

## Analysis and Design a Secure Wireless Campus Network for ABC University in Libya

[www.doi.org/10.62341/yads2010](http://www.doi.org/10.62341/yads2010)

Yonos Elmahdi Qnedi

Collage of Education Kikla, University of Gharyan  
Qnedi42@gmail.com

### Abstract

This research presents the wireless university campus network and discusses about the strengths and weaknesses of Design a secure wireless campus networks for ABC University in Libya, and about the costs and advantages of different vendor solutions. Wireless offers mobility and is available in locations where a wired outlet doesn't exist. The disadvantages of wireless include some minor interference problems and a quickly evolving and competitive group of standards. The purpose of the research is designing and implementing a secure campus network for Libyan university based on Cisco equipments. Moreover, the research can provide practical experience in network design, configuration, and security for helping organizations and institutions protect their network resources and data. Two end products or deliverables will result from the research: the first is a new architectural design for an efficient and advanced WLAN-friendly network to ensure the high performance of the data transaction process and ensure high availability of data transmissions. The second product is a report for network administrators or network architecture to guide users towards the achievement of WLAN-friendly by utilising advanced networking tools and technologies.

**Keywords:** - Campus network; Wireless Mesh Network; wireless network; Encryption; Cisco equipment; security.

## تحليل وتصميم شبكة محلية لاسلكية آمنة للحرم الجامعي في الجامعات الليبية

يونس المهدي مسعود قنيدي

جامعة غريان / كلية التربية ككلة / قسم الحاسب الآلي

Qnedi42@gmail.com

### الملخص

يقدم هذا البحث مقترح لتصميم شبكة لاسلكية للحرم الجامعي ويناقش نقاط القوة والضعف في تصميم شبكات الحرم الجامعي اللاسلكية الآمنة للجامعات في ليبيا، وحول تكاليف ومزايا الشركات المتنافسة في هذا المجال. الغرض من البحث هو تصميم وتنفيذ شبكة محلية لاسلكية آمنة للحرم الجامعي في الجامعات الليبية بالاعتماد على معدات شركة سيسكو كونها شركة عالمية رائدة في مجال تقنية المعلومات والشبكات. علاوة على ذلك، يمكن أن يوفر البحث خبرة عملية في تصميم الشبكات وتكوينها وأمنها لمساعدة المؤسسات على حماية موارد شبكتها وبياناتها. سينتج عن البحث منتج أو مخرجان نهائيان: الأول هو تصميم معماري جديد لشبكة محلية لاسلكية فعالة ومتقدمة لضمان الأداء العالي لعملية لعمليات نقل البيانات. المنتج الثاني عبارة عن تقرير لمسؤولي الشبكات أو بنية الشبكة لتوجيه المستخدمين نحو تحقيق التوافق مع شبكة محلية لاسلكية من خلال استخدام أدوات وتقنيات الشبكات المتقدمة.

**الكلمات المفتاحية:** شبكة الجامعة، شبكة لاسلكية، التشفير، معدات سيسكو، الأمن.

### Introduction:

Designing a secure wireless campus networks is an essential task for any organization or institution that wants to protect its network resources and data. A secure campus network provides a safe and reliable environment for users to access network services and resources while maintaining confidentiality, integrity, and availability of the network. By designing and implementing a secure campus network based on Cisco equipments, you can help

organizations and institutions protect their network resources and data from unauthorized access, data theft, and network attacks. The research will also provide an opportunity to learn and gain practical experience in using advanced security technologies such as firewalls and access control mechanisms. Moreover, the project will provide an opportunity to gain experience in network design, configuration, and troubleshooting. The research methodology involves two main research techniques: The literature review could be conducted to identify existing studies, research, and best practices on secure campus network design, Cisco equipments. This review could help provide the foundation for the study and identify potential areas of interest and gaps in knowledge, and Case studies of organizations that have implemented similar secure campus networks could be undertaken to understand the practical implications of implementing a secure network based on Cisco equipments.

