if it is impossible [17]. In sum, we can say that although AES is bringing much more security, the TKIP algorithm more successful than it with respect to performance.

Like WPA, there are two different versions in WPA2, Personal and Enterprise. While Personal mode is using PSK (Pre- shared key), enterprise mode uses the EAP protocol.

The Comparison of Cryptographic Techniques in Wireless Networks :

	Auth	Encryption
WEP	PSK	RC4 64 bit Low encryption Mode RC4 128 bit Low encryption Mode
WPA Personal	PSK	TKIP → RC4 128 bit
WPA Enterprise	802.1x	TKIP → RC4 128 bit
WPA2 Personal 802.11i	PSK (passphrase)	AES (w/CBC)
WPA2 Enterprise 802.11i	802.11i	AES (w/CBC)

Table 2.2 : Comparison of Cryptographic Techniques in Wireless Networks

CHAPTER 3

ARCHITECTURE OF THE CAMPUS WIRELESS NETWORK

ln this chapter, we will try to create university wireless network and security patterns as mentioned in second chapter. As university network sheltering many devices in and spreading into a large of places, as a structure having many changeable parameters. University campus network having heterogeneous structure because there are many kinds of internet users like, students, administrative and academic staff and guest. ln this context, to provide fast and safe network for a device which is connected to internet should be designed.

Our university network infrastructure :

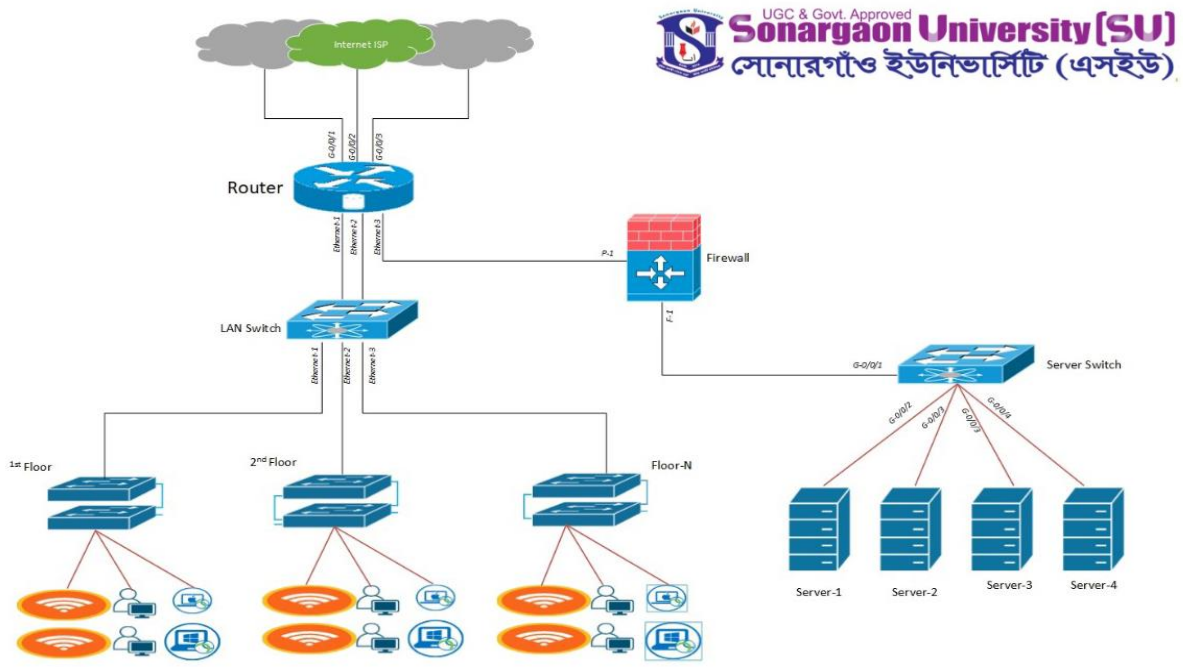


Figure 3.1 : University Network Infrastructure

There is library, student center, sport halls buildings with consisted from nine buildings for girls and boys' dormitories and approximately to a thousand of students are provided to have wifi network, besides four educational faculty.

The wifi network of our university campus we will use one core switch and over than fifty edge swithes. The wifi network of university campus is shown in upper figure. We will use around two hundred Access Points in our architecture. We will include one box solution which is known "controller" on the world of IT. It better to mention on some points about controller. Controller and some similar structures, are very important for places like universities which include many devices especially in directorship fields. If to give an example about our structure, in any Access Point settings changings which is around two hundred AP's would be huge time losing to log in and direct one by one. However, in systems where the controller like structures found any setting changes in the duration of APs on a single management interface,

enter the settings AP changes will be as short and simple. Another important advantage in this process is the margin of error based on individual APs access the management interface is very low.

