AN APPROACH TO SOLVE CAMPUS NETWORK SECURITY PROBLEMS AT THREE LAYERS OF OSI MODEL

SADEQ AL-ZAGHIR

JUNE 2017

AN APPROACH TO SOLVE CAMPUS NETWORK SECURITY PROBLEMS AT THREE LAYERS OF OSI MODEL

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY

BY
SADEQ AL-ZAGHIR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
MATHEMATICS
INFORMATION TECHNOLOGY
PROGRAM

JUNE 7102

Title of the Thesis: **AN APPROACH TO SOLVE CAMPUS NETWORK SECURITY PROBLEMS AT THREE LAYERS OF OSI MODEL**

Submitted by **SADEQ AL-ZAGHIR**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.

Prof. Dr. Can ÇOĞUN
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assoc. Prof. Dr. Fahd JARAD
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Asst. Prof. Dr. Sibel TARIYAN
Supervisor

Examination Date: 12.06.2017

Examining Committee Members

Asst. Prof. Dr. Yuriy ALYEKSYEYENKOV (Türk Hava Kurumu Univ.)

Asst. Prof. Dr. Özgür Tolga PUSATLI (Çankaya Univ.)

Asst .Prof. Dr. Sibel TARIYAN (Çankaya Univ.)

STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : SADEQ AL-ZAGHIR
Signature :
Date : 12.06.2017

ABSTRACT

AN APPROACH TO SOLVE CAMPUS NETWORK SECURITY PROBLEMS AT THREE LAYERS OF OSI MODEL

AL-ZAGHIR, Sadeq
M.S., Information Technology Department
Supervisor: Asst. Prof. Dr. Sibel Tarıyan Özyer

June 7102**,** 93 pages

With expanding dependence on computer systems all around the world for information storage and data processing, the requirement for legitimate security of data and information cannot be overemphasized. Destruction or revelation of data and unauthorized access can violate people's privacy and threaten the presence of an institution, as information is considered the live wire of an institution. Therefore, it is a necessity to secure the stored information and computer systems. The customary method for securing computer networks, such as software encryption and firewalls are ineffective and insufficient. There is a probability that the network is exposed to harm or physical attack due to its feature of management and monitoring point not being centralized, open medium dynamic changing topology, cooperative algorithms and clear line not well defended. This thesis recognizes many kinds of threats in campus network related to three layers of OSI model (physical, data-link, and network), and proposes several practical solutions from network infrastructure perspective. This study covers three main parts; first, building a campus network with principal security aspects (default configurations). The second part, addressing network's flaws, vulnerabilities and weak points that represent a back door for the network and threaten C.I.A. means (Confidentiality, Integrity and Availability). Moreover, the first important step to know the level of threat is addressing network's flaws. All threats come with three layers will be identified in this study. Also, a solution will be offered for each threat and an example will be given for each solution. Finally, as a part of evaluating the network security, some kinds of attacks will be made (before and after) applying security technologies.

The theoretical results of this study represent a reference model for a campus network security through first three layers (P., D., N.) that can be adopted as a good practice to build and secure a robust campus network for the deep information affixed to each part within the three layers. The details will include many recommendations and will be covered at design and implementation of the campus network.

The final result in this study gives a bright view about how much we have gained resources and offered more services with guaranteeing information secrecy, service availability, full mean of confidentiality. Decreasing the effect of attacks and increasing the uptime are extra benefits of this study.

Keywords: Campus Network Security, Physical Layer Security, Layer Two Security, Network Layer Security, VTP v3, Point-To-Point OSPF, BGP.

ÖZ

OSI MODELİN ÜÇ KATMANINDA KAMPÜS AĞ GÜVENLİĞİ PROBLEMLERİNİN ÇÖZÜMÜ İÇİN BİR YAKLAŞIM

AL-ZAGHIR, Sadeq
Yüksek Lisans, Bilgi Teknolojileri Anabilim Dalı
Tez Yöneticisi: Yrd. Doç. Dr. Sibel Tarıyan Özyer

Haziran 2017, 93 sayfa

Bilgi depolama ve veri işleme için tüm dünyadaki bilgisayar sistemlerine olan bağımlılığın artmasıyla, veri ve bilgilerin meşru güvenlik gereksinimi aşırı vurgulanamaz. Verilerin imha edilmesi veya ifşa edilmesi ve yetkisiz erişim insanların gizliliğini ihlal edebilir ve bir kurumun varlığını tehdit edebilir; çünkü bilgi bir kurumun canlı telidir. Dolayısıyla, depolanan bilgileri ve bilgisayar sistemlerini güvence altına almak bir zorunluluktur. Yazılım şifreleme ve güvenlik duvarları gibi bilgisayar ağlarını güvence altına almak için alışılagelmiş yöntem etkisizdir ve yetersizdir. Ağın yönetim ve izleme özelliği merkezi olma özelliği, açık orta dinamik değişen topoloji, kooperatif algoritmaları ve iyi savunulmamış net hat nedeniyle ağın zarar veya fiziksel saldırıya maruz kalma ihtimali var. Bu tez, kampüs ağında OSI modelinin üç katmanı (fiziksel, veri bağlantısı ve ağ) ile ilgili birçok tehdit tanır ve ağ altyapısı açısından çeşitli pratik çözüm önerir. Bu çalışma üç ana bölümden oluşmaktadır; İlk olarak, temel güvenlik yönleriyle (varsayılan yapılandırmalar) bir kampüs ağı oluşturmak. Ağın kusurlarını, güvenlik açıklarını ve ağın arka kapısını temsil eden zayıf noktaları ele alan ve G.D.K. (Gizlilik, Dürüstlük ve Kullanılabilirlik) 'yi tehdit eden ikinci bölüm anlamına gelir. Dahası, tehdit seviyesini bilmek için ilk önemli adım ağın kusurlarına işaret etmektir. Bu çalışmada tüm tehditler üç katmanlı olarak tespit edilecek ve her biri için bir çözüm sunulacak ve her bir çözüm için bir örnek verilecektir. Son olarak, ağ güvenliğini değerlendirmenin bir parçası olarak, güvenlik teknolojilerini uygulayan bazı tür saldırılar (önceden ve sonra) yapılacaktır.

Bu çalışmanın teorik sonuçları, ilk üç katman (F., V. B., A.) aracılığıyla bir kampus ağı güvenliği için bir referans modeli temsil etmektedir; bunlar, sabit bilgi için güçlü bir kampüs ağı oluşturmak ve bunları sabitlemek için iyi bir uygulama olarak benimsenebilir üç katmandaki her parçaya. Ayrıntılar pek çok öneriyi içerecek ve kampüs ağının tasarımı ve uygulanması konularına değinilecektir.

Bu çalışmanın nihai sonucu, ne kadar kaynağımızı kazandığımız konusunda parlak bir fikir verir ve bilgi gizliliği, hizmet kullanılabilirliği ve gizliliğin tam anlamı ile güvence altına alınarak daha fazla hizmet sunmuştur. Saldırıların etkisinin azaltılması ve çalışma süresinin uzatılması bu çalışmanın ilave faydalarındandır.

Anahtar Kelimeler: Kampüs Ağı Güvenliği, Fiziksel Katman Güvenliği, Katman İki Güvenliği, Ağ Katmanı Güvenliği, VTP v3, Noktadan Noktaya OSPF, BGP.

ACKNOWLEDGEMENTS

Thanks to the most compassionate, gracious and merciful. May Allah’s blessings and peace be upon our prophet Mohammed who protects us from the depths of darkness and leads us forth into light, and his household.

It is a pleasure to express my special thanks to my friends Samir AL-Asadi who helped me, Mohammed AL-Shimmari who inspired me and my family and other friends for their valuable support.

I would like to express my sincere gratitude to Asst. Prof. Dr. Sibel TARIYAN for her supervision, special guidance, suggestions, and encouragement through the development of this thesis.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Boundary Router
BGP	Border Gateway Protocol
BIOS	Basic Input Output System
BPDU	Bridge Protocol Data Unit
CAM	Content Addressable Memory
CIA	Confidentiality, Iintegrity, Availability
CLI	Command Line Interface
DAI	Dynamic APB Inspection
DDoS	Distributed Denial Of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DR	Designated Router
EIGRP	Enhanced Interior Gateway Routing Protocol
EoL	End of Life
GNS 3	Graphical Network Simulator 3
GUI	Graphical User Interface.
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IEEE	Institute for Electrical and Electronics Engineers
IOT	Internet Of Thing
IP	Internet Protocol
Ipsec	IP Security
ISO	International Standards Organization

ISP	Internet Service Provider
LAN	Local Area Network
LSA	Link State Advertisements
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
MITM	Man In The Middle
MMF	Multi Mode Fiber
NAT	Network Address Translation
NBMA	Non-Broadcast Multi-Access
NIC	Network Interface Card
NSSA	Not So Stubby Area
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OUI	Organizational Unique Identifier
P-2-P	Point-to-Point
PC	Personal Computer
QoS	Quality of service
RIP	Routing Information Protocol
SMF	Single Mode Fiber
SSL	Secure Sockets Layer
STP	Shielded Twisted Pair
TCAM	Ternary Content Addressable Memory
TCP	Transmission Control Protocol
ToS	Type of Services
TTL	Time To Live
UDLD	UniDirectional Link Detection
UDP	User Datagram Protocol
UTP	Unshielded Twisted Pair
VLAN	Virtual LAN

VoIP	Voice Over IP
VPN	Virtual Private Network
VTP	Virtual Trunk Protocol
WiFi	Wireless Internet

CHAPTER ONE

INTRODUCTION

1.1 Introduction

Information security has turned into a very talked about subject throughout the world in the most recent couple of years. All organizations (including educational ones) should become aware that information resource is extremely valuable and must be preserved at all cost. Therefore, Information security is no longer a luxury, but a requirement in all organizations. A lot of research has been made in educational environments. Until now, the important role of information security has not received that much attention, especially in the recent education techniques like e-learning environments. Information should be protected because of developed technologies that could be utilized to achieve a high level of information security.

Over the most recent years, education environment experienced a big change because of the quick development of technology. This development made it possible to use e-services in order for the education environment to boost their ways of education. However, it is necessary that education environments guarantee all resources (information, students and lectures) are protected against any potential threats. The progressing transition to security of networks requires secure and dependable services and network infrastructure. As networks develop from simple point to point systems to complex, distributed cloud environments, ultra-high capacity and reach, and software-defined, new security challenges increase. This study defines technical information security solutions that could increase information security within the education environment. Moreover, following three steps to build, estimate and strength the network gives us a clear vision about all parts of the network.

1.2 Definition of Security

Generally, security is “the quality or state of being secure to be free from danger.” To put it another way, protection against enemies who would cause a harm purposely. National security, as an example, is a multifaced system which protects the state sovereignty, its resources, its people, and its assets. Reaching the suitable level of security for an institution requires a multilayered system too.

An effective institution must have the following security multiple layers in order to protect its operations:

Communications security: for protecting content, technology, and communications media.

Operations security: for protecting the particular operation details or series of activities.

Personnel security: for protecting the people who have the authorization to access the Institute and its operations.

Network security: for protecting contents, connections, and networking components information security: for protecting the availability, confidentiality, and integrity of information assets, whether in transmission, processing, or storage. It can be achieved by technology, training and awareness, policy application, and education.

Physical security: for protecting physical items, objects, or areas from unauthorized access and misuse

Information security is defined by the Committee on National Security Systems (CNSS) as information protection and its crucial elements, including the hardware and systems that transmit, store, and use that information. Information Security contains wide areas of network security, computer and data security, and information security management. The CNSS model related to information security developed from a concept evolved by the computer security industry called the Confidentiality, Integrity and Availability (C.I.A.) triangle. The C.I.A. triangle has become the industry standard for computer security since the evolution of the mainframe. It depends on three identities of information that make it valuable to organizations: confidentiality, integrity, and availability. Today, the importance of security of these three characteristics of information is as it has always been, however, the C.I.A. triangle model is not anymore sufficient when processing the continuously changing environment. The threats to confidentiality, integrity, and availability of information is in developing an expansive set of events, including intentional or accidental damage, unintended or unauthorized adjustment, theft, destruction, or other misapply from human or machine threats. This recent environment of multiple permanently developing threats has encouraged the evolution of a more solid model that handles the complication of the recent information security environment. The developed model contains a list of critical features of information, that are described next.

1.3 Problem Definition

Network security is sometimes more than what individuals dependably thought it to be, virus, trojan, hackers, malware. Network security could be brought by inadvertent human mistake as well as it could be compromised by human instinct .Employees and their various errors are common network security issues most organizations facing, this happens because of improper training or inexperience, and sometimes due to reaching an incorrect assumption. Hacking is another usual network problem. It occurs when intellectual properties being stolen in spite of copyright laws presence. However, network security problem is not only caused by human errors , but also by natural forces such as lightning, floods, earthquakes fire breakouts etc .

Securing campus network from administrator perspective is an aspect of this study. Build and secure switching and routing play a critical point to shape the network and it takes place in this study with more details. Insider threat plays a dangerous role since an employee can reach more sensitive places than an outer person, this kind of threat has been treated in this study be giving a specific role and privilege.

1.4 Motivation

Cyber-attacks and crimes cost projected to reach $2 trillion by 2019 according to Forbes with more than 400,000,000 identities exposed only in 2015 according to Symantec [1]. The last two dark pictures give a glimpse about the security threats that we are facing in our modern world, which imposes the need for more tight security measurements than ever in this cat-mouse chasing scenario. From the network perspective, all the external attacks and a decent percentage of the internal attacks are taking place over the network infrastructure, that is why securing the network is the first blocking wall to face any possible breach in our environment.

Universities are encountering new difficulties with the rising worldwide economy portrayed by the significance of enhancing the effectiveness and productivity of individuals and giving faster communication services. Securing campus network is our case study in this thesis which pays attention to many aspects such as design, build, secure and check the level of security for the last version of our network.

1.5 Contributions

The work exhibited in this thesis reflects our investigation of three security network layers: Physical, data-link and network layers. We depict various shortcomings in the design and implementation of these layers that could be misused by an enemy to lead to different, and in some cases intense, attacks that undermine their essential security objectives. The effect and applicability of our work goes beyond the scholarly world and reaches out to cover the bigger group of security network designers and researchers. this work illustrates the common flaws that could affect security. Starting from scratch, a campus network will be built, state all kinds of weaknesses, attacks, flaws and threats that could face the security OSI three layers. Finally, we will attempt to shut down all flaws and vulnerabilities and keep threats away by using possible technologies presented by CISCO devices. In addition, we will be examined our work through attacking it before and after security technologies to assess its strength point regarding security.

1.6 Aims of Study

The main aim of this work is to build the campus network and secure it from attacks and threats. As well as, to apply different defense techniques used to prevent a corruption caused by an attacker. Another objective is to demonstrate the procedure of applying the best security and to expand the practices of an outsider attempt to get access to the network. Also, as a part of this study will try to find an answer to many research questions such as

In case of future campus network expanding, can we manage this expansion without affecting the security? What are the techniques used for that?

Is it enough to depend on default configurations come with switches and routers?

Which part of a network represents a source of threat? How can deal with it?

L3 represents the connection point between inside/ outside network, How can enrich this point to prevent losing privacy?

And the last question is: after securing L2, L3 what are the benefits of these solutions? and is it logical to adopt this study or not?

1.7 Thesis Structure

The thesis will be organized as follows: - chapter 2 will be an overview of network security and how it can impact a campus network, what kind of characteristics must be applied with campus network, which mechanisms are used by attackers? define some security terms, types of threats might face a network, the main differences between traditional design and hierarchical design, final part will review some previous studies concerned with security. Chapter 3 will be about the practical side of the thesis to design and secure campus network through many steps within three layers (physical, data-link, and network), covering all possible scenarios that threaten the network and the tools to mitigate those attacks. Chapter 4 will cover our results of this work and how this study will represent a strong map to build secure campus network, the result will hold a comparison between before and after using security technologies. Chapter 5 will conclude our work to show the benefits of doing this study.

CHAPTER TWO

BACKGROUND AND RELATED WORKS

This chapter explains the following; first part of this chapter shows the campus network design characteristics. The second part covers the definition of security, the goal of security, types of threats and challenges, attack mechanisms and security terms. The third illustrates OSI model, three lower layers of OSI and Backdoor attack face them, a comparison between traditional and hierarchal campus network design. Last part covers most of the previous studies related to our study for building and securing campus network.

2.1 Campus Network Characteristics

Any network design should follow a set of rules and include set of mechanisms that give essential steps to build a network. In the campus environment, there are many properties that must focus on building integrated design [3]. CISCO offers us a standard design to reach these priorities. Principle cornerstone properties for campus network are as follow:

Scalability: - Good and efficient design for any network especially campus is to offer scalable design, which needs less effort to grow and expand the network without need to redesign the network entirely. A clear example for that, when a university needs to open new department or even new campus, at this point scalable design can deal with this case. Scalability is an important way to plan for building any network through making a design flexible to grow and be larger for the future expansion.

Resilient flooring: - during real daily work of campus network, there are some challenges facing it. Therefore, a modern network has to interact and endure a failure by recurring itself as fast as possible and mitigate the effects of any event. For example, signal lost, through some activities offered by modern campus networks such as online classes and online conferences, these activities need resilience, which plays the main role when something bad occurs to reduce the damage and decrease downtime.

Independence: - what independence means is separating each department traffic logically or physically to reduce the amount of traffic via all the network, also to prevent direct access between departments. Therefore, our network design will separate each faculty in especial VLAN and put a management VLAN to access all those faculties in order to make our design more secure, also more efficient.

Rigidity: - measuring the cohesion and coherence to any network is done by measuring the resistance of that network to attacks and the level of security. In this study, we will pay more attention for this important property in order to reach the high level of security inside campus network. Moreover, exhibit and guarantee secured information and prevent all kinds of unauthorized access to the resources of the network. Also, to allow the campus environment use new trends, social tools and new ways of learning.

QoS: - new technologies came with new communication type such as online conferences, VoIP and many else, all these new trends to meet people need Quality of Service (QoS). QoS means giving high priority to some kinds of traffic such as online conferences to cover it without disconnecting or losing the signal. And less priority to other kinds of traffic that can afford the delay in transmission such as HTTP traffic. QoS called ToS (Type of Service) within layer 3.

2.2 Network Security Definition and Goals

Firstly, security as a general word means providing protection and safety. In the network world, it means to protect a network from a malicious use not only outside malicious person but also from close staff (inside) with keeping the role of networking by offering access to the data to authorized user. Also, security takes the meaning of manage and heal any effect, if there is an attack occurs. Measuring the network security could be through how much its resistance to attacks and what kinds of alternatives used by the network to alleviate the impact of the attacks. There are many studies and researches tried to find tools, which can address or offer the guarantee against changeable attacks. Network security has the main influence in different fields and has taken a huge attention of companies leaders worldwide. It is a real contest to reach the goals of security which mean to keep a specific data or things in safe place to make sure that there is no unauthorized access to these data or things, applying these aspects are different. According to many researchers who focused on making data secured but in an isolated place. In this way, data will be secured but there is no connection to the global world [4]. This method will limit the activity and the main role of the networking. Enhancing security means increase complexity and putting more checkpoints, this could be correct at some points but not always. Some researchers defined network security as a universality in the use of data with some tools to face threats, which are coming from outside. In this way, a local network can contact with outside world. But with serious and dangerous effects, which are lost personality or sometimes losing the control of entire data by vandals. The best definition of network security is combining three main rules or aspects (Confidentiality, Integrity, and Availability), that represent using new networking services on the safe side. These aspects will balance between privacy abdication or leave globalization. Confidentiality means preventing an unauthorized person to disclosure our data. In other words, it means keeping data in somewhere as drivers or computers in the network that cannot be accessed by anyone without a proper authorization, this means, having the type of authority on this data to deal with. When a user needs to transfer data, only the intended receiver will have the authority to see this data, also when this data intercepted by using a sniffer or any malicious apps, it will be unreadable data to the sniffer. Sharing data using the Internet represent a good example because data such as personal, sensitive, governmental) must be kept in a secured place, transfer in a secured milieu and read by authorized person to ensure privacy. These points are the role of confidentiality. Clarifying the relation between confidentiality and education work; the students' grades, as an example, must have high confidentiality to be seen only by the students themselves, no one can view this information to keep student's rights [5]. Integrity means the accuracy and completeness of information. When receiving data sent from someone; first, you have to make sure that the received data is the original copy without any changes whether purposely or accidentally. Therefore, any corruption in this information or even any new data added by sniffer into original data will be detected by integrity means. The same previous example about the student's grades but from instructor's perspective, the instructors should have the original copy of these grads to compare if any change (deliberately or mistakenly) has occurred. This is the role of integrity. The last goal of security is Availability. After making sure that transferred data has reached two previous security goals. Now, data must be accessible and reliable at the time to authorized person. For example, when we have a server for a web page, we should ensure working this server full time to allow authorized users reaching the data that saved on this server. The figure below shows the three security's aspects:

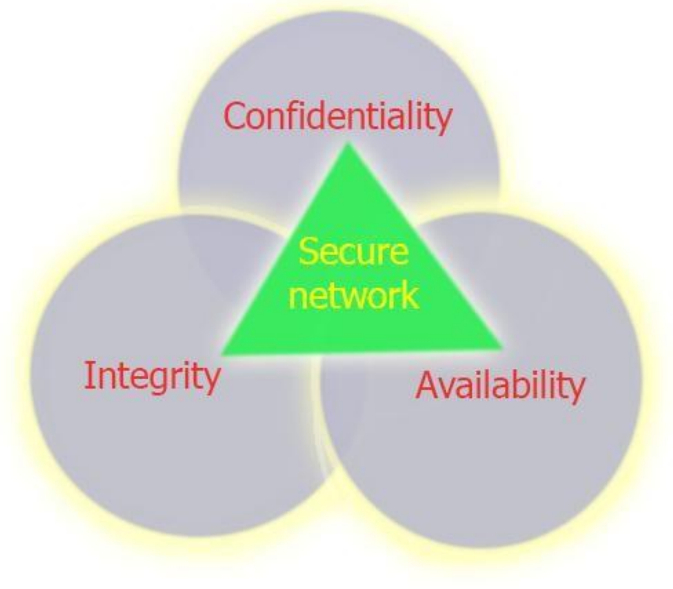


Figure 1 C.I.A.

2.3 Attack Mechanisms

Working in shadow is what the attacker wants to be to keep his tools covered and hidden to gain more benefits. The main kinds of attacks are stated below:- [6]

a- **Reconnaissance**: - The first step to collect information as much as possible to know the weak points in victim's system or network.

b- **Privilege escalation**: - Exploiting the access that given to one user to get more unauthorized access. For example, one employee, who works in human resources, has a username and password to enter to his account. What if he wants by using his username/password is to access to the data center (above his authority), he tries to capture the entire traffic. Another example, when the same employee gets direct access to network devices and tries to force a password by trying many times till getting right password.

c- **Backdoor**: - After an attacker gets access to a system or network, he needs to ensure his access in future. For this reason, the attacker uses some applications to keep gaining information from victim's device, also many backdoors are installed by the user unconsciously when clicking on a link has a threat.

d- **Code execution**: - The victim's device under attack can be controlled by the attacker, who can execute any code within the device. This kind of attack represents a harmful one because it affects confidentiality and integrity as well.

e- **Social engineering**: - The manipulation of human beings is one type of attacks which tries to deceive them and convince them to do the work leading to reveal their confidential information (such as a password). Phishing is one kind of social engineering attack that makes a fake similar page to this utilized one by a user asking for username and password, after getting information will redirect this information to an attacker.

2.4 Security Terms: -

Everyone needs to work with security, there are some basic terms should know to invest time and effort dealing with such preliminaries: [7]

1- **Asset**: - means every valuable thing that is relevant to network areas such as building, equipment, labs, data-center, employees.... etc. All these represent the first job for administrators to identify in order to secure a network.

2- **Vulnerability**: - any weakness in a network's asset should be addressed in advance to take a strong view. Vulnerabilities could be related to the operating system itself or even related to network equipment by using weak devices in the vital place.

3- **Exploit**: - is a tool that is used to take advantage of available vulnerabilities to make a damage or capture traffic of data to get important information.

4- **Threat:** - represents any hazard affecting network assets. Also, threat sometimes occurs accidentally or intentionally. It could be defined as any intended behavior in order to corrupt or steal or even threaten for getting money.

5- **Attack**: - is an action that occurs to get a leverage or compromise a network in order to make a damage. For example, DDoS attack.

2.5 OSI Model

The first important question we should find an answer for it is "WHY SECURITY IS IMPORTANT?" Clearly, the use of the Internet and networking has exponentially increased and branched out to include each piece of our life, this means easy access and contact with others regardless of geographical distances. This is the good side of the Internet. On the other hand, security issues and personality threats represent the harmful side. To give an example for this from our daily life, people use the Internet to buy and sell new things, study, communicate with family or do bank transactions and many else. All these activities become easy to perform, but also need a strong form of security over network especially over OSI model which builds the Internet. Therefore, security has to have essential aspects to keep user’s data as secure as possible such as confidential data. If we have any data about staff, business model or resources, we have to protect these data from unauthorized users and do not let any access (such as competitors) to our data. With keeping the role and the meaning of networking, not make the network locked but by using Internet’s advantages and benefits, at the same time enrich and robust our network from threats. Open System Interconnection OSI model [8] is a logical separation of the network into seven layers, each layer has a special role. The benefits of OSI is reducing the complexity and standardizes interfaces to allow different vendors to communicate together, facilitates modular engineering, ensures interoperable technology and simplifies for identifying the problems. Shortly, we will explain some rules and protocols within each layer in OSI model. OSI model divided into two main sections (lower layer and upper layers). Lower layers consist of (physical, data-link and network). Upper layers consist of (Application, presentation, session and transport). Starting from the physical layer, that represents the first gate for receiving and the last gate for sending data. Receiving data pass through physical layer Network Interface Card (NIC) which changes the electrical signal into digital bits stream as (0s or 1s). In the other side, sending data the last layer data will pass through is a physical layer that converts bits to signal. Some protocols within this layer such as (IEEE 802, IEEE 802.2, ISO 2110, ISDN) [9]. The second layer is Data Link, which plays many roles such as:-

a- Delivers and changes packets to frames in case of sending, or converts bits to frames when receiving data.

b- Deals with physical address (MAC address).

c- Error detection, data framing and requirements defined.

There are many protocols within this layer such as (Ethernet family, IEEE 802.2 LLC, Token Ring, etc.) [10].