### **Building constriction**

Actual implementation on this research which is designing a secure wireless campus network for the ABC University in Libya, we need to understand the whole campus architecture which includes building dimensions, structure, number of floors in each building, the distance which each building apart from each other, and IT infrastructure that will be used in this research. Most universities and colleges are constructed with concrete brick and sheet rock, while materials especially concrete can severely interfere with WLAN signals whereas sheetrock can only block a small portion of a signal, which means this kind of construction is WLAN-friendly. In older buildings the problems dramatically increases, where more Access Points (APs) might be required for WLAN deployment (Baker, 2004).

In older constructions, the woods wall are mostly used which reinforced chicken wire-like materials can caused significant interference and can create dead zones or at least disrupt the WLAN's Wi-Fi signals. Similarly, rebar-reinforced concrete can also do the same disruption. The materials used in construction and

the angle of antennae both can affect heavily on this research. The most common obstruction materials for Wi-Fi signals are plasterboard walls, concrete walls, glass with metal frames, cinder-block walls, metal doors in brick walls and steel-mesh reinforcement walls (Stakeholder Technology Branch, 2007). Therefore, a detailed site survey is very crucial in order to deploy WLAN research in ABC University in Libya. We have 14 buildings at University campus where as shown in (figure 1) we need to plan wireless network solution for 13 buildings where building number 1 (i.e. Car Park with 2 floors) is not included into this plan. Other 13 buildings are assumed to be not in very far distance from each other.

There are buildings as shown in (Table 1) which have up to 3 floors such as Female Hostel 1, Female Hostel 2, Female Hostel 3, and Faculty of science, Faculty of IT/Business, and Faculty of Engineering. The Main Building consists of 5 floors. All other are only a single floor building. We assumed that these buildings are not very far from each other and the distance between each building is not more than 150 meters. However, few buildings are very close to each other like Cafeteria is just 90 meter away from Main Building and Outdoor Dining is just 50 meters from Cafeteria building. Similarly, Female Hostel, Lecture Block 1 and 2 are within 100 meters far from each other as shown in Campus map below. We also assumed there are total 1000 users in this University who will use the services that include students, staff and faculty, and managements. Further, we assume that the buildings are not very old.

Therefore, necessary equipments and appropriate topology is required for the campus network design with these elements: IP address schema, IP address management, secure wireless access points, internet sharing, services and features need to be considered. In our case, we also assumed that the most of these elements are finalized such as IP address management, and IP address schema.



Figure 1. ABC University Libya MAP

**Table. 1: Building Details at ABC University Libya**

BUILDING NUMBER	
1	Car Park ( 2 Floors )
2	Main Building ( 5 Floors )
3	Female Hostel 1 ( 3 Floors)
4	Female Hostel 2 ( 3 Floors)
5	Female Hostel 3 ( 3 Floors)
6	Lecture Block 1
7	Lecture Block 2
8	Cafeteria
9	Multi Purpose Hall
10	Faculty of science (3 Floors)
11	Lecture Theatre
12	Faculty of Engineering (3 Floors)
13	Faculty of IT & Business (3 Floors)
14	Lecture Block 3

Following are the objects that we found during our initial site survey as assumed:

The walls are constructed with concrete and Sheetrock's, depending on the location and strength required. There are made of materials such as metal. The strength of students are increasing every years and this will also affect signals when the bell rings and a wave of bodies flood the corridors, this time the chances are the

signals will loss. Furniture at campus is primarily made of metals. Natural Elements: Such as trees, water, etc. Wood floors-to-floor interaction can cause AP's channel interface (i.e. Three Dimensionally). Mostly the classroom doors are closed and that affects the AP's channel interference or reduces the speed because of wood, walls, and metal used in constructions. The glasses are coated with a metallic film, which can cause the signal strength.

### **Designing a secure campus network**

Designing a secure campus network for ABC University in Libya, there are assumed 1000 users at the campus and accommodations (i.e. Hostel) and most of the buildings have the lobby which is 200 square foot (sqft) open space where wireless access points to the network is required. Only authorized person who have valid credential can only access these services. In this design, we have considered main deployment ideas to provide the secure wireless networks through wired LAN which is a conventional method and costly as well where will need the cost of cabling in a wireless LAN which can be costly when it comes to entire ABC Libyan University with 13 buildings. The second option is to use a new approach, which is Wireless Mesh Networking to span the campus internet problem. In a Wireless Mesh Network deployed several routers and each router is equipped with 802.11b/g. These routers typically placed in a secure area over the building roof and use of a high-gain antenna in order to provide long distance routes (e.g. hundreds meter or more) between routers. It can be formed a bridge to a local area network through wired Ethernet LAN or a separate 802.11 Access Points.