The schematic work logic of sample controller device :

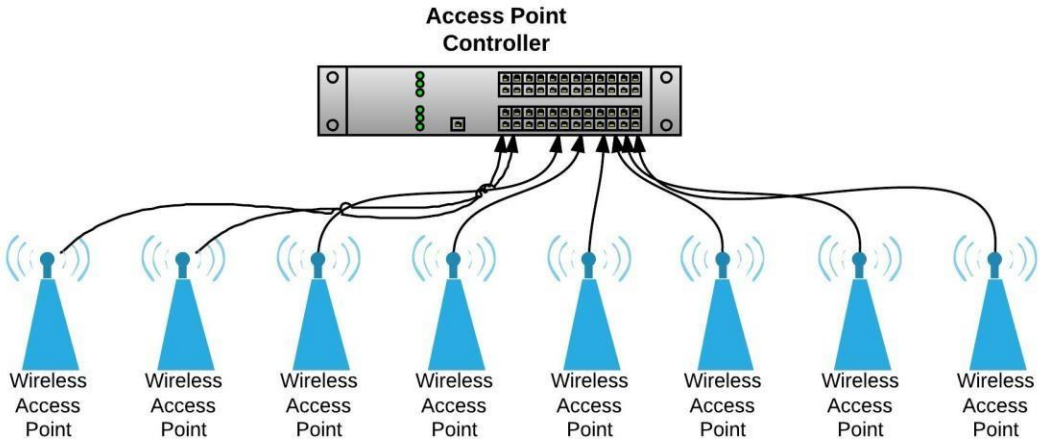


Figure 3.2 : Access Point Controller

The university network is designed to include four thousand students and three hundred staff's needs. In the meantime the network that we will design includes a thousand students users to use internet in the dormitories intensively, should be considered. Therefore, we can design the network infrastructure 7/24 should expect to be able to deliver services in a seamless manner. Nevertheless, including the 5651 number law, internet providers like universities are obliged to save information's of users and keep it for a time. We will use a software analyze to perform obliged law.

While creating university campus wi-fi network since habits of using internet differ for student and staff, it will be very important step for security to separating networks.
In the campus networks another important feature is our solution for a new device during adapting to the system fastly, it will be very easy with the structure that we will use. While delivering new staff computer, user and computer information's is saved to active directory. When domain settings are completed by authorized without any settings relevant staff will utilize from network system. What staff should do is, to code given user name and password.
Another problem in the campus networks is to provide a network for guest users. Our solution according to this problem guest user request for connection to Network Administration Unit. With request, an account with identity is created by Information Technology staff. After account created a user can utilize from the connection by the account in the student users' network. The valid of this account will last according to guest accommodation time.

Another flexible side of structure that we created is, provide network for guest groups creates account for group as it's a singular guest and for group to utilize from this account. We can design our network in this knowledge light.

Wireless network infrastructure for administrative and academic staff

Since computers of university staff are given by university administration, it's means that we can control the computers. It works a lot for us for the network structure that we will create. As it was told in initial chapter, we can use different security of modelling in the network structure. For example, in the wi-fi network structure a secure model which is encrypted with WPA2. SSID could be published in the university and we can make a solution by distributing the password. But with the structure of WPA2 downloaded an easy hacking tool won't help to hack the system, even if so, a careless user who shares his password with the third person (controlled or uncontrolled), an unauthorized person who you don't know can use your password and your network admins won't be aware from this problem. When we find out that your password is being used by third person, we should change the password in this kind of case a mistake which is done by a user we would have to reach to a hundred of users to share the new password. This would be wasting a work day and a lot of time. During such a time it's another problem for users to not be able to utilize from the internet network. Nevertheless, university staff units and groups in such a situation should have another network using system. For example, the program which is used by Financial Affairs shouldn't be allowed to use by Press Publication Department. Or a program and devices which are used by Information Technology Office shouldn't be able to reach by any other staff departments. That's why a structure that we are going to create should separate different users arrivals. By this way while providing security we project our network to be directed by making groups.

Another issue, we project that our academic and administrative staff are very dynamic for example there is going to be a presentation in the meeting room, a speaker wants to connect to network. For a sure wi-fi internet network should be healthy there. In the same way, wi-fi network should be used rapidly in the class by academic staff when he goes for lecturing. Nevertheless, when our staff change his area, he/she shouldn't code a password in each time. In our model the user to design all of our computers and wireless network, our system should recognize the credentials and authority should grant access based. Otherwise, each of our users when they want to access the internet constantly entering a user name and password if we want, we cannot talk about as user- friendly system may have different security vulnerabilities are also breed.

3.1 802.1X

We will use 802.1x to feed expectations and features of wi-fi network infrastructure which we like to provide for administrative and academic staff. Structure of 802.1x can be shortly defined as a port base identity control. It's a protocol which is used intensively in cabled network also used in wi-fi network. In the heart of this protocol authentication - authorization - accounting is provided to users. While confirming identity to prevent logins, the users who is logged in and to the rights of the users' systems sources is provided to consume. As it's said before existence of heterogeneous structure, makes safe authorization very important for designers.

To build this structure, user and in the name of including user computers information to system domain (active directory) structure should be spend to the life. Thank to this structure all users will have domain username and password. Thank to this username and password the user which identify computer would be safely and without (authentication) connected. A user who connected to wi-fi network would be used the network by side where his group belongs to. With this modeling a secure and administrative easiness would be spend on life.

In order to make working 802.1x structure devices like (AP, notebook, tablet, smartphone etc.)

