Page-de-garde-Fr-ge.pdf

dissertation-55.pdf

dissertation-56-92.pdf

Université Mohamed Khider de Biskra
Faculté des Sciences et de la Technologie
Département de génie électrique

MÉMOIRE DE MASTER

Sciences et Technologies
Télécommunication
Réseaux et Télécommunication

Réf. : Entrez la référence du document

Présenté et soutenu par :
Djouama Mohamed Rabiâ

Le : samedi 23 juin 2018

Full Design And Configuration Of Enterprise Campus Network Using Cisco Devices And GNS3

Jury :

Mr.	Sofiane AMEID	MAA	Université of Biskra	Superviseur
Dr.	Abida TOUMI	MCA	Université of Biskra	Président
Dr.	Soraya ZAHANI	MCB	Université of Biskra	Examinateur

Année universitaire : 2017 - 2018

الجمهورية الجزائرية الديموقراطية الشعبية
People's Democratic Republic of Algeria
وزارة التعليم العالي و البحث العلمي
Ministry Of Higher Education and Scientific Research

Mohamed Khider Biskra University
Faculty of Sciences and Technology
Electrical Engineering Department
Field: Telecommunication
Option: Networks and Telecommunication

Graduation Dissertation

for obtaining a Master's degree

Full Design And Configuration Of Enterprise Campus Network Using Cisco Devices and GNS 3

Presented by:

Djouama Mohammed Rabiâ

Favorable opinion of the supervisor:

Mr.Ameid Sofiane

Positive opinion of the President of the Jury

Ms. Toumi Abida

Stamp and signature

Dedication

For who candidate to lead, for who wants the best for the Motherland and who wants to change the world for the better, those we got the inspiration from them.

For those how all we know about, who wants to critic or even to smash, however who wants the worst for the beautiful world, those we got the enthusiasm from them

Acknowledgement

Thanks to merciful lord for all the countless gifts you have offered me, and thanks to my family for their love and support a specially my parents for their prayers and their supports.

It is a great pleasure to acknowledge my deepest thanks and gratitude to my supervisor Mr.Ameid Sofiane , faculty of science and technology, for suggesting the topic of this memory , and his kind supervision. it is a great honor to work under his supervision.

I would like to express my deepest thanks and sincere appreciation for all teachers who encourage me throughout the school years. However who tried to frustrate me but he had fuel my fire to keep going and staying strong.

Finally I would like to thank all of my friends their help and their support, a specially my Classmates and my closes friends.

Table of Contents

List of Figures

List of CMD-List

Cmd-List 1 : Interfaces e3/1, e3/2, e3/3**.**

Cmd-List 2 : Trunk Interfaces e0/0, e0/1.

Cmd-List 3 : VLANs signed on the switches.

Cmd-List 4 : Configuration L3 link Dist-1.

Cmd-List 5: Configurtation L3 link Dist-2.

Cmd-List 6 : OSPF Configuration Protocol.

Cmd-List 7 : Link Core-1 to ASA.

Cmd-List 8 : Link Core-2 to ASA.

Cmd-List 9 : INSIDE Interfaces.

Cmd-List 10 : SERVER Interfaces.

Cmd-List 11 : OUTSIDE Interface.

Cmd-List 12 : Default Route.

Cmd-List 13 : Sample from Object Network.

Cmd-List 14 : ICMP ECHO.

Cmd-List 15 : SSH protocol.

Cmd-List 16 : OSPF protocol.

Cmd-List 17 : ACL Collections.

Cmd-List 18 : ACL Apply interfaces.

Cmd-List 19 : NTP protocol.

Cmd-List 20 : Nat Pool.

Cmd-List 21 : EDGE Interfaces.

Cmd-List 22 : DHCP for interface e0/0 from ISP-1.

Cmd-List 23 : Security level interfaces.

Cmd-List 24 : Static Routes.

Cmd-List 25 : List of Inspected Protocols.

Cmd-List 26 : Authentication OSPF.

List of Abbreviations

LAN: Local Area Network

PCs: Personal Computers

IP: Internet Protocol

VLANs: Virtual LAN

HTTP: Hyper Text Transfer Protocol

MAC: Media Access Control

EtherChannel: Ethernet Channel

1U: one rack unit

Mbps: Mega Bit Per Second

Gbps: Giga Bit Per Second

PoE: Power Over Ethernet

OSI: Open System Interconnection

QoS: Quality of Service

ACL: Access List

GbE: Gigabit Ethernet

WANs: Wide Area Networks

SMB: Small and Medium Sized Business

SFP: Small Form-factor Pluggable

CSMA/CD: Carrier Sense Multiple Access / Collision Detection

IEEE: Institute of Electrical and Electronics Engineers

SMTP: Simple Mail Transfer Protocol

FTP: File Transfer Protocol

ARP: Address Resolution Protocol

PDU: Power Distribution Unit

SFD: Start Frame Delimiter

FCS: Frame Check Sequence

IPv4: Internet Protocol Version 4

OUI: Organizational Unique Identifier

NIC: Network Interface Card

BIA: Business impact analysis

VTP VLAN Trunking Protocol

ISL: Inter-Switch Link

BPDU: Bridge Protocol Data Unit

SVI: Switched Virtual Interface

WIC: WAN interface card

msec: Micro Second

L2: Layer 2

HSRP: hot standby redundancy Protocol

GLBP: Gateway Load-Balancing Protocol

VRRP: Virtual Router Redundancy

CPU: central processing unit

VTY: Virtual teletype

EXEC: Execute

IOS: Internetwork Operating System

SSH: Secure Shell

Telnet: Network Virtual Terminal Protocol

DHCP: Dynamic Host Configuration Protocol

GNS3: Graphical Network Simulator 3

NASA: National Aeronautics and Space Administration

ASA: Adaptive Security Appliance

QEMU: Quick Emulator

VM: Virtual Machine

DMZ: Demilitarized Zone

ISPs: Internet Service Provider

VPN: virtual private network

MB: Miga Byte

vIOS: virtual Internetwork Operating System

OSPF: Open Shortest Path First

ASAv: Adaptive Security Virtual Appliance

RAM: Random Access Memory

DC: data center

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

ICMP: Internet Control Message Protocol

DNS: Domain Name System

ECMP: Equal Cost Multi-Path

NTP: Network Time Protocol

https : Hyper Text Transfer Protocol Secure

NAT: network address translation

RADIUS: Remote Authentication Dial-In User Service

Syslog: System log

STP: Spanning Tree Protocol

ASDM: Adaptive Security Device Manager

IIS: Internet Information Server

ISAKAMP: Internet Security Association and Key Management Protocol

CCNA: Cisco Certified Network Associate

CCNP: Cisco Certified Network Professional

CCIE: Cisco Certified Internetwork Expert

Abstract

Communication and the information transmission system have now become important tool. And for that we did a research on one of the most important communication technologies, full design and configuration of enterprise campus network which supported by several network devices and protocols has used to build the entire network, then we cannot forget the methods we followed to achieve the high performance and flexibility to any design we had chose to create.

Our work is intended to study network design and configuration of campus network and test the connectivity of devices included, into each other or into the outside of the company such as internet or even another branch. Additionally, to ensure its availability if any part of the structure has been failed. Using emulator software which provided us with virtualization technologies to allow us emulate Cisco IOS (Internetwork Operating System) and Windows OS (Operating System).

One of the most important recommendations, Complete the remaining parts of the Design in particular configuration data center and policies of security, then we could use this project for any enterprise wants to expand its network to multiple branches with many users.

ملخص

أنظمة الاتصالات و نقل المعلومات أصبحت في عصرنا هذا أدوات مهمة، ولهذا قمنا ببحثنا على إحدى أهم تكنولوجيا الاتصالات، التصميم الكامل و التهيئة البرمجية لشبكة حرم مؤسسة ما، التي تحمل بمجموعة أجهزة شبكية و بروتوكولات معينة تستعمل لبناء كامل الشبكة. ثم لا يمكن أن ننسى المنهجية المتبعة للوصول إلى الأداء العالي و المرونة لأي تصميم اخترنا أن ننشئه.

هدفنا من هذا العمل هو دراسة التصميم و التهيئة لشبكة حرم مؤسسة واختبار اتصال الأجهزة خاصتها مع بعضها البعض، أو خارج المؤسسة كالاتصال بالانترنت أو حتى فرع آخر ينتمي للشركة. إضافة إلى ذلك، ضمان إتاحة الشبكة وصلاحيتها إذا ما حل عطب في احد أجزاء الشبكة. و ذلك باستعمال برامج محاكية مزودة بتقنيات الوهمية (virtualization) التي تسمح بمحاكاة أنظمة سيسكو Cisco IOS و أنظمة التشغيل Windows OS.

التوصيات الأكثر أهمية تتمثل في إكمال أجزاء الشبكة من حيث النقائص سواء في التصميم أو في التهيئة البرمجية، خاصة في تهيئة مركز البيانات والسياسات المتبعة من اجل الأمن و السرية، ثم من الممكن أن نطبق هذا المشروع في أي مؤسسة تريد بناء وتوسعة شبكتها لعدة فروع تحتوي على الكثير من المستخدمين.

General Introduction

General Introduction

The term network is used in many ways. For example, people network with one another, telephones are networked in the public telephone system, and data networks connect different computers. These uses of the term have a common thread: Networks make it possible for people or devices to communicate with each other.

A campus network is generally the portion of the network infrastructure that provides access to network communication services and resources to end users and devices that spread over a single geographic location. It might be a single floor, a building, or even a group of buildings spread over an extended geographic area.[1]

Building a Campus network is more than only interconnecting physical network infrastructure devices. The most challenging and important part of it is the planning and design phases where different technical variables and technologies need to be considered that could even effect the product selection and the design entirely. Also a good design is the key to the capability of a network to scale. This dissertation will discuss some of the technologies and design considerations that need to be taken, during the planning and design phases to design a scalable campus network. Then through all of this by using software emulating a campus network by specific tools already existed to help network professionals developing their skills and testing some designs before the real installation of physical devices.

Memory motivation:

Let us start with a questions, why we chose this topic ?what drives us, and what is the purposes ? Information technology such huge field contain a fascinating specialty, each one may make you sink. Our Obsession always was about ending stuff, creating things, overcoming the challenges until we could see the miracle as human being. Designing network then put the configuration for each design make us better and better than before, or a best version of ourselves. What skills we could get and what expertise we could earn on the career when we struggling, just to build a network has less faults and less vulnerabilities and less security errors.

Memory objective:

Designing a campus network and implementing with no disregard of requirements and needs customers, and as graduation project it's only for practicing network skills. What had as a real world enterprise network. Spending most of times to troubleshooting, and earning new concepts to design network from practical field.

Scope of The memory research:

The dissertation has planning by three chapters as the following :

first chapter: it's an overview of Campus local area network (LAN) or as a business name we could say (Medium Business Network). We take a care about the hierarchical switch LAN architecture type, and its benefits rather than flat design, and some studies about principles of hierarchical network including features of switches are used on layers of this hierarchical.

second chapter: Covering switching concepts and technologies are used for switching and forwarding the frame around the entire physical network, and the protocols are used to improve the functionality of the network without any loops or mistakes. Instead of that we cannot forget about security field and famous threats, which might occur to the switches of enterprise campus network.

third chapter: realizing of campus network could used for the enterprises by emulation software tools and testing the results by following the traffic flow from sources to destinations we have designed, with tools helped us capturing the data for analyses and tracking, and monitoring the entire network.

Chapter 1: Overview Of Campus LAN (Medium Business Network)

1 Introduction

In field of networking we take great attention to rules from basics and fundamental of network, you will know that, just when you start wondering about the polices could possibly be necessary and required by the owners of the environments company you are working for.

unfortunately there is no standard design for all companies with different policies, we need to learn couple of more commonly used rules in network engineering. furthermore, All of network Devices has the same principal whatever Cisco Mikrotik or Huawei, it has the same configuration but only the language is a little different, any information technology engineer was provided with fundamentals able to avoid primitive mistakes when designing the network. Moreover, just installation of equipment and stack it together doesn't make you network professional.

The migration from legacy to newer technology of design that due a several business need, such the cost or permanently performance of infrastructure. finally ,that put the engineers under as a metter of fact to find a solution, such a hierarchical network model.

1.2 Switched LAN Architecture.

1.2.1 Legacy Switch LAN Architecture (Flat design)

Hubs and switches were added as more devices needed to be connected. A flat network design provided little opportunity to control broadcasts or to filter undesirable traffic. As more devices and applications were added to a flat network, response times degraded, making the network unusable.[2]

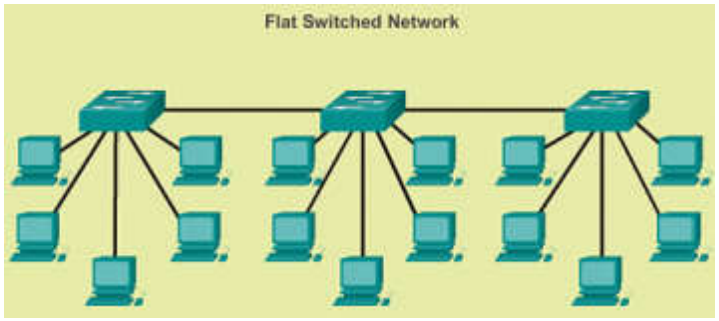


Figure 1.1 : Flat Switched Network**.** [2]

When building a switched LAN architecture that satisfies the needs of a small- or medium sized business, your plan is more likely to be successful if a hierarchical design

model is used. Compared to other network designs, a hierarchical network is easier to manage and expand, and problems are solved more quickly. [3]

1. 2.2 Hierarchy Switch LAN Architecture

Hierarchical network design involves dividing the network into discrete layers. Each layer provides specific functions that define its role within the overall network. By separating the various functions that exist on a network, the network design becomes modular, which facilitates scalability and performance.

An example of a three-layer hierarchical network design is displayed in Figure 1.2 .

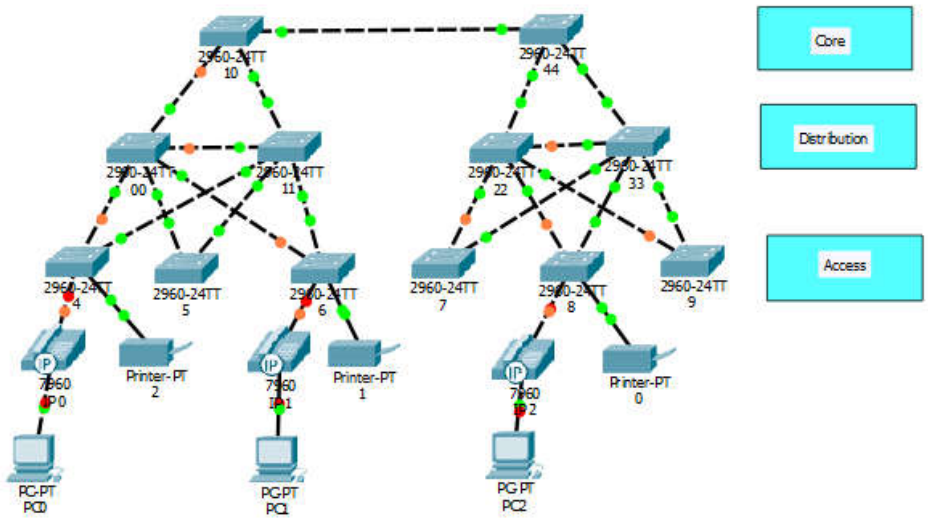


Figure 1.2 : The Hierarchical Network Model.