User in the university can connect their laptop, mobile phones, desktops (e.g. 802.11 enabled) which will have nearest access to these access points. The mesh routers provide a wireless distribution network between the separate LANs as well. As, discussed earlier that wired network can cost huge money in term of cabling the whole University, on other hand mesh solution is low cost compare to wired network. Further, it is easy to deploy and flexible for future enhancement if more routers required to expand the coverage to the car park building in future. Therefore, I

will recommend a wireless mesh solution for ABC University Libyan, which will provide coverage to the buildings. For this reason, we will require 13 routers, 13 switches and 50 access points to provide approximately 1000 users at campus.

In our proposed design for ABC University in Libya, 13 mesh routers will be placed on each building that are mentioned in diagram ( figure 1) and each router will consist of an inexpensive embedded PC (e.g. Runs an embedded Linux Distribution) with modest processing capacity and memory. Further, an 802.11g interface with high-gain Omni-directional antenna will be placed. This design will be faster and flexible as discussed earlier, in case of one router failure will not cause the failure of entire network but only the effected routers and their access points that directly connected. There will be 802.11b/g access points connected with these routers via Ethernet Switches that will provide end-users (e.g. Student, Staff and faculty) connectivity to their laptop, Smartphone's, or desktop PC equipped with wireless interface cards. In this design, 3-4 access points will be enough however, for main building which are 5 floors will require 3-4 access points. In future, access points can be increased if it is required so.

We also found in our initial site survey that there are a large number of 802.11 based wireless networks already active near the ABC University in Libya, which raises challenges for interference and channel sharing. To minimize the channel overlap and interference, Access Points cells should be designed in the way that use different channels (Stakeholder Technology Branch, 2007). 802.11b and 802.11g using channels 1, 6 and 11 are limit, therefore, the below alternating pattern will be follow in a single story building such as Lecture Block 1, Lecture Block 2, Outdoor Dining, Cafeteria, Multi-Purpose Hall, and Lecture Theatre.

With multi storied buildings will pose greater problems for interference in channels therefore, a honeycomb fashion channels design will be implemented as shown in (figure 2). The honeycomb pattern is seamless and with no holes and the same channels are well separated providing isolation from interference

and unlimited scalability in design (Stakeholder Technology Branch, 2007).

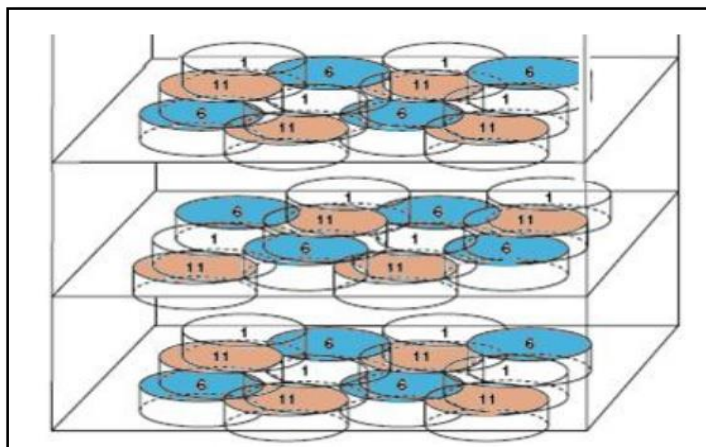


Figure 2. Channel Re-use  
Source: (Stakeholder Technology Branch, 2007)

### Possible security issues and recommended solutions

Wireless Mesh Network (WMN), which is proposed for ABC University in Libya, is different from the traditional wireless networks, which are not relying on the fixed network infrastructure. However, hosts in this design rely on each other to keep the network connected and wireless internet service providers are choosing to provide WMNs internet connectivity that allows fast, easy and cost effective network solutions. With every network, design there are security issues also presents their threats and attacks. In first stage of this section will focus on the main threats, challenges that WMN design possibly have, and in the second section we will discuss how to tackle these threats by designing security proof environment.