The 802.1x structure :

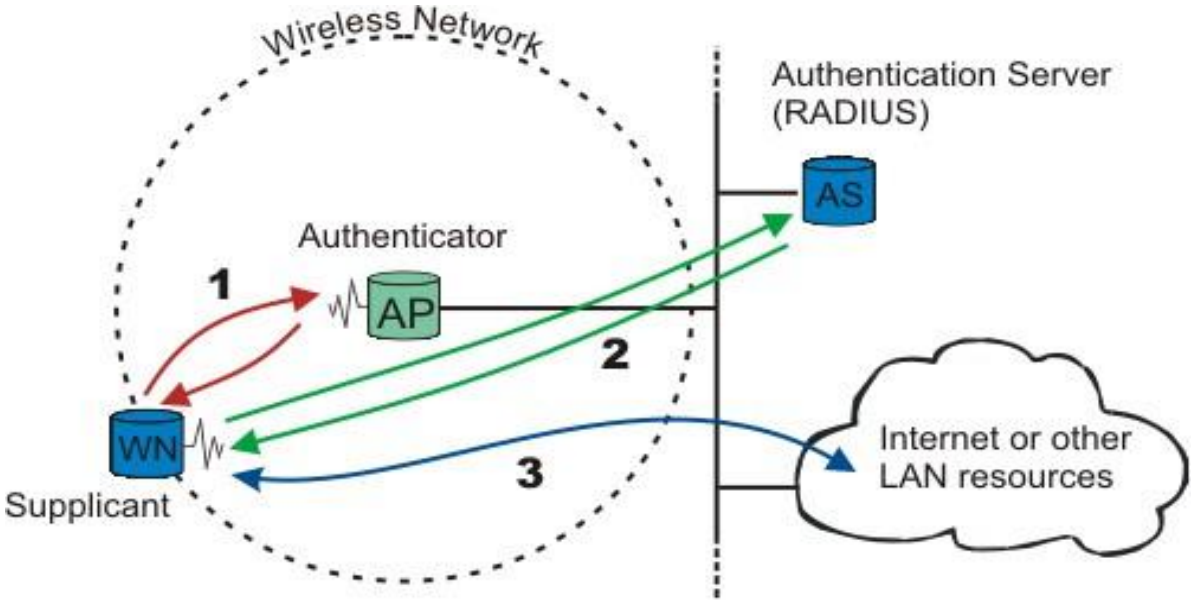


Figure 3.3 : 802.1x Technical Overview

In the 802.1x shape, there are three elements playing active role.[19]

Supplicant, represent those who would like to access to wifi network in the campus. Authenticator, the AP's that we will use in the campus (Access Point) represents. These are devices that users connect. This device works with RADIUS synchronous and will connect the user to our network after the encrypting identification correctly. This device will be switch as the same structure with cable network.

Authentication Server (RADIUS), will authenticate the credentials' structure represents. Thank to RADIUS decides which devices or which users to connect network. In the structure of campus network that we will create, working with RADIUS and AD (Active Directory) integratedly to identification service to work effectively.

As it's shown in the figure 3.3, 802.1x works like this:

1. When wireless client comes to the range of networking space, wi-fi network access point tests the wireless client.
2. Wireless client sends identity to a wireless access point. Access Point transmits this identity information to the RADIUS server.
3. RADIUS server, in order to verify the wireless client identification, asks for identity information. As a piece of this will, RADIUS server clarifies the kind of required information.
4. A wireless client would send this information's to RADIUS server.
5. RADIUS server verifies the information of wireless client. If identity is valid, RADIUS server sends an encrypted key identification confirmer to wi-fi Access Point.
6. Wireless Access Point, uses this authentication key for one point of all publisher stations session and too many points of wireless clients to transmit authentication key securely.

In the infrastructure of wi-fi network that we created in the campus, in AP's 802.1x after the setting steps which is put to many places, the domain computers of our users would connect to network securely and users-friendly mechanism on SSID 802.1x publisher.

3.2 HOTSPOT (CAPTIVE PORTAL)

Hotspot or Captive Portal system, which is called as a simple way to actually be defined as a web-based authentication. It's a system that nowadays, at many airports areas where is used intensively by people like shopping centers associated places system. Thanks to this system is used in some hotels that users' internet service through this home page from that page can pay the fee again.

The sample of hotspot login screen :