1.2.2.1 Access Layer

The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points. The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network. [3]

1.2.2.2 Distribution Layer

The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains

by performing routing functions between virtual LANs (VLANs) defined at the access layer. **VLANs** allow you to segment the traffic on a switch into separate subnetworks. For example, in a university you might separate traffic according to faculty, students, and guests. Distribution layer switches are typically high-performance devices that have high availability and redundancy to ensure reliability. [3]

1.2.2.3 Core Layer

The core layer of the hierarchical design is the high-speed backbone of the internetwork. The core layer is critical for interconnectivity between distribution layer devices, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly. [3]

1.3 A Hierarchical Network in a Medium-Sized Business

The hierarchical on the field of business are different than logical topology. It is much harder to see these hierarchical layers when the network is installed in a business.

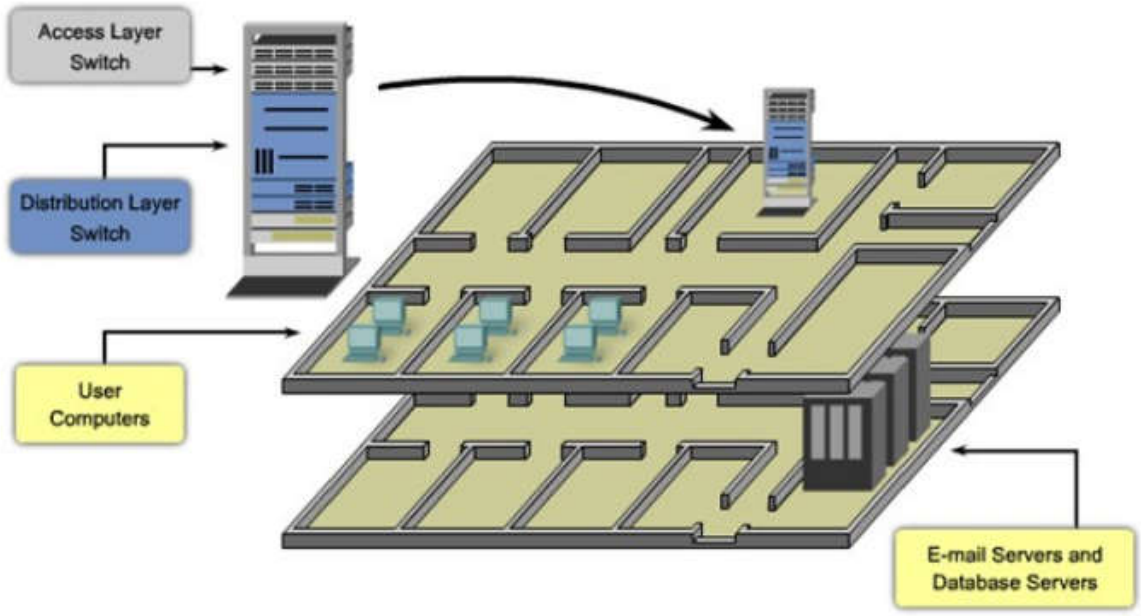


Figure 1.3 : A Hierarchical Network in a Medium-Sized Business. [4]

Let us see the transformation from logical topology to physical Closet on real with using packet-tracer simulation.

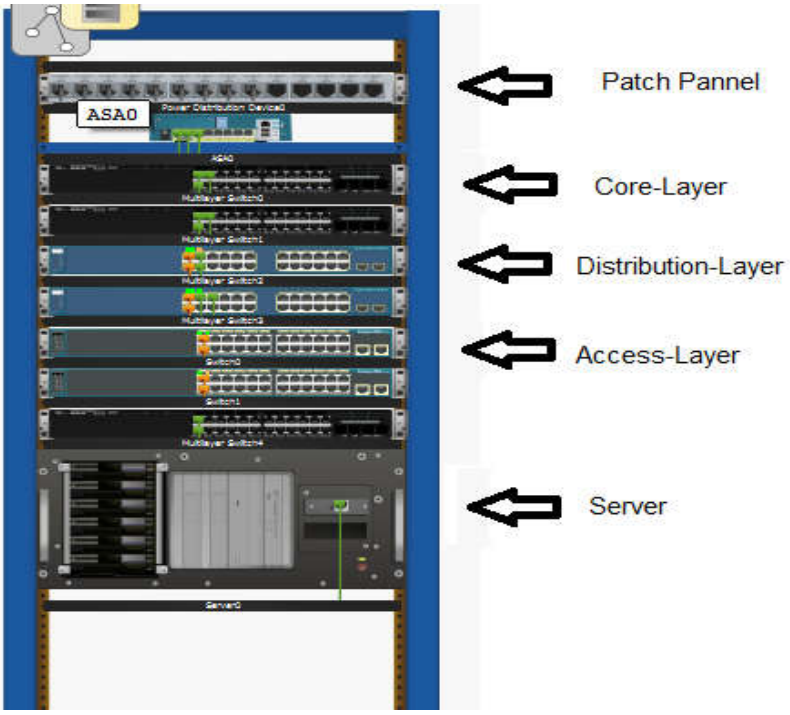


Figure 1.4 : Closet of Campus Design in the reality.

1.4 Benefits of a Hierarchical Network [3]

Many benefits are associated with hierarchical network designs:

- Scalability
- Redundancy
- Performance
- Security
- Maintainability

Scalability

Hierarchical networks scale very well. The modularity of the design allows you to replicate design elements as the network grows. Because each instance of the module is consistent, expansion is easy to plan and implement. For example, if your design model consists of two distribution layer switches for every 10 access layer switches, you can continue to add access layer switches until you have 10 access layer switches cross connected to the two distribution layer switches before you need to add additional distribution layer switches to the network topology. Also, as you add more distribution layer switches to accommodate the load from the access layer switches, you can add additional core layer switches to handle the additional load on the core.

Redundancy

As a network grows, availability becomes more important. You can dramatically increase availability through easy redundant implementations with hierarchical networks. Access layer switches are connected to two different distribution layer switches to ensure path redundancy. If one of the distribution layer switches fails, the access layer switch can switch to the other distribution layer switch. Additionally, distribution layer switches are connected to two or more core layer switches to ensure path availability if a core switch fails. The only layer where redundancy is limited is at the access layer. Typically, end node devices, such as PCs, printers, and IP phones, do not have the capability to connect to multiple access layer switches for redundancy. If an access layer switch fails, just the devices connected to that one switch would be affected by the outage. The rest of the network would continue to function unaffected.

Performance

Communication performance is enhanced by avoiding the transmission of data through low performing, intermediary switches. Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases. The distribution layer then uses its high-performance switching capabilities to forward the traffic up to the core, where it is routed to its final destination. Because the core and distribution layers perform their operations at very high speeds, no contention for network bandwidth occurs. As a result, properly designed hierarchical networks can achieve near wire speed between all devices.

Security

Access layer switches can be configured with various port security options that provide control over which devices are allowed to connect to the network. You also have the flexibility to use more advanced security policies at the distribution layer**.** You may apply access control policies that define which communication protocols are deployed on your network and where they are permitted to go. For example, if you want to limit the use of HTTP to a specific user community connected at the access layer, you could apply a policy that blocks HTTP traffic at the distribution layer. Restricting traffic based on higher layer protocols, such as IP and HTTP, requires that your switches are able to process policies at that layer.

Maintainability

hierarchical networks are easy to maintain but in other network topology designs, maintainability becomes increasingly complicated as the network grows. In some of network design models, there is a finite limit to how large the network can grow before it becomes too complicated and expensive to maintain. In the hierarchical design model, switch functions are defined at each layer, making the selection of the correct switch easier. Adding switches to one layer does not necessarily mean there will not be a bottleneck or other limitation at another layer. For a full mesh network topology to achieve maximum performance, all switches need to be high-performance switches because each switch needs to be capable of performing all the functions on the network. In the hierarchical model, switch functions are different at each layer. You can save money by using less-expensive access layer switches at the lowest layer, and spend more on the distribution and core layer switches to achieve high performance on the network.

1.5 Principles of Hierarchical Network Design [3]

Just because a network seems to have a hierarchical design does not mean that the network is well designed**.** This section will help you differentiate between well-designed and poorly designed hierarchical networks, and transforming a flat network topology into a hierarchical network topology.

Network Diameter

Diameter is traditionally a measure of distance, but this term in networking used to measure the number of devices. Network diameter is the number of devices that a packet has to cross before it reaches its destination. Keeping the network diameter low ensures low and predictable latency between devices.

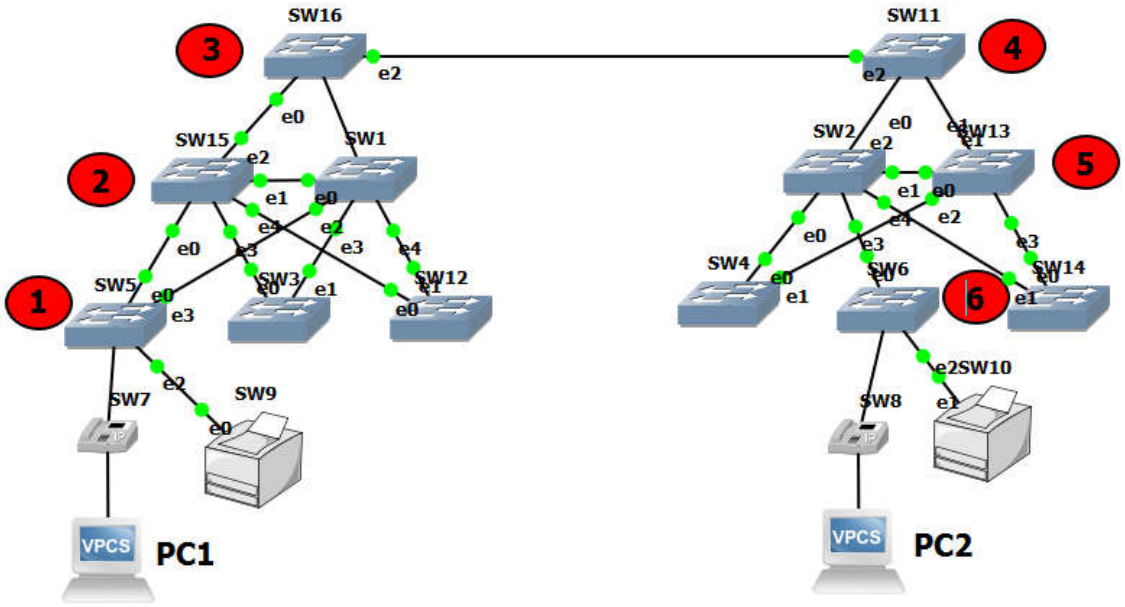


Figure 1.5 : Network Diameter**.**

In Figure 3, PC1 communicates with PC2. Up to six interconnected switches could be between PC1 and PC2. In this case, the network diameter is six. Each switch in the path introduces some degree of latency. Network device latency is the time spent by a device as it processes a packet or frame. Each switch has to determine the destination MAC address of the frame, check its MAC address table, and forward the frame out the appropriate port. Even though that entire process happens in a fraction of a second, the time adds up when the frame has to cross many switches.

In the three-layer hierarchical model, Layer 2 segmentation at the distribution layer practically eliminates network diameter as an issue. In a hierarchical network, network diameter is always going to be a predictable number of hops between the source and destination devices.

Bandwidth Aggregation

Each layer in the hierarchical network model is a possible candidate for bandwidth aggregation. Bandwidth aggregation is the combining of two or more connections to create a logically singular higher bandwidth connection. Each layer in the hierarchical network model is a possible candidate for bandwidth aggregation. Bandwidth aggregation is the combining of two or more connections to create a logically singular higher bandwidth connection. After bandwidth requirements of the network are known, links between

specific switches can be aggregated. Link aggregation allows multiple switch port links to be combined so as to achieve higher throughput between switches. Cisco has a proprietary link aggregation technology called EtherChannel, which allows multiple Ethernet links to be consolidated.

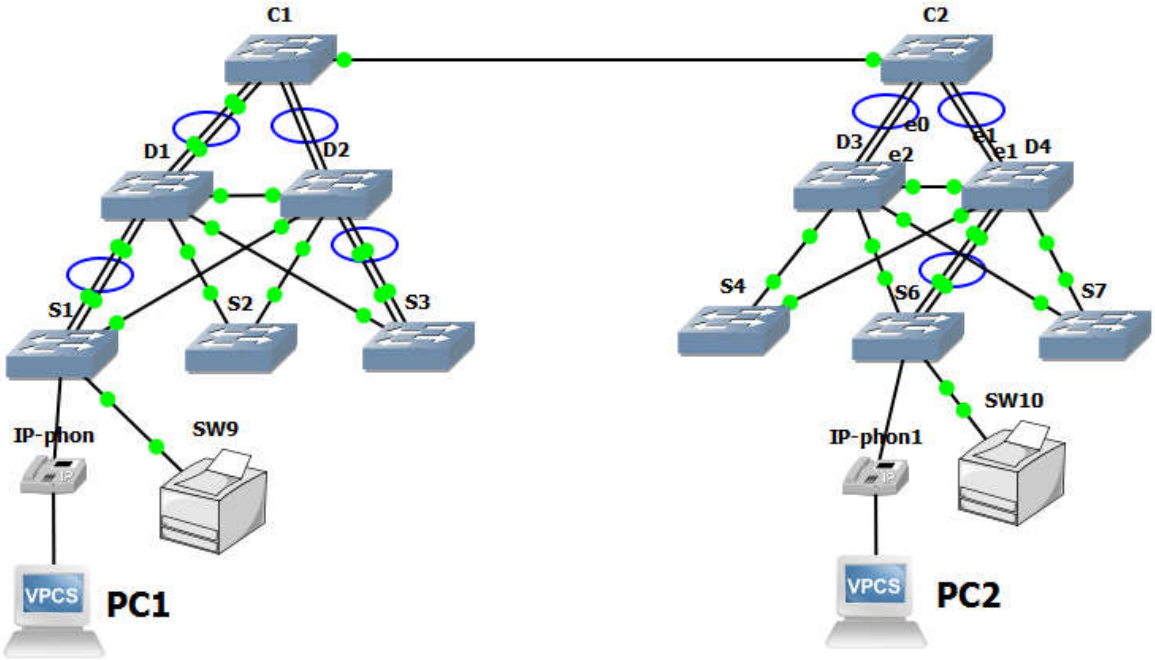


Figure 1.6 : Bandwidth Aggregation**.**

In Figure 1-4, computers PC1 and PC3 require a significant amount of bandwidth because they are frequently used for streaming video. The network manager has determined that the access layer switches S1, S3, and S5 require increased bandwidth. Following up the hierarchy, these access layer switches connect to the distribution switches D1, D2, and D4. The distribution switches connect to core layer switches C1 and C2. Notice how specific links on specific ports in each switch are aggregated. In this way, increased bandwidth is provided for in a targeted, specific part of the network. As is customary, aggregated links are indicated in this figure by two dotted lines with an oval tying them together. The path PC1-S1-D1-C1-C2-D4-S5-PC3 enjoys the enhanced bandwidth resulting from aggregating links.