As WMNs become increasingly popular wireless networking technology because of its nature which is good deployment for campus area network, home networking environment, and neighborhood networking. However, the nature of the connectivity and broadcast nature in the wireless medium creates several



security issues which can be exploited by external and internal attackers causing damage to the network performance and disruption of services (Weber and Bahadur, 2013). The nature of wireless networks attract most of the attackers because the easy availability of the signals that can be accessed from parking Lot, near building, inside building and similar areas near to the device. The design flaws in the security mechanisms of the standards 802.11 also attract many potential attackers. These attacks can enable intruders to enter into ABC University Libya wireless network and cause damage to the information.

### **Authentication and tunneling technologies**

Most of the wireless network is using some kind of security setting in order to avoid attacks from intruders. These security mechanisms are define as authentication, encryption, tunneling technologies (like VPN – Virtual Private Network) and many more. These options are embedded inside the wireless network devices such us in our case routers where we have to configure manually these settings in order to perform security checks. There must be a carefully read these options because if one could not configure properly the security level which is expected will not achieve properly.

Authentication is used by wireless devices to know exactly who is accessing the information and it is used by users when they want to connect with the wireless device or access point to use internet. In authentication a user need to provide their credential in order to authorize to connect with the services that wireless network is providing. If the credential such as password and user name is not correct the authentication will fail when deploying a WLAN network it is important to deploy the security as well (Snajoli and Singh, 2013). There are different methods but authentication and authorization are very common for security purposes. The aim of these security measures are to keep protects the network from unauthorized people to access the university important data. There are three major methods of authentications that include open

authentication, shared authentication and EAP (Extensible Authentication Protocols) authentication.

In open authentication method is very simple where other devices who want to connect with the network just required Service-Set Identifier (SSID) to connect and as long as devices know the SSID they are allowed to connect with the network. This type of authentication method is not recommended in the university environment because the data need to be secure and any other person or attacker can take advantages from this technique and can connect their device to the university wireless network. The other authentication method is shared authentication in which used the shared key (Pre-Shared Key – PSK) for the connection purposes. This kind of authentication process is commonly used in small and medium sized enterprises (SMEs) or at individual level. This kind of authentication required both side to match the key and if these keys match they will connected with each other which is better security measure than open authentication (Dworkin, 2007). The third method is Extensible Authentication Protocols (EAP) which is the most common used for more secure environment such as university level or enterprise level. The EAP method utilizes the authentication server which used several credential methods to perform checks.

WLAN Encryption is very important along with the authentication methods in order to deployment of secure wireless network at ABC University in Libya. There are different encryptions methods that wireless network devices such as in our case router used for this purpose. These encryption methods include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and Wi-Fi Protected Access 2 (WPA2) (Wilkins, 2011). The first and widely used early encryption method is Wired Equivalent Privacy well known as WEP algorithm for security which utilizes RC4 for encryption and has been depreciated because it compromised on different security keys issues. In response to these vulnerabilities found other encryption method which is called Wi-Fi Protected Access (WPA) which utilizes Temporal Key Integrity Protocol (TKIP) and which utilizes the dynamic keys difference from WEP

and RC4 for encryption (Wilkins, 2011). This protocol (TKIP) was widely used with WPA until further security vulnerabilities were discovered. In that response of WPA/TKIP security vulnerabilities the new IEEE 802.11i standard was introduced with WPA2 which replaced TKIP with Counter Mode with Chopper Block Chaining Message Authentication Code Protocol (CCMP) based on Advanced Encryption Standard (AES). It is now common these days for WPA2 encryption to be known as AES.