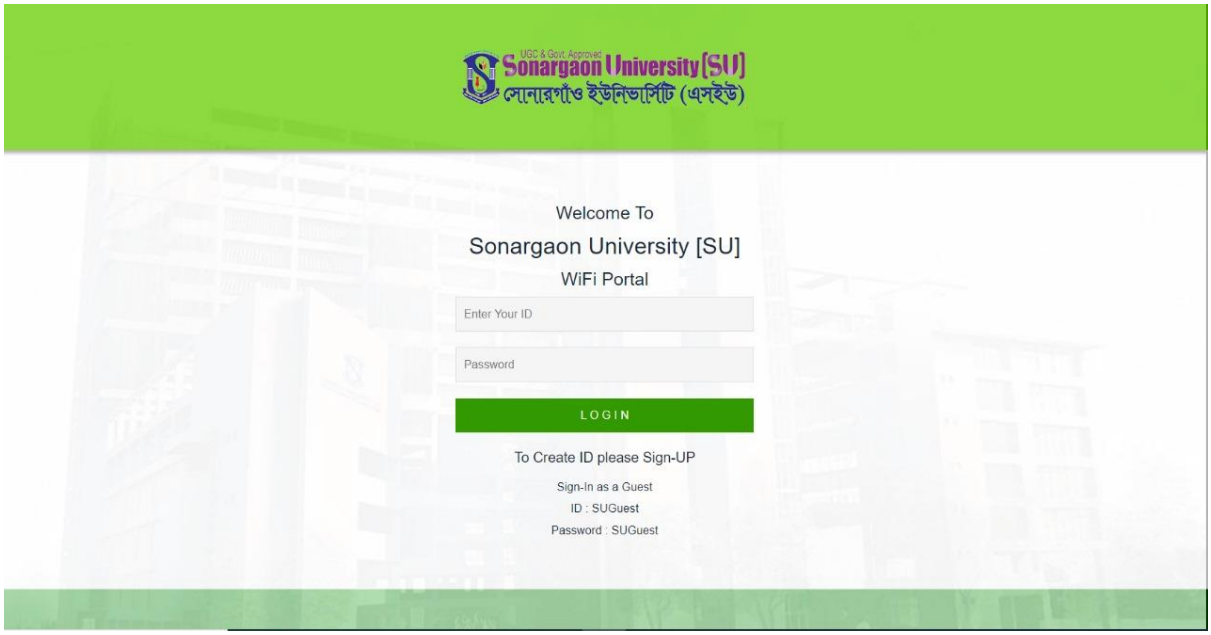


Figure 3.4 : Hotspot Login Page

Now almost all firewall devices supported by this system, we design the university campus wireless network for the use of students and guests will be evaluated in the areas we create. The system contains very easy working logic. We will tell on the created university campus network how system works. User, for connecting internet network will be directed identity control web page by which is broadcasting and set as a hotspot SSID when clicked.

On this web page there are spaces like username and password those should be coded by users as shown in the figure. Besides if a user’s code the username and password spaces correctly, connection permission will be provided by system, if not so the connection won't be provided. The model that we created user, will be asked to read and accept the service provider connection rules after user codes the username and password. The user who accepted the connection rules and codes necessary information correctly will have the right to connect network. These procedures are automatically done in the created structure. Each student eligible to study at university, Student Information System allocated to it for use in the identification of the username and password to login to the network at the same time will have earned the right. Thus, a student who wants to access the network, to engage in extra of

Information Technology Unit will be prevented. In addition, working in sync with the information system of this nature in the student information system that uses the username and password that you use to connect to the network automatically if you change the username and password will also be changed. This suggests the use of user-friendly structure.
The front working logic of hotspot is told in upper paragraph, how does this infrastructure work in the background? As we use for academic and administrative staff connecting network model 802.1x is similar to instructional system, instead of RADIUS there is identification service where Student Information System keeps the students and guest users identifications. Shortly it's works so:
When the user wants to access the network with using hotspot, the system enforces the user to communicate with Access Point. Then the authentication process for the database server is running. If the username and password is valid for database provider the user will be connected.

The schematic work logic:

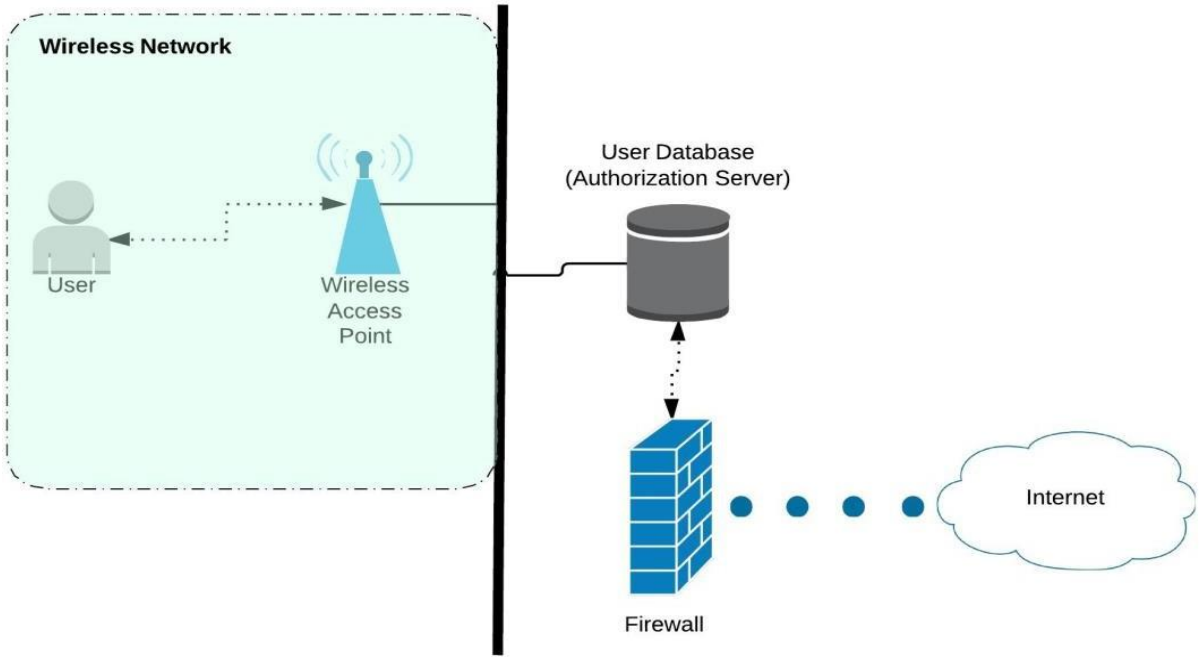


Figure 3.5 : Hotspot Technical Overview

One of the important feature of hotspot structure is that the hotspot doesn't need any settings by client. The devices which will be used in 802.1x structure are not expected to support the system and need some setting to be done in hotspot structure. This feature can be evaluated users-friendly branch in hotspot structure.

CHAPTER 4

PERFORMANCE TESTS

In this chapter, we provide performance measurement results to better understand the design decisions of the wireless network. We provide test cases to investigate the capacity, performance and the security of the designed network.

We have done all the measurements at the morning time when nobody was accessing the internet except the testers. There were ten users participating in the experiments. The tests were conducted in the university dormitory buildings.

The summary of the tests:

- We tested the impact of the capacity of backbone links in the campus network to the wireless internet access speeds.
- We tested our wireless network to provide a healthy simultaneous login performance for concurrent users.
- We tested the impact of the concurrent user downloads through the access points to other user download speeds.
- We tested the impact of the two different security methods on login performance of users.

The main purpose of the tests conducted in this chapter is to choose the correct access points, understand the impact of backbone links for end user performance and to clarify the impact of two different security methods on login performance.

4.1 DOWNLOAD SPEED TEST FOR WIRELESS LINKS

It is aimed in our measurement to explain the difference among the performance effects of the variation of two different locations infrastructure on the users who use our network in these locations.

In this context, while one of our dormitory buildings were connected with 10 Gb fiber infrastructure to the center switch, the other dormitory building was connected with 1 Gb fiber infrastructure to the center switch. After that, we simultaneously started two downloading process in the test with the same AP model, the same distance, same computer, same browser, and of course the same download link was used in two different locations.

The settings of the network :

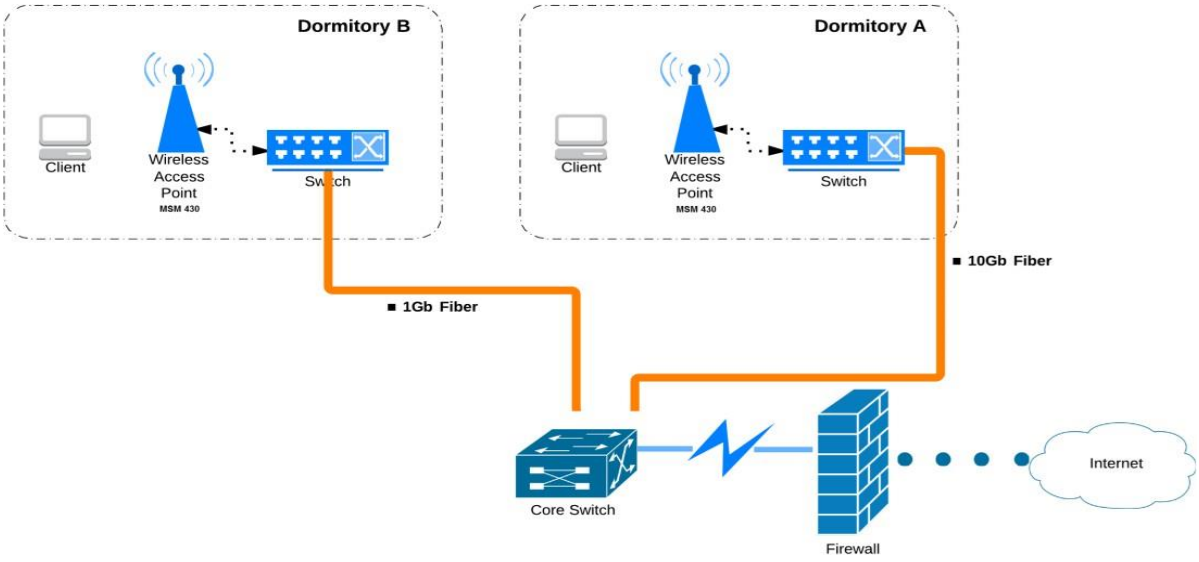


Figure 4.1 : Fiber Infrastructure Links Between Core Switch and Dormitories

While a user who connects to center switch with a 10 Gb fiber infrastructure to a file which has 350 MB, he/she can download in 49 minutes by 120KB/s, the other user who connects the same center switch with a 1 Gb fiber infrastructure he/she can download in 58 minutes by 100KB/s download speed.

In our downloading process, we have observed that the download speed of our dormitory building which has 10 Gb fiber infrastructure is approximately 20% higher than the other dormitory connected with 1Gb module to the center switch.