Redundancy

Redundancy is one part of creating a highly available network. Redundancy can be provided in a number of ways. We can build redundancy into the distribution and core layers of the network, but We can't build it at the access layer because of the cost and limited features in the end devices.

In Figure 6, redundant links are shown at the distribution layer and core layer. At the distribution layer are four distribution layer switches; two distribution layer switches is the minimum required to support redundancy at this layer. The access layer switches, S1, S3, S4, and S6, are cross-connected to the distribution layer switches. The bolder dotted lines here indicate the secondary redundant uplinks. This protects your network if one of the distribution switches fails. In case of a failure, the access layer switch adjusts its transmission path and forwards the traffic through the other distribution switch.

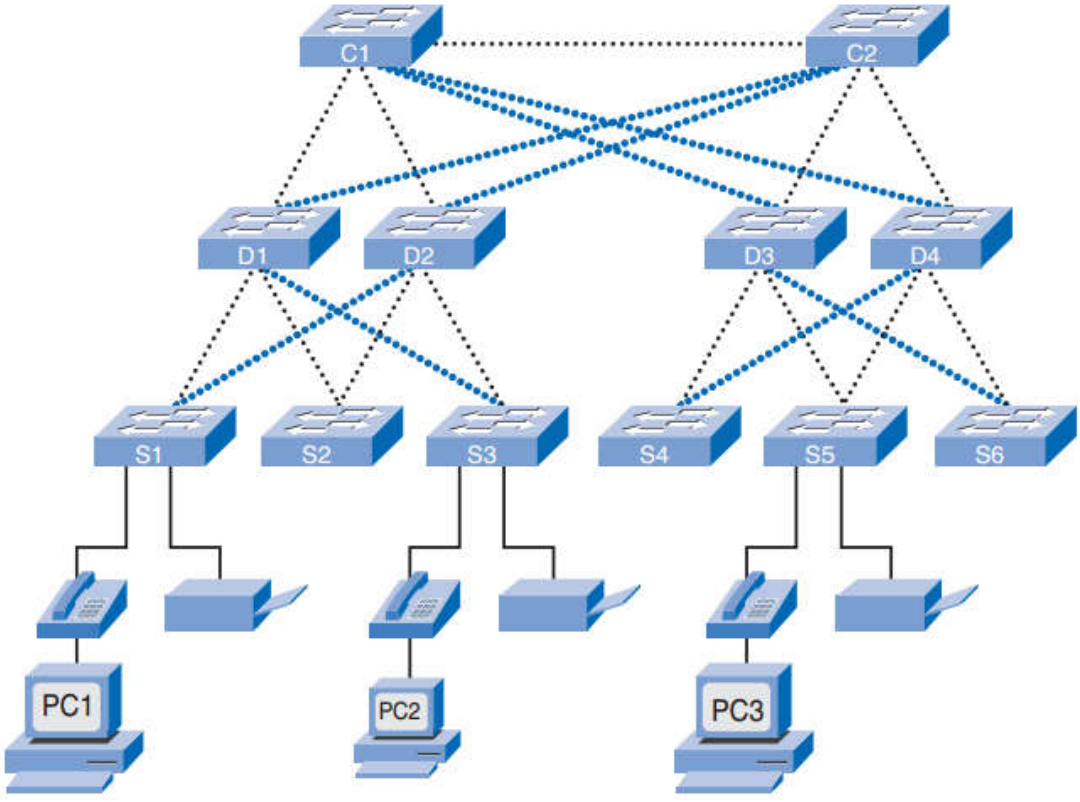


Figure 1.7 : Redundancy**.** [3]

1.6 Matching Switches to Specific LAN Functions [3]

In the hierarchical network layers there are appropriate switch for every layer we have to select, we need to have specification that detail the target traffic flows, user

community, data stores, and data servers. Depend of switched LAN design we will discuss about switch features by details like the form factors, performance and the L3 functionality with technology Power Over Ethernet.

1.6.1 Switch Features

We will see the key of switches that are used in hierarchical networks, and the mean of all acronyms and word phrases when we look up the specifications for a switches, also the mean of PoE and forwarding rate.

1.6.1.1 Switch Form Factors

We need to decide between fixed configuration or modular configuration, and stackable. Another consideration is the thickness of the switch expressed in number of rack units. For example, the fixed configuration switches shown in Figure 1.8 are all 1 rack unit (1U). The physical size of the switches can be an important consideration when selecting switches to be deployed. Networking equipment in a hierarchical design is placed into central locations, such as the wiring closets; oftentimes, the space in these areas is limited, and switch form factors (physical configuration) becomes a significant issue.

Fixed Configuration Switches

Fixed configuration switches are fixed in their configuration. We cannot add features or options to the switch those that beyond originally came with the switch. For example, if you purchase a 24-port gigabit fixed switch, you cannot add additional ports when you need them.

Figure 1.8 : Switch Form Factors**.**

Modular Switches

Modular switches come with different sized chassis that allow for the installation of different numbers of modular line cards. The line cards contain the ports. The larger the chassis, the more modules it can support. As you can see in Figure 1.8**.** We can choose from many chassis sizes. The modular switch with a 24-port line card could easily add an additional 24-port line card to bring the total number of ports up to 48.

Stackable Switches

Cisco introduced StackWise technology in one of its switch product. StackWise allows you to interconnect up to nine switches using fully redundant backplane connections. In Figure 1.8 switches are stacked one atop of the other, and cables connect the switches in daisy-chain fashion and they effectively operate as a single larger switch Stackable switches are desirable where fault tolerance and bandwidth availability are critical and a modular switch is too costly to implement Using cross-connected connections, the network can recover quickly if a single switch fails. Stackable switches use a special port for interconnections and do not use line ports for connection switches, because it will be slower.

1.6.1.2 Switch Performance

We consider the capability of the switch to support the port density, forwarding rates, and bandwidth aggregation requirements of your hierarchical network.

Port Density

Port density is the number of ports available on a single switch. High port densities allow for better use of space and power when both are in limited supply. If we have two switches that each contain 24 ports, we would be able to support up to 46 devices because we lose at least one port per switch to connect each switch to the rest of the network. In addition, two power outlets are required. Moreover, if we have a single 48-port switch, 47 devices can be supported, with only one port used to connect the switch to the rest of the network, and only one power outlet needed to accommodate the single switch.

Figure 1.9 : Port Density**.**

Forwarding Rates

Forwarding rates define the processing capabilities of a switch by rating how much data the switch can process per second. If the switch forwarding rate is too low, it cannot accommodate full wire-speed communication across all its switch ports. Wire speed is the data rate that each port on the switch is capable of attaining either 100 Mbps Fast Ethernet or 1000 Mbps Gigabit Ethernet. For example, a 48-port gigabit switch operating at full wire speed generates 48 Gbps of traffic. If the switch supports a forwarding rate of only 32 Gbps, it cannot run at full wire speed across all ports simultaneously. Fortunately, access layer switches typically do not need to operate at full wire speed because they are

physically limited by their uplinks to the distribution layer. This allows you to use less expensive, lower-performing switches at the access layer, and use the more expensive, higher-performing switches at the distribution and core layers, where the forwarding rate makes a bigger difference.

Figure 1.10 : Forwarding Rates.

Link Aggregation

Link aggregation helps to reduce these bottlenecks of traffic by allowing up to eight switch ports to be bound together for data communications, providing up to 16 Gbps of data throughput when Gigabit Ethernet ports are used. Cisco uses the term EtherChannel when describing aggregated switch ports.

1.6.1.3 Power over Ethernet

Power over Ethernet (PoE) allows the switch to deliver power to a device over the existing Ethernet cabling. We can plug any of IP phone, access point into the PoE, without consider how to run ordinary power to the device.

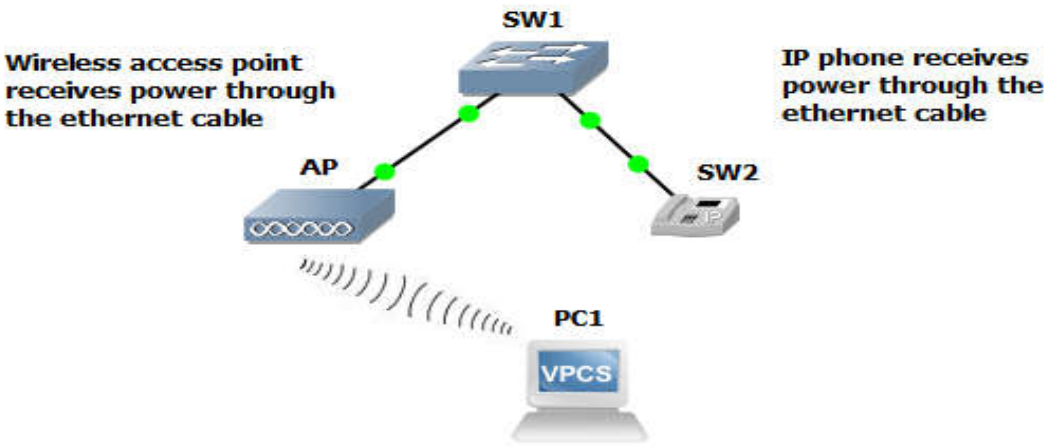


Figure 1.11 : Power over Ethernet**.**

1.6.1.4 Layer 3 Functionality

Typically, switches operate at Layer 2 of the OSI reference model, where they deal primarily with the MAC addresses of devices connected to switch ports. Layer 3 switches offer advanced functionality which is routing. Otherwise, instead of deal with physical addresses they deal with IP addresses. Layer 3 switches are also known as multilayer switches.

1.6.2 Switch Features in a Hierarchical Network

In this part we are going to examine which features are required at each layer in a hierarchical network.

1.6.2.1 Access Layer Switch Features

Access layer switches facilitate the connection of end node devices to the network. For this reason, they need to support features such as port security, VLANs, Fast Ethernet/Gigabit Ethernet, PoE, and link aggregation as shown in Figure 1.12**.**

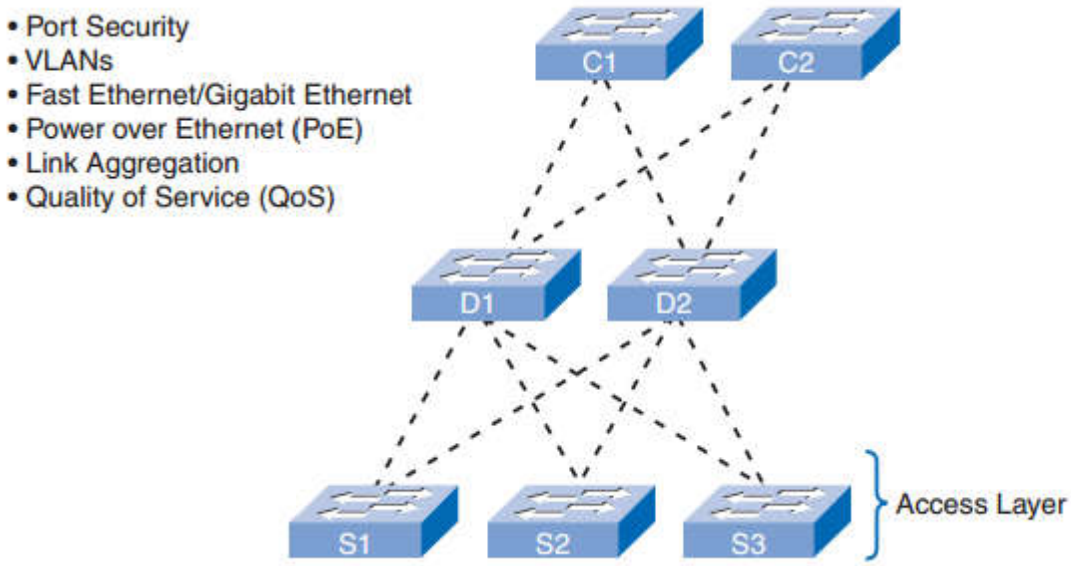


Figure 1.12 : Access Layer Switch Features**.**

Port security allows the switch to decide how many or what specific devices are allowed to connect to the switch**.** Port security is applied at the access.

VLANs are important component for separate the traffic, voice traffic can be supported with more bandwidth, more redundant connections, and improved security.

Access layer switches allow you to set the VLANs for the end node devices on your network.

Port speed is also a characteristic for access layer switches. Most modern devices, such as workstations, notebooks, and IP phones, support Gigabit Ethernet. This allows for much more efficient data transfers, enabling users to be more productive.

PoE should be considered only when voice convergence is required or wireless access points are being implemented, and power is difficult or expensive to run to the desired location.

access layer switches need to support QoS (Quality of Service) to maintain the prioritization of traffic. Cisco IP phones are types of equipment that are found at the access layer. When a Cisco IP phone is plugged into an access layer switch port configured to support voice traffic, that switch port tells the IP phone how to send its voice traffic. QoS needs to be enabled on access layer switches so that voice traffic from the IP phone has priority over, for example, data traffic.

1.6.2.2 Distribution Layer Switch Features

Distribution layer switches receive the data from all the access layer switches and forward it to the core layer switches. Distribution layer switches provide the inter-VLAN routing functions so that one VLAN can communicate with another on the network.

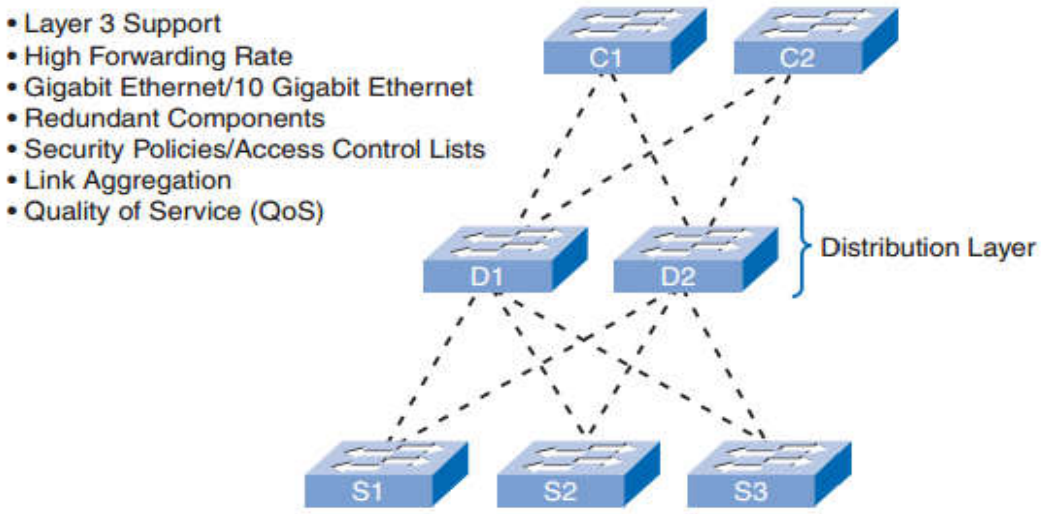


Figure 1.13 : Distribution Layer Switch Features**.**

Distribution layer switches provide the inter-VLAN routing functions so that one VLAN can communicate with another on the network. This routing typically takes place at the distribution layer because distribution layer switches have higher processing capabilities than the access layer switches. Distribution layer switches alleviate the core switches from needing to perform that task, because the core is busy handling the forwarding of very high volumes of traffic. Because inter-VLAN routing is performed at the distribution layer, the switches at this layer need to support Layer 3 functions, and because of the advanced security policies that can be applied to network traffic.