ABC University in Libya required reliable, secure and fast way to share their wireless network to their students, staff and faculty. The one popular technology which can provide these three elements for ABC University goals is a Virtual Private Network (VPN) which is a private network that uses public network (e.g. Internet) to connect remote sites or networks together (Crawford, 2014). The VPN uses virtual connection routed through Internet or routers to share information across networks in encrypted data. In traditional methods, the connection between different sites or buildings were made through leased line such as ISDN (Integrated Services Digital Network, 128 Kbps) which provided by telecommunications company. However, today the more ISPs (Internet Service Providers) are providing more fast and robust way to increase the speed and reliability of Internet. This also introduced the new technique which is secure, fast and reliable is VPN. The main purpose of the VPN's is to provide secure and reliable private connection between different hosts which main purpose is to share the information between different hosts securely (How stuff works, 2014). There are two main types of VPNs includes Remote-access VPN as shown in (figure 3) and Site-to-site VPN as shown in (figure 4) below. A remote-access VPN allow individual uses to establish connection with remote computer networks which also called VPDN (Virtual Private Dial-up network). The main benefit of using Remote-access VPN is to connect entire remote office securely with hundreds of employees.

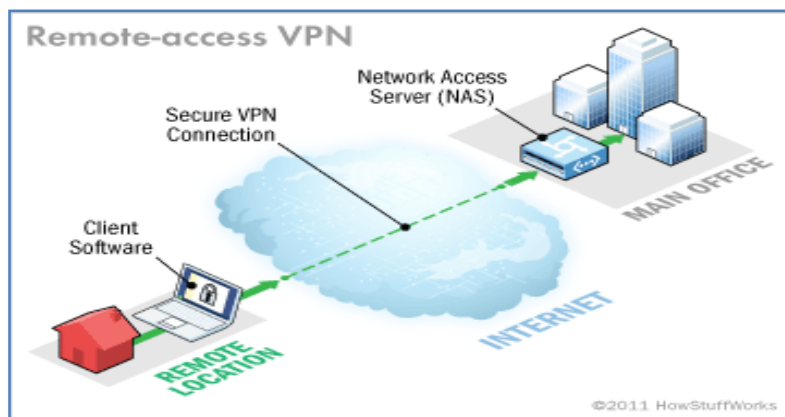


Figure 3. Remote-Access VPN Source: (howstuffworks.com, 2014)

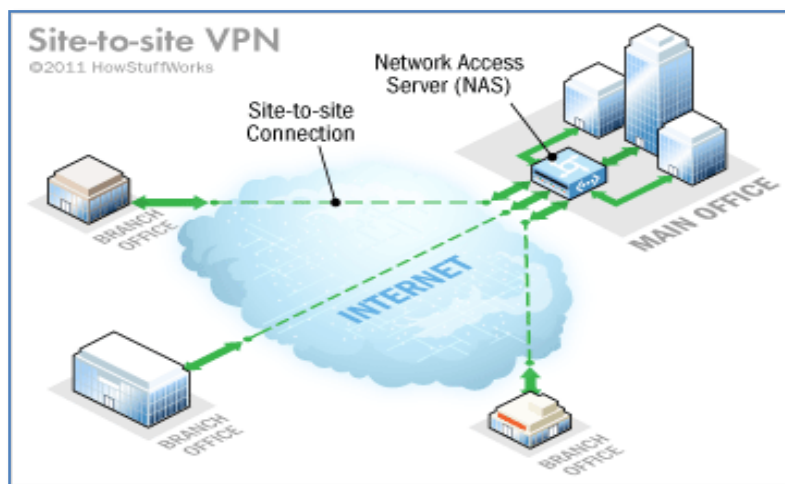


Figure 4. Site-To-Site VPN Source: (howstuffworks.com, 2014)

On other hand site-to-site VPN allows offices, branches or campuses network connect with each other through secure lines. This will allow University to distribute its wireless networks from one building to another building securely and also available to all users at university campus. Those who are not allowed to connect such as Building number 1 Car Parking with 2 floors cannot make

connection with these VPN connections. There are two main types of site-to-site VPNs such as Intranet-based, and extranet-based. In Intranet based connection, the university has one or more networks to connect with single private network. It will create an intranet VPN to connect separate LAN to a single WAN. Extranet-based can build an extranet VPN to connect with multiple LANs.