According to the measurement, the average of the download performance changed around 20 % by using the same Access Point models in our systems which are connected to the center switch by difference of 10 Gb and 1 Gb fiber infrastructure. And we can say that, in a dormitory building which used a lower fiber infrastructure, the download is lower than a dormitory building in which used a higher fiber infrastructure. And this difference cause of waste time. This time is around ten minutes.

Test results :

	Download Speed (Average)	Download Time (Average)
Dormitory A (10Gb Fiber)	120KB/s	49min
Dormitory B (1Gb Fiber)	100KB/s	58min

Table 4.1 : Download Results of Dormitories

4.2 PERFORMANCE TESTS OF LOGIN PAGES

In our tests we measure the capacity, the login page meeting-time were tested simultaneously and in the intensive-using of the Internet. According to our structure we try to occur, one of our students wanting to access the internet will be redirected to a page (as the welcome page) that he or she can enter by using the default user name and password when he or she wants to connect to the network.

In this study, we are looking for answers to questions such as how fast does this redirect page's arrival speed have in the intensive-use of the Internet and how much time are students waiting in case of simultaneous access?

Our aim in this measurement is to make easy the simultaneous access, especially in the intensive-use of the internet. It means that we try to make our system strong and enough to the users' needs and to make minimum delaying of the login page.

In this context, we use two different AP-models (MSM430 and MSM410). While AP MSM410 has 3 pieces broadcasting antenna and the wireless transmission speed max 54Mbit/s, AP MSM430 has the 6 pieces broadcasting antenna and its wireless transmission speed max 300 Mbit/s at level.

The comparative table of the Access Points which are used in testing period :

	Transmission Speed	Antenna
Access Point MSM410	54Mbit/s	3
Access Point MSM430	300Mbit/s	6

Table 4.2 : Comparison of Access Points

We have used the dormitory buildings connected with 1 Gb fiber infrastructure to the center switch in our tests we have done with same computer, browser and at equal distances from Aps.

The form :.

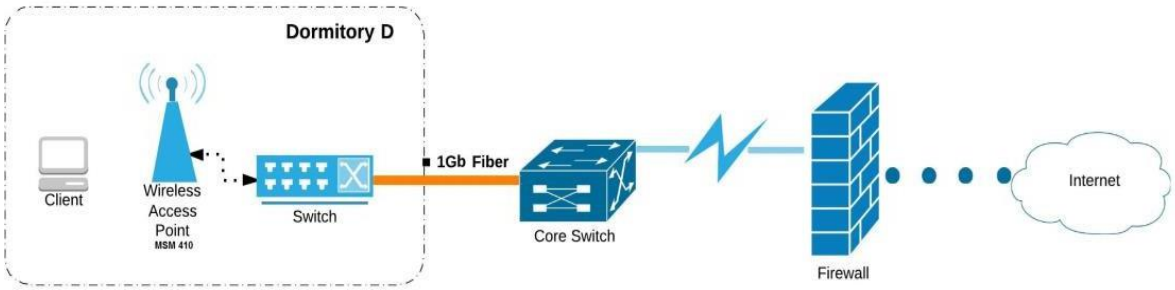


Figure 4.2 : Dormitory D and Core Switch Connection

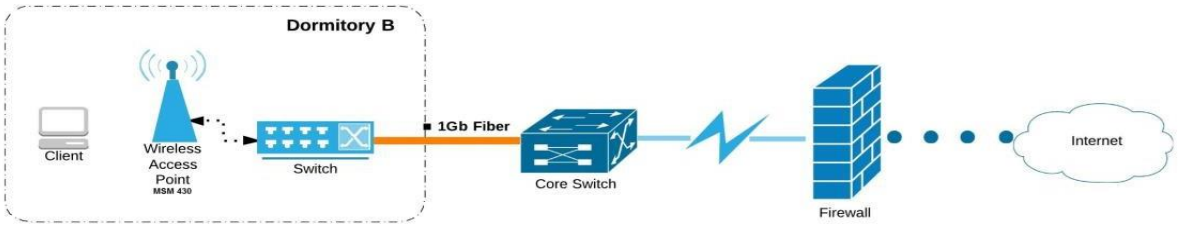


Figure 4.3 : Dormitory B and Core Switch Connection

When two clients want to access the internet simultaneously, there is no any loss in the login page meeting-time. While the time loss of the login page meeting-time is near half a second when four clients want to access the internet simultaneously, in case there are five people this time-loss is increasing up to 1 second.

CHAPTER 5

CONCLUSION

In our thesis, university or equivalent sized campus network infrastructure for a wireless network was designed. The standards used in wireless networks and wireless security solutions were investigated. In the light of this information and as a result of the tests conducted, we have designed our wireless network.

We have seen that the design and the healthy operation of a wireless network for university campuses with various kinds of users is not an easy matter. Many security measures need to be taken into account. In addition, the performance of the wireless system needs to be monitored continually.

In the introduction chapter, we have determined five main criteria for the design of a wireless internet infrastructure in a university campus. In this section, we explain the design decisions we have made and the conclusions we have obtained for each criterion.