Access lists are used to control how traffic flows through the network. An access control list (ACL) allows the switch to prevent certain types of traffic and permit others. ACLs also allow you to control which network devices can communicate on the network. Using ACLs is processing intensive because the switch needs to inspect every packet to see if it matches one of the ACL rules defined on the switch.

Because distribution layer switches accept incoming traffic from multiple access layer switches, they need to be able to forward all that traffic as fast as possible to the core layer switches. As a result, distribution layer switches also need high-bandwidth aggregated links back to the core layer switches. Newer distribution layer switches support aggregated 10 Gigabit Ethernet (10GbE) uplinks to the core layer switches.

Finally, distribution layer switches need to support QoS to maintain the prioritization of traffic coming from the access layer switches that have implemented QoS. Priority policies ensure that audio and video communications are guaranteed adequate bandwidth to maintain an acceptable quality of service. To maintain the priority of the voice data throughout the network, all the switches that forward voice data must support QoS; if not all the network devices support QoS, the benefits of QoS will be reduced. This results in poor performance and quality for audio and video communications.

1.6.2.3 Core Layer Switch Features

Core layer switches are responsible for handling the majority of data on a switched LAN**.**

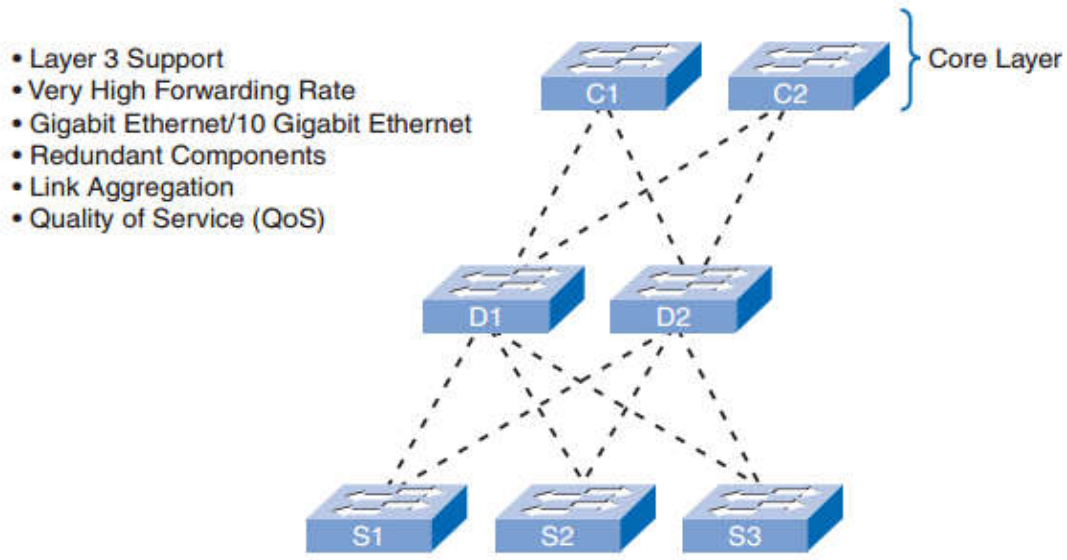


Figure 1.14 : Core Layer Switch Features**.**

The core layer is the high-speed backbone of the network and requires switches that can handle very high forwarding rates.

The availability of the core layer is also critical, so you should build in as much redundancy as you can. Layer 3 redundancy typically has faster convergence than Layer 2 redundancy in the event of hardware failure. Convergence in this context refers to the time it takes for the network to adapt to a change**.** Also, look for core layer switches that support additional hardware redundancy features, such as redundant power supplies that can be swapped while the switch continues to operate.

Because of the high workload carried by core layer switches, they tend to operate hotter than access or distribution layer switches, so they should have more sophisticated cooling options. Many true core-layer capable switches have the capability to swap cooling fans without having to turn the switch off.

The core layer also needs to support link aggregation to ensure adequate bandwidth coming into the core from the distribution layer switches. Core layer switches should have support for aggregated 10 Gigabit Ethernet connections, which is currently the fastest available Ethernet connectivity option. This allows corresponding distribution layer switches to deliver traffic as efficiently as possible to the core.

QoS is an important part of the services provided by core layer switches. For example, service providers (who provide IP, data storage, e-mail, and other services) and

enterprise widearea networks (WANs) are adding more voice and video traffic to an already growing amount of data traffic. At the core and network edge, mission-critical and time-sensitive traffic such as voice should receive higher QoS guarantees than less time-sensitive traffic such as file transfers or e-mail. Because high-speed WAN access is often prohibitively expensive, adding bandwidth at the core layer is not an option. Because QoS provides software-based solution to prioritize traffic, core layer switches can provide a cost-effective way of supporting optimal and differentiated use of existing bandwidth.

1.7 Switches for Small and Medium Sized Business (SMB)

Cisco currently has seven switch product lines. Each product line offers different characteristics and features, allowing you to find the right switch to meet the functional requirements of your network. The Cisco switch product lines are as follows:

- Catalyst Express 500
- Catalyst 2960
- Catalyst 3560
- Catalyst 3750
- Catalyst 4500
- Catalyst 4900
- Catalyst 6500

first of all we need to define how many devices depend on the size business as follows :

- **Small network**: Provides services for up to 200 devices.[2]
- **Medium-size network**: Provides services for 200 to 1,000 devices.[2]
- **Large network**: Provides services for 1,000+ devices. [2]

We select a three specific Cisco product lines depend on hierarchical layer :

Catalyst 3560 [3]

The Cisco Catalyst 3560 series is a line of enterprise-class switches that include support for PoE, QoS, and advanced security features such as ACLs. These switches, shown in Figure 1.15, are ideal access layer switches for small enterprise LAN access or branch-office converged network environments.

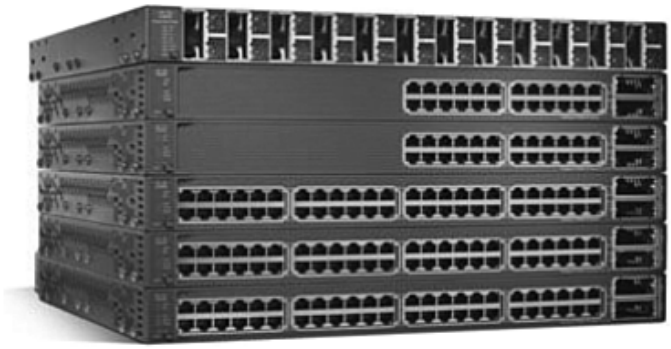


Figure 1.15 : Catalyst 3560.

The Cisco Catalyst 3560 series supports forwarding rates of 32 Gbps to 128 Gbps (Catalyst 3560-E switch series).

The Catalyst 3560 series switches are available in different fixed configurations:

- Fast Ethernet and Gigabit Ethernet connectivity.
- Up to 48 10/100/1000 ports, plus four small form-factor pluggable ports.
- Optional 10 Gigabit Ethernet connectivity in the Catalyst 3560-E models.
- Optional integrated PoE (Cisco prestandard and IEEE 802.3af); up to 24 ports with 15.4 watts or 48 ports with 7.3 watts.

Catalyst 4500 [3]

The Catalyst 4500, shown in Figure 15, is the first midrange modular switching platform offering multilayer switching for enterprises, small- to medium-sized businesses, and service providers.

Figure 1.16 : Catalyst 4500.

With forwarding rates up to 136 Gbps, the Catalyst 4500 series is capable of managing traffic at the distribution layer. The modular capability of the Catalyst 4500 series allows forvery high port densities through the addition of switch port line cards to its modular chassis. The Catalyst 4500 series offers multilayer QoS and sophisticated routing functions.

The Catalyst 4500 series switches are available in different modular configurations:

- Modular 3, 6, 7, and 10 slot chassis offering different layers of scalability.
- High port density: up to 384 Fast Ethernet or Gigabit Ethernet ports available in copper or fiber with 10 Gigabit uplinks.
- PoE (Cisco prestandard and IEEE 802.3af).
- Dual, hot-swappable internal AC or DC power supplies.
- Advanced hardware-assisted IP routing capabilities.

Catalyst 6500 [3]

The Catalyst 6500 series modular switch, shown in Figure 16, is optimized for secure, converged voice, video, and data networks. The Catalyst 6500 is capable of managing traffic at the distribution and core layers. The Catalyst 6500 series is the highest-performing Cisco switch, supporting forwarding rates up to 720 Gbps. The Catalyst 6500 is ideal for very large network environments found in enterprises, medium-sized businesses, and service providers.

Figure 1.17 : Catalyst 6500.

The Catalyst 6500 series switches are available in different modular configurations:

- Modular 3, 4, 6, 9, and 13 slot chassis.
- LAN/WAN service modules.
- PoE up to 420 IEEE 802.3af Class 3 (15.4W) PoE devices.
- Up to 1152 10/100 ports, 577 10/100/1000 ports, 410 SFP Gigabit Ethernet ports, or 64 10 Gigabit Ethernet ports.
- Dual, hot-swappable internal AC or DC power supplies.
- Advanced hardware-assisted IP routing capabilities.

1.8 Conclusion

On this chapter, we had began exploring some of principles that are used to design a hierarchical network. The switched LAN architecture based on hierarchical network, and we listed a several rules that are followed to select the correct switch, switches are the best suited for each hierarchical layer of the network depending on their features. Each layer with their specific functions make the network easier to manage and expand, and problems are solved more quickly.

Chapter 2 : Switch Concepts And Protocols

2.1 Introduction

Our studies in this chapter, the principal Ethernet operation, we will see how Ethernet communication function and how a switch play a role in this communication, and what are the function that enable a switch to forward Ethernet frame in a LAN inside every campus network. Moreover, our interest is about the malicious threats to switches, and how we could prevent that risk at least by basic security configuration.

2.2 Ethernet/802.3 Networks [3]

The key components of the Ethernet standard that play a significant role in the design and implementation of switched networks. exploring how Ethernet communications function and how switches play a role in the communication process.

Ethernet/802.3 networks rely on carrier sense multiple access/collision detect (CSMA/CD), unicast transmission, broadcast transmission, multicast transmission, duplex settings, switch port settings, and MAC address table management.

2.2.1 CSMA/CD

Ethernet signals are transmitted to every host connected to the LAN using a special set of rules to determine which station can access the network. The set of rules that Ethernet uses is based on the IEEE carrier sense multiple access/collision detect (CSMA/CD) technology. Recall that CSMA/CD is used only with half-duplex communication typically found with hubs. Full-duplex ports do not use CSMA/CD. [3]

In the CSMA/CD access method, all network devices that have messages to send must listen before transmitting. If a device detects a signal from another device, it waits for a specified amount of time before attempting to transmit. When there is no traffic detected, a device transmits its message. While this transmission is occurring, the device continues to listen for traffic or collisions on the LAN. After the message is sent, the device returns to its default listening mode. [3]

If the distance between devices is such that the latency of the signals of one device means that signals are not detected by a second device, the second device may also start to transmit. The media now has two devices transmitting signals at the same time. The messages propagate across the media until they encounter each other. At that point, the

signals mix and the messages are destroyed, a collision. Although the messages are corrupted, the jumble of remaining signals continues to propagate across the media.

When a device is in listening mode, it can detect when a collision occurs on the shared media because all devices can detect an increase in the amplitude of the signal above the normal level. When a collision occurs, the other devices in listening mode, as well as all the transmitting devices, detect the increase in the signal amplitude. Every device that is transmitting continues to transmit to ensure that all devices on the network detect the collision.

When a collision is detected, the transmitting devices send out a jamming signal. The jamming signal notifies the other devices of a collision so that they invoke a backoff algorithm. This backoff algorithm causes all devices to stop transmitting for a random amount of time, which allows the collision signals to subside.

After the delay has expired on a device, the device goes back into the "listening before transmit" mode. A random backoff period ensures that the devices that were involved in the collision do not try to send traffic again at the same time, which would cause the whole process to repeat. However, during the backoff period, a third device may transmit before either of the two involved in the collision have a chance to retransmit.

2.2.2 Ethernet Communications

Reference Figure 17 for the Ethernet communications discussion that follows. Communications in a switched LAN occur in three ways: unicast, broadcast, and multicast.

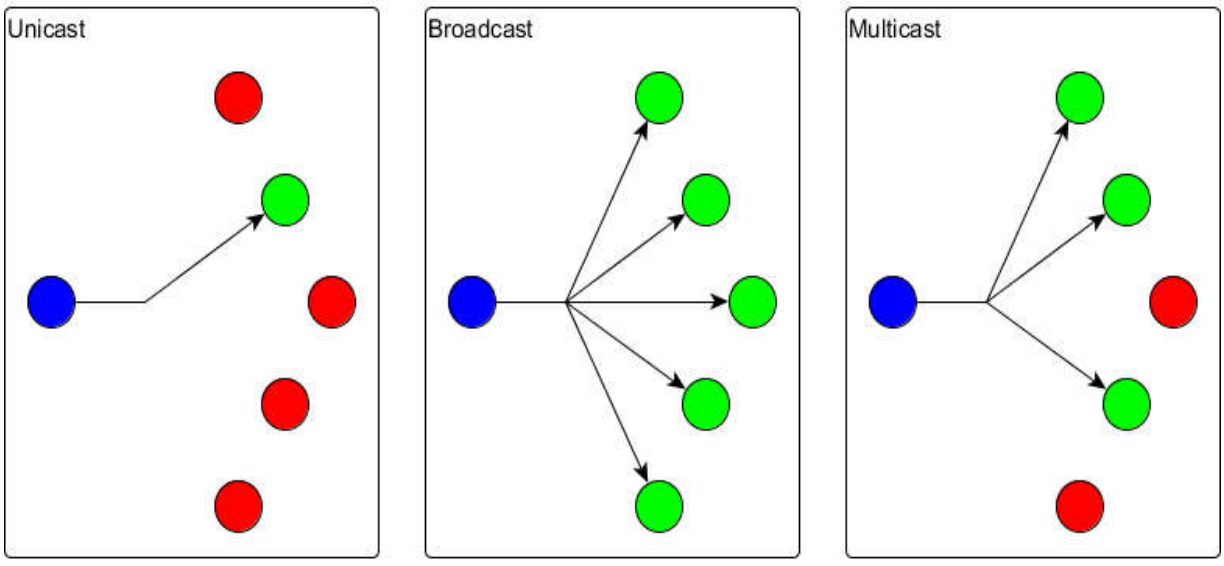


Figure 2.1 : Ethernet Communications. [5]

With unicast communication, a frame is sent from one host and addressed to one specific destination. In unicast transmission, there is just one sender and one receiver. Unicast transmission is the predominant form of transmission on LANs and within the Internet. Examples of unicast transmissions include HTTP, SMTP, FTP, and Telnet.