Network layer deals with a logical address (IP address) and represents the gateway for a network; protocols works within it are (IPv4, IPv6, ICMP, Routing Protocols, etc.) [11] our work will focus on those three layers by securing and guarding them because of the important role performed by them. Upper four layers of OSI model do not care about network devices and addresses, all they care about is encoding data and starting and terminating sessions, also they care about the applications that help to connect to the network like internet explorer, Google chrome and so on. Transport layer defines the type of connection whether connectionless (UDP) or connection-oriented (TCP) [12]. Session layer role is opening sessions through specific ports for each request coming from an end user and receiving the response though same ports. Protocols within this layer are (Net BIOS, Sockets, named Pips, RPC) [43]. Presentation layer works to encrypt, compress and translate data for different types of source data. Protocols in this layer are (SSL, Shell and Redirectors, MIME). The last layer is application layer, it is an interface to end-user to use the network services, there are many applications to ease access to the Internet by searching, sending an Email, making a call or any other activities. Some protocols working in this layer are (DNS, NFS, BOOT, DHCP, SNMP, etc.). Following figure show OSI model's layers.

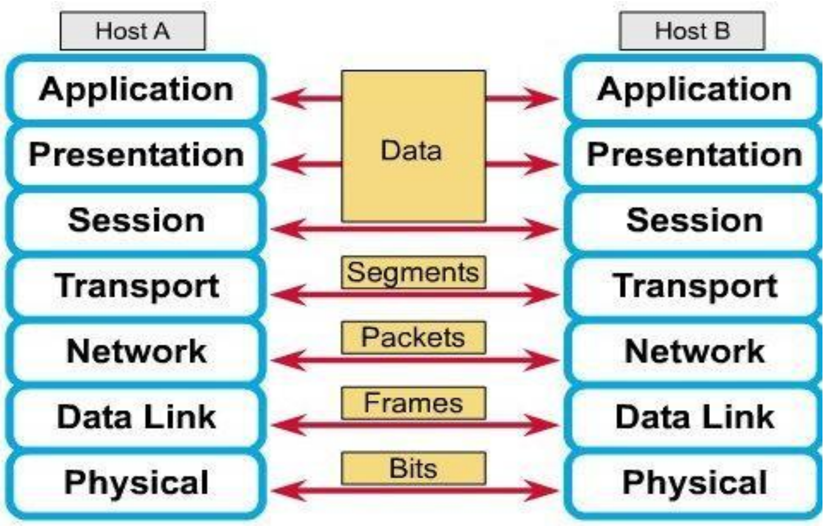


Figure 2 OSI Model Layers

2.6 Threat and Challenge Types (in Three Lower OSI's layers)

In order to protect a network, first, we must identify which kind of threats could face the network to know how to employ security features/technologies. This part will explain in details the relevant information with three lower layers of OSI model that present the networking world, kinds of flaws, threats, attacks and the features and methods that guard the three layers. Behind each threat there is a goal, some of them try to damage files, financial goal, to get fame by attacking famous websites or even for political reasons.

2.6.1 Physical layer's threats

First of all, why will this part focus only on the physical layer? Because many attacks take advantages residing in physical layer even the other layers in this network are guarded, the result of violating physical layer could be detrimental. The physical layer is the first step to secure a network and networking linkage. There are many techniques to enrich and empower the security for physical security such as alarmed systems, video camera control and so on, these tools work to prevent or mitigate the damage that could occur if an unauthorized person gets direct access to the data center's devices. The physical layer is represented in two sides: geographic place (data center room) and devices, each of them should have a suitable security characteristic to start building other layers. Reaching that through stating the essential characteristics for those two sides. First, data center building must have many certain properties, monitoring and maintaining a controlled environment where all the devices can operate in an efficient way and eliminating all the threat's factors caused by unexpected issue as humidity and temperature. In addition, it must be containing backup devices (power devices and network devices) to ensure keeping the network working. Moreover, we must use security personnel to keep access just for authorized person. The other side of the physical layer is devices that shape a network. Cheap and non-specialized devices, misconfigurations, poor network design or apathy of users all these affect security. An indignant user can play a bad role in violating the network security [13]. at this point, we must focus on choosing last versions and more secure devices to prevent vulnerabilities that are caused by a cheap type of devices. In chapter 3 we will state some products of CISCO devices that provide us with a stable version and strong features. With physical layer, there are some challenges that could be used by an attacker to gain access to the network equipment such as:-

1- Messy data center.
2- No prove authentication required to enter data center room.
3- No assistive devices when a problem occurred.
4- No password on network's devices (switches, routers).
5- Natural disaster.

Some of the security features in the physical layer:

- Monitoring the data centers and the telecom rooms around the clock on including the vital environmental elements as the temperature and humidity.
- Choosing secured location for the data centers and telecom rooms to meet the security standards and provide safe locations in case of any natural disaster.

- Having continues data and configuration backups in case of any data loss or the need to a hardware replacement.
- Using redundancy cabling between the switches in case of any cable cut or a full path become unavailable.
- Providing a monitored and authorized access to the data centers and telecom rooms based on smart cards and fingerprints with full events logs.
- Configuring the *UDLD* feature on all the fiber cables to prevent the loops or packet loss in case the fiber cut in only one transmit or receive pairs.
- Using only standards and well-known vendors (CISCO in our case study) to make sure that all their products are fully secured.
- Using auditing agencies to test and evaluate the security of our premises.

2.6.2 Challenges with Data-Link and Network layers

The case is different with the data link and network layers, challenges are often represented with weak configuration especially when an administrator has low experience to control the network such campus size network. Data-link layer represents an easy part that can be compromised by attackers and all types of attaches looking to find a weak point to pass through.

Data link challenges are:- [14]

1- The unauthorized device could attach the network equipment.
2- The loop could occur in this layer that puts a network in infinity loop and depletes network's resources without end.
3- A malicious person could add his device to take responsibility as a root for a network traffic.
4- Flooding CAM (Content Addressable Memory) table.
5- BPDU flooding attack that influences whole network's paths.
6- Creating Man-In-The-Middle attacks for the ARP traffic (ARP Spoofing).
7- VLAN Hooping attack.

Network layer works with logical address IP. Like other layers, network layer has many flaws and threats. Challenges with layer three –network- are as follow:-

1- Denial of Service Attacks: DDoS (Distributed Denial of Service) & DoS (Denial of Service).

2- Router-in-the middle OSPF and BGP attacks.

3- Plain configuration for BGP.

4- Calming the Designated Router role in OSPF.

5- Changing the Router-ID in OSPF and BGP due to changing the IP addresses on the layer 3 device.

2.7 Traditional (Flat) Design VS Hierarchical Campus Design

In this part, we will explain the differences between two network designs (traditional and hierarchical) to address the weaknesses in classic design. Firstly, traditional design [15] does not have multi-layers network design, this makes managing view more complicated. If there is a simple problem in one department, it will cause failure in large part of campus's network. Moreover, it will be hard to find the reason of this problem. with tradition design, if a campus needs to expand its departments or open a new campus, this will force the administrator to redesign the entire network. This means more effort, more time and more cost, in addition to stopping the services of the network for a long time. The figure 3 shows traditional design.

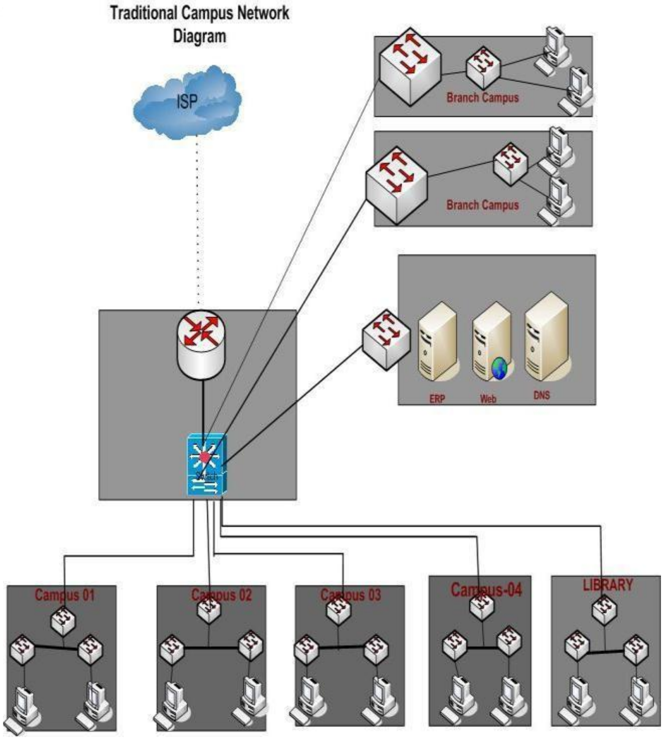


Figure 3 Traditional Campus Design

Secondly, with the hierarchical design [16] it is easier to determine the sources cause of the problem. Furthermore, the hierarchical design provides redundancy paths which offer more flexibility to mitigate network failure. It offers an expandable design with easy steps. For example, if there is any new department or even new group of new departments, it could be easier to add new devices with some commands to finish the adding task. Grouping each department's devices in hierarchical design offers traffic management efficiently and decrease complexity in design and implementation the network, dividing a campus's departments to many blocks. Hierarchical design makes the network design more sensible and understandable by aggregating devices in each layer (access, distribution and core) to smaller parts, and take one link as uplink for each block to connect it with upper layer, this will reduce effort of tracking a problem if occurred and keeping design easy [50]. On the other hand, these features are not available with traditional design. figure 4 below shows hierarchical design.

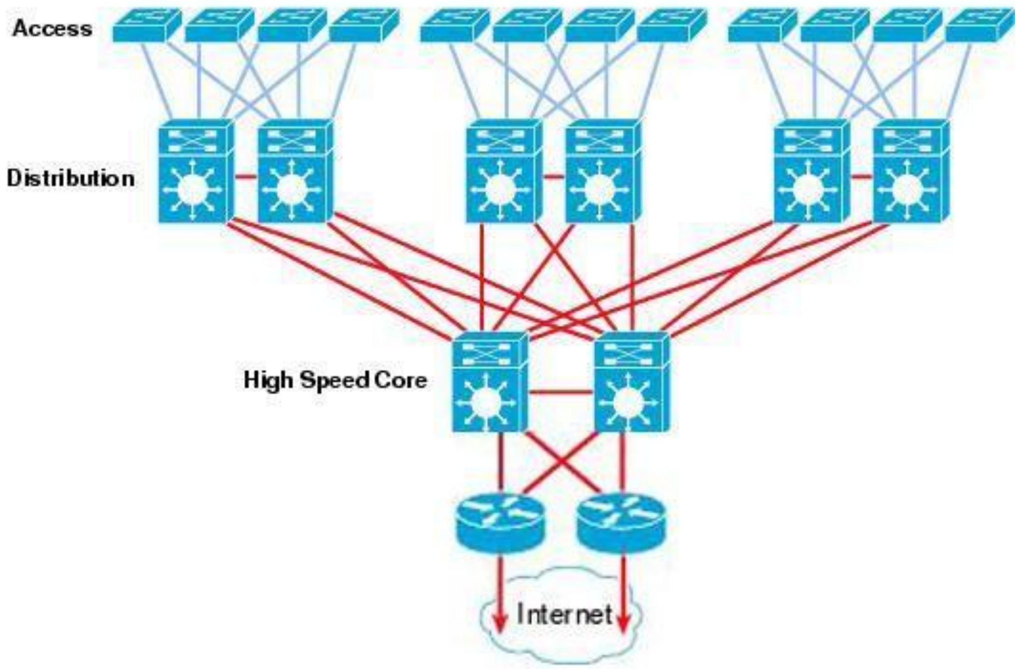


Figure 4 Hierarchical Campus Design

2.8 Kali LINUX

It is an operating system built to test the security of a network, supported with many security tools to learn ethical hacking for trainers, security specialist and students. Ethical hacking means use either own system to do these hacking or have to take a permission to do it for ethical reasons [38]. Also, another reason for ethical hacking is to know vulnerabilities and weaknesses of a network to try to mitigate or close them[2], [3]. Also, this version of LINUX is Debian-based could use GUI interface or command line. There are hundreds of hacking tools can download from official website of Kali Linux to implement a real attack but with taking a permission or using your own lab to do this. As a part of our work, we used Kali Linux to check our network by using some types of attacks before applying security and take the results. After that, we put many security features through three layers of our network and made same attacks. In this study we have used a virtual machine to install Kali Linux Light version. Figure 45 shows a general view of Kali desktop interface with some security tools that came with it. Also, as all Linux operating system, Kali has strong tools using command line interface although it supports GUI environment.

2.9 Related Work

Network security has high priority role because of importance in any network all around the world. Wherefore, there are many researches focused on addressing and offering solutions for potential threats. In this section, we will try to enumerate some of those researches that had taken a campus network as a work area.

Cuihong Wu [17], had presented in his paper "the problem in campus network information security and its solution" general types of threats that face any network, especially campus environment. After monitoring and analyzing campus traffic, he decided to explain the results and gave a suitable solution for threats, and he stated some causes like: - Poor infrastructures that shape the campus network, lack of knowledge to manage the network, imperfect network administrators, and no robust network security system. After he stated theses causes, he tried to suggest a number of advises to mitigate the effect of these security issues like :- Every campus network should have integrated clear defined plan , also should use new techniques such as:- Use Virtual Local Area Network (VLAN), use firewall device and software, use encryption, and use Virtual Private Network (VPN). Centralize management of the network keeps monitoring. After all that, he did not implement any practical work.

Hu Ning and Xu Bingin [18] in their paper "The research and analysis of the security of campus network" focused on defining the terms of network security within two parts (hardware and software) as one part in security term. Also, they defined the secured system by preventing access against unauthorized changing and information seeping. After that they stated main properties of network security like: - They defined secrecy as securing information from being exposed to an unauthorized individual, business, and procedure. Confidentiality and guard are shaped in equal levels of the network system. In physical layer, as they supposed, should ensure that system stops revealing information by using interconnection. In the level of operation, it ensured system offers service because of authorization. Therefore, that system is prohibited to be used by not authorized person, attacked by a hacker. They defined integrality as ensured prevent any changing, insertion, and deletion in original data without permission. Also, they defined availability as, that legal person who can access his information at any time he needs. They counted on network security as a group of security tools and application such as strong operating system, anti-virus, intrusion detection with firewall, keep monitoring traffic, etc. They concluded their study by giving advices to update the security tools to be able to detect and prevent new types of attacks.

Dawei Song and Fengiuan Ma[19] in 2012 in their "Strategy and implementation of campus network security" they addressed the security problem inside campus environment relevant to poor security experiences in staff and suggested to increase staffs' ability. Also, the old version of software one flaw represents a big challenge to network security. Finally, they advised to use firewall device from another perspective, they found that some campuses know about flaws inside campus network and turn a blind eye or use a slow procedure to solve it. In addition, supporting new services of learning at home need security tools such as firewall, anti-spam and so on. From physical security, they focused on constructing safety, used security equipment, as well as to secure data center, and they defined system security by two sides, first the operating system itself and the security settings of the operating system. In application layer, they suggested focusing on database servers, web services, E-mail systems, and firewall as well.

Connecting network architecture with security in campus environment was a paper published by Mohammed Nadir Bin Ali et al., IEEE 2013 [15]. They started by defining network security from architecture view. It represents a serious growing problem with education side. And it was facing real challenges related to how it built and they discussed this because increasing security issues of education and counted it is a necessary step to secure educate place and staff from attacks. They presented hierarchical campus network as a solution for some types of threats such as, when there was a fail in one part the other network parts continue to work without interruption, also backups copy in different sites is important to make sure having a working copy of the data. Some campuses need redundancy with devices that present the backbone network (switches, routers). They connected these weaknesses with money and how the campus should depend on money and role of the network. They addressed threats into two types internal was a type caused by direct access from one person inside the campus that represent by viruses, worms, and trojan. Also, they gave the solution for this type by using anti-virus. And second threat as external represented through an attack comes from outside.

Rajiv O.Verma, 2013 [20], used VTP version 2 and access-list to enhance security within an enterprise environment. Using this technology, he reduced administration effort for the network and made it more secure by limiting direct access to other VLAN. He used one physical interface and divided it into three virtual sub-interfaces to monitor the ingress and egress traffic by using an access-list to prevent hopping VLAN attack. Also, he had implemented a small network to show his work. He used a password with VTP to ensure keeping connectivity with authorized devices. As a result, he concluded his work by giving the recommendation to make sure that the revision number of newly added switch must be zero to prevent changing the whole map of VLANs' database. In our work, firstly, we will use VTP version 3 that reduces or prevents intentional or accidental change within VLANs' map. Besides that, VTP version 3 has unlimited support with IEEE 802.1Q VLAN range up to 4096 [21]. It provides a secure VLAN feature (Private VLAN). Additionally, VTP v3 prevents a switch with high configuration revision number to corrupt VLAN's database. Using VTP server mode in version 3 is not enough to manage a network VLANs, there must be VTP primary server to take responsibility and authority to manage the network. Secondly, to reduce the consumption of bandwidth between network's VLANs, we will use pruning feature that prevents unnecessary traffic to travel through unused VLANs. Thirdly, we will encrypt all passwords inside our network to prevent sniffing attacks [22]. After having a glance at all these researches. We will explain our points in our study. Firstly, in this work, we will focus more on fundamental choice by applying practical side more than theoretical within first three layers in OSI model through using all features that make campus network more secure. Moreover, we will adopt best practice aspects to enhance the security of the campus network. We will be applying features and functions support security in campus's devices and keeping the cost low by enabling features that robust security and instead of buying new devices to make redundancy, we will make redundancy through the same device but with different Ethernet group and using the ether-channel technique. Ether-channel technique provides more bandwidth and redundancy. For the design, we will adopt the hierarchal design that provides redundancy, scalability, understandability, and expandability.

CHAPTER THREE

THE EXPERIMENTAL SIDE

Facilitating the understanding of our study, this chapter will cover practical steps. The following figure shows the main steps for this study.

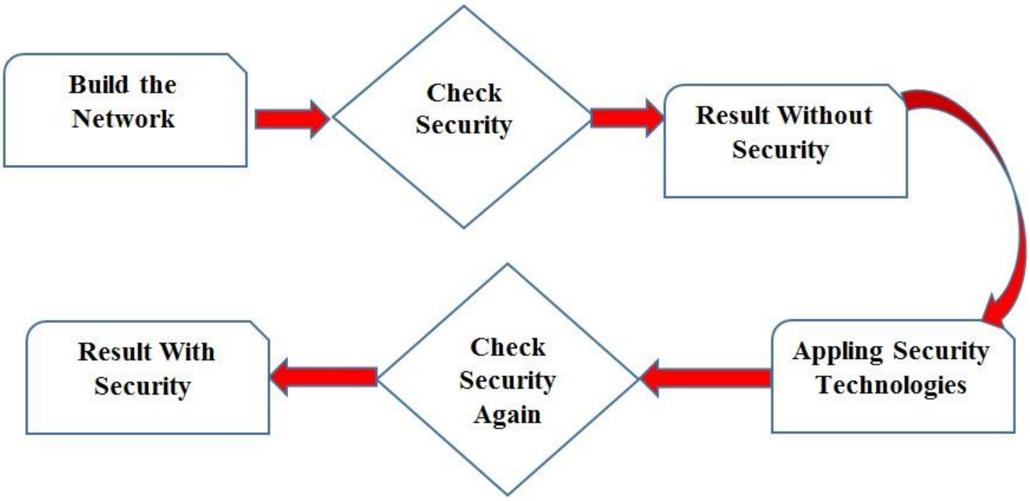


Figure 5 The Practical Steps

3.1 Campus Architecture

As the design of the network was getting more and more complicated due to many factors as the rapid increase in the size of modern networks and introduce new technologies and platforms together the need to a standardized uniform of the network start becoming a necessity for comparison the same factors led to the creation of the OSI model concept. Addressing this challenge many companies and organizations introduced their vision about the umbrella of sets, rules, and regulations that network designer should follow and as the leader of networking and communications sector CISCO was the main player in this standardization movement, which led to the introduction of "Campus Design Network" [23].

The idea behind this unified design is to provide the engineers with guidelines to design and maintain an efficient, secure and scalable form of the network. This hierarchal design is made of three layers (access, distribution and core) layers and the idea behind it is isolation the local traffic on each layer and letting only the needed traffic to communicate inter-layers.

The main advantages of such hierarchical design that it is always easier to deal with smaller blocks of components (network devices or traffic) and in the case of any problem or issue. The troubleshooting will be much easier by isolating the layer of the problem to reach the source of it.

This ergonomic design will make the network more scalable. On the other hand saving time, effort and money. That means fewer resources needed to design networks that are more complex. Security is another aspect of this design where traffic engineering and filtration both intra-layer and inter-layer are easier and more controllable. Also, changes, which is an important factor in any design specifications is much easier when dealing with smaller blocks and know their boundaries. The same design uses by other network companies such as HP, with little change in a name such as distribution layer called in HP design aggregation layer [45].

The benefits of using hierarchical design [24]

1- Effortless troubleshooting.

2- Flexible.

3- Increasing the network’s performance.

4- More secure.

The following figure shows the main characteristic in each layer in hierarchical campus design.

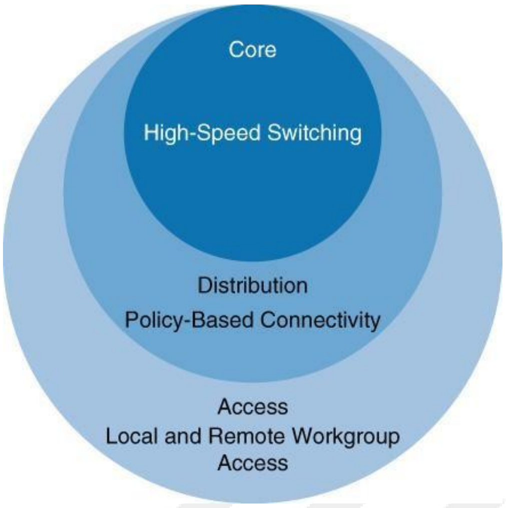


Figure 6 Hierarchical Campus Network [47]

To have a better understanding of this design we need to understand its components' blocks that will try to summarize bellow:

3.1.1 Access Layer

This layer is an end-user facing layer where all end users' devices like computers, printers, cell phones... etc. will be connected whether wirelessly or wired but all the connections will end up on the access layer switches.

One of this layer characteristics that it is a full layer two (speaking OSI wise) and because of that it is separated to different VLANs (Virtual LAN). Which in our case, we have one VLAN per department. The VLAN separation will provide a better traffic isolation, control, and traffic engineering. On the other hand, the VLANs configuration mean that all switches within the same VLAN will share the same broadcast domain. It is a better practice to keep our VLANs locally and not span them geographically across multiple building (unless it is necessary where in our case we have a couple of VLANs that we need to keep all over our network mostly for management and control).

This layer is the richest layer when it comes to functions and features and due to its nature and the fact that it is the first line of defense facing the end-users that imply that securing this layer should be on the list of any network engineer's top priorities. The security of this layer comes in many ways and flavors including securing the access to the switches themselves and securing the all functions that this layer offers. One of the important factors to take in considerations when designing this layer is the fact that we need a high port density and capacity where every single device will need a dedicated single port on the switch (plus a percentage for the future expansion). When speaking on port capacity it is better to go with switches that support Gbps traffic rate since most of the modern devices and laptops and cellphones supporting it already.

3.1.2 Distribution Layer

This layer works as an aggregation point for all the connections from the access layer where all the uplinks from the access layer switch will be connected. In its turn, the distribution switch will either switch the traffic (within the layer two boundaries as the same VLAN) or route it between different networks. CISCO recommendation that the functionality of this layer should reflect the size of the network. Therefore, if we are having a wide network then this layer should be a layer three where routing can take place to absorbs some of the layer 3 traffic from the core layer. The switches in this layer have to be capable when it comes to hardware and software aspects. They should be multi-layer switches to be able to support both switching and routing (if needed) and the hardware should be reliable and long-lasting because this layer will act as a failure point that can take the whole network down in case of any problem because access layer and core layer will not be able to communicate with each other.

3.1.3 Core Layer (Backbone)

This layer as its name implies is the center of any network where it works solely on layer 3 and it is the end point where all the connections from the distribution switches are connected and provides high-speed traffic switching between networks and campuses also it communicating with the routers that connect the campus with the outer world. This layer provides high availability where hardware issues are not tolerated that is why redundancy is one of the most important aspects of this layer.

3.2 GNS3

In our implementation, has been used GNS3 (*Graphical Network Simulator*). It is open source free software that can anyone downloads and uses it [44]. It supports real CISCO IOS environment. It offers many features such as installing a virtual operating system and adding new routers or switches to mimic real one. In this study, many routers and switches versions have been used. Additional, Kali Linux operating system has been used to make attacks [25]. Wireshark has been used to capture (sniff) all traffic to monitor the effect of threats on our network.

3.3 VLAN Per Department and Network Addressing

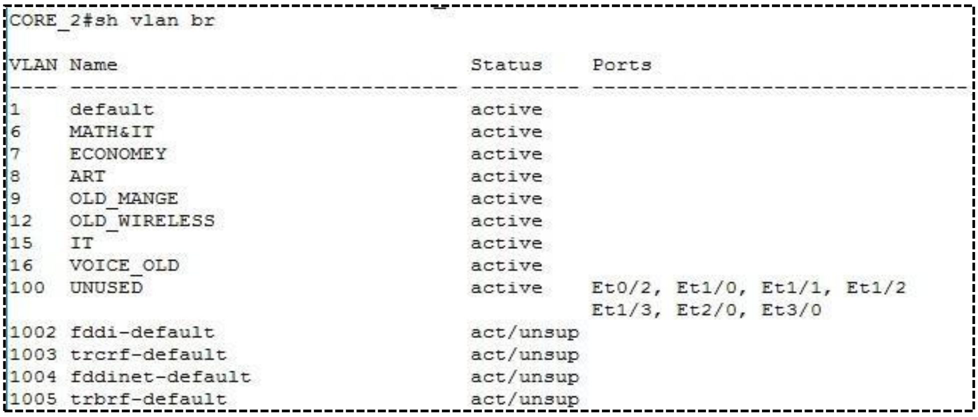
As the CISCO Hierarchal Design suggests, we should isolate the broadcast domains on a geographical base where the single VLAN should not span between multiple buildings (unless needed). In our project, we developed the concept one more step by creating a VLAN per department event if the departments are sharing the same building. This design will offer many advantages toward the main goal of creating more secure and scalable network and some of these benefits are decreasing the size of the broadcast domain and the noisy traffic on the segment will be less and here we are speaking about the broadcast and multicast traffic inside the VLAN. Minimizing the broadcast domain will provide a cleaner traffic with less TCP retransmit and packet loss issues.

The second advantage of creating a single VLAN per department, that it will provide a solid base for any kind of traffic engineering. All the rules and regulations applied to a single VLAN traffic will be kept within the VLAN boundaries and not affect the other VLANs which gives much more flexibility when configuring any traffic engineering or quality of service solutions. There is a security aspect to this design also where any type of layer two attacks will keep within the VLAN that is under the attack because VLANs are incapable of communicating with them on layer 2 base and need a layer 3 device to act as a gateway for the traffic.