### **Design a very secure wireless network solution**

Finally after reading and searching about the different wireless network solutions and security threats that are associated with these kinds of networks, proposed networks solutions in figure 5 below. The reason for this proposed solution is the security and availability. The network consists of 13 mesh routers (i.e. Matrix Kit Mark II 802.11 enabled embedded PC) for thirteen different buildings shown in (figure 1) above where building 1 car parking with 2 floors is not selected for network availability. The range will also cover this area but people there would not be able to connect with the nearest access points because of the WPA2 encryption to be known as AES. There will be around 34 access points (Cisco Aironet – 1131 A/B/G enabled) will be installed there around these buildings depending on the floors. For example at main building which consists of 5 floors there are 4 to 5 access points will be installed in order to provide high strength availability to the users. These access points will be directly connected with high quality Cisco Switches (i.e. Cisco Catalyst 2940 with minimum 8-ports).

The routers will be placed on each building at safe place and all access points will be provided near to the users access area where mostly users trying to connect with the wireless networks. Users of the university will connect with the wireless network via 802.11 networks either from their laptops, desktop (i.e. equipped with wireless interface) or Smartphone. The routing protocols in this case are implemented by the routers can highly robust to packet loss, congestion, interference and dynamically selecting optimal routing paths. Therefore, I will suggest different famous dynamic

routing protocols such as EIGRP (Enhanced Interior Gateway Routing Protocols), OSPF (Open Shortest Path first) protocol and EXT-based, However, EIGRP is a proprietary Cisco Protocol. In this case because the network is not very big where we have to define different areas (in case of OSPF), the better is EXT-based routing protocols which will count the path based on the expected transmission count of each packets that will ensure the correct path. This design will lead to decentralized network architecture which means a failure of a router will not affect the overall network functioning only those buildings which access points are directly connected with the failure router would effect. Further, this kind of network is flexible and scalable because in case in future if new building is build the new mesh router can be installed and connect in same way without re-engineering the whole network architecture. Table 2 describes the main hardware components of Cisco equipments.

**Table. 2: The main hardware components of Cisco equipments**







Devices	Description
	Mesh Routers, Matrix kit Mark II 802.11 enabled embedded PC.
	Access Points, Cisco Aironet (1131 A/B/G)
	Cisco Switches, Cisco Catalyst (2940 minimum 8-ports) Required for Access Points to communicate with Mesh routers.
	Laptops, that could be used at campus to connect with access points.
	Desktops with wireless card enabled, that could be used at campus to connect with access points.
	Smartphone's that could be used at campus to connect with access points.

Table 3 describes the number of access points, routers and switches that are needed to deploy at each building.

تم استلام الورقة بتاريخ: 2024/9/24 م وتم نشرها على الموقع بتاريخ: 2024/10/20 م

**Table 3. The number of access points, routers and switches**

Building	Description	Access Points	Routers	Switches
1	Car Park (2 floors)	none	none	None
2	Main Building (5 floors)	5	1	1
3	Female Hostel (3 floors)	3	1	1
4	Female Hostel (3 floors)	3	1	1
5	Female Hostel (3 floors)	3	1	1
6	Lecture Block 1	2	1	1
7	Lecture Block 2	2	1	1
8	Cafeteria	1	1	1
9	Multi-Purpose Hall	2	1	1
10	Faculty of Science (3Floors)	3	1	1
11	Lecture Theatre	2	1	1
12	Faculty of Engineering (3 floors)	3	1	1
13	Faculty of IT/Business (3 floors)	3	1	1
14	Lecture Block 3	2	1	1
<b>Total</b>		<b>34</b>	<b>13</b>	<b>13</b>