With broadcast communication, a frame is sent from one address to all other addresses. In this case, there is just one sender, but the information is sent to all connected receivers. Broadcast transmission is essential when sending the same message to all devices on the LAN. An example of a broadcast transmission is the address resolution query that the address resolution protocol (ARP) sends to all computers on a LAN.

With multicast communication, a frame is sent to a specific group of devices or clients. Multicast transmission clients must be members of a logical multicast group to receive the information. An example of multicast transmission is the video and voice transmissions associated with a network-based, collaborative business meeting.

To briefly review the Ethernet frame structure, recall that the Ethernet frame adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent. Both the Ethernet header and trailer have several sections (or fields) of information that are used by the Ethernet protocol. Figure 2-2 shows the structure of the current Ethernet frame standard, the revised IEEE 802.3 (Ethernet).

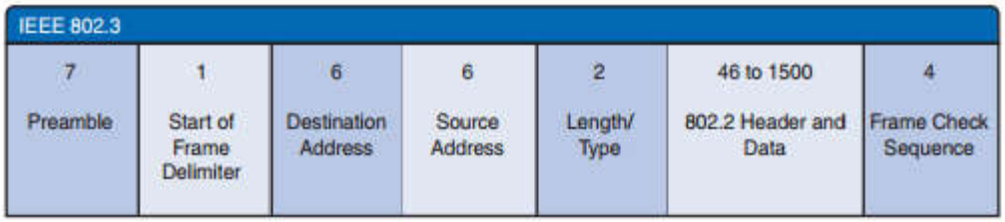


Figure 2.2 : Ethernet Frame.

The Preamble (7 bytes) and Start Frame Delimiter (SFD) (1 byte) fields are used for synchronization between the sending and receiving devices. These first 8 bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.

The Destination MAC Address field (6 bytes) is the identifier for the intended recipient. This address is used by Layer 2 to assist a device in determining whether a frame

is addressed to it. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame.

The Source MAC Address field (6 bytes) identifies the frame's originating NIC or interface. Switches use this address to add to their lookup tables.

The Length/Type field (2 bytes) defines the exact length of the frame's data field. This field is used later as part of the Frame Check Sequence (FCS) to ensure that the message was received properly. Only a frame length or a frame type can be entered here. If the purpose of the field is to designate a type, the Type field describes which protocol is implemented. When a node receives a frame and the Length/Type field designates a type, the node determines which higher layer protocol is present. If the two-octet value is equal to or greater than 0x0600 hexadecimal or 1536 decimal, the contents of the Data Field are decoded according to the protocol indicated; if the two-byte value is less than 0x0600, the value represents the length of the data in the frame.

The Data and Pad fields (46 to 1500 bytes) contain the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, an IPv4 packet. All frames must be at least 64 bytes long (minimum length aides the detection of collisions). If a small packet is encapsulated, the Pad field is used to increase the size of the frame to the minimum size.

The FCS field (4 bytes) detects errors in a frame. It uses a cyclic redundancy check (CRC). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error has occurred. If the calculations do not match, the frame is dropped.

An Ethernet MAC address is a two-part 48-bit binary value expressed as 12 hexadecimal digits. The address formats might be similar to 00-05-9A-3C-78-00, 00:05:9A:3C:78:00, or 0005.9A3C.7800. All devices connected to an Ethernet LAN have MAC-addressed interfaces. The NIC uses the MAC address to determine whether a message should be passed to the upper layers for processing. The MAC address is permanently encoded into a ***read-only memory (ROM)*** chip on a NIC. This type of MAC address is referred to as a burned-in address (BIA). Some vendors allow local modification of the MAC address. The MAC address is made up of the **organizational unique**

identifier (OUI) and the vendor assignment number. The OUI is the first part of a MAC address. It is 24 bits long and identifies the manufacturer of the NIC card. The IEEE regulates the assignment of OUI numbers. Within the OUI are 2 bits that have meaning only when used in the destination address, the broadcast or multicast bit and the locally administered address bit, shown in Figure 19.

Figure 2.3 : OUI Composition.

The broadcast or multicast bit in a MAC address indicates to the receiving interface that the frame is destined for all or a group of end stations on the LAN segment.

The locally administered address bit indicates whether the vendor-assigned MAC address can be modified locally.

The vendor-assigned part of the MAC address is 24 bits long and uniquely identifies the Ethernet hardware. It can be a BIA or it can be modified by software indicated by the local bit.

2.2.3 Duplex Settings

There are two types of duplex settings used for communications on an Ethernet network: **half duplex** and **full duplex**.

Half-duplex communication relies on unidirectional data flow where sending and receiving data are not performed at the same time. This is similar to how walkie-talkies or two-way radios function in that only one person can talk at any one time. If someone talks while someone else is already speaking, a collision occurs. As a result, half-duplex communication implements CSMA/CD to help reduce the potential for collisions and detect them when they do happen. Half-duplex communications have performance issues due to the constant waiting, because data can flow in only one direction at a time. Half-duplex connections are typically found in older hardware, such as hubs. Nodes that are attached to hubs that share their connection to a switch port must operate in half-duplex mode because the end computers must be able to detect collisions. Nodes can operate in a

half-duplex mode if the NIC card cannot be configured for full-duplex operations. In this case, the port on the switch defaults to a half-duplex mode as well. Because of these limitations, full-duplex communication has replaced half-duplex in more current hardware.

In full-duplex communication, data flow is bidirectional, so data can be sent and received at the same time. The bidirectional support enhances performance by reducing the wait time between transmissions. Most Ethernet, Fast Ethernet, and Gigabit Ethernet NICs sold today offer full-duplex capability. In full-duplex mode, the collision-detect circuit is disabled. Frames sent by the two connected end nodes cannot collide because the end nodes use two separate circuits in the network cable. Each full-duplex connection uses only one port. Full-duplex connections require a switch that supports full duplex or a direct connection between two nodes that each support full duplex. Nodes that are directly attached to a dedicated switch port with NICs that support full duplex should be connected to switch ports that are configured to operate in full-duplex mode.

2.2.4 Switch Port Settings

A port on a switch needs to be configured with duplex settings that match the media type. The Cisco Catalyst switches have three settings :

- The **auto** option sets autonegotiation of duplex mode. With autonegotiation enabled, the two ports communicate to decide the best mode of operation.
- The **full** option sets full-duplex mode.
- The **half** option sets half-duplex mode.

2.2.5 Switch MAC Address Table

A switch determines how to handle incoming data frames by using its MAC address table. A switch builds its MAC address table by recording the MAC addresses of the nodes connected to each of its ports. After a MAC address for a specific node on a specific port is recorded in the address table, the switch then knows to send traffic destined for that specific node out the port mapped to that node for subsequent transmissions.

When an incoming data frame is received by a switch and the destination MAC address is not in the table, the switch forwards the frame out all ports, except for the port on which it was received. When the destination node responds, the switch records the node’s MAC address in the address table from the frame’s source address field. In

networks with multiple interconnected switches, the MAC address tables record multiple MAC addresses for the ports connecting the switches that reflect the nodes beyond.

The following six steps describe the process used to populate the MAC address table on a switch :

- Receives a broadcast frame from PC1 on Port 1, as seen in Figure 20.
- The switch enters the source MAC address and the switch port that received the frame into the address table.
- Because the destination address is a broadcast, the switch ***floods*** the frame to all ports, except the port on which it received the frame.

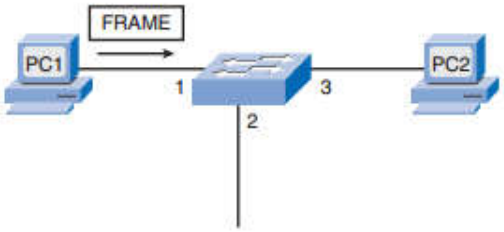


Figure 2.4 : MAC Address Table Population.

- The destination device replies to the broadcast with a unicast frame addressed to PC1.
- The switch enters the source MAC address of PC2 and the port number of the switch port that received the frame into the address table. The destination address of the frame and its associated port are found in the MAC address table.
- The switch can now forward frames between source and destination devices without flooding, because it has entries in the address table that identify the associated ports.

```
Switch#sh mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0005.5e7b.59dd    DYNAMIC     Fa0/1
   1    0030.a303.edbb    DYNAMIC     Fa0/2
Switch#
```

Figure 2.5 : Example Mac-Address-Table using Packet-tracer.

2.3 Design Considerations for Ethernet/802.3 Networks [3]

This section focuses on broadcast and collision domains and how they affect LAN designs.

2.3.1 Bandwidth and Throughput

A major disadvantage of Ethernet 802.3 networks is collisions. Collisions occur when two hosts transmit frames simultaneously. When a collision occurs, the transmitted frames are corrupted or destroyed. The sending hosts stop sending further transmissions for a random period, based on the Ethernet 802.3 rules of CSMA/CD.

Because Ethernet has no way of controlling which node will be transmitting at any time, we know that collisions will occur when more than one node attempts to gain access to the network. Ethernet's resolution for collisions does not occur instantaneously. Also, a node involved in a collision cannot start transmitting until the matter is resolved. As more devices are added to the shared media, the likelihood of collisions increases. Because of this, it is important to understand that when stating that the bandwidth of the Ethernet network is 10 Mbps, full bandwidth for transmission is available only after any collisions have been resolved. The net throughput of the port (the average data that is effectively transmitted) will be considerably reduced as a function of how many other nodes want to use the network. A hub offers no mechanisms to either eliminate or reduce these collisions, and the available bandwidth that any one node has to transmit is correspondingly reduced. As a result, the number of nodes sharing the Ethernet network will have an effect on the throughput or productivity of the network.

2.3.2 Collision Domains

When expanding an Ethernet LAN to accommodate more users with more bandwidth requirements, the potential for collisions increases. To reduce the number of nodes on a given network segment, you can create separate physical network segments, called collision domains, as shown in Figure 2.6.

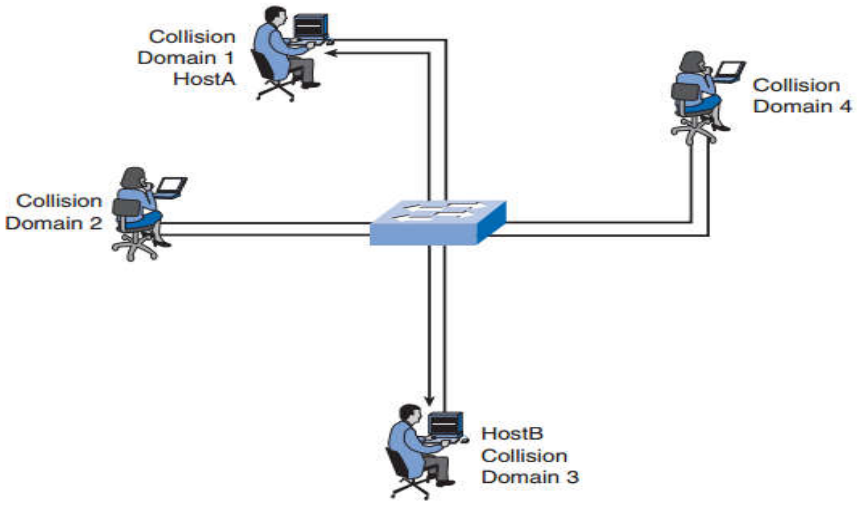


Figure 2.6 : Collision Domains.

The network area where frames originate and collide is called the collision domain. All shared media environments, such as those created by using hubs, are collision domains. When a host is connected to a switch port, the switch creates a dedicated connection. This connection is considered an individual collision domain because traffic is kept separate from all other traffic, thereby eliminating the potential for a collision. The figure shows unique collision domains in a switched environment. For example, if a 12-port switch has a device connected to each port, 12 collision domains are created.

As you now know, a switch builds a MAC address table by learning the MAC addresses of the hosts that are connected to each switch port. When two connected hosts want to communicate with each other, the switch uses the switching table to establish a connection between the ports. The circuit is maintained until the session is terminated. In Figure 22, HostA and HostB want to communicate with each other. The switch creates the connection that is referred to as a microsegment. The microsegment behaves as if the network has only two hosts, one host sending and one receiving, providing maximum utilization of the available bandwidth.

Switches reduce collisions and improve bandwidth use on network segments because they provide dedicated bandwidth to each network segment.

2.3.4 Broadcast Domains

Although switches filter most frames based on MAC addresses, they do not filter broadcast frames. A collection of interconnected switches forms a single broadcast

domain. Only a Layer 3 entity, such as a router, or a **virtual LAN (VLAN)**, can bound a Layer 2 broadcast domain. Routers and VLANs are used to segment both collision and broadcast domains.

The broadcast domain at Layer 2 is referred to as the MAC broadcast domain. The MAC broadcast domain consists of all devices on the LAN that receive frame broadcasts by a host on the LAN.

When a switch receives a broadcast frame, it forwards the frame to each of its ports, except the incoming port where the switch received the broadcast frame.