Security

Some wireless network systems authorize users to login the wireless network based on their MAC addresses of wireless cards. This poses a serious security threat, since MAC addresses of wireless cards can be copied to other machines. Malicious users may copy the MAC addresses of valid users and join the wireless network by impersonating them. Therefore, MAC address-based security system is not used in our design. We construct username and passwords for each user and they login by using their username and passwords.

Addition of new access points to the wireless network is managed carefully. Uncontrolled access points may login unauthorized users to the wireless network and man-in-the-middle attacks may be performed. Therefore, each access point is added by the permit of network admin people. A trusted link is established between the access points and the switches by operating the relevant ports of the switches in the trusted mode. Moreover, a separate VLAN is constructed for access points.

It is very important to prevent the sniffing of unauthorized users the packages that are transmitted between the user machine and the access points. To achieve this, the client tunnel security feature of wireless controller is activated. This is performed for students and guests. For wireless connections of staff, WPA security method of 802.1x is used.

Capacity

The placement of access points is very important to cover all users in various places around the campus. Particularly the placement of access points in crowded areas is critical. We monitor the load of the access points and introduce new ones as needed. Our performance tests have shown that up to 10 concurrent users can connect through an access point watching a high-definition video stream. Therefore, at least 10 concurrent users can comfortable supported by an access point.

Performance

The university has a bandwidth of 200Mbps to the national backbone. This bandwidth needs to be divided among the various groups of users adequately. In addition, the bandwidth needs of users change with respect to the time of the day and the day of the week. During the work hours between 8.30am and 5.30pm for weekdays, 130Mbps of the bandwidth is dedicated to students and guests. Remaining 70Mbps of the bandwidth is dedicated to academic and administrative staff. Outside of working hours, 180Mbps of the bandwidth is dedicated to students and guests. Remaining 20Mbps of the bandwidth is dedicated to academic and administrative staff. These values are calculated by monitoring the average internet traffic of users. Outside of the working hours, majority of the bandwidth is used by students who are staying in the dormitories on the campus. In addition, some heavy users may starve others of the bandwidth. To prevent this, the bandwidth of students and guests are reduced to 1Mbps after they had downloaded 250MB of daily data. On the other hand, there is no bandwidth reduction for academic and administrative staff. So far, there was no such need.

In the performance tests we have conducted, we have seen that the selection of the access point devices and the capacity of the fiber channels on the campus are very important. We have observed that the access points with 300Mbps bandwidth provide approximately 25% more capacity compared to the access points with 54Mbps bandwidth. In addition, providing a 10Gbps fiber channel capacity to the main switch of the campus increases the end user download capacity around 20% compared to the 1Gbps fiber channel.

User-friendliness

All users are provided with a single sign on capability. All students have a single username-password to access various information services provided by the university. They use the same credentials to access the wireless network, student information systems and Moodle learning management system. When student's login to the wireless network, their connection stays active for 24 hours. They don't need to re-login during this period of time. Furthermore, academic and administrative staffs do not require entering a username and password to access the wireless network, since 802.1x authentication system. In addition, there is no limit on the number of devices a user can use to connect to the wireless network.

Manageability

MAC address-based authentication is not selected in our wireless network system, since it is difficult for both users and administrators to collect and manage the MAC addresses. When using MAC address-based solutions, students go to the IT departments to register their wireless devices. This puts an extra load on both the admin people and the students. With our current design, students only need to know their username and passwords.

There are approximately 200 access points in our campus. It is very important to centrally monitor and manage them. We use an HP Access Controller to monitor and remotely manage the access points.

We use Active Directory service to authenticate and authorize the users. We manage and monitor the users with this service. This service lets us to identify the connected users and diagnose the possible problems.

REFERENCE

[1] Llamas, R., R. Reith, and M. Shirer. "Worldwide smartphone shipments top one billion units for the first time." (2014).

[2] Ergen, Serdar. Design of a wireless network infrastructure for a university campus. MS thesis. Fen Bilimleri Enstitüsü, 2014.

[3] Hornbeck, E. (2017). We Know Not Where We Go: Protecting Digital Privacy in New York City's Municipal Wi-Fi Network. Fordham Urb. LJ, 45, 699.

[4] Spacey, Rachel, et al. "Filtering wireless (Wi-Fi) Internet access in public places." Journal of Librarianship and Information Science 49.1 (2017): 15-25.

[5] Aly, Heba, and Moustafa Youssef. "An analysis of device-free and device-based WiFi-localization systems." International Journal of Ambient Computing and Intelligence (IJACI) 6.1 (2014): 1-19.

[6] Hornbeck, Eric. "We Know Not Where We Go: Protecting Digital Privacy in New York City's Municipal Wi-Fi Network." Fordham Urb. LJ 45 (2017): 699. 6

[7] Patel, Krupa C., and Priyanka Sharma. "A Review paper on pfsense-an Open source firewall introducing with different capabilities & customization." IJARIIE 3 (2017): 2395-4396.

[8] Banerji, Sourangsu, and Rahul Singha Chowdhury. "On IEEE 802.11: wireless LAN technology." arXiv preprint arXiv:1307.2661 (2013).