Our design involves two campuses. Within Balgat campus, we have three departments where each one of them will have its own VLAN beside five general purposes VLANs that span all over the campus to add up the total to 8 VLANs. The table and figure below explain the name of the VLANs (which have been by their functionality), the port capacity that needed for each VLAN on the Access Layer switches and the IP address subnet that used by the VLAN:

Table 1 VLAN Allocation For Balgat Campus

Name of VLAN	Role	Size	Subnet
Management	Manage	255 host	192.168.22.0/24
Wireless	Wireless service	1024 host	192.168.14.0/22
VOICE	Phone service	255 host	192.168.32.0/24
Unused	Unused ports	255 host	-
IT	Manage entire network	255 host	192.168.26.0/24
Art	Art department	512 host	192.168.24.0/23
Economy	Economy department	512 host	192.168.18.0/23
Math and IT	Math and IT department	512 host	192.168.8.0/23



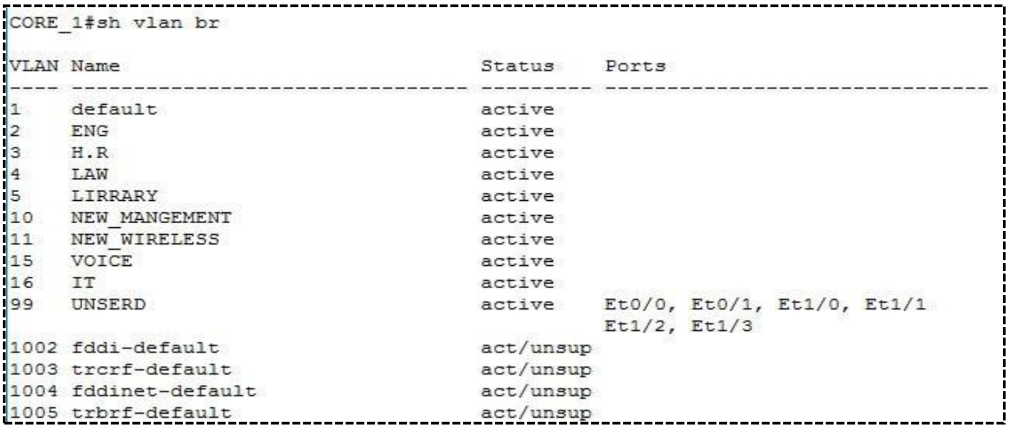
```
CORE_2#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
6    MATH&IT                          active
7    ECONOMEY                         active
8    ART                              active
9    OLD_MANGE                        active
12   OLD_WIRELESS                     active
15   IT                               active
16   VOICE_OLD                        active
100  UNUSED                           active    Et0/2, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et3/0
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Figure 7 VLANs within Balgat Campus

In the new campus, we also have four departments with three dedicated VLANs and five general purposes VLANs including the voice VLAN for the voice-over-IP communications, wireless VLAN for the wireless coverage and the management VLAN as the table and figure showing bellow:

Table 2 VLAN Allocation For New Campus

Name of VLAN	Role	Size	Subnet
Management	Manage	255 host	192.168.20.0/24
Wireless	Wireless service	1024 host	192.168.10.0/22
VOICE	Phone service	255host	192.168.31.0/24
Unused	Unused ports	255 host	-
IT	Manage entire network	255 host	192.168.28.0/24
Engineering	Engineering department	512 host	192.168.0.0/23
Human Resources	H.R. department	512 host	192.168.2.0/23
Law	Law department	512 host	192.168.4.0/23
Library	Library building		192.168.6.0/23



```
CORE_1#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    ENG                              active
3    H.R                              active
4    LAW                              active
5    LIRRARY                          active
10   NEW_MANGEMENT                    active
11   NEW_WIRELESS                     active
15   VOICE                            active
16   IT                               active
99   UNSERD                           active    Et0/0, Et0/1, Et1/0, Et1/1
                                                Et1/2, Et1/3
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Figure 8 VLANs within New Campus

Beside the VLANS that dedicated to each department, we have some multi purposes VLANs that spans between the two campuses because the nature of their functionality and these VLANs are:

- Voice VLAN: CISCO environment provides the capability of separating the Voice-over-IP traffic in a dedicated VLAN. That will prove more security since this traffic will be first separated from the normal traffic and secondly it will be encrypted beside while having this feature we still treat the end user ports as access ports and feed them with normal VLAN traffic and voice VLAN traffic instead of the need to configure them as the trunk. The third advantage that voice traffic will have its own automatic QoS configuration to dedicated the necessary resources due to its nature that is using UDP and cannot tolerant the delay or packet loss.
- Wireless VLAN: this VLAN will provide the underlay for the wireless coverage all around the two campuses where people can connect their personal devices to a more secure environment that will provide them with access only to the authorized sites with a decent bandwidth rate.
- IT Management VLAN: this VLAN will be used to control and access our IT resources as our switches and routers mostly through SSH protocol. Due to its sensitive function of this VLAN, it should provide very high-security measurements from layer 2 all the way to layer 3.

3.4 Redundancy

Redundancy is one of the most important aspects of the modern networks since downtime cannot tolerate. Increasing the resilience of the network to have a work around any issue in a way to ensure the uptime is getting more and more important. There are many faces for the redundancy on both the physical and configuration parts of the network. Speaking about hardware redundancy. It might be obvious that having redundant hardware is the easiest redundancy solution (which might be the case if the cost is not a factor) this not the most efficient one for a couple of reasons.

starting with cost aspect where increasing the hardware will take the cost of building the network up in a high percentage and the second reason, that it will increase the complexity of the network for managing, cabling, monitoring and configuring. For these two reasons, we will use Port-Channel technology.

Ether-Channel (Port-Channel): - Increasing transmit speed and use redundancy line can be through this technology. Port-channel works on bundling two or more physical links (up to 8) to play as one logical link in order to invest links speed. For example, if we bundle 8 links (1 Gbps for each) the capacity will be 8 Gbps. If 10 Gbps for each link the total will be 80 Gbps. The benefits of using this technology are as follow:-

- Higher bandwidth: It bundles more than one link speed into one logical port that will increase speed.
- Provide load-balancing: It uses an algorithm to balance amount of traffic through each participant link. Instead of passing entire traffic through one link, port-channel balances this traffic using many attributes.
- Offer a redundant path to get uplink devices where if there is any problem in one participant link the other link can carry the traffic for failure link.

Figure 9 explains the benefits of using port-channel. Instead of using one link, it will invest the speed of each participated link (3 links). But, without port-channel, just one link will work (depending on STP, it will be *Root Port*) that means losing those speed. Figure 10 shows that.

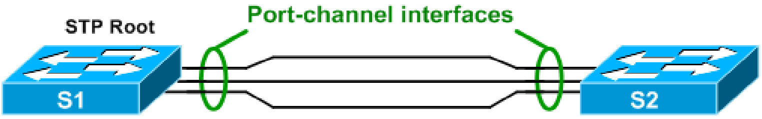


Figure 9 STP with Ether-Channel

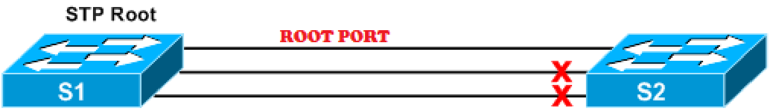


Figure 10 STP without Ether-Channel

There are some rules should pay attention to them when decide to use this technology:- [27]

- Each link has the same duplex.
- Same ports' mode whether it is (access or trunk mode).
- EtherChannel must use same mode (PagP (Port Aggregation Protocol), on, LACB (Link Aggregation Control Protocol))
- Links type must be same layer either layer two or layer three.
- Any difference in one link it will fail to bundle them.

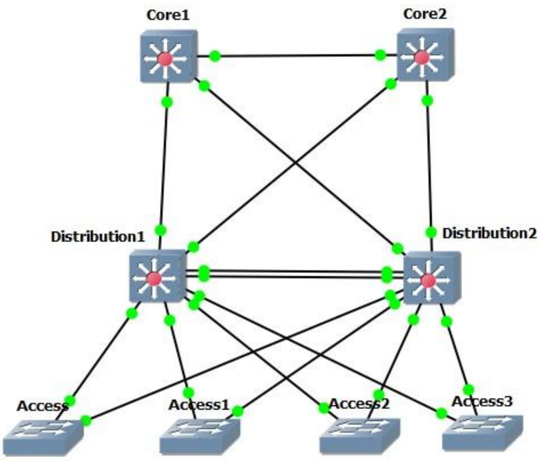


Figure 11 Redundancy without Ether-Channel

Figure 11 shows the traditional means of redundancy by using the main device and a backup device for it. This means adding more cost to the main cost for building a campus network.

The alternative redundancy solution is providing the physical redundancy through the devices that already in service like having a reliable hardware and use stackable and modular hardware. A problem in part of the hardware will keep the rest of the system up and run. The technology that we will rely on for the redundancy will be the *port channel* redundancy where multiple interfaces will be mapped together as one virtual interface. Therefore, if a physical interface within the port-channel went down for any reason the rest of the interfaces sharing the same port channel will keep forwarding the traffic. This feature not only will provide a redundancy on the interface level but also will increase the capacity of our uplinks by grouping them in one spanning tree instance. Thus, the all will be in forwarding mode instead of been blocked by STP. The below figure shows that.

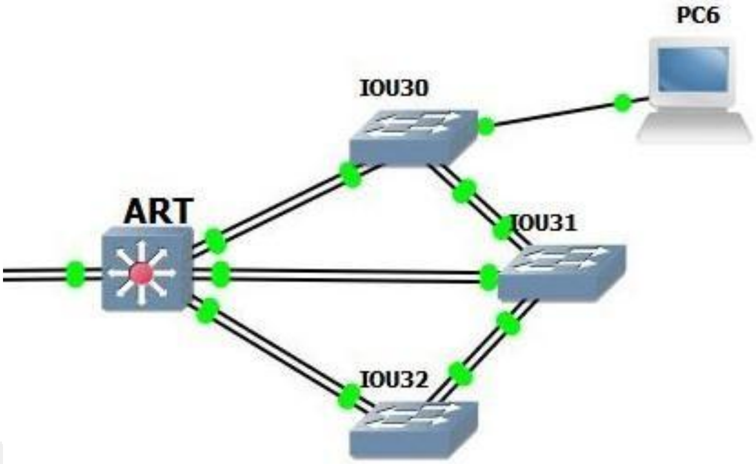


Figure 12 Redundancy with Ether-Channel

Each side has a specific port-channel with its neighbor. As above figure, we can observe that to connect access devices with uplink (ART device), it could through two or more paths, one path works and the others stand by, this method save money and offer a redundant path to keep our network working as well.

3.5 Physical Layer

This part will cover all the physical aspects of the data centers including location, equipment, standards of cabling and the physical security. Covering all the security threats and challenges.

3.5.1 Location

The location is one of the crucial elements in designing the data center due to many factors as providing the needed immunity against natural disasters as floods, earthquakes...etc. That is why planning the physical location considered a security application where the location should be accessible only by authorized people using any authentication mechanism as smart IDs or fingerprints. In addition, the location should reflect the accessibility of the data center from the connectivity and cabling stand of the pin where it is easy to bring all the fiber and other connections to the data center from both inside and outside the campus [30].

3.5.2 Building

This part will focus on the criteria of selecting the data center and the conditions that must be existed to secure it [31]. One of the criteria is monitoring and maintaining a controlled environment where all the devices can operate in an efficient way and eliminating all the threat factors caused by unexpected issue as humidity and temperature. Usually, the temperature is a critical part of any data center design because the nature of the devices in the data center that needs to operate within the well-set temperature range. Moreover, these devices are a great source of heat, that is why most data centers have central and redundant AC units. The security of the data center is another factor influencing the location of the data center where the data center should be fully secure and under monitoring. The monitoring includes security personnel all around the clock, surveillance cameras, and access control systems with access logs.

Firefighting system is another component in securing the data center. Where in the case of fire, we need to make sure that we have the system that can take down the problem in the least time but also by the least damage to the infrastructure and devices, which is why firefighting systems in the data centers use chemical powder instead of water.

In our scenario, we have two campuses, where each of them consists of multiple buildings with two floors each, more information about the campuses as follows:

Balgat campus has three departments:

- Mathematics and IT Department: consist of two floors. The first floor has two labs with 20 computers each, and a couple of administration offices. In total, the port capacity needed to cover this floor is 52 ports, which means the need for three switches with 24 ports each, where the rest of the 20 ports will be for the future expansion. The second floor is the same as the first one so the will need the same capacity which makes the total number of access switches needed for this department is six.

- Economics Department: it consists of two floors, where the first one has the classrooms which can be covered by 50 ports which is the equivalent of three switches and the second floor has the faculty and staff offices that need 60 ports and can be covered by three witches as well. The total of switches needed for this department is six.
- Literature Department: as all other departments, this one has two floors. The first floor has a lab, two classrooms and couple of offices that need 46 ports in total, which means three switches to cover. The second floor has only offices that need two switches to cover. Therefore, the total number of switches in this department is five.

The new campus has four departments:

- Engineering: this department has many majors as computers, civil, mechanical, electronic and communications. From a design perspective they all share the same plan, thus, we will take computer engineering as an example. It has two floors made of two labs with 30 ports each and 20 ports for faculty and staff, the total number of needed switches will be four switches taking in considerations the future expansion. Based on the above the total number of switches in the engineering department will be 16 (since we have four major departments with four switches each).
- Human Resources: it is also made of two floors. The first floor consists of 10 offices with 4 ports each which make 40 ports in total and it is the exact same case with the second floor which makes the total number of ports 80 which can be translated to 4 switches.
- Law Department: As all other departments, it has two floors. The first one lab, two classrooms and a couple of offices with 46 ports which means three switches to cover it. The second floor has only offices that need two switches, which makes the total switches in this department five.
- The Library: will need six switches to cover its three floors that have two labs, offices and the Wi-Fi services.

Adding all the information together, we will need 31 switches to cover the new campus and 17 switches for Balgat campus, which makes the total of the access switches 48.

For the distribution layer switches, we will need a single switch per department, so the total will be three switches for Balgat campus and seven switches for the new campus. The total number of the distribution switches that we will have is 10.

All the connections from the distribution switches will go to a single high-availability core in each campus. And there is a provider router in the new campus acts as the gateway of our network where traffic from both campuses need to go through it to go the internet.

3.5.3 Equipment

There is a wide spectrum list of devices used or needed in any data center including (but not limited to) servers, firewalls, patch panels, wireless controllers…etc [32]. Our study will cover the switches and routers which are the heart of any network and responsible for moving (switching & routing) the traffic within our network parts and to other external networks.

3.5.4 Cabling Types

There are many cables types and standards that we cannot cover all of them, instead, we will cover only the cabling types and standards that we are using in our project and in this case, we have three types of cables:

The first one is the connection between the end users and the access switches and for this case we will use Unshielded Twisted Pair (UTP) CAT 6 because this type of cable provides a fast data transfer rate up to 1Gbps of data which should be more than enough for the end users without causing and drops or traffic bottle-nick . The UTP is designed to be used indoor because it is not shielded which makes it cheaper than the Shielded Twisted Pair (STP). Both can carry the signals up to 100 M. The main difference between the STP and UTP cables that the STP cable had a metal shield covers the cable providing extra protection from the outdoor conditions as the weather and electric signals and since these factors are not included in our indoor usage, will go with UDP [33].

The second type of connections between all the switches and the routers within the same campus. This connection is between the access switch and the distribution from one side and the core and the distribution on the other side. We will use a Multi-Mode Fiber (MMF) connection as this type of fiber provides a very high speed in data transferring that the normal copper cable cannot provide, and it is the best practice to use multi-mode fiber optic within the same building or indoor where it can transmit the data up to 10 KiloMeters [34].

The third type of connections will be used to connect the two cores between our campuses and to connect our ISP router with the ISP. We will use Single-Mode Fiber (SMF) [35] for this connection that is highly protected comparing to multimode fiber, since it will be used outside and through long distances that go up to 100KM and it provides a high capacity of bandwidth that is needed to move all the traffic outside our campus. The main problem could occur with fiber cables is when there is a cut the fiber, the solution for this problem through Unidirectional Link Detection Protocol (UDLD).

UDLD**: -** Fiber cable has two sides one to transmit (TX) and the other to receive (RX). What will happen if a cut occurs on one side of a fiber? One side will continue sending traffic, the other side will receive nothing. How can we know that? CISCO proprietary UDLD answer that. UDLD is a layer two protocol works with layer one (physical layer) to determine the state of fiber cable by sending a message every 15 seconds. In case, there is a problem in one side of fiber the other side will know when there is no reply received, sending data through the damaged side will stop and put this port in errdiable. Enabling UDLD protocol between two neighbors devices on two sides. The participation devices must support this protocol and enable it on ports that connect two terminals. In case, there is a cut occurred it will send a message on console screen and port 1/2 shutdown as follow:-

```
"UDLD-3-DISABLE: Unidirectional link detected on port 1/2. Port disabled"
```

The following figure shows the UDLD problem

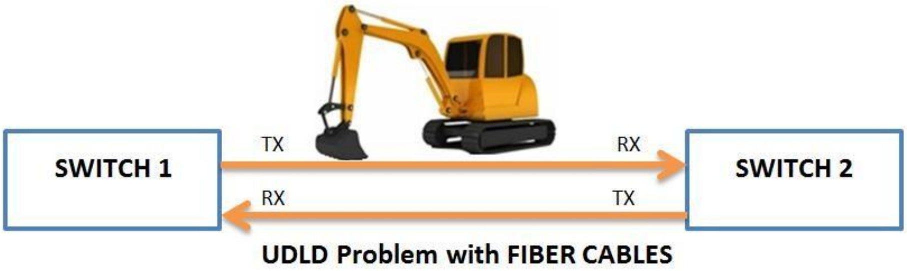


Figure 13 UDLD Problem with Fiber Cables

UDLD has two modes for ports (normal, aggressive) the difference between two modes of action that will take by UDLD protocol. Normal mode UDLD Protocol mark the state of port as undetermined and send a sys message to the administrators, but with aggressive mode UDLD tries to re-establish the state of port by sending a UDLD message ever 1 second for about 8 seconds in hope to get answer, if not, UDLD will put this port in errordiable and send an error message to the console.

3.5.5 Network Devices

As we are following CISCO campus design in our network, we will go with CISCO hardware for the components of the network for many reasons that can summarize in a couple of points:

- Very stable hardware and software compared to other vendors.
- CISCO leading the networking standards and they have a long list of proprietary technologies and protocols that we need to use like CDP and UDLD.
- CISCO have a full line of products that covers all layers of our project starting from the access layer all the way to the core layer
- The advanced support and documentation that CISCO provides for their products.
- High compatibility with the rest of our data center equipment as the firewalls, servers and load balancers.
- It is easier and more efficient to find technical people working with CISCO environment comparing to other vendors.

Starting with the access layer, we have a couple of options for the hardware in this layer that are mostly part of the catalyst series, where we will go with one of the latest of them, which is CISCO C2960X-24. The reasons behind choosing this model that it has the needed port's capacity with a port speed of 1Gbps with up to 10Gbps for the uplinks and providing a fiber optics connection for the uplinks toward the distributions. This switch is rich with its layer2 and security features that needed in the access layer and its robust hardware that is critical for the access layer since it is the layer that faces most of the hardware issue. The CATALYST series also provide the stacking feature that we will use to increase the flexibility and decrease the configuration on the access layer [36].

The distribution layer will use CISCO CATALYST 4500 series for many reasons as the high port density (all fiber optics ports) that needed to cover all the connections coming from the access layer switch and the uplinks going toward the core layer. These switches have a strong computing capacity as a high number of queues and TCAM (Ternary Content Addressable Memory) size which makes it ideal for fast switching. The hardware itself is very stable and redundant as a line card and power redundancy. These switches are multi-layer switches thus we can use them depending on the size of our network where we can configure them as layer 3 switches when having a huge network and need to decrease the pressure on the core layer.

Our choice for the core layer is the CISCO CATALYST 6500 series (6509 and 6511) which are very capable devices from both the hardware and the software perspectives. We cannot afford any downtime in the core layer since it is the heart of our network and any problem in this area will stop the inter-VLAN communications. Redundancy is one of the most important factors to take in consideration when choosing and configuring this layer’s devices and the 6500 series is fully redundant with load of features as the multiple power supplies, line cards, supervisors and even the VSS (Virtual Switching System) feature that allows two switches to act as one virtual device.

3.5.6 Best Practices

- It is a good practice to have an automated way of taking a copy of all the data and configurations of our systems in case of any failure. There are many applications for the data backup whether on a periodic base or at the time of any change in the current version of the data. The backup data should be well organized and saved and be accessible only by authorized personnel.
- Makes sure that our software and hardware are up to date as often as possible. Having a stable device does not mean that we can ignore updates and upgrades because these update will not provide new features only but also will fix and provide solutions to any possible bug that the current version has. The procedure of the upgrade in the network level should be prepared in advanced because it will cause an outage in most of the times due to the need to reload the device. Another important factor related to the hardware of the network that all the switches and routers have an End of Life (EoL) support, that means at a certain point the vendor (CISCO in our case) will stop supporting this hardware and will no longer issue version upgrades and bug fixes for it. That is why most of the papers suggest keeping the network fresh by replacing the hardware (mostly in the access layer) every five years.
- Follow the best design clues for the layer one like the type of cables and the cabling standards and the distances between the telecom rooms and the end users to avoid any traffic congestion and lost.

3.5.7 Physical layout

After covering the types of the hardware, cables and the standards that we will follow it is the time to discuss the connectivity on the floor level where we will have a telecom room in each floor. The function of this telecom room is to have access layer switches and connect them to the end users from one side and the distribution switch from the other side. Since we are using CAT6 cable for the end user connectivity the location of the telecom room should be in a central location to provide a full connectivity in all directions with less than 100M each, since this is the maximum distance that the CAT6 cable can transmit the data.

As any other IT or data center room the telecom room should be fully secure and safe from temperature, humidity, and fire conditions and we should grant access to authorized personnel only.

One of the handy technologies that will make life easier in the access layer is the stacking technology where a couple of switches (up to 8 switches in C2960X) can be cabled and stacked together to act as one virtual switch. The benefit of this technology that it will reduce the needed configuration, management, and monitoring and will provide a type of redundancy besides decreasing the needed cabling between the access layer and distribution layer. A single switch on the stack will be elected as the master that controls the other switches [37]. The following figure shows that.

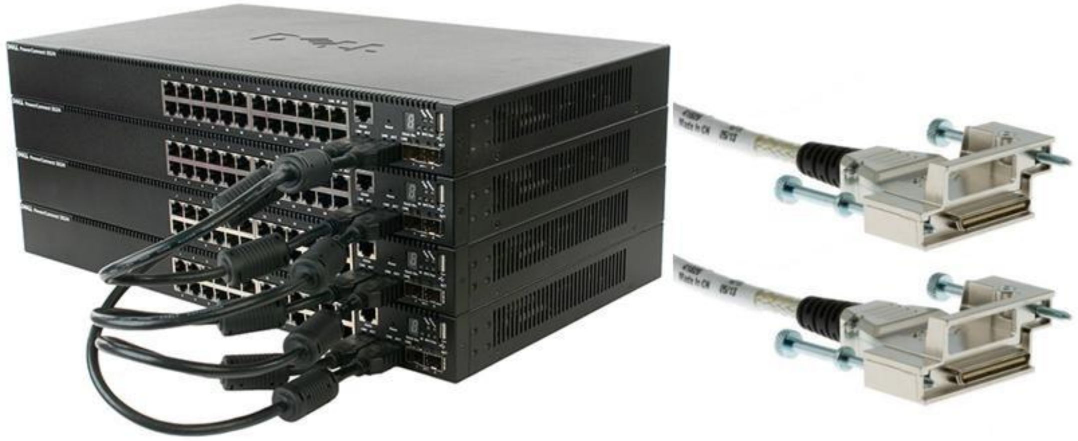


Figure 14 Switch Stacking

As one of the important features and services that should be available on any campus, wireless services need to configured in our environment to cover the whole campus in a way allows all the staff, faculties, students and the guests to connect and have access to the different online services. As the wireless services considered a weak link in the security chain we need to take a good care of securing this services in a way prevents any unauthorized access either by authorized people or to services that they do not have the permission for them. Roaming is an important part of the wireless services all around the campus in a way ensures the coverage, connectivity and making sure that there are no congestion points in the coverage. To have a full integration of wireless service all around the campuses we used single VLAN for the wireless to have more control over its functions as QoS and authentication and will need to use Wireless Lan Controller (WLC) appliance to control the synchronization between all the access points.

Voice VLAN is an important feature also in the campus design where all the voice applications will be separated in a dedicated voice VLAN that have couple of benefits like providing more security because the voice traffic will be isolated from the normal traffic, as a result, any data collection or capture will not lead to voice traffic leak. Since the voice applications use UDP and need a real time response it is crucial to have a higher QoS comparing to another type of traffic, which the voice VLAN provides by default. The other advantage of using the voice VLAN that we will no longer need to have two cables going to the same person one for the normal data and one for the phone instead the end user will have the same cable carrying his data and voice traffic.