2.4 Switching protocols

We have two types of switching, first the layers 2 switch which we have already done. The heart of a Layer 2 switch is its MAC address table. So now we could understand the layer 3 switches how its work, A Layer 3 switch performs all the same functions as a router. Including **switching** topic we have several protocols and policies could configure it in the switches, Virtual LANs, trunks, spanning tree protocols, VTP protocol. [3]

2.4.1 Virtual LANs

A VLAN (virtual LAN) is a logical grouping of networked nodes that communicate directly with each other on Layers 2 and 3. VLANs are also called logical LANs because they aren't created physically using Layer 1 media and devices. Instead, they're created logically or virtually through the configuration on a router or switch. [6]

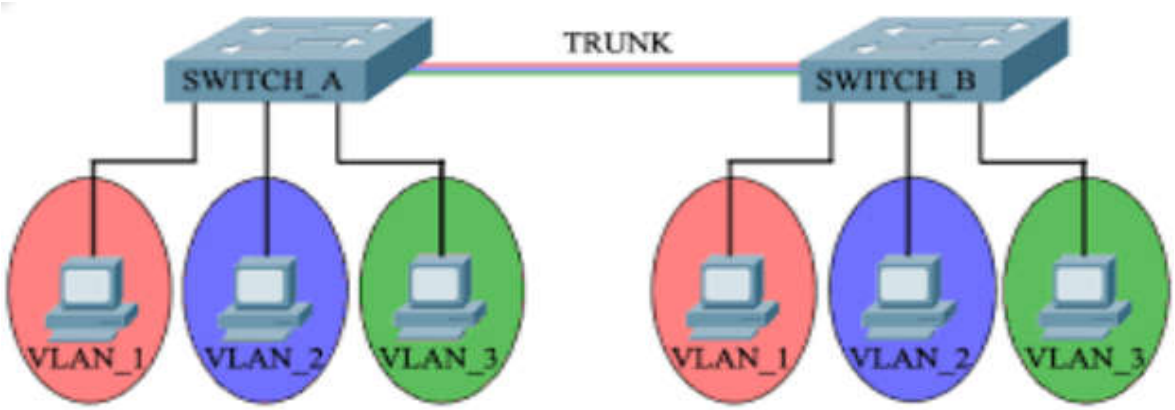


Figure 2.7 : Topology VLANs groups. [7]

2.4.2 trunk

Normally, segmenting a LAN with switches involves the creation of at least two VLANs across two or more switches. After the VLANs are created, any information about them is shared between the switches using a trunking protocol. [6]

trunking methods:

- **Inter-Switch Link (ISL):** ISL is a proprietary Cisco protocol that's supported only between Cisco Devices.
- **IEEE 802.1Q:** The 802.1 subcommittee defines this as an industry standard protocol that allows VLAN information exchange between dissimilar manufacturers equipment. [6]

2.4.3 Spanning Tree Protocol

sometimes we need redundancy between two switches. Unfortunately for us redundancy also brings **loops**. take a look at the figure 2.8 :

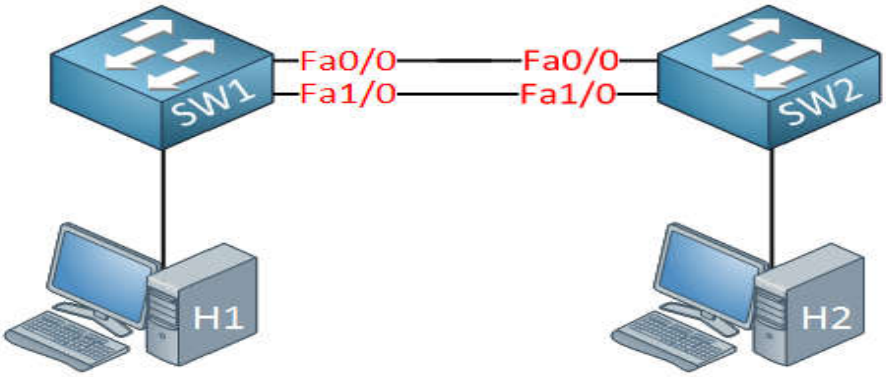


Figure 2.8 : redundancy between two switches. [8]

Why do we have a loop in the scenario above?

- H1 sends an ARP request because it’s looking for the MAC address of H2. An ARP request is a broadcast frame.
- SW1 will forward this broadcast frame on all it interfaces, except the interface where it received the frame on.
- SW2 will receive both broadcast frames. [8]

Spanning-tree will help us to create a **loop-free topology** by blocking certain interfaces. Since spanning tree is enabled, all our switches will send a special frame to each other called a **BPDU (Bridge Protocol Data Unit)**. [8] In this BPDU there are two pieces of information that spanning-tree requires:

- MAC Address.
- priority.

The switch with the **lowest** MAC Address and priority is the best one.

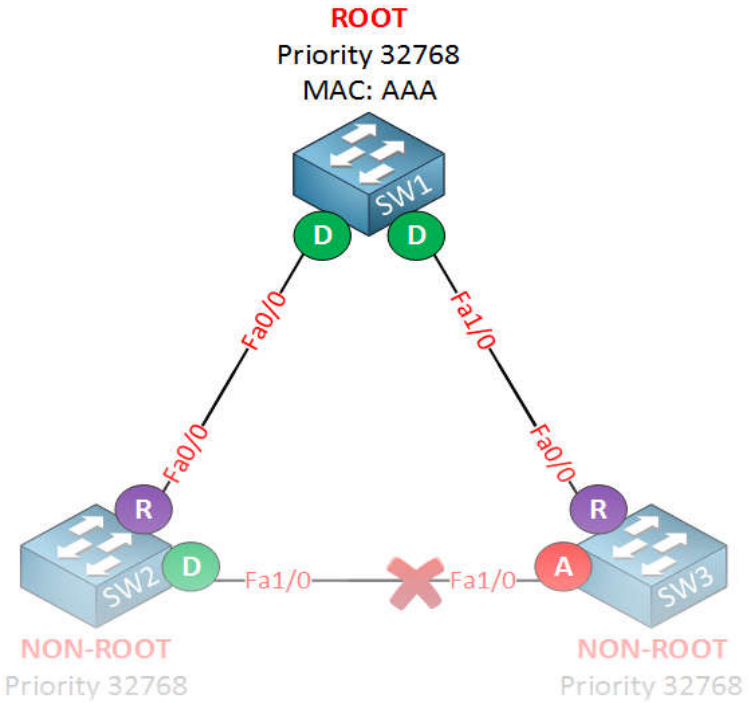


Figure 2.9 : Describe of root bridge selection.[8]

2.4.4 VTP (VLAN Trunking Protocol)

VLAN Trunking Protocol (VTP) will let you create VLANs on one switch and all the other switches will synchronize themselves. [9]

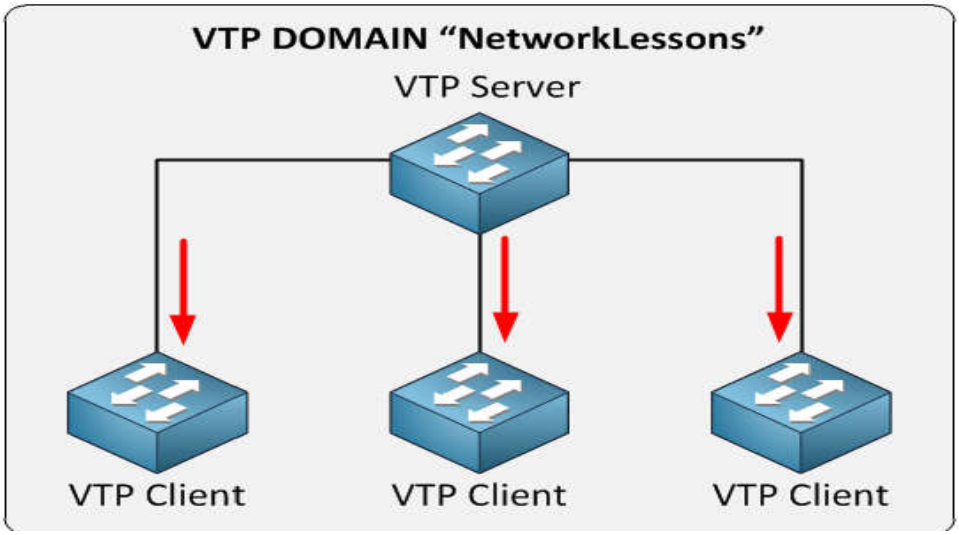


Figure 2.10 : Represent VTP Domain. [9]

We have one VTP server which is the switch where you create / modify or delete VLANs. The other switches are VTP clients. The VTP configuration has a revision number which will increase when you make a change. Every time you make a change on the VTP server this will be synchronized to the VTP clients. Oh and by the way you can have multiple VTP servers since it also functions as a VTP client so you can make changes on multiple switches in your network. In order to make VTP work you need to setup a VTP domain name which is something you can just make up, as long as you configure it to be the same on all your switches. [9]

2.4.5 SVI (Switched Virtual Interface)

To allow remote access to a Cisco IOS Catalyst switch with protocols like telnet or SSH, we need to configure an IP address on the switch. You also need this if you want to use any network management tools to monitor your switch. [10]

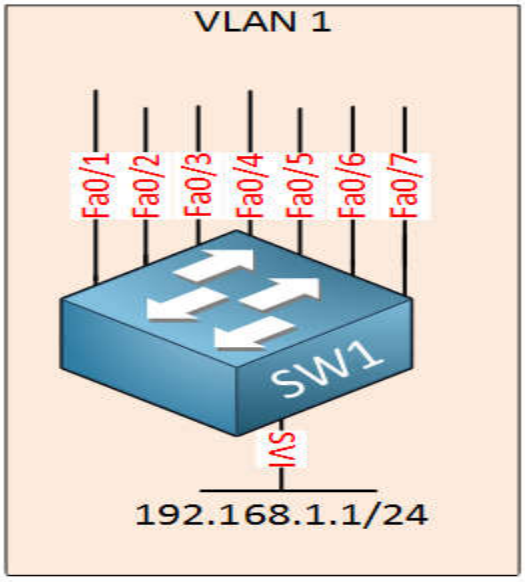


Figure 2.11 : Switched Virtual Interface. [10]

2.5 Comparison Between L2 And L3 Switching [3]

A Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address. A Layer 2 switch is completely transparent to network protocols and user applications. Recall that a Layer 2 switch builds a MAC address table that it uses to make forwarding decisions.

Figure 2.12 illustrates the icons reserved for Layer 2 and Layer 3 switches. Instead of learning only which MAC addresses are associated with each of its ports, a Layer 3 switch can also learn which IP addresses are associated with its interfaces. This allows the Layer 3 switch to direct traffic throughout the network based on IP address information.

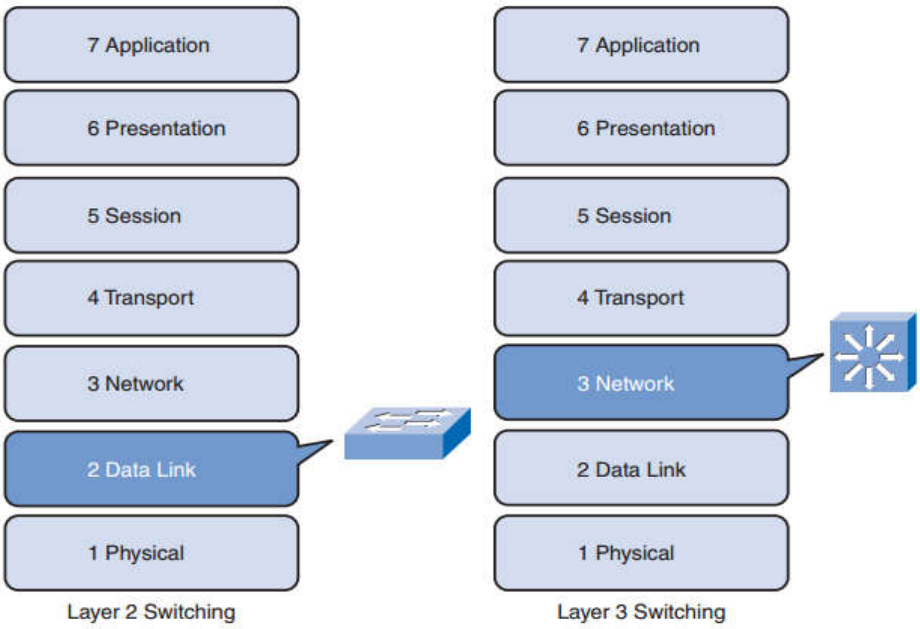


Figure 2.12 : Layer 2 and Layer 3 Switching. [3]

Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN. Because Layer 3 switches have specialized switching hardware, they can typically route data as quickly as they can switch data.

It should be emphasized that Layer 3 switches do not completely replace the need for routers on a network. Routers perform additional Layer 3 services that Layer 3 switches are not capable of performing. Routers are also capable of performing packet-forwarding tasks not found on Layer 3 switches, such as establishing remote access connections to remote networks and devices. Dedicated routers are more flexible in their support of WAN interface cards (WIC), making them the preferred, and sometimes only, choice for connecting to a WAN. Layer 3 switches can provide basic routing functions in a LAN and reduce the need for dedicated routers.

2.6 Intelligent network technology

Triangles not Squares

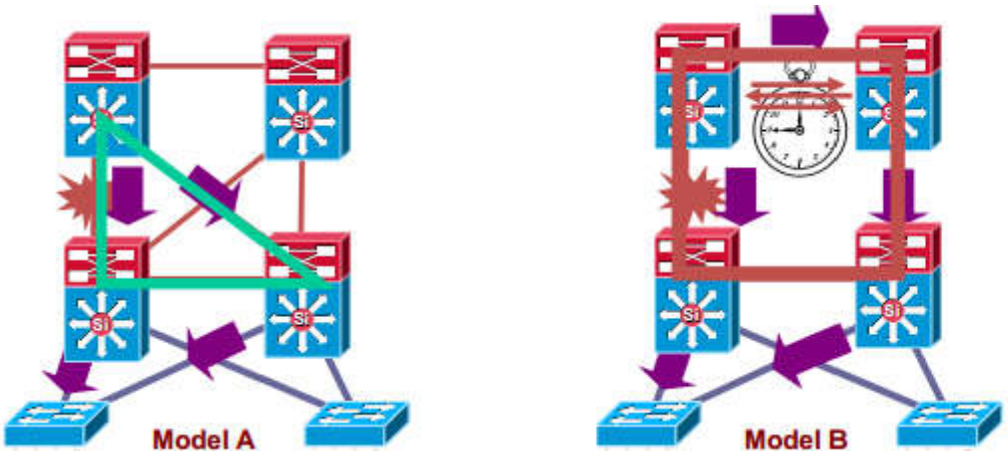


Figure 2.13 : Redundant Triangles Versus Redundant Squares. [11]

On the left of Figure 2.13, the multilayer switches are connected redundantly with a triangle of links that have Layer 3 equal costs. Because the links have equal costs, they appear in the routing table (and by default will be used for load balancing). If one of the links or distribution layer devices fails, convergence is extremely fast, because the failure is detected in hardware and there is no need for the routing protocol to recalculate a new path, it just continues to use one of the paths already in its routing table. In contrast, on the right of Figure 2.13, only one path is active by default, and link or device failure requires the routing protocol to recalculate a new route to converge. [12]

Redundancy and Protocol Interaction

Configuring L3 routed interfaces provides for faster convergence than an L2 switch port with an associated L3 SVI

Figure 2.14 : Layer 2 and 3 Comparison**.** [11]

the comparison comes when the link between the two Building Distribution switches goes down, some of msec will lost. The left one is L3 link when it goes down the interface down then routing update will begin after 8 msec rather than L2 link when it had goes

down the interface down and SVI down and other technologies using by default will down then the routing update would began after 150-200 msec. [11]

Redundancy Protocols

If Layer 2 is used between the Building Access switch and the Building Distribution switch, convergence time when a link or node fails depends on default gateway redundancy and failover time. Building Distribution switches typically provide first-hop redundancy (default gateway redundancy) using HSRP, Gateway Load-Balancing Protocol (GLBP), or Virtual Router Redundancy Protocol (VRRP). [12]