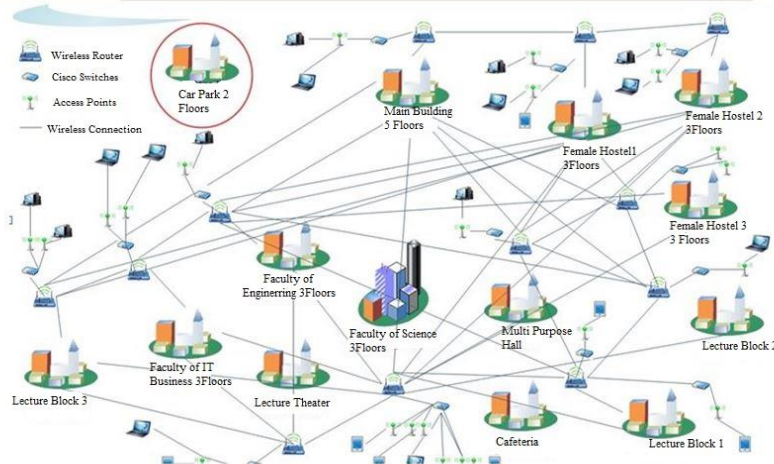


Figure 5. Proposed Mesh Network Diagram

### Detailed cost of implementing wireless solution

The deployment cost is estimated \$23,240 (According to prices in year 2022 ) and it will long two months to complete. This will required purchase of equipment for all 13 building excluding one building (i.e. Car Park – 2 floors). Further, charges are also included from managers and technicians who will involved in installations and configuration process.

Table 4 describes the price in dollar and in Libyan dinar for he used items.

**Table 4. The items prices in dollar and in Libyan dinar**

Items	Quantity	Unit Price	Total by Dollar	Total By Dinars	Description
Mesh Routers	13	\$125.00	\$1,625.00	7800 LYD	Matrix kit Mark II 802.11 enabled embedded PC.
Access Points	34	\$105.00	\$4200.00	20160 LYD	Cisco Aironet (1131 A/B/G)
Ethernet Switches	13	\$115.00	\$1,495.00	7176 LYD	Cisco Catalyst (2940 8-ports) Required for Access Points to communicate with Mesh routers.
Desktop Wireless Cards	50	\$25.00	\$1,250.00	6000 LYD	To enable desktop to connect with these access points.
Cat6 Ethernet Cabling	8000m	\$4500	\$4,500.00	21600 LYD	Required for in-building cabling the components.
Network Managers	3	\$800/month	\$4,800.00	23040 LYD	For network design and infrastructure review.
Technician	6	\$500/month	\$6,000.00	28800 LYD	Required for installation purposes.
<b>TOTAL</b>			<b>\$23,870.00</b>	<b>114,576L YD</b>	

### Encryption scheme

In today environment, encryption is an important part of the computing where you can secure the access to your personal computer and the data. It will keep the conversation secure and put



a mechanism which will keep the files in security mode. Encryption is the process which takes data and decode into such form which will not be readable or writeable from non-authorized user.

There are two main type of encryption scheme that are mainly used these are symmetric key and public key encryption. A symmetric key is using same key to encrypt and decrypt data which allow faster data transmission and less processing power then public key encryption techniques (Tschabitscher, 2013). However, there are few problems of using systematic key encryption techniques because you have to keep safe the key somewhere secure and also need to transfer the key safely to the other party where you need to establish the communication channel. On other hand public key encryption technique uses two keys a public and private key to establish their communication channel (Tschabitscher, 2013).



Figure 6. Two way communication Process

Source: (IFT, 2012)

Imagine you need to communicate through email with someone and there is a third person who needs to ease drop on your conversation as shown in (figure 6) above then if you are using public key encryption technique then other person need a public key which can be send and if even a third person get hand on to this key he/she could not use this key to crack the message unless he/she have another key which is private key. So, in this case for intruder it will be hard to crack the key even if he/she succeeded attaining public key as illustrate in figure 7.

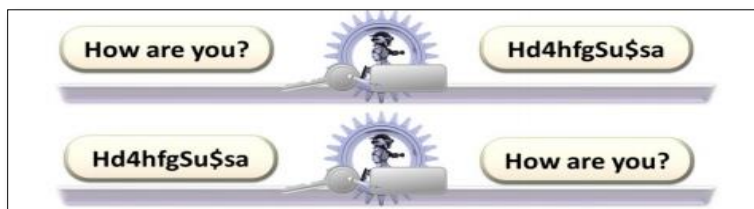


Figure 7. Symmetric Key encryption process  
Source: (IFT, 2012)

In this case when you send an email, your contents are open to everyone to read, like I will give you an example of postcard, everyone can read when they gets it in their hands. Now to keep data secure in your email you need to encrypt this process where you allow only recipient can be able to decipher the message while anybody else see as gibberish contents.