[9] Frodigh, Magnus, et al. "Future-generation wireless networks." IEEE Personal Communications 8.5 (2001): 10-17.

[10] Medepalli, Kamesh, et al. "Voice capacity of IEEE 802.11 b, 802.11 a and 802.11 g wireless LANs." IEEE Global Telecommunications Conference, 2004. GLOBECOM'04.. Vol. 3. IEEE, 2004.

[11] Deshpande, Suyog D. "Software implementation of IEEE 802.11 b wireless LAN standard." Proceeding of the SDR 04 Technical Conference and Product Exposition. 2004.

[12] Vassis, Dimitris, et al. "The IEEE 802.11 g standard for high data rate WLANs." IEEE network 19.3 (2005): 21-26.

[13] Perahia, Eldad. "IEEE 802.11 n development: history, process, and technology." IEEE Communications Magazine 46.7 (2008): 48-55.

[14] Roshan, Pejman, and Jonathan Leary. 802.11 Wireless LAN fundamentals. Cisco press, 2004.

[15] Helal, Sumi, et al. "An architecture for wireless LAN/WAN integration." 2000 IEEE Wireless Communications and Networking Conference. Conference Record (Cat. No. 00TH8540). Vol. 3. IEEE, 2000.

[16] Koripi, Malyadri. "A review on secure communications and wireless personalarea networks (WPAN)." Wutan Huatan Jisuan Jishu 17 (2021).

[17] Wong, Luis Carlos. "An overview of 802.11 wireless network security standards & mechanisms." Published by SANS Institute InfoSec Reading Room (2004).

[18] Lashkari, Arash Habibi, Farnaz Towhidi, and Raheleh Sadat Hosseini. "Wired equivalent privacy (WEP)." 2009 International Conference on Future Computer and Communication. IEEE, 2009.

[19] Edney, Jon, and William A. Arbaugh. Real 802.11 security: Wi-Fi protected access and 802.11 i. Addison-Wesley Professional, 2004.

APPENDIX

 # Configure IP address for LAN and WAN interfaces

```
/ip address
add address=172.16.0.1/24 comment=LAN disabled=no interface=ether1 network=172.16.0.0
add address=192.168.2.1/24 comment=WAN disabled=no interface=ether2 network=192.168.2.0
```

 # ADD IP pool for hotspot users

```
/ip pool
add name=hs-pool-1 ranges=172.16.0.10-172.16.0.255
```

 # Add GOOGLE DNS for resolving

```
/ip dns
set allow-remote-requests=yes cache-max-ttl=1w cache-size=10000KiB max-udp-packet-size=512 servers=8.8.8.8
```

 # Add DHCP Server

```
/ip dhcp-server
add address-pool=hs-pool-1 authoritative=after-2sec-delay bootp-support=static disabled=no interface=ether1 lease-time=1h name=dhcp1

/ip dhcp-server config set store-leases-disk=5m

/ip dhcp-server network add address=172.16.0.0/24 comment="hotspot network" gateway=172.16.0.1
```

 # Add HOTSPOT profile

```
/ip hotspot profile

set default dns-name="" hotspot-address=0.0.0.0 html-directory=hotspot http-cookie-lifetime=3d http-proxy=0.0.0.0:0 login-by=cookie,http-chap name=default rate-limit="" smtp-server=0.0.0.0 split-user-domain=no use-radius=no

add dns-name=login.aacable.net hotspot-address=172.16.0.1 html-directory=hotspot http-cookie-lifetime=1d http-proxy=0.0.0.0:0 login-by=cookie,http-chap name=hsprof1 rate-limit="" smtp-server=0.0.0.0 split-user-domain=no use-radius=no

/ip hotspot
add address-pool=hs-pool-1 addresses-per-mac=2 disabled=no idle-timeout=5m interface=ether1 keepalive-timeout=none name=hotspot1 profile=hsprof1
```

 # Add HOTSPOT User Profile like 256k and 512k

/ip hotspot user profile set default idle-timeout=none keepalive-timeout=2m name=default shared-users=1 status-autorefresh=1m transparent-proxy=no add address-pool=hs-pool-1 advertise=no idle-timeout=none keepalive-timeout=2m name="512k Limit" open-status-page=always rate-limit=512k/512k shared-users=1 status-autorefresh=1m transparent-proxy=yes add address-pool=hs-pool-1 advertise=no idle-timeout=none keepalive-timeout=2m name="256k Limit" open-status-page=always rate-limit=256k/256k shared-users=1 status-autorefresh=1m transparent-proxy=yes /ip hotspot service-port set ftp disabled=yes ports=21 /ip hotspot walled-garden ip add action=accept disabled=no dst-address=172.16.0.1 /ip hotspot set numbers=hotspot1 address-pool=none /ip firewall nat add action=masquerade chain=srcnat disabled=no /ip hotspot user add disabled=no name=admin password=123 profile=default add disabled=no name=zaib password=test profile="512k Limit" server=hotspot1 add disabled=no name=test-256k password=test profile="256k Limit" server=hotspot1 /ip route add disabled=no distance=1 dst-address=0.0.0.0/0 gateway=192.168.2.2 scope=30 target-scope=10