3.5.8 The Topology:

The topology for Balgat campus of Cankaya University will be as follows:

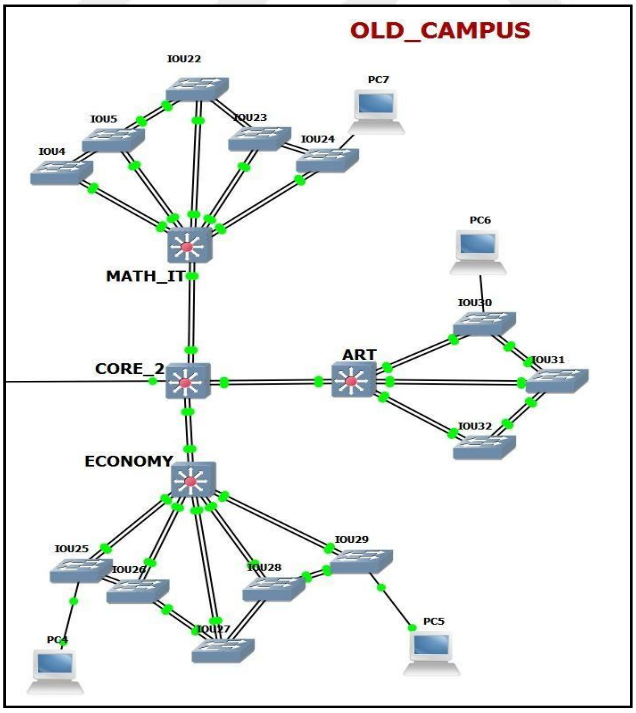


Figure 15 Balgat Campus Topology

While the topology for the new campus will look, like

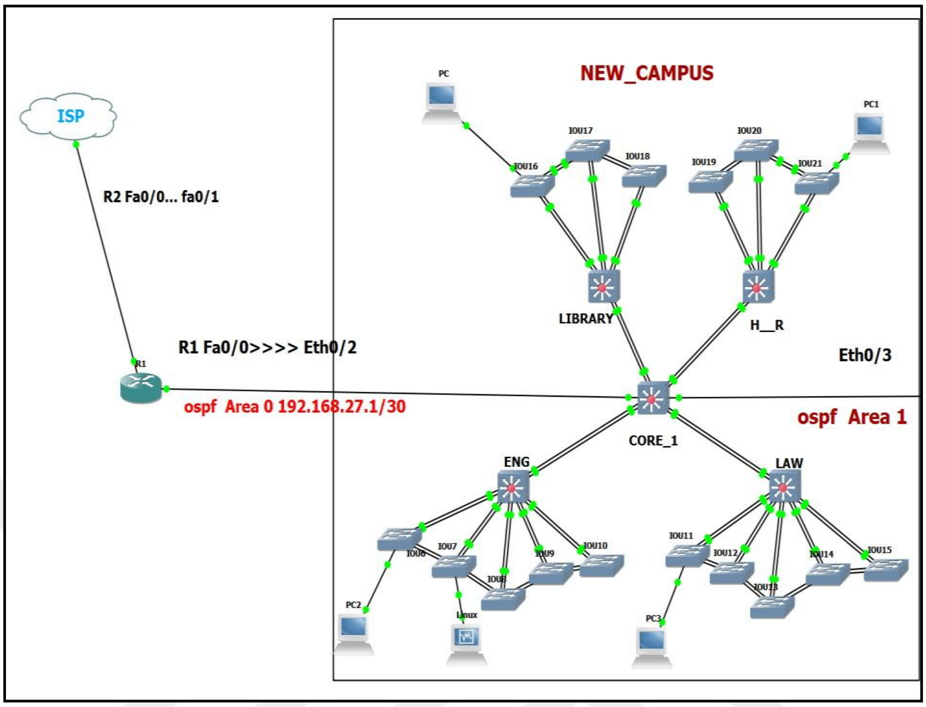


Figure 16 New Campus Topology

Figures 15 and 16 show the topology for two campuses. The design is identical between the two campuses. Starting with the access layer switches where every switches group represents a floor on the department and these access switches will be stacked together as a virtual single switch. The access switches have fiber uplinks toward the distribution as part of a port-channel for capacity and redundancy and connect with the access switch next to them (in a box design) as an alternative path in case of losing the whole path toward the distribution. On the distribution level, all the links coming from the access switches will be grouped and will have port-channel uplinks toward the core switch in the campus. The core layer switch connects to the distribution switches with Multi-Mode Fiber from one side and to the core switch on the other campus through a Single Mode Fiber on the other side. All the connections between the switches are fiber, Gbps or higher and configured as trunks to allow all the need VLANs. There is an extra connection on the core layer switch on the new campus which is the connection to our ISP router.

3.5.9 Security Challenges and Solutions in the Physical Layer

Some of the security challenges in the physical layer include:

- Unidirectional problems with the fiber connections.
- The physical security of the devices and the data centers.
- Physical security related to choosing the wrong or less secured devices and models.
- Security threats related to natural disasters as floods and volcanos.

Some of the security features in the physical layer:

- Around the clock monitoring of the data centers and the telecom rooms including the vital environmental elements as the temperature and humidity.
- Choosing a secure location for the data centers and telecom rooms to meet the security standards and provide safe locations in case of any natural disaster.
- Having continues data and configuration pack ups in case of any data loss or the need to a hardware replacement.
- Using redundancy cabling between the switches in case of any cable cut or a full path become unavailable.
- Providing a monitored and authorized access to the data centers and telecom rooms based on smart cards and fingerprints with full events logs.
- Configuring the UDLD feature on all the fiber cables to prevent the loops or packet loss in case the fiber cut in only one transmit or receive pairs.
- Use only standards and well-known vendors (CISCO in our case) to make sure that all their products are fully secured.
- Use auditing agencies to test and evaluate the security of our premises.

3.6 Data-Link Layer

This layer is so far one of the most important rich-in-functions layer in the network due to its nature and functions. The most important functions of this layer are error detection (although no data correction happening at this layer) the second function that it set the base for the data transmit over the media or layer one where the data coming from upper layer as packets from layer three will be clustered as frames. This layer helps in building the next hop map for the inter-network communications where this layer is responsible for the MAC address that is used to forward the traffic within the same network.

Since this layer is the richest in functions and the possibility of loops in this layer there are serious security threats that need to be addressed and planned well, which we will do every time we implement any layer two function.

3.6.1 Layer Two Technologies:

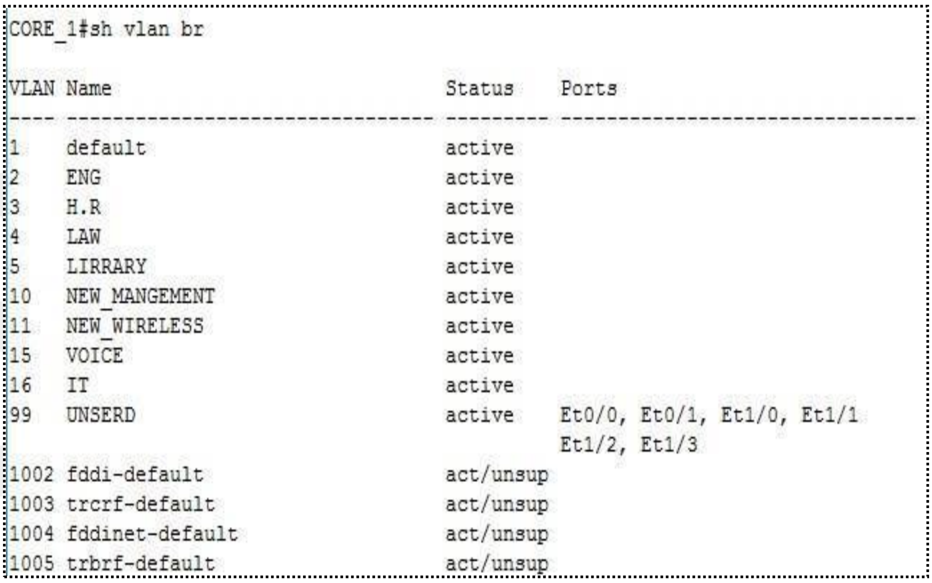
1. **Virtual Local Area Network (VLAN)**: this feature is one of the most used functions in any networking where a physical broadcast domain (the whole switch) can be divided into smaller broadcast domains where we can add or remove interfaces from any given broadcast domain. The advantage of this function include:
    - More control over the traffic separation that helps in case of traffic engineering and quality of service or any other type of filtration.
    - More security where any loop or security threat within a VLAN will be kept within the borders of the VLAN.
    - Cost saving: this function helps to take the implementation cost down dramatically because there is no more need for physical devices for each network in our environment.

    Because of using the VLAN feature all the communications between the switches should be tagged with the VLAN number, as a result, there is no traffic leaking except for the native VLAN that will not be tagged by default. The connections in the network will be two types: trunk where all VLANS can be sent over the same media tagged to keep them separated. The second type is access where the media is passing only one VLAN traffic.

    It is always a good practice to keep the VLAN domain as small as possible to decrease the possibility of the loops and traffic storms within the layer two domain. That is why CISCO recommends keeping the VLANs separated geographically as much as possible and makes the inter-building communications as layer 3 which we do in our design (except for a couple of VLANs that we need to span all over our network).

We have a dedicated separated VLAN for each department that we have therefore in the case of any traffic engineering or quality of services needed we can do that easily on the layer two level.

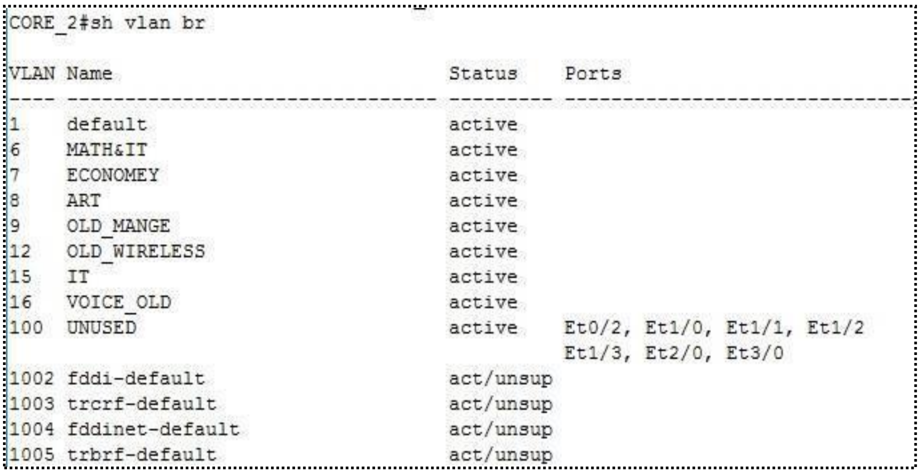
The list of the VLANs that we have for the new campus can be seen from the shown bellow:



```
CORE_1#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
2    ENG                              active
3    H.R                              active
4    LAW                              active
5    LIRRARY                          active
10   NEW_MANGEMENT                    active
11   NEW_WIRELESS                     active
15   VOICE                            active
16   IT                               active
99   UNSERD                           active    Et0/0, Et0/1, Et1/0, Et1/1
                                                Et1/2, Et1/3
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Figure 17 VLANs in New Campus

For the old campus the list is:



```
CORE_2#sh vlan br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
6    MATH&IT                          active
7    ECONOMEY                         active
8    ART                              active
9    OLD_MANGE                        active
12   OLD_WIRELESS                     active
15   IT                               active
16   VOICE_OLD                        active
100  UNUSED                           active    Et0/2, Et1/0, Et1/1, Et1/2
                                                Et1/3, Et2/0, Et3/0
1002 fddi-default                     act/unsup
1003 trcrf-default                    act/unsup
1004 fddinet-default                  act/unsup
1005 trbrf-default                    act/unsup
```

Figure 18 VLANs in Old Campus

2. Virtual Trunk Protocol VTP

The use of VLAN in almost every network introduced the challenge of keeping the VLAN database updated all around our environment. The manual update (adding and removing VLANs) is becoming a challenge especially in case of large networks (campus in our case), which led to the introduction of VTP. The way VTP works is by having a single point (switch) in the network populating the VLAN database to other devices thus in case of the need for any update on the database the update has to come through this centralized point. There are many advantages of using the VTP as:

- Having a centralized point of control over our VLAN database where all the database updates will take place.
- Decrease the chance of any VLAN discrepancy through our environment.
- Less effort to create, manage and maintain the VLAN database.

The way that VTP works is, we have three modes for the switches. Server mode, where the switch is allowed to create and delete VLANs. Client mode, where the switches are getting their VLAN updates from the server and they are not allowed to add or remove VLANs. The third type is transparent, where the switch in this mode has its own VLAN database that can add and remove the VLANs only locally on its *vlan.dat* file and has no interaction with the VTP domain. Each switch has what called a revision number reflect how up to date its VLAN database is. Therefore, when we connect a new switch to our domain it will interact with the VTP server providing with its revision number. If the server’s revision number is higher then the server will share its VLAN database with the new switch otherwise, the new switch will give its VLAN database to the server who will share it with the rest of the domain. We have three versions of VTP with enhancements and new features with every new version. The most recent version is version 3 and it is the most stable and secure version with some features that are not available in the other versions as the support of private VLANs and the feature of the primary and secondary server.

Due to the nature of the VTP, it posted a lot of threats to any network that is why we should always take it very seriously because it might take our network down by changing or deleting our VLAN database either through a poor design or by hacking our VTP domain.

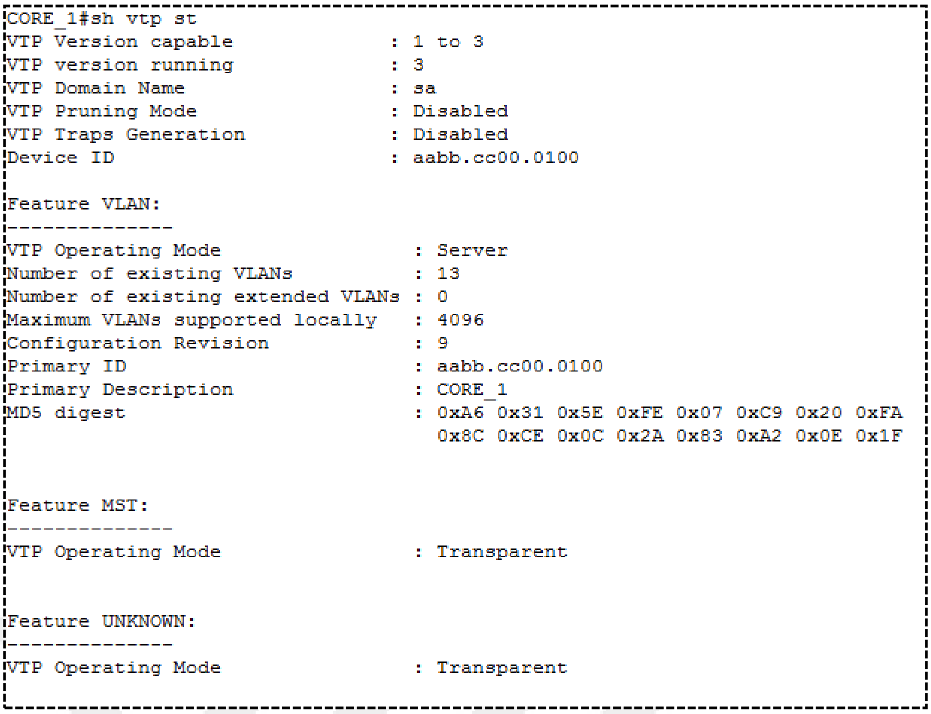
The threats that facing the implementation of the VTP are:

- A switch with a higher revision can change our VLAN database.
- Having more than VTP server device within the domain.
- Sniffing the VTP communications.
- Having no domain name which will allow any new switch can join our VTP domain without checking.

For the above reasons we are implementing VTP version 3 that has many security features providing the right answers to the previous concerns as:

- Configuring a single VTP server in each campus and it is the only authorized switch to manipulate the VLAN database. Besides being the server, the switch will be acting as the active server, which is a feature available only in VTP v3. The core in each campus will act as our server.
- Configuring a domain name, the new switches cannot join our VTP domain by default. The VTP domain in our case will be (sa).
- Configuring an encrypted password where the switches need the authentication to start the communications with the server even if they are in the right domain. The password that we are using is (sa) (we used a very easy password to show the new strong feature in VT v.3) and it will show encrypted on the show logs.

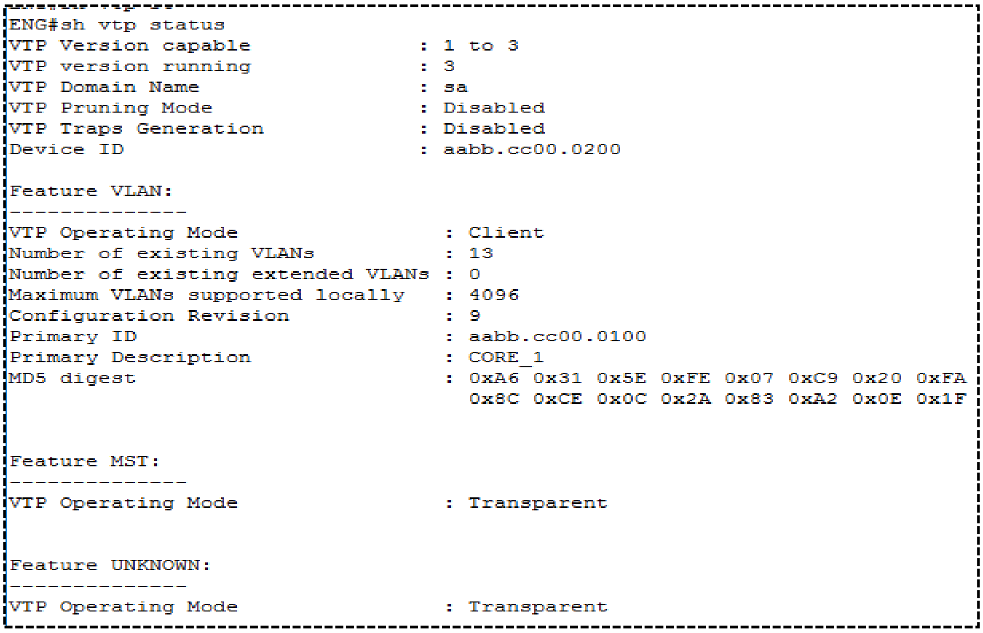
The “*show vtp status logs*” bellow showing the information of the VTP from the core_1 perspective as its role as VTP server, the domain name, the use of the MD5 and the revision number.



```
CORE_1#sh vtp st
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : sa
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0100

Feature VLAN:
--------------
VTP Operating Mode                : Server
Number of existing VLANs          : 13
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 4096
Configuration Revision            : 9
Primary ID                        : aabb.cc00.0100
Primary Description               : CORE_1
MD5 digest                        : 0xA6 0x31 0x5E 0xFE 0x07 0xC9 0x20 0xFA
                                    0x8C 0xCE 0x0C 0x2A 0x83 0xA2 0x0E 0x1F


Feature MST:
--------------
VTP Operating Mode                : Transparent


Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
```

Figure 19 VTP Server Status

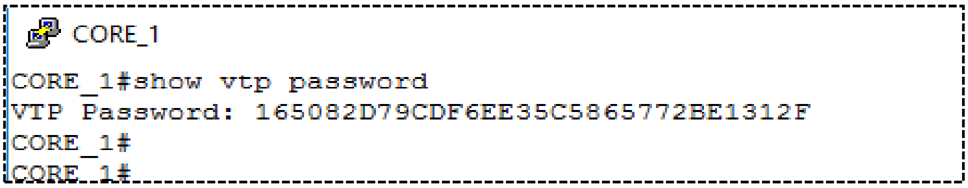
Show vtp status on the ENG_distribution switch, on the second hand showing the same information except that this switch is the client not server and having the same domain, revision and number of VLANs and the server:



```
ENG#sh vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : sa
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.0200

Feature VLAN:
--------------
VTP Operating Mode                : Client
Number of existing VLANs          : 13
Number of existing extended VLANs : 0
Maximum VLANs supported locally   : 4096
Configuration Revision            : 9
Primary ID                        : aabb.cc00.0100
Primary Description               : CORE_1
MD5 digest                        : 0xA6 0x31 0x5E 0xFE 0x07 0xC9 0x20 0xFA
                                    0x8C 0xCE 0x0C 0x2A 0x83 0xA2 0x0E 0x1F


Feature MST:
--------------
VTP Operating Mode                : Transparent


Feature UNKNOWN:
--------------
VTP Operating Mode                : Transparent
```

Figure 20 VTP Client Status

The show VTP password command will show the digest of the MD5 password that we are using instead of showing the clear text password, which is another security feature.



```
CORE_1#show vtp password
VTP Password: 165082D79CDF6EE35C5865772BE1312F
CORE_1#
CORE_1#
```

Figure 21 VTP Password

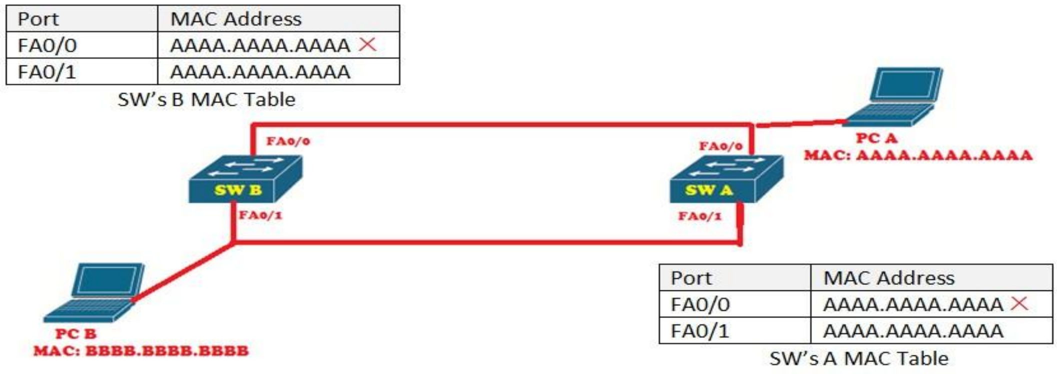
3. **Spanning Tree Protocol:**

   This is one of the most important technologies in any layer two domain because it is the only way to face the loops. It is crucial to find right flavor of STP to use in our network since there are many types of STP. The reason behind forming loops in layer 2 that the frame in this layer doesn’t have a Time To Live (TTL) field of the packet in layer 3 that will kill the frame automatically after reaching 0 instead of letting the frame looping endlessly in the domain. Implementing the STP will solve many loop-related issues as:

   - Traffic loops: with no way to kill the looping traffic these frames will keep looping in the layer two domain endlessly causing high CPU usage on the switches and high interface output traffic that will kill the legit traffic and in some extreme cases will take the whole layer two domain down. This reason is why we need to keep the layer two domain as small as possible.
   - MAC address table corruption: - is an ideal case we should have a single interface referring to the MAC address in our MAC address table. In the case of the loop will have multiple interfaces showing that they have access to the same MAC address, which will cause a loop in the domain.
   - Broadcast storms: the broadcast and multicast traffic (that is not destined to a single device) to the broadcast MAC address

FFF.FFF.FFF and 0000.0c07.ACxx for HSRP multicast will cause a loop if our network is not designed in a good way thus the broadcast or multicast traffic will keep looping within the domain.

The following figure show the loop without using STP



Port	MAC Address
FA0/0	AAAA.AAAA.AAAA ✗
FA0/1	AAAA.AAAA.AAAA

SW's B MAC Table

Port	MAC Address
FA0/0	AAAA.AAAA.AAAA ✗
FA0/1	AAAA.AAAA.AAAA

SW's A MAC Table

Figure 22 Layer Two without STP

The way STP works that within the network segment a single switch will be elected as the root and all the layer two traffic should flow through it. The root device should have two important features:

- Hardware capable of supporting and switching all the traffic passing through it.
- In a central location for the network segment making it easier to reach it by all other devices.

That is why we should have control over the selection of the root switch to match the above conditions.

The procedure of electing the root bridge is based on the following conditions:

- Bridge ID (BID): which is a number between 0 and 61440 increasing by the increment of 4096 and the default value is 32768. The switch with the lowest BID will be elected as the root. If we have a tie in the BID then moving to the next condition.
- MAC address: the switch with the lowest MAC address will be elected as the root.

Since all the switches have the same BID by default then the MAC address will determine the root bridge and the lowest MAC address (which means the oldest switch) will be the root bridge. We cannot allow this case because we will lose the predictability in our STP domain that is why it is better to manipulate the BID to set the root manually.

3.A Types of STP

There are many types of STP. We need to know the differences between them in order to take the right decision about which one to implement.

- Common STP: - is an IEEE standard 802.1D. All VLANs use same STP topology. This is suboptimal STP because other links waiting ROOT port to fail then, they may work. By default, when connecting more than one layer two device (switch), STP will active automatically, the lowest bridge ID and MAC address will be the root for STP. The 802.1D represents the first version of STP. Nowadays, it is out of services in real networks because it needs high convergence time to recalculate a new map if there is any change in the network has occurred. Time to recalculate a network simple STP need 50 seconds to complete it, but new high-speed devices need more efficient types of STP.
- Per-VLAN STP: - CISCO enhanced STP 802.1D to produce this type, which gives each VLAN a specific ROOT. PVST creates an instance for every VLAN, this will put more load to the CPU performance and memory usage. PVST+ is the update for PVST. It works under the standard of IEEE 802.1Q [28].
- Multiple STP (MSTP): - is an IEEE standard 802.1s, and CISCO enhanced it further. It works like PVSTP but instead of having a single instance per VLAN we can bundle a group of VLANs in one instance especially if they all have the same traffic path, which will reduce the resources needed to support its work as the CPU.
- Rapid STP (RSTP): - is an IEEE standard 802.1w, CISCO also enhanced this type to Rapid PVST+. The main goal behind RSTP is to

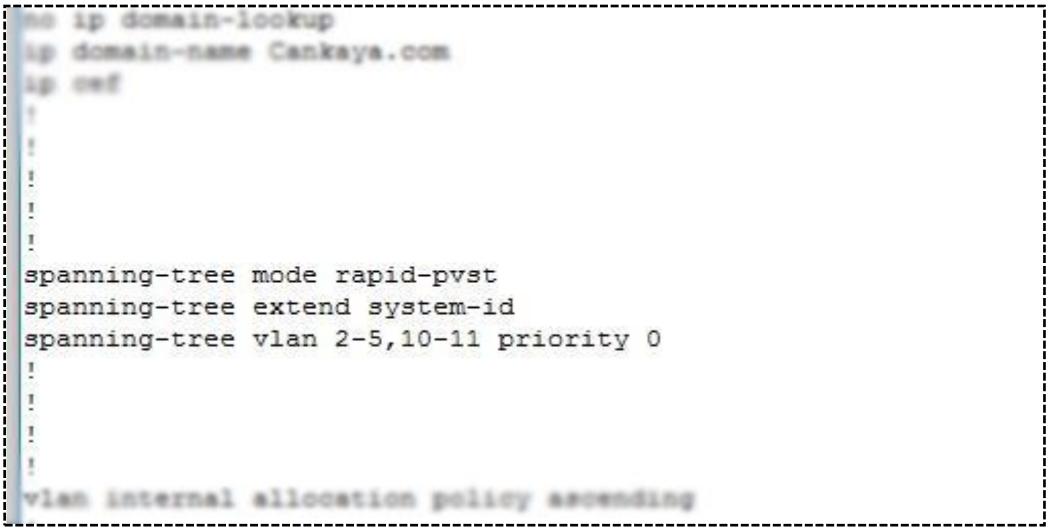
decrease the time of convergence, wherein previous STP, the convergence time is 50 seconds, but in RSTP could converge in (2 or 3 seconds) in some cases. RSTP decreased the port states from 5 states to 3 states by combining (Disable, Blocking, Listening) to one state (Discarding) and (learning, forwarding). RPVST+ separates VLANs by dividing them to many instances [27][28]. The following table shows all STP types.

Table 3 STP's Types Review

Protocols	Standard	Convergency	Ports States Number	Number of Tree
STP	802.1D	50 seconds	5	One
PVST, PVST+	CISCO	50 seconds	5	One for every VLAN
MSTP	802.1s	50 seconds	5	Two
RSTP	802.1w	30 seconds	3	One
RSTP (RPVST)	CISCO	30 seconds	3	One for every VLAN

From our perspective, Rapid-PVST is making the best option for the STP deployment due to the fast convergence that it provides compared to common STP and does not consume high hardware resources as the PVSTP.

One of the security challenges in the STP domain that a rouge switch takes the role as the root bridge that is why we are changing the bridge ID manually in a way making sure that the root will always act as the root by giving it the BID of 0. The distribution will be our backup in case we lost the core by giving it the second lowest BID 4096. The access switches will have the highest BID of 61440, which will prevent them from playing the root role.

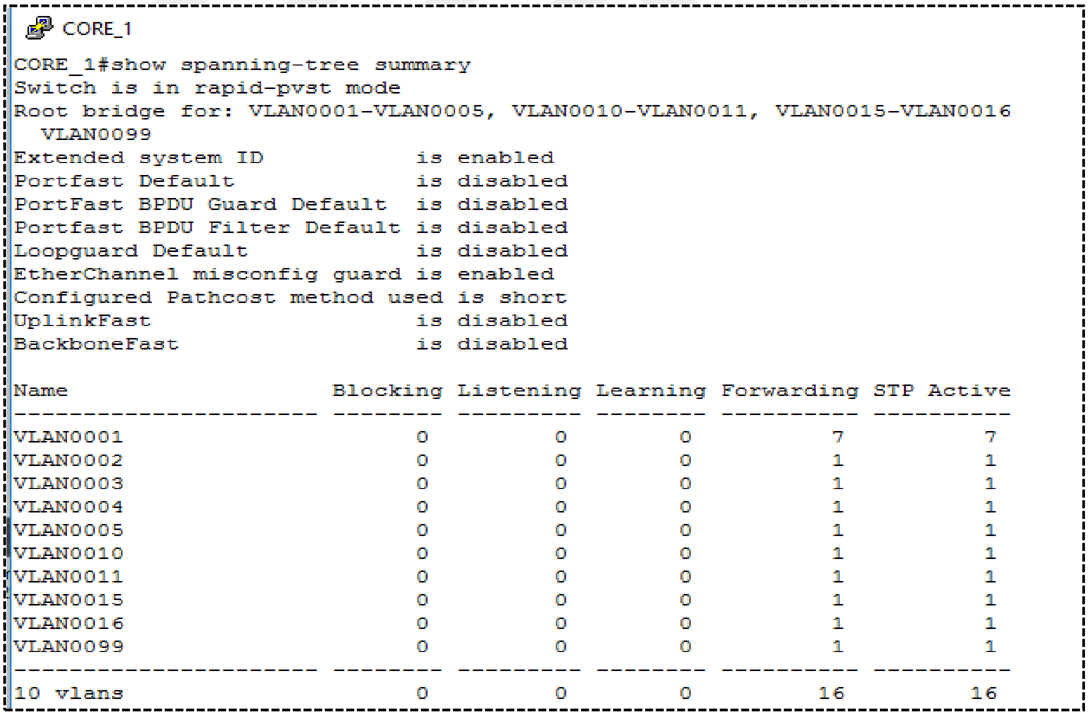