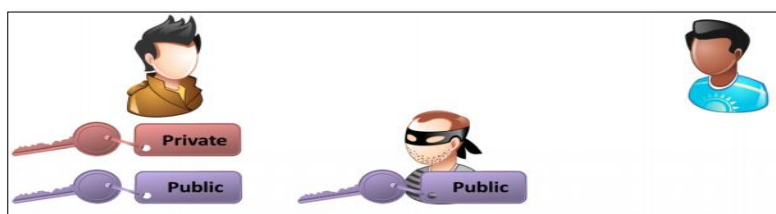


Figure 8. Public Key encryption process  
Source: (IFT, 2012)

Recommend using public key encryption method as shown in (figure 8) above which will keep your email content secure. The sender's encryption program will make sure the message delivered to authorize recipients without tempering to the original message. A third-party can produce a public key with recipient's name but to read the complete content of email they must require private key as well.

The most secure public key encrypted method for use is (PGP) Which is secured and trusted way of encrypting technology. Moreover, Mozilla's email program, Thunder bird with the

Enigmail extension the easiest tool to use, you also will need to download free GNUPGP software for windows.

### Results and discussion

The findings of this research conclude that there are various network designs in campus networking. However, there is a need to plan a network so that the cost involved in selecting and planning a network should be kept low and all the devices within a university campus should get access to the internet. Since there are various types of internet connections available, thus various network equipments can be used to design a smart network, so that the cost involved is utilized up to the maximum. Moreover, a smart design can secure a network also by keeping intruders from accessing the authorized data and the network access either wired or wireless can be provided to all the devices within a university campus. Thus if a campus network is designed properly, then the setup cost and maintenance cost will be very low and the design of a university campus network will last for a long time.

### Conclusion

In conclusion, designing a secure campus network based on Cisco equipments and Windows Server technology is a crucial aspect of modern organizations. It provides protection against cyber threats, allows for efficient data management and communication, and helps to ensure regulatory compliance. However, to create a secure campus network, organizations need to follow a set of design principles, including implementing multiple layers of security, dividing the network into smaller segments, limiting access based on least privilege, using strong authentication and authorization mechanisms, implementing monitoring and logging tools, and ensuring compliance with regulatory requirements. While there are limitations to implementing a secure campus network based on Cisco requirements organizations can continue to enhance their network by implementing automation tools.

### References

- Baker, R.W. (2004) Membrane Technology and Applications. 2nd Edition, John Wiley & Sons, Ltd., Hoboken. <https://doi.org/10.1002/0470020393>.
- Crawford, K., & Schultz, J. (2014). Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. Boston College Law Review, 55, 93-128. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2325784](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784)
- Dworkin, M. (2007) 'Recommendation for block cipher modes of operation: Galois/counter mode (gcm) and gmac'. NIST Special Publication 800-38D.
- IFT (2013) 'Symmetric key and public key encryption'. [Online]. Available at: <http://itfreetraining.com/Handouts/Certificates/SymmetricAndPKI.pdf> (Accessed: 15 April 2023).
- Stakeholder Technology Branch (2007) 'Area Network (WLAN) Best Practices Guide'. [Online]. Available at: <http://education.alberta.ca/media/822010/wirelessbestpracticesguid.pdf> (Accessed: 29 April 2022).
- Tschabitscher, H. (2013). 'How to protect your email with password and encryption ion windows'. [Online]. Available at: [http://email.about.com/od/secureemailbyencryption/qt/et\\_private\\_mail.htm](http://email.about.com/od/secureemailbyencryption/qt/et_private_mail.htm) (Accessed: 18 April 2023).
- Weber, C. and Bahadurl, G. (2013) 'Wireless Networking Security'. [Online]. Available at: <http://technet.microsoft.com/en-us/library/bb457019.aspx> (accessed: 22 April 2023).
- Wilkins, S. (2011) 'WLAN Authentication and Encryption'. [Online]. Available at: <http://blog.pluralsight.com/wireless-encryption-authentication> (Accessed: 23 April 2023).