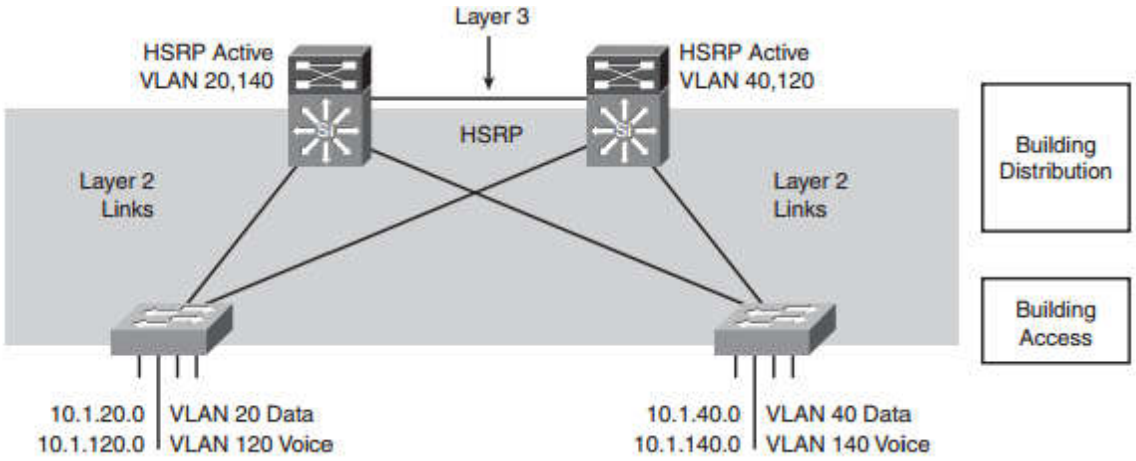


Figure 2.15 : Layer 3 Distribution Switch Interconnection. [12]

Passive Interfaces for IGP (interior gateway protocol)

Another recommended practice is to limit unnecessary peering across the access layer**.** , the distribution layer devices send routing updates and attempt to peer with the remote distribution layer devices across the links from the access switches on every VLAN, This connections provides no benefit and wastes resources (including CPU processing time and memory). [12]

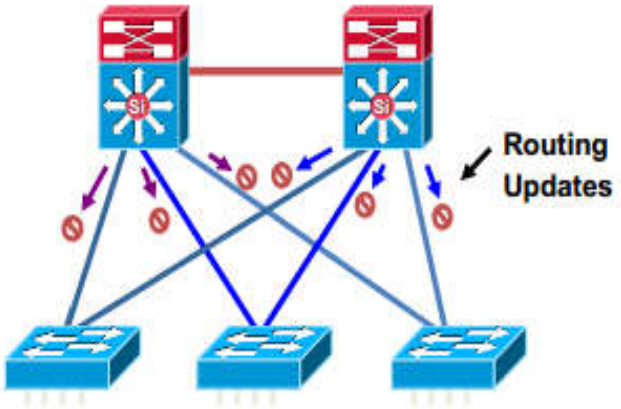


Figure 2.16 : Limit Unnecessary Peering Across the Access Layer. [11]

Summarize at the Distribution

In route summarization, a single summary address in the routing table represents a set of routes. Summarization reduces the routing update traffic, the number of routes in the routing table, and the overall router overhead in the router receiving the routes. [12]

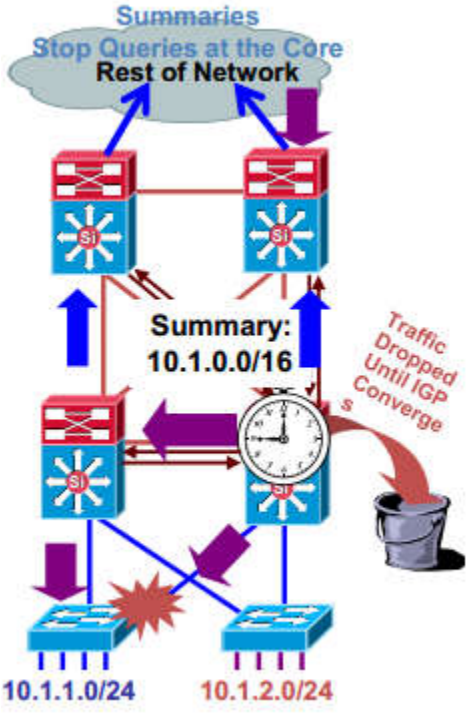


Figure 2.17 : Summary at the Distribution Layer Reduces Routing Traffic. [11]

2.7 Switch Security [3]

In modern networks, security is necessary to implement any device, protocol or technology. by help secure your LAN by configuring password options, login banners, Telnet and SSH, and port security. We are going to see common security attacks and tools for mitigating these attacks.

2.7.1 Basics Security options

2.7.1.1 Password Options

Securing the switches starts to protect them from unauthorized access. We have to start configuring passwords for the console line, virtual terminal lines, and access to privileged EXEC mode. We have also to see how to encrypt passwords on a switch.

Securing Console Access

You can perform all configuration options directly from the console. To access the console, you must have local physical access to the device. If you do not secure the console port properly, a malicious user could compromise the switch configuration.

Securing Virtual Terminal Access (Virtual teletype)

the accessing to the devices remotely, The VTY lines on a Cisco switch give us the ability to access without needing of physical access to the switch, so it is very important to secure the VTY lines. Any user with network access to the switch can establish a VTY remote terminal. If the VTY lines are not properly secured, a malicious user could compromise the switch configuration.

Securing Privileged EXEC Access

Privileged EXEC mode allows any user to access this mode through the Cisco switch to configure any option available, and to see all settings currently configured on the switch, including some unencrypted passwords, so it is very important to secure access to privileged EXEC mode.

Encrypting Switch Passwords

All passwords in the configuration of switches are stored in clear-text format within startup-config and running-config files. In Figure 2.18 we have abbreviated screen output

from the **show running-config** command on the switch, then we have a clear-text password but in Figure 2.19 we are going to use Cisco IOS command **service password-encryption** encrypts the passwords in the configuration file.

```
<output omitted>
!
line con 0
 password cisco
 login
line vty 0 4
 password cisco
 no login
line vty 5 15
 password cisco
 no login
!
end

S1# configure terminal
S1(config)# service password-encryption
S1(config)# end
```

Figure 2.18 : Clear-text Passwords in the running-config File.

```
S1# show running-config
<output omitted>
!
line con 0
 password 7 030752180500
 login
line vty 0 4
 password 7 1511021F0725
 no login
line vty 5 15
 password 7 1511021F0725
 no login
!
end
```

Figure 2.19 : Encrypting Passwords in the **running-config** File.

2.7.1.2 Login Banners

If anyone wants to logging on the switch, he will see messages are called login banners, we can configure this messages by using the **banner login** command in global configuration mode then write specific message.

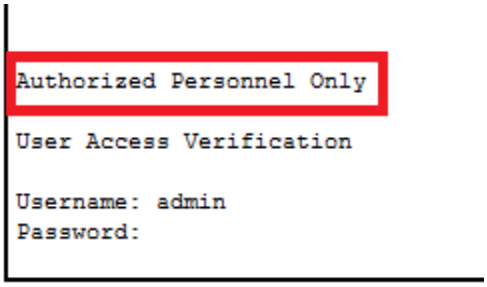


Figure 2.20 : Display Message Banner Login.

2.7.1.3 Telnet and SSH

Telnet is a popular protocol used for terminal access because most current operating systems come with a Telnet client built in. But it is an insecure way of accessing a network device, an attacker can read every type of data that is sent between the Telnet client and the Telnet service running on the Cisco switch. So SSH has become the preferred protocol for remotely accessing virtual terminal lines on a Cisco device. Because Communication between the SSH client and SSH server is encrypted.

2.7.1.4 Port Security

the network administrator has to configure port security to limit the number of MAC addresses each switch port can learn. If the number of MAC addresses exceeds the set limit, the administrator would like the port to be shutdown, , the port does not forward packets with source addresses outside the group of defined addresses.

2.7.2 Security Attacks

2.7.2.1 MAC Address Flooding

The key to understanding how MAC address table overflow attacks work is to know that MAC address tables are limited in size. MAC flooding makes use of this limitation to bombard the switch with fake source MAC addresses until the switch MAC address table is full. The switch then enters into what is known as a fail-open mode, starts acting as a hub, and broadcasts packets to all the machines on the network. As a result, the attacker can see all of the frames sent from a victim host to another host.

MAC flooding can be performed using a network attack tool. The network intruder uses the attack tool to flood the switch with a large number of invalid source MAC addresses until the MAC address table fills up.

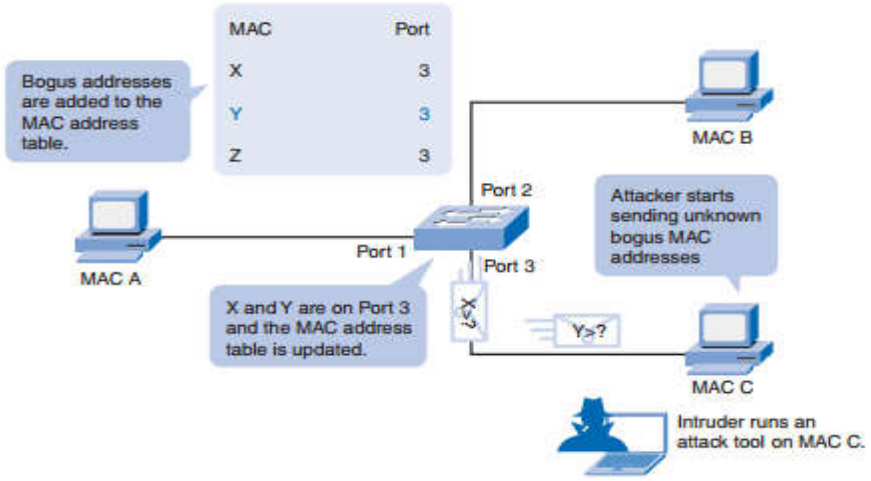


Figure 2.21 : Host C Sends Frames with Bogus Sources.

As long as the network attack tool is left running, the MAC address table on the switch remains full. When this happens, the switch begins to send all received frames out every port so that frames sent from Host A to Host B are also sent out of port 3 on the switch.

2.7.2.2 Spoofing Attacks

We can say is it spoofing responses that would be sent by valid DHCP server. The DHCP spoofing device replies to client DHCP requests. The intruder DHCP reply offers an IP address and supporting information that designates the intruder as the default gateway or Domain Name System (DNS) server. In the case of a gateway, the clients then forward packets to the attacking device, which in turn, sends them to the desired destination. And that what make the attackers what called man-in-the-middle attack**.**

Another sort of DHCP attack called a DHCP starvation attack. The attacker PC continually requests IP addresses from a real DHCP server by changing the source MAC addresses of the requests. If successful, this kind of DHCP attack causes all the leases on the real DHCP server to be allocated, thus preventing the real users (DHCP clients) from obtaining an IP address.

To prevent DHCP attacks, use the DHCP snooping and port security features on the Cisco Catalyst switches. Ports are identified as trusted and untrusted, as illustrated in Figure 2.22**.**

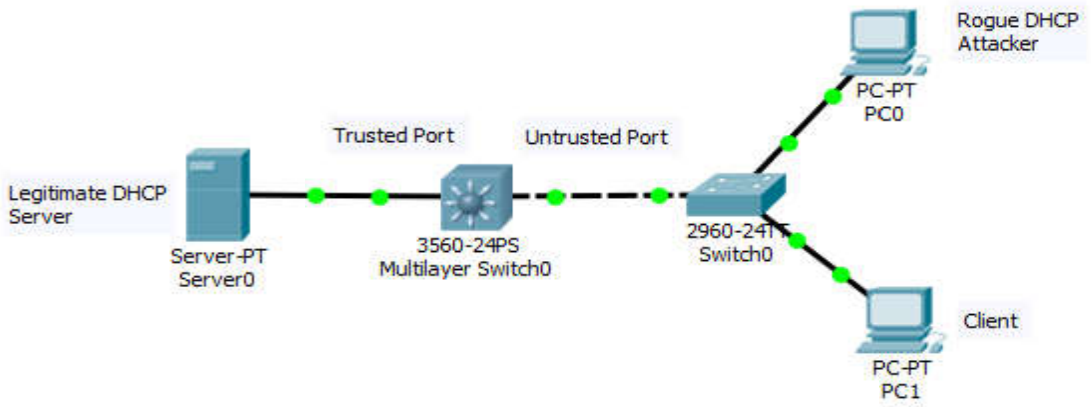


Figure 2.22 : DHCP Snooping to Prevent DHCP Attacks.

These steps illustrate how to configure DHCP snooping on a Cisco IOS switch :

- Enable DHCP snooping using the **ip dhcp snooping** global configuration command.
- Enable DHCP snooping for specific VLANs using the **ip dhcp snooping vlan number** [*number*] command.
- Define ports as trusted or untrusted at the interface level by defining the trusted ports using the **ip dhcp snooping trust** command.
- (Optional) Limit the rate at which an attacker can continually send bogus DHCP requests through untrusted ports to the DHCP server using the **ip dhcp snooping limit rate** *rate* command.

2.2.8 Conclusion

This chapter define the technology and protocols are used on platform of the network, in particular case of switching. The purpose of all this is to build a network with robust and intelligent. Otherwise, smart network could handle every fault could happen, and kept data forwarding around the entire network with small delay users cannot feel on it. Finally, to achieve full intelligence and security around this design, we have to secure this network from every threat could possibly being on the whole network.

Chapter 3 Campus Network Using Cisco Devices (Design, Configuration, And Test)

3.1 Introduction

The chapter includes emulation for Medium Business Network (Campus LAN) using real tools are used in fact business, software tools including VMware and GNS3 to emulate a real Operating Systems and Cisco IOS. Furthermore, we used our practical skills to configure the entire network on different layers and modules in our network platform. Moreover, we used analysis software tools and monitoring tools as Wireshark and Syslog server respectively. Finally, we care about connectivity between devices to determining network readiness.

3.2 Software Tools

3.2.1 GNS3

Graphical Network Simulator-3 (shortened to GNS3) is a network software emulator first released in 2008. It allows the combination of virtual and real devices, used to simulate complex networks. It uses **Dynamips** emulation software to simulate Cisco IOS.[17] GNS3 is used by many large companies including NASA, and is also popular for preparation of network professional certification exams. [13]

Dynamips is an emulator computer program that was written to emulate Cisco routers.[14]

3.2.2 Wireshark

Wireshark is a free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development. [15]

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports. [15]

3.2.3 VMWARE

VMWARE is a subsidiary of Dell Technologies. [16] It's abbreviation for Virtualization Software, It's a program that enables you to operate several virtual devices on your physical device to work as a real devices by using local hardware, hard drive,

CPU, NIC...etc. This program is used for education or virtualization technology to provide companies multiple service on one hardware device and save cost.

Benefits of using VMWARE

- Software Testing to avoid any risk could beat your local system.
- Help network professionals and managers to test any update before apply it on the real design.
- Allows users to use many operating systems simultaneously.