```
no ip domain-lookup
ip domain-name Cankaya.com
ip cef
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 2-5,10-11 priority 0
!
!
!
!
vlan internal allocation policy ascending
```

Figure 23 Spanning-Tree Priority

The figure above shows STP configuration on the core showing the priority value of 0 to make it the root.

The core is showing as the root for all VLANs as the following figure.

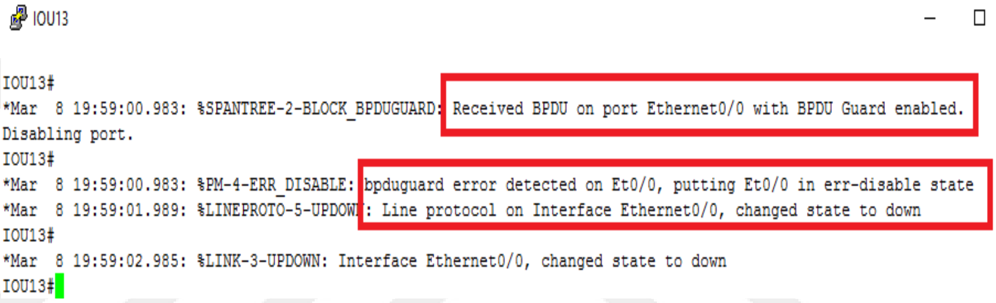


```
CORE_1#show spanning-tree summary
Switch is in rapid-pvst mode
Root bridge for: VLAN0001-VLAN0005, VLAN0010-VLAN0011, VLAN0015-VLAN0016
  VLAN0099
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
Configured Pathcost method used is short
UplinkFast                   is disabled
BackboneFast                 is disabled

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                     0         0        0          7          7
VLAN0002                     0         0        0          1          1
VLAN0003                     0         0        0          1          1
VLAN0004                     0         0        0          1          1
VLAN0005                     0         0        0          1          1
VLAN0010                     0         0        0          1          1
VLAN0011                     0         0        0          1          1
VLAN0015                     0         0        0          1          1
VLAN0016                     0         0        0          1          1
VLAN0099                     0         0        0          1          1
---------------------- -------- --------- -------- ---------- ----------
10 vlans                     0         0        0         16         16
```

Figure 24 Spanning-Tree Summary

3.6.2 Other Security Features in the STP Include

- **BPDU Guard**: - BPDU is the switches' language; they are exchanging BPDU between them. BPDU carries much information such as port number, source and destination address, cost and so on. Consequently, an attacker tries to get the advantage of this feature by attaching his switch to change the layer two map, some malicious program might send some kinds of traffic to confuse the root switch, and this will affect the entire network. BPDU guard will prevent access port (end user) to send BPDU frame. This feature will act as the border for our network where we do not expect to see any BPDU after it, meaning there should be no switches at this point so no malicious switches can exist [29].



```
IOU13#
*Mar  8 19:59:00.983: %SPANTREE-2-BLOCK_BPDUGUARD: Received BPDU on port Ethernet0/0 with BPDU Guard enabled.
Disabling port.
IOU13#
*Mar  8 19:59:00.983: %PM-4-ERR_DISABLE: bpduguard error detected on Et0/0, putting Et0/0 in err-disable state
*Mar  8 19:59:01.989: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down
IOU13#
*Mar  8 19:59:02.985: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to down
IOU13#
```

Figure 25 BPDU Guard

Above figure shows there is an attack coming from access port (user PC) for this reason BPDU guard shut down source port and send a message to the administrator.

- **ROOT Guard**: - When a switch receives an inferior frame, which means there is a lower bridge ID switch has added to the network. Therefore, this new device will be a root bridge. Access layer ports' (end user) must prevent this type of frame because; we do not expect to add any switch to end user's port. Guarding access layer with this feature will drop any inferior frame could send from end user port to prevent any attack. Ignoring use this feature could represent a serious problem facing layer two traffic, where there are much malicious software can act like a real switch to send an inferior frame in order to change layer two maps, for example, attaching malicious devices within a network in order to capture entire traffic. Therefore, this feature one of the best practice of network security [29].

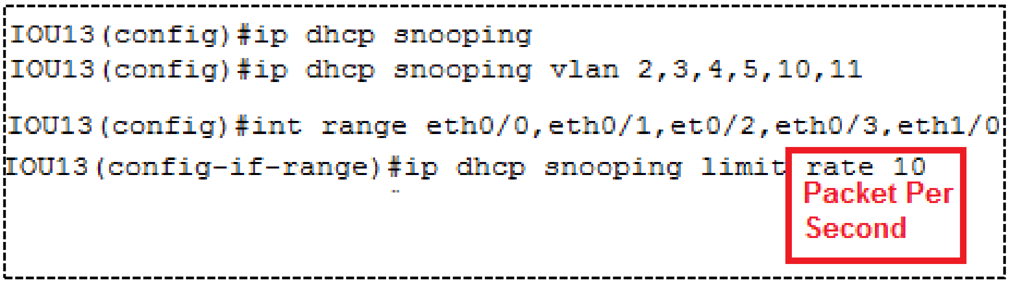
- **Port Fast**: - this feature reduces the amount of waiting time for a user to change port's status. In the normal case, the port's status change from blocking to listening and from listening to learning and finally make the port to forward, these steps need more time. This feature will change the port from blocking to forwarding state. Enabling this feature requires first enable one/both (port security, BPDU guard) to make sure use this feature will not adversely affect the network security.

3.6.3 Layer Two Security Features and Best Practices

There is a group of the security features and practices that we need to apply in our network to provide more security. We already walked through the security challenges when it comes to VLANs, VTP and STP and we have more technologies and network aspects to cover as

1. **Port security**: this feature plays a great role in preventing many threats and attacks such as MAC address flood, Man In The Middle MITM and many others. It works by limiting the maximum MAC addresses learned through a single port; determine the method to learn MACs whether statically or dynamically. In case, the number of MACs exceeds than what defined already, it performs two actions; first send a message to inform the admin, second, prevent an attack by changing the port state to one of three states (shut down, restrict and protect) [29]. It is always a good practice to fix the MAC address manually on the interfaces connected to fixed devices like printers and faxes and fixed laptops in the labs.
2. **DHCP Snooping**: - DHCP works to provide an IP address for each device working in a specific range. Some attackers try to deplete DHCP’s IPs in order to provide IPs by attacker’s device. The DHCP snooper works to define all access devices as untrusted ports to prevent sending DHCP (offer, acknowledgment), and if any violate act occurred, it will drop all frames.

Also, it can limit the request numbers coming from each port to prevent exhaust all IPs as in the following figure.



```
IOU13(config)#ip dhcp snooping
IOU13(config)#ip dhcp snooping vlan 2,3,4,5,10,11

IOU13(config)#int range eth0/0,eth0/1,et0/2,eth0/3,eth1/0
IOU13(config-if-range)#ip dhcp snooping limit rate 10
```

Packet Per Second

Figure 26 DHCP Snooping

3. **Dynamic ARB Inspection (DAI)**: - Communication between two hosts must make a mapping for IP and MAC for the destination host. For example, host A has the IP address for host B but does not have the MAC address for B (MAC-B), the normal procedure is sending a request to the switch, which will send an ARP request to consist of (IP-A, MAC-A, IP-B, Broadcast). The ARP request goes to all hosts within the network, only host B will reply to this request by sending MAC-B. An attacker tries to get the advantage of this mechanism by sending poisoning ARP request saying that the MAC address of host B is MAC-C (attacker's MAC). In same time sending to host B that MAC address for host A is MAC-C to play the role of MITM to capture all traffic flow between two hosts, or to drop all traffic flow between them making DoS attack. Preventing this kind of threat by using a technology called DAI, which works like a policeman on each port to check if the ARP is normal or poisoning. However, the question here is how can know all real MACs addresses for all ports? The answer is by using either DHCP snooping binding table or ACL (Access Control List) to determine all ports addresses manually. Next command shows how to enable this technology:-

```
ENG(config)# ip arp inspection VLAN 2,3,4,5,10,11
```

It can enable for interface, single VLAN or even for a group of VLANs, it will put all ports in the untrusted state. To make sure allow trunk ports to trust port, go to each trunk port and do the command:-

```
ENG(config-if)ip arp  inspection trust
```

To limit the number of packets per second on each access ports as follow:-

```
ip arp inspection limit rate 10
```

4. **Access Control List (ACL)**: - Using ACL to Control the traffic flow through a network. An ACL contains multiple entries to determine which IP must be permitted or denied. We can apply an ACL to different places, different technologies and in many forms. For example, it could permit IP1 to come into the router and block IP2 to come in, or allow IP1 inbound traffic and block it outbound or vice versa. An ACL processed Top-Down, where in case, we permit an IP (10.0.0.1/24) in the first statement there is explicit permit will allow a specific subnet IP and there implicit will deny all other subnets as in below command

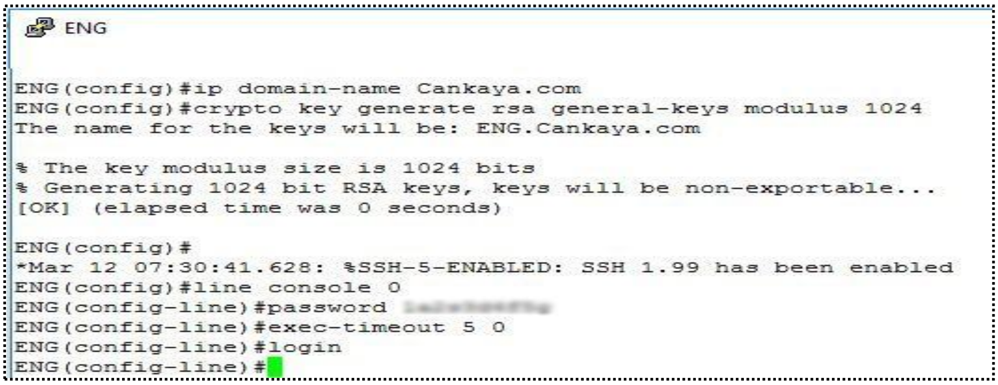
```
access-list 1 permit 10.0.0.1 255.255.255.0
```

ACL has many types depending on identifier number:-

- **Standard**: - which can filter traffic based on source IP address, using a number from 1 to 99 will define a standard access list.
- **Extended**: - can permit or deny traffic based on source and destination IP address and the port number in both sides. It takes a number from 100 to 199 and we can use the name instead of the number.

3.6.4 Secure Access Point for Devices: - one of most obvious steps to secure any network is by securing the access to the network devices in all aspects as

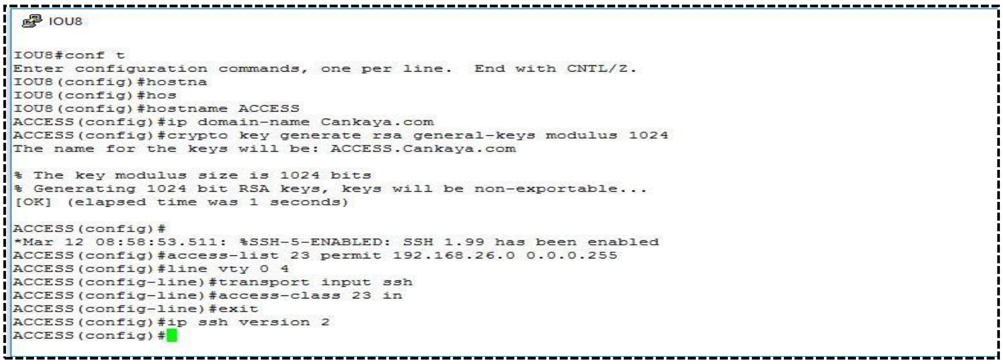
- Securing the console access by configuring a password on the console. Although connecting to the console means that the intruder is already inside our data center and next to cable to physically console to it but there are cases when we have console servers or what called Out of Band Access (OOB). The password will be handy in this case, plus there is a chance that the intruder will try to access the switch without the need to physically harm it so the password on the console will stop him from doing so. The following figure shows that.



```
ENG(config)#ip domain-name Cankaya.com
ENG(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: ENG.Cankaya.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

ENG(config)#
*Mar 12 07:30:41.628: %SSH-5-ENABLED: SSH 1.99 has been enabled
ENG(config)#line console 0
ENG(config-line)#password [redacted]
ENG(config-line)#exec-timeout 5 0
ENG(config-line)#login
ENG(config-line)#
```

Figure 27 Enable Console Password

- Securing the remote access: this is the most important way of securing the access to our equipment and providing access to authorized people only. Most of the access attempts (whether legit or not) will be remotely that is why we need to secure all the remote access aspects. The first way to secure the switch is disabling the default remote access protocol, which is TELNET because this protocol lacks the security, and does not encrypt the communication that can be incepted and monitored. The next step is enabling SSH v2 as our default remote access protocol since it is very secure and use encrypted communications. The other step is setting a MD5 password on the SSH access thus only people with the right password will have the access. Besides all the previous there is another security step which is determining the IP address ranges that allowed to access our switches hence a person with the right password will not be able to access the switch from not authorized networks or IP addresses. The way to configure this conditional access is by configuring an access list ACL on the VTY level. Enabling SSH as next figure.



```
IOU8

IOU8#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IOU8(config)#hostna
IOU8(config)#hos
IOU8(config)#hostname ACCESS
ACCESS(config)#ip domain-name Cankaya.com
ACCESS(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: ACCESS.Cankaya.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

ACCESS(config)#
*Mar 12 08:58:53.511: %SSH-5-ENABLED: SSH 1.99 has been enabled
ACCESS(config)#access-list 23 permit 192.168.26.0 0.0.0.255
ACCESS(config)#line vty 0 4
ACCESS(config-line)#transport input ssh
ACCESS(config-line)#access-class 23 in
ACCESS(config-line)#exit
ACCESS(config)#ip ssh version 2
ACCESS(config)#
```

Figure 28 SSH Steps

3.6.5 Miscellaneous Layer 2 Security Features

Besides all the security features that we covered for the technologies that we are applying there are other features that can help tighten the security measurements over our network like:

- Keeping away from using VLAN 1: since this is the default VLAN and it is untagged, acts as the native VLAN by default, and cannot be removed. All the malicious traffic will try to hack the VLAN that is why it is always a good practice not to use it and keep it isolated.
- Shut down all not in use interfaces: not in use interfaces that are enable can make a threat to our network where unauthorized people can use them to enter our network by connecting their PCs, sniffing tools or even switches. It is always a good practice to keep these interfaces manually down until we need to enable them again.
- Keep the idle interfaces in an isolated not used VLAN. Although we already recommended keeping these interfaces down, there is another layer of security here by adding them to a *not used VLAN* therefore if we enabled any interface by mistake or we had to enable it and there is a not authorized device connected to it. This device will have no access to our network.
- Tagging all our VLANs, even the native VLAN which means no VLAN leaking can happen and that will help separate the traffic of each VLAN.

- Using the banner feature to put a message that will be seen by anyone connecting to the switch showing the legal consequences of unauthorized access to the network devices.

3.7 Network Layer

The main function of the network layer that it will provide a way to communicate between the different networks based on the IP address as a reference. For example, to send traffic between two different devices on two different VLANs we need a layer three device in the middle builds the path that the two devices can take to reach each other. Based on the above all the internet communications are network layer type of communications which gives an idea about the importance of this layer and how it is important to design and configure it the right way. The way that a layer three device will create the path between two networks that it will build what called a routing table. The routing table is a table that consists of the networks, the interfaces or addresses to reach this network and the cost to reach it from the device perspective and the cost based on the method or the protocol that the device is using. One way to build the routing table is manual, by teaching the layer three device how to reach the different networks. However, this is not a practical way by any means for many reasons as we cannot keep up with the increasing number of the networks and we cannot update the routing table manually every time there is a change on a network in our table like if the network is not reachable anymore.

For the reasons above and the huge number of the networks, we created the different routing protocols that would build the routing table automatically. To see what routing protocol that we will choose for our thesis we need to understand the pros and cons of each of them and weight them to come up with the best solution.

Based on the scoop of the routing protocol, we have two types of them: Interior Gateway Protocols (IGP) and External Gateway Protocol (EGP)

3.7.1 Interior Gateway Protocols (IGP)

The routing protocols that exchange routes and networks within the same autonomous network (such as the campus in our case) There are two types of IGP

- Distance-vector routing protocols: they called this type of routing protocols “learning by rumors” because the router will have a neighbor relationship with its direct neighbors and learn about the networks behind these neighbors from them. Therefore, losing a neighbor will lead to losing all the networks behind it. The advantage of this type of routing protocols that they are fast in building the routing table because we do not need to hear from all the routers in the domain. The disadvantage is, if there is any change in the routing protocol behind a neighbor, they will be slow in learning the new changes because the routing table will be different from one router to another. These routing protocols would usually use the hop count as a way to calculate the cost (except for EIGRP that has other factors as the speed, reliability, and availability of the link). We can see RIP and EIGRP as examples of this type of routing protocols.
- Link-State routing protocols: unlike the Distance-Vector, this routing protocol is building the routing table by having neighbor relation with all the routers in the domain. Accordingly, all the routers will have the same version of the routing protocol which makes it an easier way to converge in the case of any change at any part of the network but it would be a bit slow while building the routing table for the first time since there will be a huge number of connections to establish. The cost is depending on the routing protocol itself. We can see OSPF and IS-IS as examples of this type of routing protocol.

From the information above and taking the needs of our design we have been chosen to go with the OSPF for some reasons that can summarize in the following:

- OSPF is a standard routing protocol comparing with EIGRP, which is CISCO proprietary, meaning that we can configure it on routers from different vendors.

- Each router in the domain will have a full vision of the routers on the domain making the updates and changes very fast to learn and converge.
- It uses the bandwidth as a factor to calculate the cost that is easy to manipulate and work with.
- It has the concept of the areas, where we can divide our domain to sub-domains. Hence, the communications within the same area will be as link state while it will act as a distance vector for the inter-area communications, which will lead to less overhead and broadcast traffic and decrease the convergence time.
- It has many security features that support the safe implementation of the routing protocol like MD5 authentication and the introducing of the stubby-area concept.

The way that we will implement OSPF within our environment is; we will have two areas. The first one is the backbone area or area zero and it is a mandatory area in any OSPF implementation. All the other areas should connect to area zero. In this case, area zero will include the connection between the core switch and the ISP router as in figure 29 bellow.

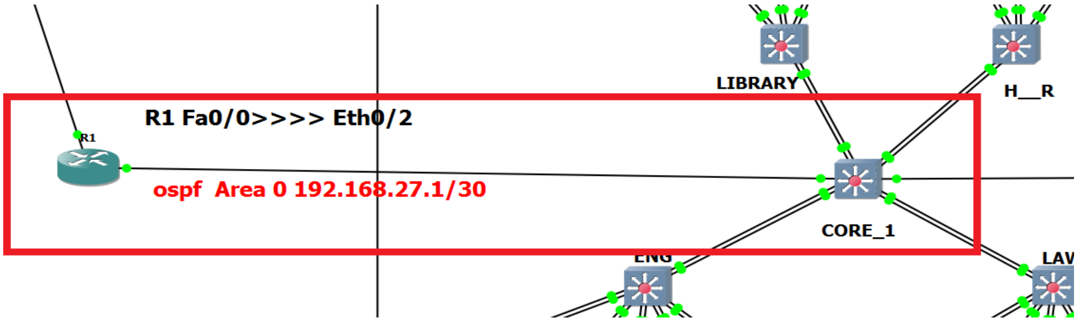


Figure 29 OSPF Area 0 (Backbone)

We will have area one that will connect the link between the two campuses core routers, figure 30 shows that.

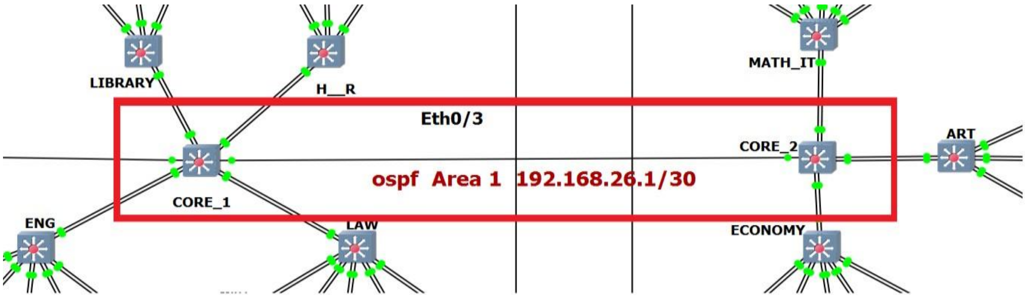


Figure 30 OSPF Area 1

The way that OSPF works that within the area, all the routers will elect what called a Designated Router (DR) and a Backup Designated Router (BDR). Their main function is to receive all the updates and changes from the routers in the area and broadcast them to all the routers in the area. The point behind the DR and BDR election that we will have a central point of updates in the area, which will increase the security and compatibility and decrease the multicast overhead within the area. This design will also decrease all the noisy traffic by preventing the neighbors from talking to each other directly. The way to elect the DR that the router with the highest router ID (RID) will be elected as the DR and the value of the RID can be set manually. The router with the second highest RID will be elected as the BDR as a backup if we lost the DR and it will copy the function of the DR.

First, when a router running OSPF comes up it will send hello packets to discover its neighbors and elect a designated router. The hello packet includes link-state information, as well as a list of neighbors. Providing information about the neighbor to that neighbor serves as an ACK, and proves that communication is bi-directional. OSPF is smart about the layer 3 topology if we are on a point-to-point link, it knows that this is enough, and the link considered “up.” If we are on a broadcast link, the router must wait for an election before deciding if the link is operational. The database exchange is part of bringing up adjacencies after the hello packets are exchanged, and it is very important. If the databases are out of sync (synchronization), we could risk routing loops, black holes and other perils. The third part of bringing up an adjacency is Reliable Flooding or LSA exchange that we will cover later.

The way that OSPF calculate the cost on its link is based on the bandwidth of the link where there is an equation of (100000/bandwidth in bit per second) hence the cost of a FastEthernet link will be one and the cost of a 10Mbps link will be 10. There is a problem with this equation that since it is an old equation there was no link faster than 100Mbps back then, the scenario that with this bandwidth reference all the links equal or faster than 100Mbps will have the cost of one. As a workaround, we need to change the reference bandwidth to 1000000 or greater. Beside the DR and the BDR, there are other types of routers in OSPF like the Area Border Router (ABR). The ABR is the router that has legs in two different areas or more one of them is area zero. The function of the ABR is to move traffic between the different areas and work as a gateway for the area, therefore; it has the routing table of each area it has a leg into it.

Another type of routers in the OSPF area is the Autonomous System Boundary Router (ASBR), which is the router that connects the OSPF area with another autonomous system as another routing protocol, or another instance of the OSPF and it is responsible of redistributing the routes from the autonomous system and injecting them into the OSPF area.

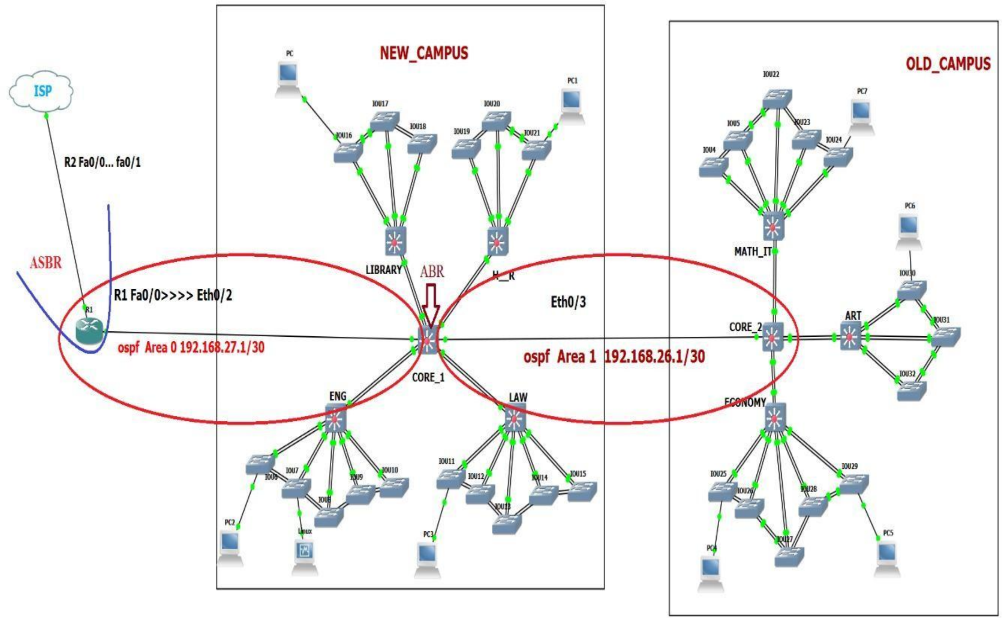
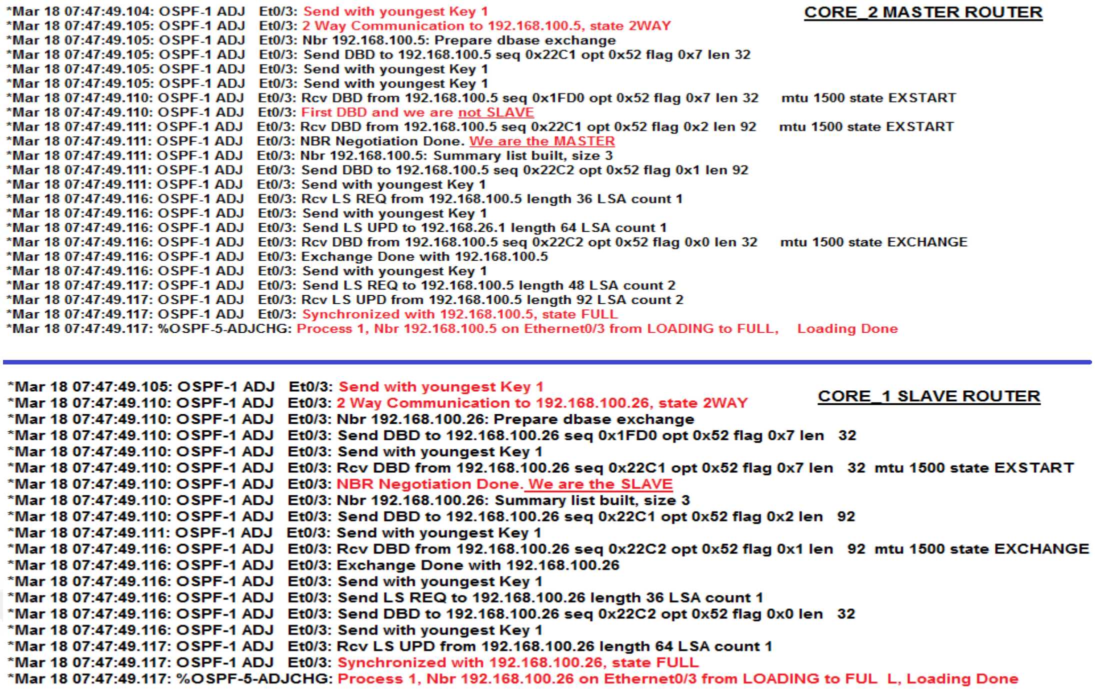


Figure 31 OSPF ARB Router and ASBR router

The way that OSFP works that we will have, special types of communication will generate by different routers to keep all the routers on the same page and act as feeds for the synchronization. These types of communications called the Link State Advertisements LSA including:

- LSA Type 1: Router LSA: generated by all routers within the area. Telling the DR and the BDR about the routes and networks that they have in their routing table and can reach.
- LSA Type 2: Network LSA: generated by the DR and the BDR and will reach all the routers in the area updating them about the routes that each router have with the next-hop value.
- LSA Type 3 (Summary LSA): this is the LSA that the ABR will generate for each area including the networks and routes and advertising itself as the next hop for them,
- LSA Type 4 (Summary ASBR LSA): generated by the ABR to show the path to reach the ASBR in case of any traffic need to leave our autonomous system.
- LSA Type 5 (Autonomous system external LSA): this type of LSAs will be created by the ASBR to inject the routes from another autonomous system into the OSFP declaring itself as the next hop for them.

There are other types of LSAs are not included in our design and have special cases for their implementation. The following figure shows the OSPF steps to confirm connectivity.



```
*Mar 18 07:47:49.104: OSPF-1 ADJ   Et0/3: Send with youngest Key 1                                        CORE_2 MASTER ROUTER
*Mar 18 07:47:49.105: OSPF-1 ADJ   Et0/3: 2 Way Communication to 192.168.100.5, state 2WAY
*Mar 18 07:47:49.105: OSPF-1 ADJ   Et0/3: Nbr 192.168.100.5: Prepare dbase exchange
*Mar 18 07:47:49.105: OSPF-1 ADJ   Et0/3: Send DBD to 192.168.100.5 seq 0x22C1 opt 0x52 flag 0x7 len 32
*Mar 18 07:47:49.105: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.105: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Rcv DBD from 192.168.100.5 seq 0x1FD0 opt 0x52 flag 0x7 len 32     mtu 1500 state EXSTART
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: First DBD and we are not SLAVE
*Mar 18 07:47:49.111: OSPF-1 ADJ   Et0/3: Rcv DBD from 192.168.100.5 seq 0x22C1 opt 0x52 flag 0x2 len 92     mtu 1500 state EXSTART
*Mar 18 07:47:49.111: OSPF-1 ADJ   Et0/3: NBR Negotiation Done. We are the MASTER
*Mar 18 07:47:49.111: OSPF-1 ADJ   Et0/3: Nbr 192.168.100.5: Summary list built, size 3
*Mar 18 07:47:49.111: OSPF-1 ADJ   Et0/3: Send DBD to 192.168.100.5 seq 0x22C2 opt 0x52 flag 0x1 len 92
*Mar 18 07:47:49.111: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Rcv LS REQ from 192.168.100.5 length 36 LSA count 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send LS UPD to 192.168.26.1 length 64 LSA count 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Rcv DBD from 192.168.100.5 seq 0x22C2 opt 0x52 flag 0x0 len 32     mtu 1500 state EXCHANGE
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Exchange Done with 192.168.100.5
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.117: OSPF-1 ADJ   Et0/3: Send LS REQ to 192.168.100.5 length 48 LSA count 2
*Mar 18 07:47:49.117: OSPF-1 ADJ   Et0/3: Rcv LS UPD from 192.168.100.5 length 92 LSA count 2
*Mar 18 07:47:49.117: OSPF-1 ADJ   Et0/3: Synchronized with 192.168.100.5, state FULL
*Mar 18 07:47:49.117: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.5 on Ethernet0/3 from LOADING to FULL,    Loading Done
```

```
*Mar 18 07:47:49.105: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: 2 Way Communication to 192.168.100.26, state 2WAY        CORE_1 SLAVE ROUTER
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Nbr 192.168.100.26: Prepare dbase exchange
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Send DBD to 192.168.100.26 seq 0x1FD0 opt 0x52 flag 0x7 len   32
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Rcv DBD from 192.168.100.26 seq 0x22C1 opt 0x52 flag 0x7 len   32  mtu 1500 state EXSTART
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: NBR Negotiation Done. We are the SLAVE
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Nbr 192.168.100.26: Summary list built, size 3
*Mar 18 07:47:49.110: OSPF-1 ADJ   Et0/3: Send DBD to 192.168.100.26 seq 0x22C1 opt 0x52 flag 0x2 len   92
*Mar 18 07:47:49.111: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Rcv DBD from 192.168.100.26 seq 0x22C2 opt 0x52 flag 0x1 len   92  mtu 1500 state EXCHANGE
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Exchange Done with 192.168.100.26
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send LS REQ to 192.168.100.26 length 36 LSA count 1
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send DBD to 192.168.100.26 seq 0x22C2 opt 0x52 flag 0x0 len   32
*Mar 18 07:47:49.116: OSPF-1 ADJ   Et0/3: Send with youngest Key 1
*Mar 18 07:47:49.117: OSPF-1 ADJ   Et0/3: Rcv LS UPD from 192.168.100.26 length 64 LSA count 1
*Mar 18 07:47:49.117: OSPF-1 ADJ   Et0/3: Synchronized with 192.168.100.26, state FULL
*Mar 18 07:47:49.117: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.100.26 on Ethernet0/3 from LOADING to FUL  L, Loading Done
```

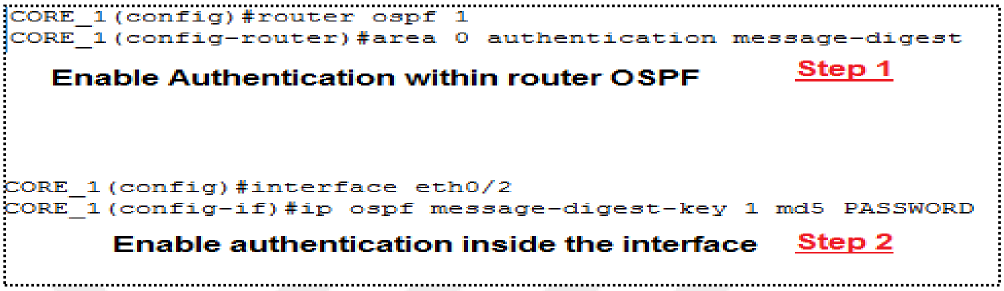
Figure 32 OSPF Talk Messages

3.7.2 Security Challenges and Solutions in OSF

As any network implementation, the default configuration of any technology or protocol will bring a list of security challenges that we need to address.

Securing the technology that we are applying is a key factor in having a sustainable and reliable service. The phase of securing our configuration should be well though during the planning and choosing the technologies and should be a high-weight factor in preferring a technology comparing to the others. OSPF as any other routing protocol has many security challenges need to be addressed as:

- Man In The Middle attacks MITM: where a router will be introduced to the network and try to communicate to the other OSPF routers and poisoning the routing table. One of the ways to face this issue is by implementing the point-to-point type of OSPF where the neighbors, in this case, will communicate directly over their directed link instead of using the broadcast IP address that OSPF uses by default. In this case, they will have a full routing table between them. To increase the security on this type of the OSPF connection it is better to keep the subnet that connects the routers as smaller as possible so there is no place free IP addresses that a hacker can hijack. There are another solution and security measure for that type of attacks or the rogue routers in the OSPF domain, which is applying an MD5 password on the OSPF and only the routers with the right OSPF, will exchange the LSAs and Hellos even. The rouge router will not be able to communicate with the rest of the routers even if it has the right configuration. Below is an example of password configuration on the OSPF domain:



```
CORE_1(config)#router ospf 1
CORE_1(config-router)#area 0 authentication message-digest
```

Enable Authentication within router OSPF — Step 1

```
CORE_1(config)#interface eth0/2
CORE_1(config-if)#ip ospf message-digest-key 1 md5 PASSWORD
```

Enable authentication inside the interface — Step 2

Figure 33 Enabling MD5 Authentication in OSPF

- Another good practice when configuring OSPF to build their boundaries of our domain is to configure the passive feature on all the interfaces where OSPF domain ends. This feature will stop sending or receiving any OSPF traffic that will stop having any neighbors behind this point. Stubby-area feature has some security implementations also in a way of isolating the areas where we do not anticipate seeing neighbors and can be seen as a dead-end for the OSPF domain.
- Changing the DR: this is a dangerous type of the OSPF attacks where the hacker will try to manipulate the process of the DR election. We need to fix the value that will use to elect the DR and the BDR by making it based on the RID instead of any other factor. If the routers have a tie on the RID then the next factor in choosing the DR will be the higher IP address on a loopback interface then the higher IP address on a physical interface. Every time we configure a new loopback or physical interface we are threaten the process of electing the DR. Therefore we need to configure the RID manually in a way that we always have a control over what router to be elected as the DR and this router should be in a central location where all the routers in the area can reach and capable from the hardware stand of point to handle all the updates within the area.

- We should keep the size of the area as small as possible for many reasons including decreasing the multicast domain. By having fewer routers within the area will decrease the effect of any attack and isolate it within the area without reaching too many routers.
- Enable OSPF per link instead of per subnet to have more control over the interfaces where we will enable OSPF in a way that OSPF will not be configured in parts of our network that we do not want them to participate in OSPF.

3.7.3 External Gateway Protocol (EGP):

Unlike the Internal Gateway Protocols, this type of protocols used to connect networks to different autonomous systems and the most used routing protocol of this type is BGP (Border Gateway Protocol). Practically this routing protocol runs the internet and brings the whole world together. Some people will argue that BGP is not a routing protocol or it is a hybrid one for the reasons that [48]:

- Unlike other routing protocols, BGP can connect neighbors that are not directly connected but as a result, we need to have an IGP connection between the neighbors to be able to establish a BGP peering which is not the case with other routing protocols where the neighbors always directly connected to each other. This feature is an important factor in the wide applications of the BGP where ISPs all over the world having BGP peering despite the geographical boundaries.
- BGP does not have its own Protocol number like other protocols. EIGRP has the protocol number of 88 and OSPF is 89. Instead, BGP uses the normal TCP port number 179 for communications.

Despite the points above BGP provides a wide range of advantages making it the best choice for inter-autonomous systems communications, these advantages can be summarized in the following:

- Reliable updates and communications since it uses TCP, which is a reliable way of communicating.

- Designed to scale to huge internetworks up to the entire internet, which cannot do with any other routing protocol.
- It has a special version where we can use it in our autonomous system especially in the large autonomous systems and network (Internal BGP).
- It is very efficient when it comes to traffic engineering because unlike other routing protocols the BGP attributes (the equivalent of the cost in other routing protocols) are based on the single subnet rather than based on the link hence on the same link we can treat subnets differently which we cannot do by using other routing protocols.

The way that BGP works by having what called Autonomous System Number AS for each network. This AS is unique to the autonomous system and cannot duplicate. The assigning of the AS is the responsibility of the Internet Assigned Number Authority (IANA) and it ranges from one to 65535.

After that, the routers need to initiate peering configuration by identifying the IP address of the neighbor that we can reach over the IGP and the neighbor AS and we have the option of adding MD5 authentication to our session. The next step that, the two routers will exchange hello messages that will include the information needed for the BGP peer formation. The last step that, the routers will exchange their BGP routing tables and keep monitoring each other through keep-alive packets to make sure that the other side still reachable and the networks behind it still reachable.

The two types of BGP are:

- External BGP: where the two peering routers are in two different autonomous networks and having two different sets of AS numbers and different public IP address ranges that they need to exchange. This is the BGP application that we have in our project to communicate with the outer world through our provider.
- Internal BGP: where the peering routers belong to the same autonomous network and having the same AS number and can exchange private IP addresses besides the public IP addresses. The

main area for applying this type of BGP is in the large-scale networks especially Wide Area Network (WAN) and Datacenters where we can make use of the high scalability, flexibility, and the highly capable traffic engineering.

The differences between these two types of BGP can explain the difference in the way they functioning and we can see the differences as bellows:

- External BGP has the TTL of one by default meaning that the far end peer has to be one hop away and we can change the behavior that we have for security reasons. Internal BGP, on the other hand, have the TTL of 255.
- In Internal BGP, the network learned through internal BGP neighbor cannot be advertised to another internal BGP neighbor. This is a loop prevention mechanism solves the black-hole issues but on the other part, it causes design problem. We need to have a full BGP mesh to come over this problem, which is inconvenient in the large networks so there are a couple of works around including. Route Reflector implementation where a router will be the central point of the network and all routers will have BGP peering with it (the same way Designated Router works within the OSPF area) and the other solution in the *Clusters* where routers will have internal BGP peering together with a virtual AS number.
- The other difference between the two types is the AS number where in the case of the External BGP we have to have a unique AS number to be assigned by the Internet Assigned Number Authority (IANA) and it ranges from 1 to 64511 (we can see it as the public IP addresses). Internal BGP uses the private range of the AS number from 64512 to 65535.

The way we implementing BGP in our environment as a gateway protocol as follows:

We have a gateway router that has OSPF connection with the core switch in the new campus and has a BGP peering with the ISP provider that is directly connected to our router (one hop away). The AS on our side is 5000 while the one on the ISP side is 4000 as follow.

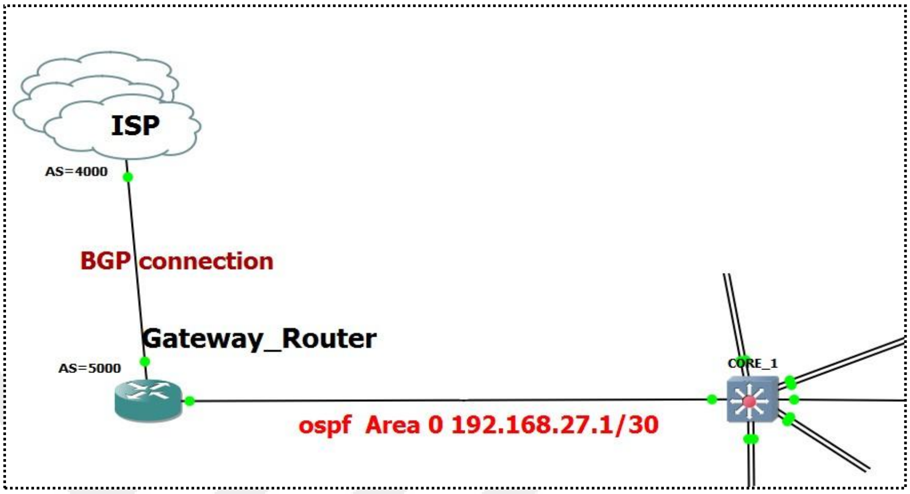
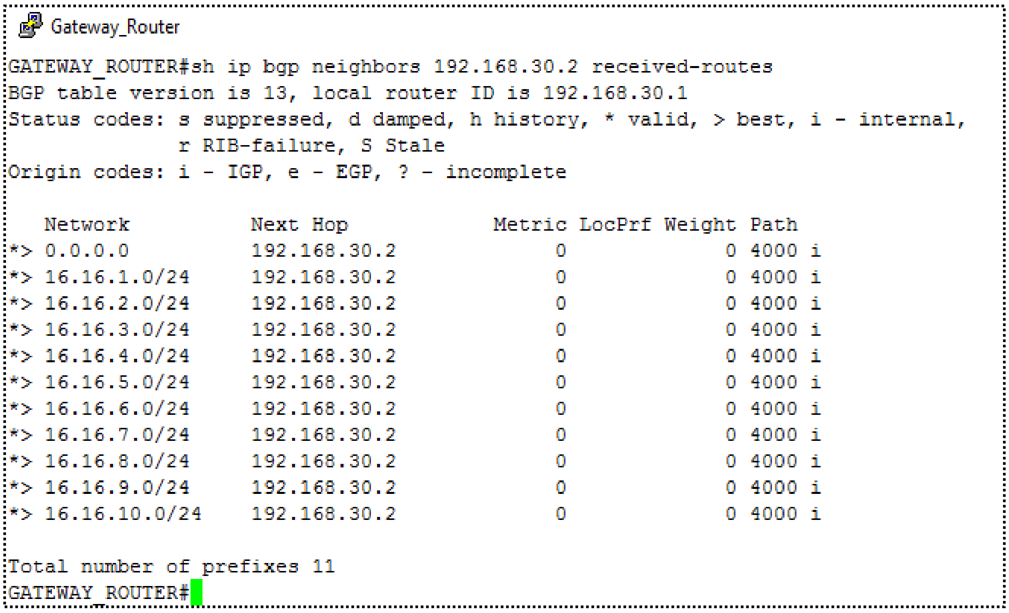


Figure 34 BGP Topology

In total, we are learning 10 different subnets from the ISP that we carry down through our network. The list of the subnets that we are learning through BGP is:



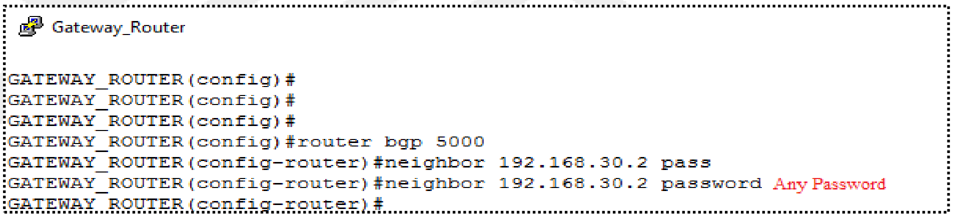
```
GATEWAY_ROUTER#sh ip bgp neighbors 192.168.30.2 received-routes
BGP table version is 13, local router ID is 192.168.30.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 0.0.0.0          192.168.30.2             0             0 4000 i
*> 16.16.1.0/24     192.168.30.2             0             0 4000 i
*> 16.16.2.0/24     192.168.30.2             0             0 4000 i
*> 16.16.3.0/24     192.168.30.2             0             0 4000 i
*> 16.16.4.0/24     192.168.30.2             0             0 4000 i
*> 16.16.5.0/24     192.168.30.2             0             0 4000 i
*> 16.16.6.0/24     192.168.30.2             0             0 4000 i
*> 16.16.7.0/24     192.168.30.2             0             0 4000 i
*> 16.16.8.0/24     192.168.30.2             0             0 4000 i
*> 16.16.9.0/24     192.168.30.2             0             0 4000 i
*> 16.16.10.0/24    192.168.30.2             0             0 4000 i

Total number of prefixes 11
GATEWAY_ROUTER#
```

Figure 35 Received IPs Subnet Using BGP

From our side, we advertising one public IP address subnet to the provider. As any other technology, BGP implementation brings series of security threats especially we are dealing with routers outside our network. It is important to address these challenges and figure out their solutions.

Some of these challenges are:

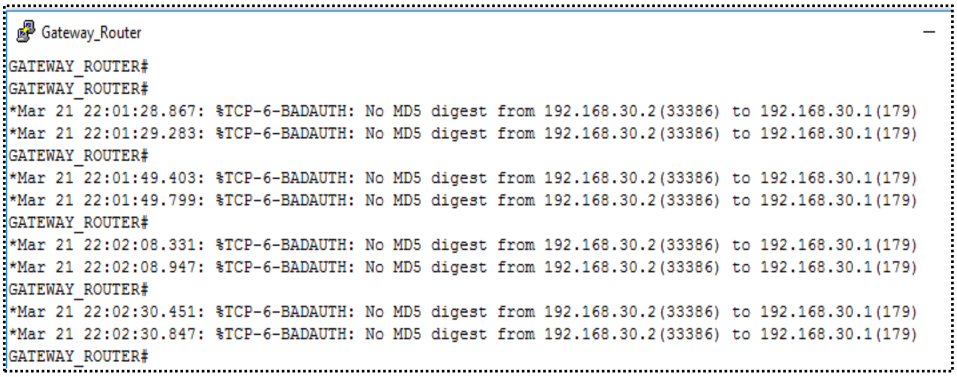
- Man In The Middle attacks where a router introduces itself as a legit one and due to the nature of BGP it is even harder to address this issue with BGP comparing to other routing protocol because the BGP peer can be away and do not have to be directly connected. We have a couple of steps to mitigate this problem including using the MD5 authentication on forming the peering which prevents the rogue router from forming adjacency as we can see from the figure bellow:



```
GATEWAY_ROUTER(config)#
GATEWAY_ROUTER(config)#
GATEWAY_ROUTER(config)#
GATEWAY_ROUTER(config)#router bgp 5000
GATEWAY_ROUTER(config-router)#neighbor 192.168.30.2 pass
GATEWAY_ROUTER(config-router)#neighbor 192.168.30.2 password Any Password
GATEWAY_ROUTER(config-router)#
```

Figure 36 BGP's Password

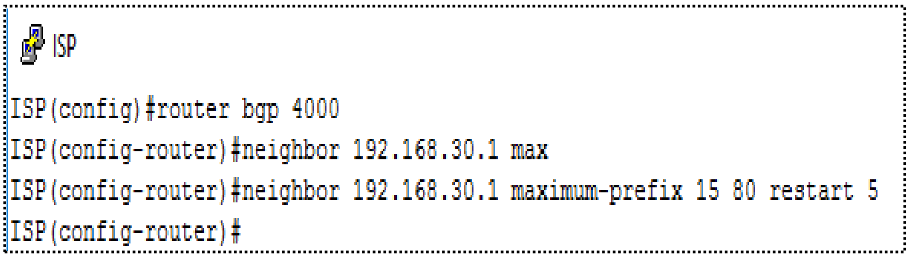
The errors that we face on the router in case of missing the MD5 password can be seen bellow:



```
GATEWAY_ROUTER#
GATEWAY_ROUTER#
*Mar 21 22:01:28.867: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
*Mar 21 22:01:29.283: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
GATEWAY_ROUTER#
*Mar 21 22:01:49.403: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
*Mar 21 22:01:49.799: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
GATEWAY_ROUTER#
*Mar 21 22:02:08.331: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
*Mar 21 22:02:08.947: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
GATEWAY_ROUTER#
*Mar 21 22:02:30.451: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
*Mar 21 22:02:30.847: %TCP-6-BADAUTH: No MD5 digest from 192.168.30.2(33386) to 192.168.30.1(179)
GATEWAY_ROUTER#
```

Figure 37 BGP Password Mismatch

- In total, we have around 600000 subnets covering the public IP addresses that the ISPs exchange. In consequence, keeping these subnets and managing them is very resources extensive and it can kill the CPU of the router that makes a real threat. On the other side, we do not need to have a full copy of the global routing table instead, we can have only the routes that we are interested in (in our case we have only ten routes from the provider). The way to counter this problem is by applying any kind of filtration on our gateway router (as access lists and route maps) allowing only the routes that we are looking for. There is a drawback to the previous solution though, the filtration that we configure can be resources extensive also because every received route needs to be matched against the route map or access list before deciding to keep it or drop it. Another solution is by determining the number of the prefixes that we should expect from the provider and have a threshold representing a percentage of the total expected number of routes that will ring an alert and after reaching the maximum number of excepted routes will reset the BGP session for a certain period of time as configured bellow:

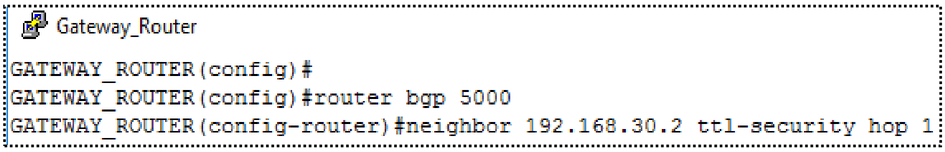


```
ISP(config)#router bgp 4000
ISP(config-router)#neighbor 192.168.30.1 max
ISP(config-router)#neighbor 192.168.30.1 maximum-prefix 15 80 restart 5
ISP(config-router)#
```

Figure 38 Limit The Number of Received Subnets

Where the configured number of excepted routes is 15 and we should see an alert on the router logs after receiving 80% of them (which is 12 routes) after receiving more than 15 routes we will reset the BGP session for 5 minutes.

- Another security threat due to the nature of the BGP is the idea that BGP does not have its own protocol instead it use TCP port 179. Although this is an advantage in a way that the peers do not have to be directly connected but there is a problem that the rouge router can be many hops away and can duplicate the communication of a legit router.To solve this issue we can use a feature called TTL security that determines the exact number of hops the far end peer is away instead of using the normal TTL and the configuration is below:



```
GATEWAY_ROUTER(config)#
GATEWAY_ROUTER(config)#router bgp 5000
GATEWAY_ROUTER(config-router)#neighbor 192.168.30.2 ttl-security hop 1
```

Figure 39 Determine How Far is The ISP

3.8 IP Addresses Scheme:

IP addresses are the main block in layer 3 networks that used as a way to build our routing tables and determine the next-hop value. There are two types of IPv4 that we will use them both in our project.

- The first type is the private IP addresses and these addresses are locally used within the autonomous network and cannot be used to reach networks out of our autonomous subnets. That is why these IP addresses are widely used by any network because we cannot use public IP addresses within our network for two reasons: first that we cannot have enough number of public IP addresses to cover the need within the network and secondly it is a bad security practice to use public IP addresses internally. The ranges of the private IP addresses are 10.0.0.0/8, 172.16.0.0-172.31.25.255 and 192.168.0.0/16.

  We have a single network for every VLAN we have to have more control over the traffic in case of any need to filtration or quality of service application.The list of our VLANs and their networks are:

Table 4 Private IP Addresses Scheme

Private IPs	
Old Campus	
Name of VLAN	Subnet
Management	192.168.22.0/24
Wireless	192.168.14.0/22
VOICE	192.168.32.0/24
IT	192.168.26.0/24
Literature	192.168.24.0/23
Economy	192.168.18.0/23
Math and IT	192.168.8.0/23
New Campus	
Name of VLAN	Subnet
Management	192.168.20.0/24
Wireless	192.168.10.0/22
VOICE	192.168.31.0/24
IT	192.168.28.0/24
Engineering	192.168.0.0/23
Human Resources	192.168.2.0/23
Law	192.168.4.0/23
Library	192.168.6.0/23

- Public IP Addresses: these unique IP addresses cannot be cross used by multiple autonomous networks. The Internet Assigned Numbers Authority (IANA) oversees global IP address allocation. In our network, the public IP address range that we have and advertise for our provider is 10.10.1.0/24 and the IP addresses that we are receiving are:

Table 5 Public IP Addresses Scheme

Public IP Addresses
0.0.0.0
16.16.1.0/24
16.16.2.0/24
16.16.3.0/24
16.16.4.0/24
16.16.6.0/24
16.16.7.0/24
16.16.8.0/24
16.16.9.0/24
16.16.10.0/24

3.9 Network Address Translation (NAT)

For the following three main reasons:

- The limited number of public IP addresses
- Security challenges in using public IP addresses internally
- We cannot use the private IP addresses in inter-autonomous networks communication.

We need to translate our private IP addresses to public addresses for the traffic going from inside to outside and vice versa. The NAT feature is one of the reasons that we still widely using IPv4 instead of moving everything over to IPv6 because it introduced the possibility of converting multiple private addresses to a single public IP, which decreased the demand for the limited-already public IP addresses. The following figures show NATing example.

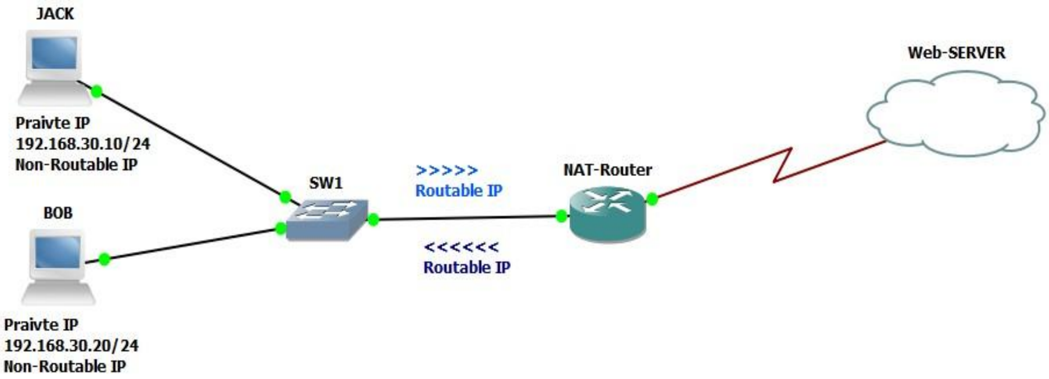


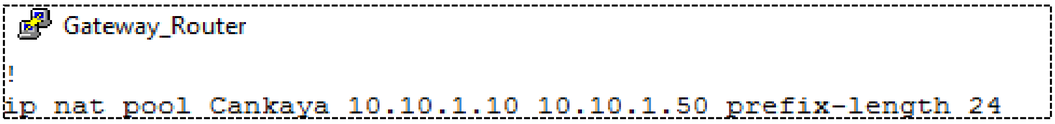
Figure 40 NATing Example

There are different flavors of NAT: -

- Static NAT: - this is mostly a one-to-one converting where a single public IP address will be translated to a single private IP address. The most common application of this type of NAT is servers that need to be always available for traffic from outside like public firewalls and web servers. The challenges with that type of NAT that it faces higher chances of security threats as DDoS because the public IP address is always the same. the second challenge that it is a resource consuming because we are dedicating a public IP address to a single private IP address instead of sharing it among a group of private IPs.
- Dynamic NAT: - in this type of NAT, we have a pool of public IP addresses where the private IP addresses choose from usually using round-robin algorithm. The issue with this type of NAT that we still doing the one-to-one translation.
- Port Address Translation PAT: - this is a type of the dynamic translation where beside the private-to-public translation will attach a port number to decrease the needed number of public IP addresses. A session needs translating will get a public IP address from the pool beside a port number in a result more than one session can have the same public IP address at the same time and this type of NAT is by far the most common type of NAT.

3.9.1 NAT Implementation:

Taking the public to private IP addresses ratio we are using Port Address Translation PAT in our network where we first created a 40 IP addresses pool serves all our private IP addresses

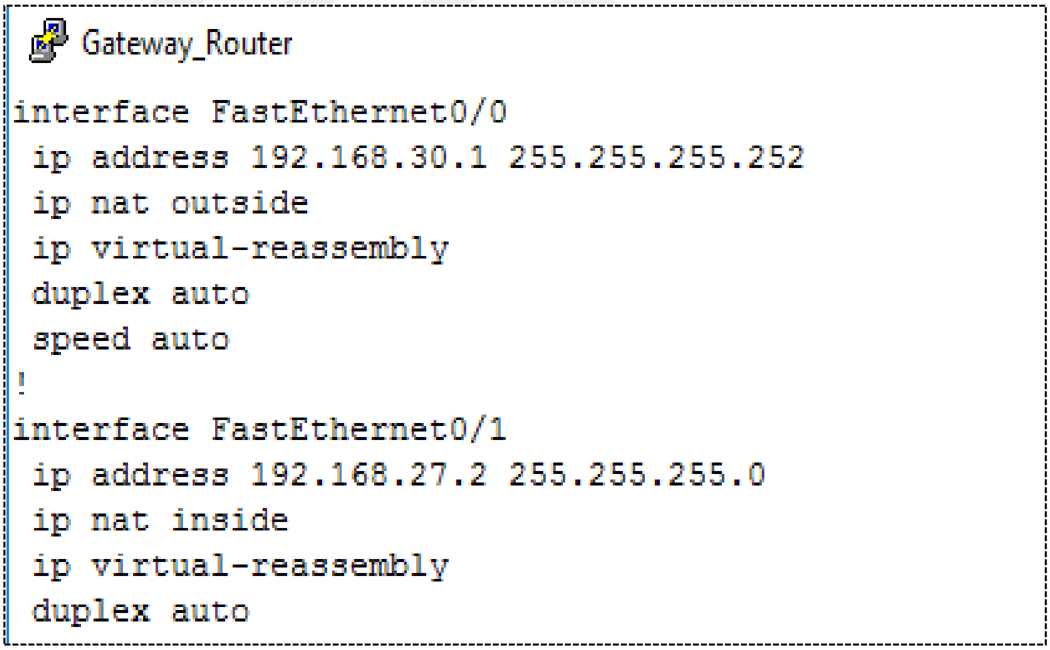


```
!
ip nat pool Cankaya 10.10.1.10 10.10.1.50 prefix-length 24
```

Figure 41 Create a POOL for NAT

The next step is setting the boundaries for each type of the IP addresses where the inside NAT interface will set the boundaries that a public IP address can reach. Meaning no public IP address can pass this point in our network.

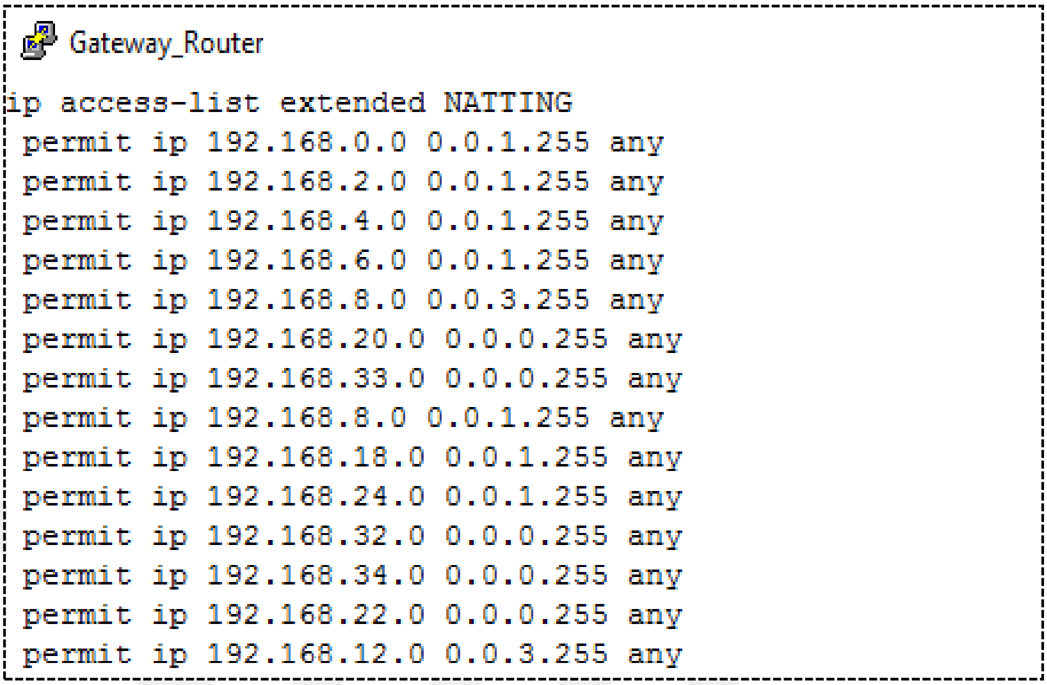
Outside NAT interface will set the boundaries for the private IP address where no private communications allowed after this interface.



```
interface FastEthernet0/0
 ip address 192.168.30.1 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.27.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
```

Figure 42 NAT (Inside and Outside) Interfaces

After creating, the public addresses pool and setting the inside and outside interfaces, the next step is determining the private IP addresses that allowed to be translated because we might not want to translate all our private IP addresses as loopback addresses. The way to configure this step is through an access list where each entry is a subnet represent an SVI in our network as follows:

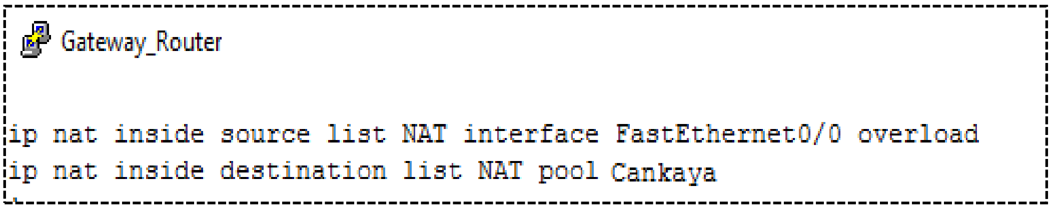


Gateway_Router

```
ip access-list extended NATTING
 permit ip 192.168.0.0 0.0.1.255 any
 permit ip 192.168.2.0 0.0.1.255 any
 permit ip 192.168.4.0 0.0.1.255 any
 permit ip 192.168.6.0 0.0.1.255 any
 permit ip 192.168.8.0 0.0.3.255 any
 permit ip 192.168.20.0 0.0.0.255 any
 permit ip 192.168.33.0 0.0.0.255 any
 permit ip 192.168.8.0 0.0.1.255 any
 permit ip 192.168.18.0 0.0.1.255 any
 permit ip 192.168.24.0 0.0.1.255 any
 permit ip 192.168.32.0 0.0.0.255 any
 permit ip 192.168.34.0 0.0.0.255 any
 permit ip 192.168.22.0 0.0.0.255 any
 permit ip 192.168.12.0 0.0.3.255 any
```

Figure 43 Private IP Addresses Access List

The last step of the configuration is to set the source and destination addresses as bellow:



Gateway_Router

```
ip nat inside source list NAT interface FastEthernet0/0 overload
ip nat inside destination list NAT pool Cankaya
```

Figure 44 Command for Enabling NAT (PAT)

The functions of the last two commands to tell the router that we a translating all the private IP addresses that matching the access list to public IP addresses from the pool that we created and attaching a port number to it.

CHAPTER FOUR

RESULTS

This chapter presents the results of attacks in graph form to address the problems posed in chapter 3 of this thesis. It focuses on executing some attacks on a Local Area Network in order to display both of effects and resources consumed due to the most occurrence attacks. We utilized tools such as MACOF and Yersinia pre-installed under Kali Linux. Our way of work was first examine the normal traffic of the mentioned LAN, then, flood it using the attacks. Hence, the result was about 5000 packets/second on only 4 switches as well as Denial-of-service (DoS) happened.

Thereafter, we simulated our entire network which contains 37 switches armed with the available security techniques. Similarly, we checked the normal traffic and applied the same attacks afterward. Sure enough, we found that the network was not affected by the attacks thanks to these techniques preserved the resources from the attacks and secured the network.

In this chapter will use Kali-Linux (as mentioned in 2.8) the main intererface for this OS as the figure bellow:-

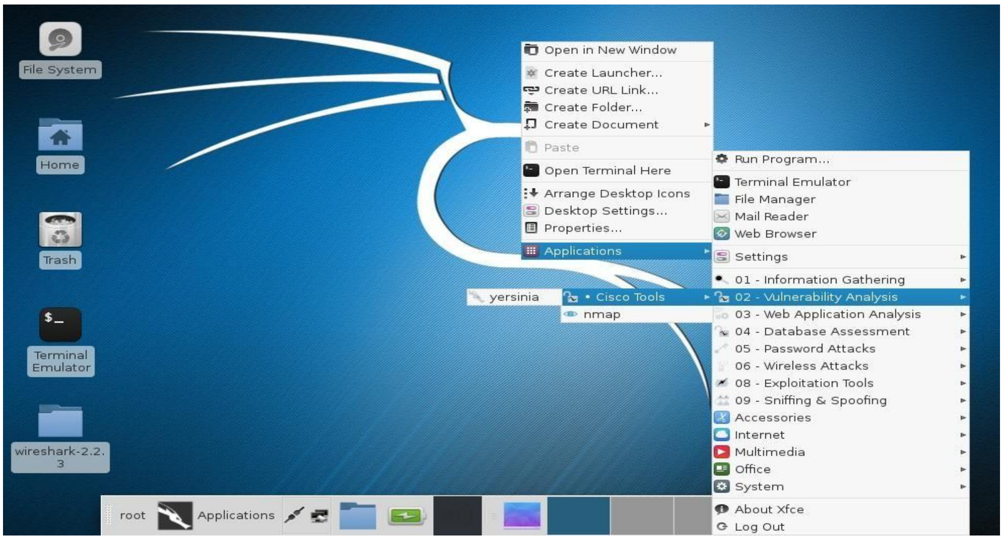


Figure 45 Kali Linux Interface

4.1 MACOF Attack

This attack is to flood the network and to cause DoS. Initially, the average of packets sent was below 5 packets/second then surprisingly changed to 2500 packets/second after executing the attack. Moreover, the average of packets kept increasing to reach more than 5000 packets/second as the figure illustrates:

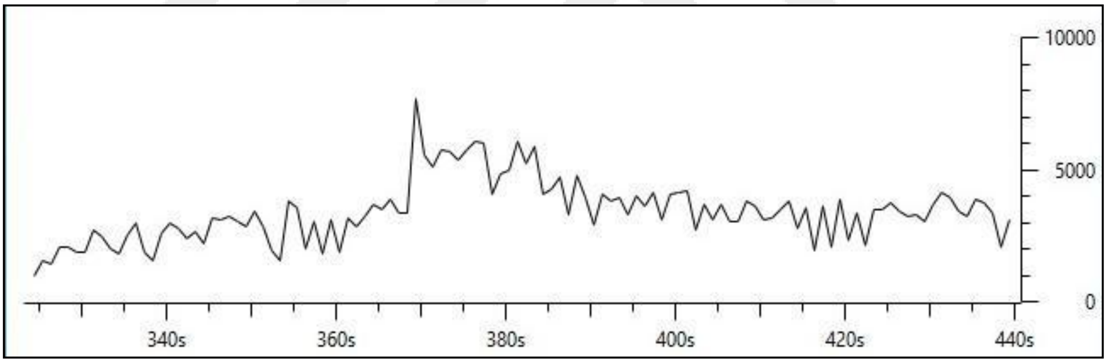
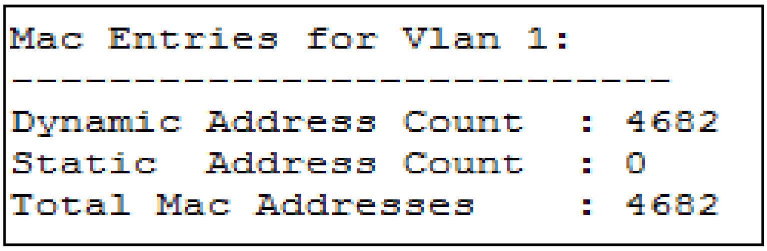


Figure 46 MACOF without Security Technologies

In addition, a MACOF attack on a single department consisting of only 4 switches gave a big number of MAC addresses in a limited time causing the switches to change behavior and DoS to occur as the screenshot below from our terminal (putty) shows:



```
Mac Entries for Vlan 1:
---------------------------
Dynamic Address Count   :  4682
Static  Address Count   :  0
Total Mac Addresses     :  4682
```

Figure 47 Number of MAC Addresses During MACOF Attack

However, the network continued to work properly without any effect caused by the attacks destined to it when we applied the security techniques for entire two campuses consist of 37 switches. While the attacker was trying to destroy the network, a log message of caution had been sent showing that unusual behavior coming from the port the attacker was plugged to resulting the port to shut down and keeping the danger away, as the following figure shows:

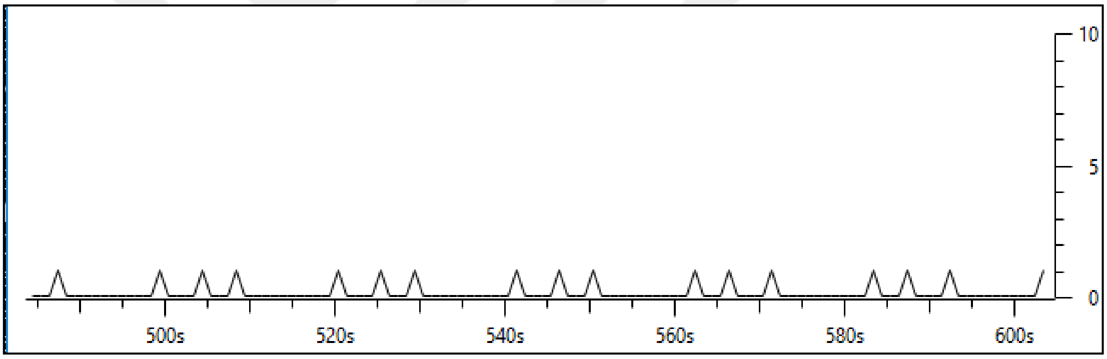


Figure 48 MACOF with Security Technologies

4.2 DoS Attack

This attack occurs when the attacker takes the advantage of "CDP Neighbor" feature. We found that DoS attack is more hazardous than the previous one since it causes the whole simulator to collapse. The average of packets per second not only increases gradually but also consumes the CPU and other resources. Figure 49 demonstrates that the attack started at a high level causing the network to stop and the computer to hang:

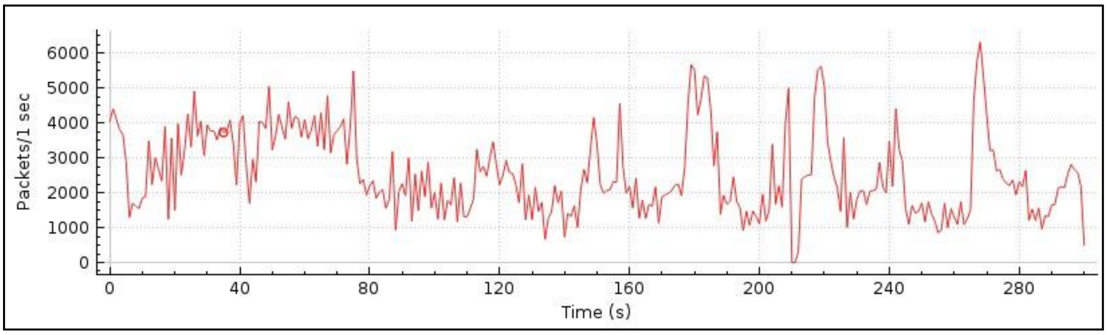
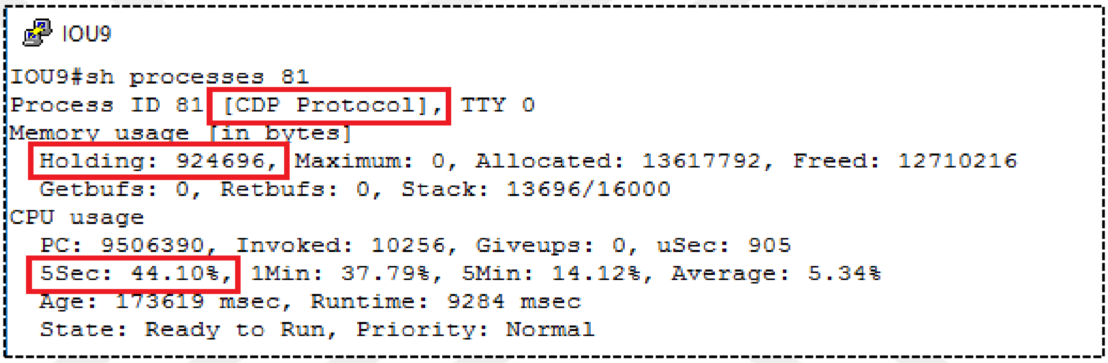


Figure 49 CDP Attack

This kind of attack consume huge amount of memory and CPU process as the following figure explain that



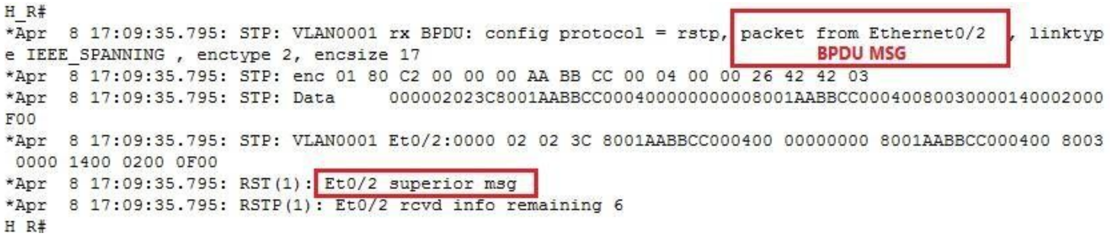
```
IOU9#sh processes 81
Process ID 81 [CDP Protocol], TTY 0
Memory usage [in bytes]
  Holding: 924696, Maximum: 0, Allocated: 13617792, Freed: 12710216
  Getbufs: 0, Retbufs: 0, Stack: 13696/16000
CPU usage
  PC: 9506390, Invoked: 10256, Giveups: 0, uSec: 905
  5Sec: 44.10%, 1Min: 37.79%, 5Min: 14.12%, Average: 5.34%
  Age: 173619 msec, Runtime: 9284 msec
  State: Ready to Run, Priority: Normal
```

Figure 50 Consumed Resources by CDP Attack

We have been solved this threat by disabling CDP neighbors through all untrusted ports (access ports) and the result was preventing any kinds of CDP attacks.

4.3 Changing Root STP

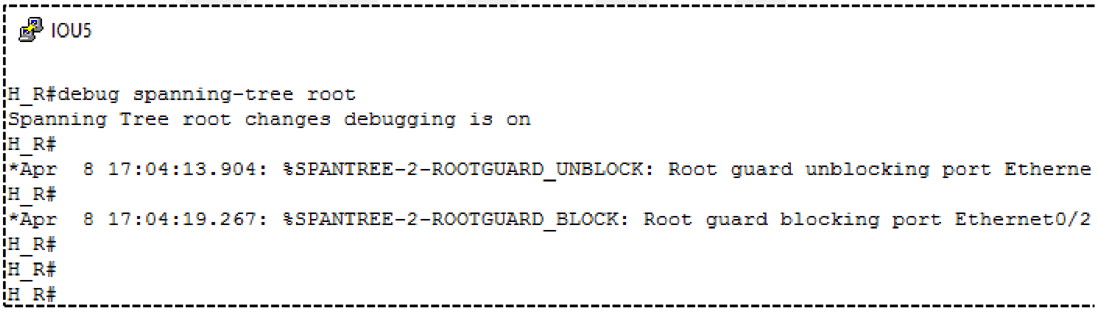
The attacker tries to use any tool to capture and destroy the network‘s resources. This type of attack sends a superior BPDU message, which means, there is a new lower bridge ID attached, as below figure explain that:



```
H_R#
*Apr  8 17:09:35.795: STP: VLAN0001 rx BPDU: config protocol = rstp, packet from Ethernet0/2  , linktyp
e IEEE_SPANNING , enctype 2, encsize 17
*Apr  8 17:09:35.795: STP: enc 01 80 C2 00 00 00 AA BB CC 00 04 00 00 26 42 42 03
*Apr  8 17:09:35.795: STP: Data     000002023C8001AABBCC000400000000008001AABBCC0004008003000014000200
F00
*Apr  8 17:09:35.795: STP: VLAN0001 Et0/2:0000 02 02 3C 8001AABBCC000400 00000000 8001AABBCC000400 8003
 0000 1400 0200 0F00
*Apr  8 17:09:35.795: RST(1): Et0/2 superior msg
*Apr  8 17:09:35.795: RSTP(1): Et0/2 rcvd info remaining 6
H R#
```

Figure 51 STP Attack

In this scenario, there is a network consists of many CISCO switches (this network has a root switch as the center for layer two's traffic) and an attacker's PC (connected through Ethernet 0/2). In this case, there is no protection against changing STP attack, which causes putting the attacker switch successfully instead of the real root switch by sending a superior message (this type of message must not send by access port such as the attacker's port). The worst side in this attack is controlling the entire layer two's traffic. Our solution is enabling BPDU guard, which prevent any kind of BPDU message sends from access ports as below figure shows that:



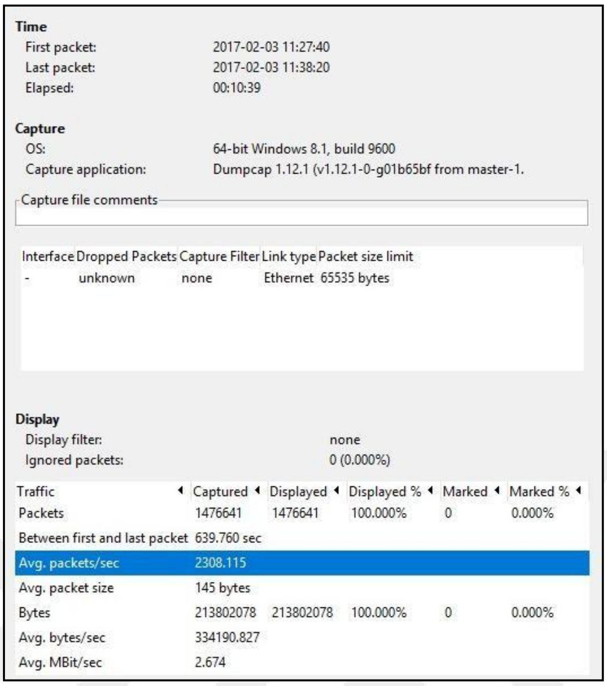
```
H_R#debug spanning-tree root
Spanning Tree root changes debugging is on
H_R#
*Apr  8 17:04:13.904: %SPANTREE-2-ROOTGUARD_UNBLOCK: Root guard unblocking port Etherne
H_R#
*Apr  8 17:04:19.267: %SPANTREE-2-ROOTGUARD_BLOCK: Root guard blocking port Ethernet0/2
H_R#
H_R#
H_R#
```

Figure 52 BPDU Guard

This figure tells us, an unusual behavior is coming from access port (attacker's PC connect to Ethernet 0/2) and BPDU guard takes responsibility to prevent it through blocking attacker's port from sending BPDU message.

4.4 Network Performance with/without Security

To compare the network performance with and without security technologies, we have some figures to show the average of packets per second in the certain amount of time approximated to 10 minutes and so seconds. The first capture counted 1476641 packets within 10 minutes and 39 seconds, figure 53 shows that the average of packets per second was 2308.115 and the average packet size was 145 bytes on a network of 4 switches attack:



Time
First packet: 2017-02-03 11:27:40
Last packet: 2017-02-03 11:38:20
Elapsed: 00:10:39

Capture
OS: 64-bit Windows 8.1, build 9600
Capture application: Dumpcap 1.12.1 (v1.12.1-0-g01b65bf from master-1.

Capture file comments

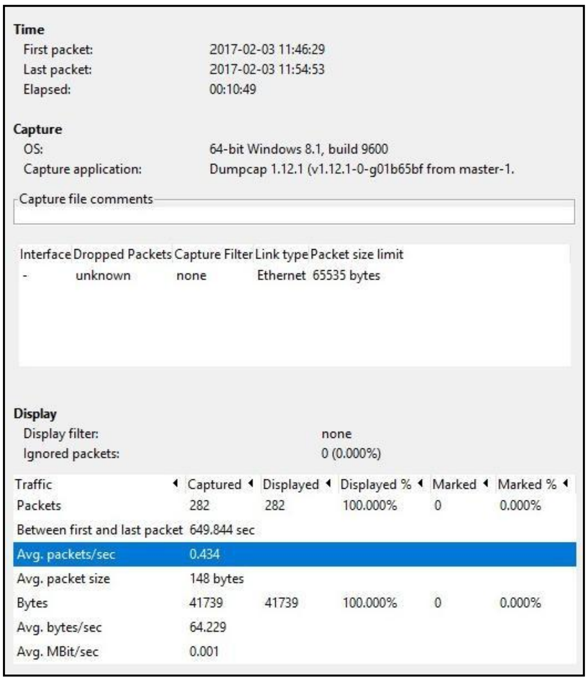
Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
-	unknown	none	Ethernet	65535 bytes

Display
Display filter: none
Ignored packets: 0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	1476641	1476641	100.000%	0	0.000%
Between first and last packet	639.760 sec				
Avg. packets/sec	2308.115				
Avg. packet size	145 bytes				
Bytes	213802078	213802078	100.000%	0	0.000%
Avg. bytes/sec	334190.827				
Avg. MBit/sec	2.674				

Figure 53 MACOF Attack Result

On the other hand, the next capture displays the activity of tools used to block the attack also in 10 minutes with way less number of packets as the figure shows:



Time
First packet: 2017-02-03 11:46:29
Last packet: 2017-02-03 11:54:53
Elapsed: 00:10:49

Capture
OS: 64-bit Windows 8.1, build 9600
Capture application: Dumpcap 1.12.1 (v1.12.1-0-g01b65bf from master-1.

Capture file comments

Interface	Dropped Packets	Capture Filter	Link type	Packet size limit
-	unknown	none	Ethernet	65535 bytes

Display
Display filter: none
Ignored packets: 0 (0.000%)

Traffic	Captured	Displayed	Displayed %	Marked	Marked %
Packets	282	282	100.000%	0	0.000%
Between first and last packet	649.844 sec				
Avg. packets/sec	0.434				
Avg. packet size	148 bytes				
Bytes	41739	41739	100.000%	0	0.000%
Avg. bytes/sec	64.229				
Avg. MBit/sec	0.001				

Figure 54 Blocking MACOF Attack Result

The last figure was performed on two simulated campuses with 37 switches secured with all security techniques and applying the same attacks we executed before monitoring the results with Wireshark.

4.5 Implications of Attacks

This part explains the effects of attacks without using security weapons and the gained resources with using security technologies which have been applied in this study, the results have been represented as a table as well in a graph to make it easy for observation.

Table 6 Gained Resources

With/ Without Security	Attack Aame	Number of Packect Per Second	Time MM:SS	Total Number of Packets	DoS Attack
Without	**MAC flood**	5000	10:39	1476641	Yes
With	**MAC flood**	0.434	10.49	282	No
Without	**CDP attack**	4633.5	04.28	1243792	Yes
With	**CDP attack**	0.750	12.20	555	No

We conclude from previous table, which shows only two attacks, that after applying security technologies we have increased the level of campus security and kept the traffic of the campus as normal as possible. Moreover, preventing the effects of DoS can be observed clearly from the table, where these two attacks causing DoS however, we have blocked this attack. The average of packets per second represents a big difference between with/without security technologies, where in CAM flood the number exceed 5000 packets/second which is very higher than normal rate and at same time is deplete the network’s resources such as CPU, memory… etc.

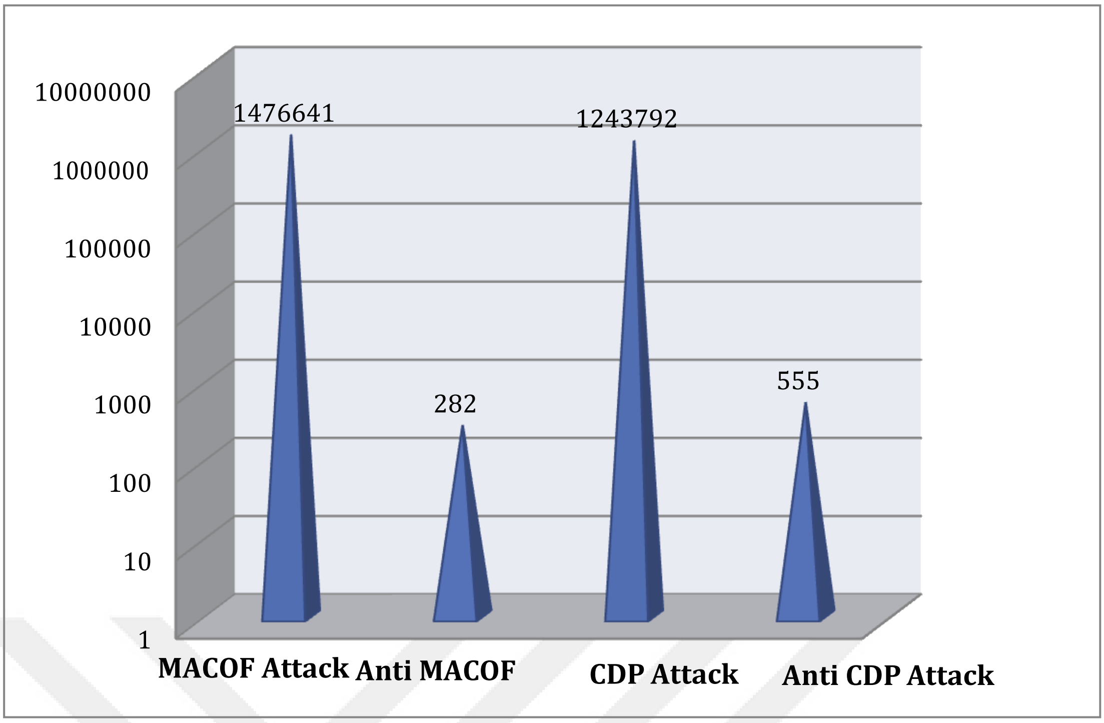
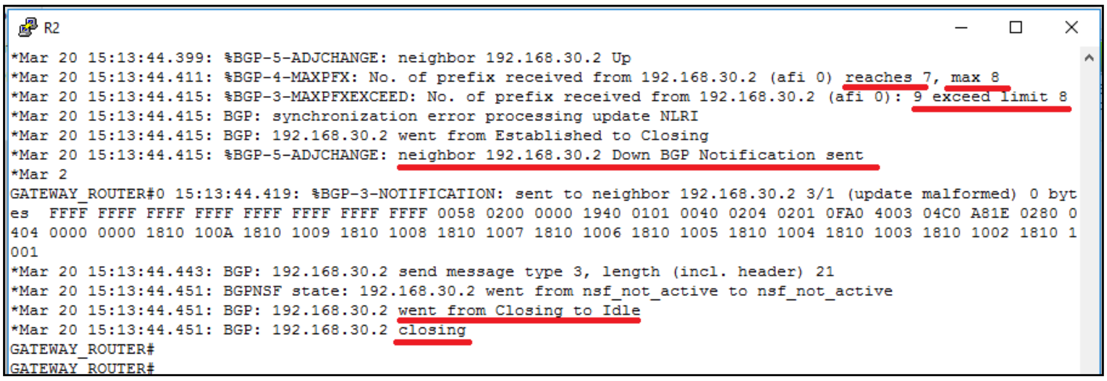


Figure 55 Gained Resources Chart

Above chart explains the huge difference between the sitation without applying security and with applying security technologies and features. In the other hand, it explains what we have been enhanced and the amount of resources we have been gained.

4.6 Network Layer Security

In network layer of OSI model, we lowered the number of IPs we receive from outside (ISP provider) the campus to a specific threshold, in case of exceeding this threshold we configured the campus to inform the administrators when the received number of total IPs reach 80% and if it continue in coming will shut down the receiving port for a certain time to allow the network administrator to figure out what is happening. The figure below shows that the IP 192.168.30.2 which is our ISP started to over send IPs reaching 80% of allowed percent. This causes to send an alert to the security feature to shut down BGP on that port for five minutes to check this state. This feature blocked the routing table from being flooded with a high number of IPs that may consume the CPU of the router to process them:



```
*Mar 20 15:13:44.399: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Up
*Mar 20 15:13:44.411: %BGP-4-MAXPFX: No. of prefix received from 192.168.30.2 (afi 0) reaches 7, max 8
*Mar 20 15:13:44.415: %BGP-3-MAXPFXEXCEED: No. of prefix received from 192.168.30.2 (afi 0): 9 exceed limit 8
*Mar 20 15:13:44.415: BGP: synchronization error processing update NLRI
*Mar 20 15:13:44.415: BGP: 192.168.30.2 went from Established to Closing
*Mar 20 15:13:44.415: %BGP-5-ADJCHANGE: neighbor 192.168.30.2 Down BGP Notification sent
*Mar 2
GATEWAY_ROUTER#0 15:13:44.419: %BGP-3-NOTIFICATION: sent to neighbor 192.168.30.2 3/1 (update malformed) 0 byt
es  FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF 0058 0200 0000 1940 0101 0040 0204 0201 0FA0 4003 04C0 A81E 0280 0
404 0000 0000 1810 100A 1810 1009 1810 1008 1810 1007 1810 1006 1810 1005 1810 1004 1810 1003 1810 1002 1810 1
001
*Mar 20 15:13:44.443: BGP: 192.168.30.2 send message type 3, length (incl. header) 21
*Mar 20 15:13:44.451: BGPNSF state: 192.168.30.2 went from nsf_not_active to nsf_not_active
*Mar 20 15:13:44.451: BGP: 192.168.30.2 went from Closing to Idle
*Mar 20 15:13:44.451: BGP: 192.168.30.2 closing
GATEWAY_ROUTER#
GATEWAY_ROUTER#
```

Figure 56 Limiting The Number of Receiving IPs

CHAPTER FIVE

CONCLUSION

The best approach to have a fully secured network is by covering all the OSI layers that invoking network functionality, which are physical layer, data-link layer and the network layer. Our work methodology was to identify the most common security threats and weaknesses at the level of the network design hence we can suggest the appropriate solutions and work around. This approach is better than peregrinating these challenges to the implementation phase that makes it more offensive approach. We divided our study into three main parts:

The first one is the network design, including the size, hardware and technologies used to provide a fully functional network. The second part is the security threats facing each layer, and its technologies that we are using. The last one covers the security solutions that we tailored together to provide a security-net for our network. What differentiates this thesis from similar works is that, instead of focusing on a single technology and its security leaving the rest of the network compromised. We covered all the well-known security threats and best practices making it a good reference for any security implementation plan in any in-production network no matter its size or functionality.

The study answered these questions:

In case of future campus network expanding, can we manage this expansion without affect the security? What are the techniques used for that?

Adopting Campus Hierarchical Design, the network will offer more flexibility, expandable design and more secure, which means that possibility to expand the network without redesign it from scratch. Instead of one layer of design, hierarchical offers three-separated layers with a specific role for each. From security perspective, hierarchical design offers more security because of separation of the access layer (the most vulnerable point) from other layers (distribution and core). Moreover, this design gives more pliability in case of creating new department or making maintenance for another.

Is it enough to depend on default configurations come with switches and routers?

Depending of default configurations has been proved as a dangerous point in any kind of network especially campus network and should be hardcoding to put control over all parts in order to prevent speculation and make a map changing for entire our network's parts. Because of weakness comes with L2 (Data-Link layer) and to enrich this layer, we have discussed all possible scenarios that could face L2 and offered a handy way to deal with. Preventing DoS related to L2 also has been prevented by using security tools such as port-security, DAI, disabling CDP feature and using an ACL to identify who has the authority to get direct access to the data-center equipment.

Which part of a network represents a source of threat? How can we deal with it?

Connection point represents the weakest point whether this point is to connect users to the network or to connect entire network with the global network (the Internet). That means, access layer for inside users and gateway for outside connection, what we have done in this study is securing access layer and gateway by flowing a well-studied strategy to deal with each single part. For example, access layer has a full protection strategy and we put more than three defense lines for each access port (each user's port)), apply many security walls in order to reduce the effects and prevent an attacker to take advantage of offered services in our network.

L3 represent another connection point between inside/outside network, how can we enrich this point to prevent losing privacy?

It is recommended to control each part within a network, L3 represents a valuable point that should take a serious attention in order to protect the network. This study has taken great two steps with L3; first, choosing a secure type of OSPF (Point-To-Point), assign small range of subnet to connect two routers and strengthening the

OSPF's areas using MD5 authentication. Second, BGP protocol gives us many features to control ingress/ egress traffic, also we have done more security features with BGP to protect our network from outside harmful users.
And the last question is: after securing L2, L3 what are the benefits of these solutions? Is it logical to adopt this study or not?

Network administrators always need to consolidate their networks. This study takes the responsibility to offer all possible threats that might face L2 and L3, as well as identify all possible flaws and vulnerabilities related to these two layers. A reasonable decision to choose tools are tested in enhanced security like what we have in this study. In addition, this study gives a clear-cut view about building and securing campus network that would be followed to get tested result with less effort.

5.1 Findings

This section will review the experimental conclusions in this study.
We live in serious security crisis due to the dramatically increasing the number of connected devices to the Internet every day around the world. The campus network is one important kind because of its value contains. For this reason, we have discussed securing campus network from three layers of OSI model perspective (Physical, Data-Link, and Network) by addressing the kinds of challenges within each layer and we have applied all possible solutions offered by CISCO devices and closed all flaws related to three layers.
This part will try to summarize findings we gained from this study. First, choosing a robust design represents a solution factor for many problems in any kind of network especially campus network for a couple of reasons such as management, future expansion, and security. For this reason, we have employed Hierarchical Campus Network as a design way in this study. Second, addressing all possible vulnerabilities facing three layers (P., D., N.) and offer a solution for each vulnerable point. In addition, testing the result is covered in order to prove that our network has resisted the effects of different types of attacks.

Reducing the amount of harmful effect of L2 attacks is one finding in this study, where we have minimized the effects of L2 attacks to reach the lowest level of impact on our network. At the same time, this study offered the highest level for three security rules (confidentiality, integrity, and availability) for campus users. Moreover, we presented many dangerous kinds of attacks related to L2 such as CAM flood attack, DoS attack, L2 loop attack, CDP attack, VLAN hopping attack, changing STP root attack and MITM attack.

Controlling the traffic flow between different networks has been covered and enhanced in this study. OSPF threats represent a serious problem that could affect the confidentiality aspect, therefore changing default configuration come with enabling OSPF by choosing the Point-To-Point type that prevents MITM attack. Moreover, using a limit subnet to connect the routers within an area represents a good way to limit MTM attack. Talking about BGP threats, again MITM attacks plays a harmful threat. In this study, this attack has been solved by using an encrypted password MD5 to make sure there is no possibility to attach any device to our network. In addition, flooding our network with unwanted subnets has been stopped by limiting the coming subnets from ISP, using an ACL to watch and monitor the amount of traffic (subnets), and sending an alert message to the network administrator in case exceeding the defined amount of subnets.

5.2 Limitations

Covering all these security features needs vital elements to reach results that are more useful. However, what has been limiting us in expanding our study is a group of limitations, including First, using an emulator Graphical Network Simulator GNS3. Where, it provides a limit number of security features. At the same time, it needs a computer with high requirements to simulate real attacks and provide a high effectiveness. The computer used in this study has limit requirements that cause many problems during this study such as stuck entire activities provided by the computer when we needed to execute more than one attack on a small network. In addition, the problem was more complex when we completed the entire network and needed to check the security with it. Second, real CISCO’s devices, dealing with an emulator cannot give us a clear view like a real device. Nevertheless, because of limited support for this study, the results came limited. It would be awesome to apply all the configurations on a real world campus by using Cisco equipment for both wired and wireless devices with better results. In addition, we can make the realistic topology running dual stack protocols.

5.3 Future studies:

This work is done by using simulated environment with only three layers of OSI model. It can be extended to include the other four layers (application, presentation, session and transport). Each layer has its threats and security issues so it is good to cover all of them. Connecting this network to the Internet is also a good idea to test and measure the effectiveness of our study.

5.4 Conclusion:

In the light of presented findings within the limitations, we conclude that the potential impact of applying security technologies with OSI model on our campus can give us enormous benefits in spite of the challenges the encounter campus environment. We found the solution to well-known threats facing campus network and used suitable weapons that solve the problem. We made a clear map for network administrators it would adopt in real world, where we insisted to address all best practices within campus network and we covered that during this study starting from design stage to build stage to secure stage finally to test stage. Answering the questions that shape this study have covered also to expand the benefits of applying the steps in this study.

REFERENCES

1. Internet Security Threat Report, 2016 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf last access 11/5/2017.
2. **Agueda Sofia Tavares**, 2011. Network Architecture for University Campus Network.
3. **Bishop, M.** (2003). What is computer security?. IEEE Security & Privacy, 99(1), 67-69.
4. **Stallings, W.** (2006). Cryptography and network security: principles and practices. Pearson Education India.
5. **Stallings, W.** (2006). Cryptography and network security: principles and practices. Pearson Education India.
6. **Raitman, R., Ngo, L., Augar, N., & Zhou, W.** (2005, July). Security in the online e-learning environment. In Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference on (pp. 702-706). IEEE.
7. **Edwards, J., & Bramante, R.** (2009). Networking Self-teaching Guide: OSI, TCP/IP, LANs, MANs, WANs, Implementation. Management and maintenance, Wiley Publishing, Inc.
8. **Bloch, M., & Barros, J.** (2011). Physical-layer security: from information theory to security engineering. Cambridge University Press.
9. DCN - Data-link Layer Introduction, , an article https://www.tutorialspoint.com/data_communication_computer_network/data_link_layer_introduction.htm last access 1/5/2017.
10. OSI Network Layer, an article http://www.highteck.net/EN/Network/OSI_Network_Layer.html last access 1/5/2017.
11. TCP vs. UDP http://www.diffen.com/difference/TCP_vs_UDP last access 1/5/2017.
12. Session layer (port layer), posted by Margaret Rouse http://searchnetworking.techtarget.com/definition/Session-layer last access 1/5/2017.
13. **Cole, E.** (2011). Network security bible (Vol. 768). John Wiley & Sons.
14. **Sulaimon, A. A.** (2012). Network security.
15. **Ali, M. N. B., Hossain, M. E., & Parvez, M. M.** (2015). Design and Implementation of a Secure Campus Network. International Journal of Emerging Technology and Advanced Engineering, 5, 370-374.
16. **Thomas, T.** (2000). OSPF network design solutions.
17. **Wu, C.** (2010, July). The problems in campus network information security and its solutions. In Industrial and Information Systems (IIS), 2010 2nd International Conference on (Vol. 1, pp. 261-264). IEEE.

18. **Ning, H., & Bing, X.** (2011, August). The research and analysis of security of campus network. In Information Technology and Artificial Intelligence Conference (ITAIC), 2011 6th IEEE Joint International (Vol. 2, pp. 25-27). IEEE.
19. **Song, D., & Ma, F.** (2012, May). Strategy and implementation of campus network security. In Systems and Informatics (ICSAI), 2012 International Conference on (pp. 1017-1019). IEEE.
20. **Verma, R. O., & Shriramwar, S. S.** (2013, April). Effective VTP Model for Enterprise VLAN Security. In Communication Systems and Network Technologies (CSNT), 2013 International Conference on (pp. 426-430). IEEE.
21. VTP Version 3, 2008, CISCO press, white paper http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/solution_guide_c78_508010.html last access 1/5/2017.
22. **Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide,** Release 12.2(25)EW, Cisco Systems, Inc. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf.pdf last access 1/5/2017.
23. **Campus Network for High Availability Design Guide**, 2008, Cisco Systems,Inc. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html#wp1107563. last access 1/5/2017.
24. **Lück, I., Schäfer, C., & Krumm, H.** (2001). Model-based tool-assistance for packet-filter design. Policies for Distributed Systems and Networks, 120-136.
25. Kali Linux Official Documentation http://docs.kali.org/introduction/what-is-kali-linux last access 1/5/2017.
26. Understanding VLAN Trunk Protocol (VTP), 2014, CISCO press http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html
27. **Catalyst 3750-X and 3560-X Switch Software Configuration Guide**, chapter 39, Configuring EtherChannels and Link-State Tracking. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swethchl.pdf
28. **Understanding Rapid Spanning Tree Protocol**, Document ID: 24062 http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html last access 1/5/2017.
29. **Cisco IOS Software Configuration Guide**, Release 12.2SX, chapter 62, http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.html#wp1055296 last access 1/5/2017.
30. **McGregor, M.** (1998). Cisco CCIE Fundamentals: Network Design and Case Studies.
31. **Moss, A. J., Hall, W. J., Cannom, D. S., Klein, H., Brown, M. W., Daubert, J. P., ... & Pfeffer, M. A.** (2009). Cardiac-resynchronization therapy for the prevention of heart-failure events. New England Journal of Medicine, 361(14), 1329-1338.

32. What are Types of Servers? 2015 http://wifinotes.com/computer-networks/server-types.html last access 1/5/2017.
33. Enterprise Campus 3.0 Architecture: Overview and Framework, 2008 http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/campover.html last access 1/5/2017.
34. Single Mode vs. Multi-Mode Fiber Optic Cable, http://www.multicominc.com/training/technical-resources/single-mode-vs-multi-mode-fiber-optic-cable/ last access 1/5/2017.
35. **Fiber Types in Gigabit Optical Communications**, White Paper, 2008 Cisco Systems, Inc. http://www.cisco.com/c/en/us/products/collateral/interfaces-modules/transceiver-modules/white_paper_c11-463661.pdf last access 1/5/2017.
36. Cisco Catalyst 2960-X Series Switches, 2017 Cisco and/or its affiliates http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/data_sheet_c78-728232.html last access 1/5/2017.
37. Cisco Networking Academy, “Catalyst 3750-X and 3560-X Switch Software Configuration Guide”, Cisco Press, Retrieved from: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg.html last access 1/5/2017.
38. Catalyst 3750-X and 3560-X Switch Software Configuration Guide, Release 12.2(55)SE,2014. http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html last access 1/5/2017.
39. Beaver, K. (2007). Hacking for dummies. John Wiley & Sons. http://uap.unnes.ac.id/ebook/Dummies%20Ebooks,%2055%20Ebooks/Wiley%20Publishing%20-%20Hacking%20for%20Dummies%20%5B2004%5D.pdf last access 1/5/2017.
40. **Karina Astudillo B.**, 2015, ETHICAL HACKING 101.
41. MAC Address Flooding – MAC address table overflow attacks https://howdoesinternetwork.com/2011/mac-address-flooding last access 1/5/2017. last access 1/5/2017.
42. Session layer (port layer), Margaret Rouse http://searchnetworking.techtarget.com/definition/Session-layer last access 1/5/2017.
43. **Mike Fuszner – version 1.0**, Graphical Network Simulator. https://www.csd.uoc.gr/~hy435/material/GNS3-0.5-tutorial.pdf last access 1/5/2017.
44. The four qualities of a successful cyber security start-up, 2016 http://www.information-age.com/four-qualities-successful-cyber-security-start-123461243/. last access 1/5/2017.
45. **Hewlett-Packard (HP) Development Company**, 2011, FlexCampus Reference Architecture Guide.

https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#72d7947a3a91 last access 11/5/2017.

46. **Canavan, J. E.** (2001). Fundamentals of network security. Artech House.
47. **Rekhter, Y., Li, T., & Hares, S.** (2005). A border gateway protocol 4 (BGP-4) (No. RFC 4271).

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: AlZaghir, Sadiq Hilal Mousa

Date and Place of Birth: 03 November. 1985, Babylon, Iraq

Marital Status: Mirred

Phone: +90538989689

Email: Sadiq1985@yahoo.com

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya University	2017
B.Sc.	University of Babylon	2008
High School	Al-Imam Ali School	2004

FOREIN LANGUAGES

- English: Good
- Turkish: Intermediate
- Arabic: Native

HOBBIES

- Traveling.
- Reading.
- Computing.
- Swimming.
- Reading poets.
- Running.