3.2.4 Cisco product used in emulation

3.2.4.1 Cisco IOS

Cisco IOS (originally Internetwork Operating System) is a family of software used on most Cisco Systems routers and current Cisco network switches. and we had used :

For routers :

c7200-adventerprisek9-mz.152-4.S6.image

For three layer switches :

i86bi-linux-l2-adventerprisek9-15.1a.bin

To understand this abbreviation :

- c7200 : showing us the platform that the operating system belongs.
- adventerprisek9 : advanced enterprise services which mean all features for enterprise are enabled, k9 showing us that this version has 3DES encryption.
- mz : showing us that this version are compressed.
- 152-4 : number of this version.
- S6 : updates happened on this version.

3.2.4.2 Cisco ASA

The firewall is the barrier between a trusted and untrusted network, often used between your LAN and WAN. Cisco Adaptive Security Appliance Software, is Cisco's line of network security devices. On this lab we had used :

Cisco ASAv Version 9.8 which is virtual version that performed by QEMU from GNS3.

QEMU (short for Quick Emulator) is a free and open-source hosted hypervisor that performs hardware virtualization. [17]

3.2.5 Operating system used in emulation

In this laboratory we used as an operating system windows server 2008 for network management and windows 7-Ultimite and windows server 2003 to exchange available services in the network.

GNS3.VM.VMware.Workstation.2.0.3, The GNS3 VM is recommended for most situations when you are using Windows or Mac OS. The GNS3 development team has worked hard to create a lightweight, robust way of creating GNS3 topologies that avoids multiple common issues when using a local install of GNS3.

3.3 Our Campus Network Project

We had created a simple GNS3 network topology for practicing my networking skills**.** What we can consider it as a humble enterprise campus network. And we are going to focus on campus network which was the difficult one in the enterprise configuration.

3.3.1 Logical Topology

Logical topology is the arrangement of devices on a computer network and how they communicate with one another logical topology is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. So we are going to represent the logical topology from our project of enterprise campus as shown in figure 3.1 below.

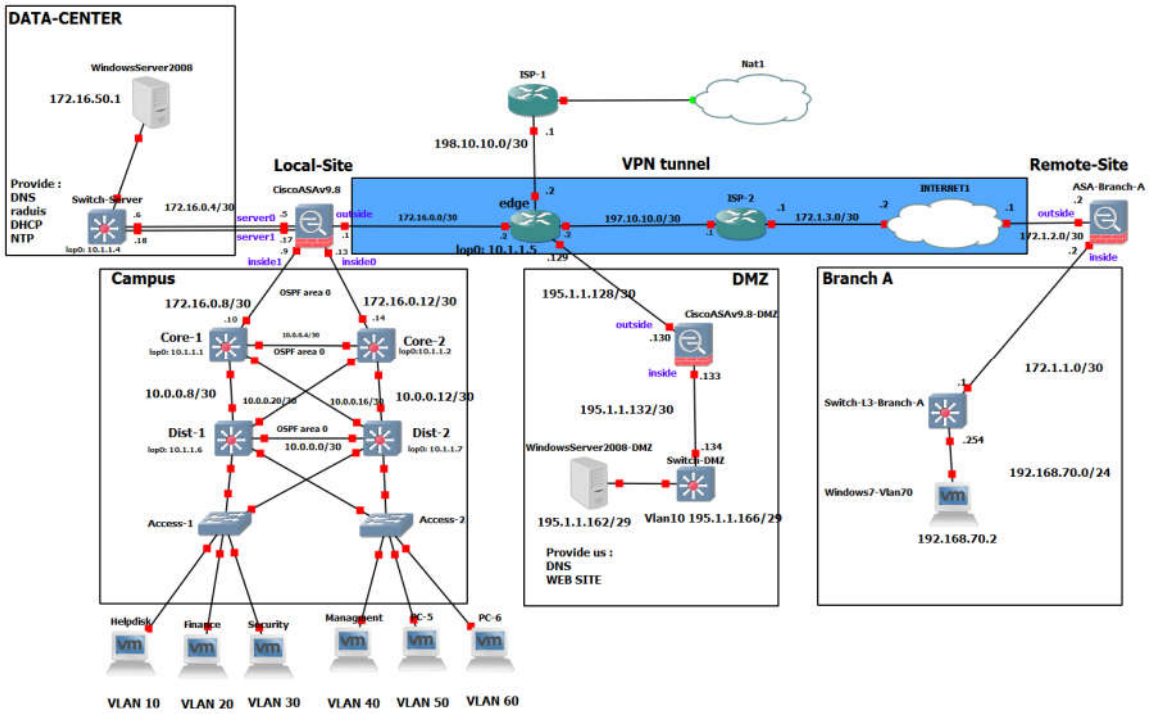


Figure 3.1 : logical topology of enterprise campus network.(illustrated Behind this page)

3.3.2 Background / Scenario

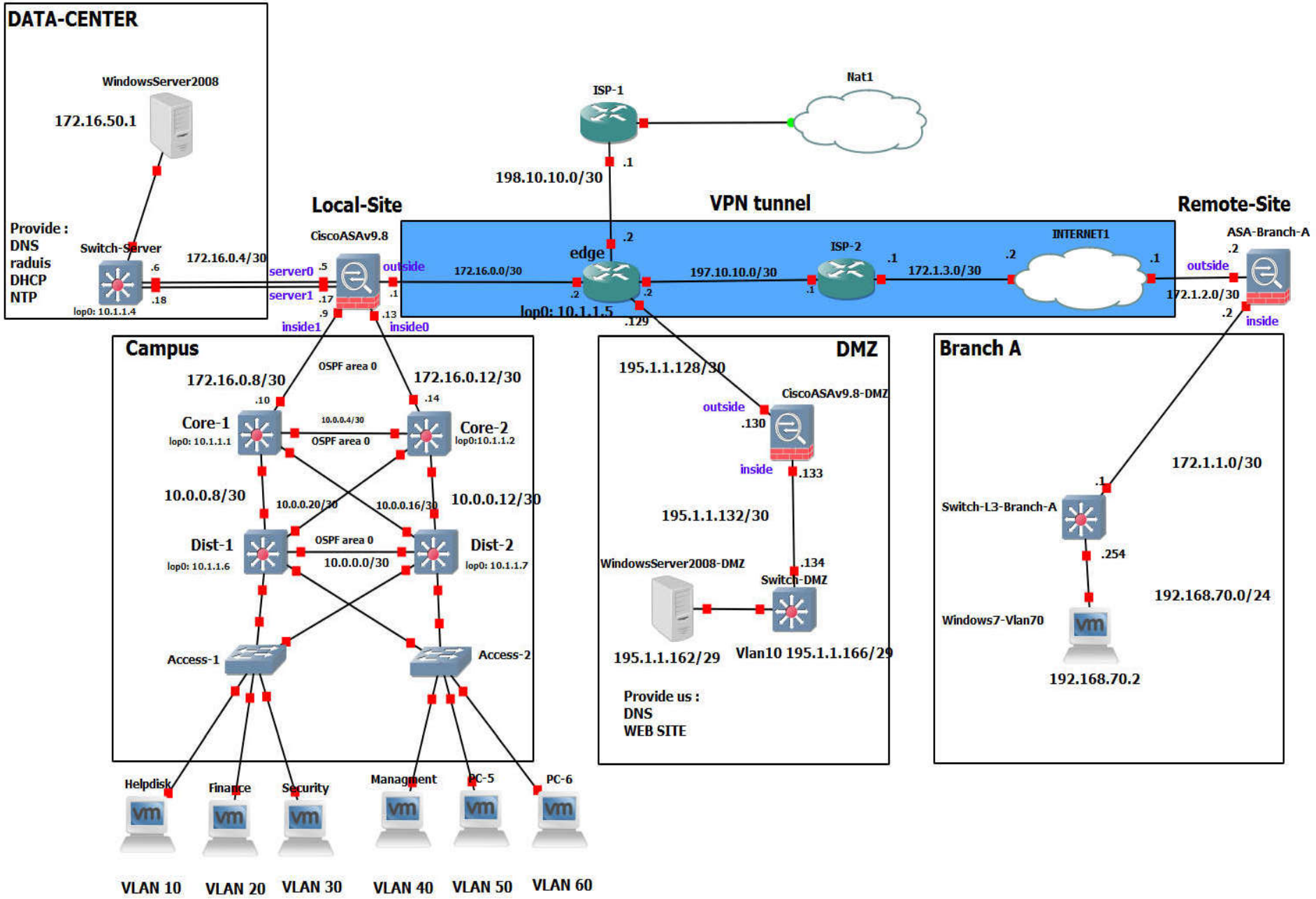
Our enterprise network project consist of a Campus, which is a portion of network design providing performance and scalability and availability that provides access to network communication services and resources to end users and devices that are spread over a single geographic location such us Data Center and DMZ network block to provide the enterprise with a Web Server.

Our Edge of the design has connected with Dual ISPs to save the company from internet disconnection when some of ISPs goes down, that to ensure the availabilities and the permanence of internet connection.

We have also created another branch (Branch A) as a Remote Site to communication with Local Site (Campus) through internet using VPN Site-To-Site.

3.3.3 Configuration

Now we are going to separate our design configuration by parts with considerations the modular network design.


DATA-CENTER
WindowsServer2008
172.16.50.1
Provide :
DNS
raduis
DHCP
NTP
Switch-Server
lop0: 10.1.1.4
172.16.0.4/30
.6
.18
ISP-1
Nat1
.1
198.10.10.0/30
Local-Site
VPN tunnel
Remote-Site
CiscoASAv9.8
server0
server1
.5
.17
.9
.13
outside
.1
inside1
inside0
edge
.2
.2
172.16.0.0/30
lop0: 10.1.1.5
.129
ISP-2
.1
.2
197.10.10.0/30
.1
172.1.3.0/30
.2
INTERNET1
.1
ASA-Branch-A
.2
outside
172.1.2.0/30
.2
inside
Campus
OSPF area 0
172.16.0.8/30
.10
172.16.0.12/30
.14
Core-1
lop0: 10.1.1.1
10.0.0.4/30
OSPF area 0
Core-2
lop0:10.1.1.2
10.0.0.8/30
10.0.0.20/30
10.0.0.16/30
10.0.0.12/30
Dist-1
lop0: 10.1.1.6
OSPF area 0
10.0.0.0/30
Dist-2
lop0: 10.1.1.7
Access-1
Access-2
Helpdisk
Finance
Security
Managment
PC-5
PC-6
VLAN 10
VLAN 20
VLAN 30
VLAN 40
VLAN 50
VLAN 60
DMZ
195.1.1.128/30
outside
.130
CiscoASAv9.8-DMZ
inside
.133
195.1.1.132/30
WindowsServer2008-DMZ
.134
Switch-DMZ
195.1.1.162/29
Vlan10 195.1.1.166/29
Provide us :
DNS
WEB SITE
Branch A
172.1.1.0/30
.1
Switch-L3-Branch-A
.254
192.168.70.0/24
Windows7-Vlan70
192.168.70.2

Part 1 : Access layer

The access layer provides access for end users to the network . They are two access switches located inside the access layer. The access switches access-1 and access-2 are the Cisco vIOS-l2 Qemu appliances on qcow2 disks**.** and they have assigned 256 MB memory by GNS3**.**

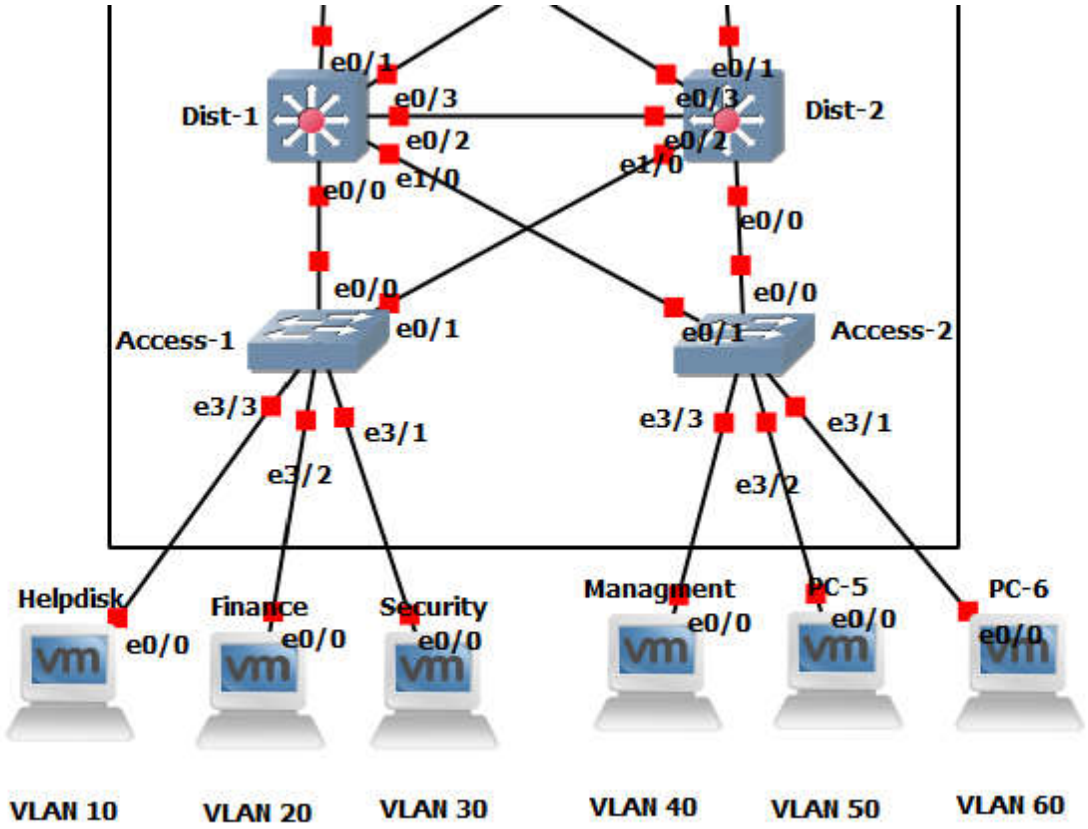


Figure 3.2 : Access Switches Connected to Distribution Layer.

The ports Ethernet 3/3 and 3/2 and 3/1 on all both switches are configured as access ports and they connect PCs to the campus network. The port e0/0 and e0/1 are uplinks that connect access switches to the distribution switches. They are configured as trunk ports, carrying traffic from multiple VLANs. Thanks to redundant uplink connection, the access switches remain connected to the upper layer, even in case of the failure one of the distribution switch.

As an example from the project by using command Show Run in privilege mode we obtain the configuration below in List 1 and 2, to see the configuration on every single ports .

```
interface Ethernet3/1
 switchport access vlan 30
 switchport mode access
 duplex auto
!
interface Ethernet3/2
 switchport access vlan 20
 switchport mode access
 duplex auto
!
interface Ethernet3/3
 switchport access vlan 10
 switchport mode access
```

Cmd-List 1 : Interfaces e3/1, e3/2, e3/3.

```
interface Ethernet0/0
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
 no routing dynamic
!
interface Ethernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30
 switchport mode trunk
 duplex auto
 no routing dynamic
```

Cmd-List 2 : Trunk Interfaces e0/0, e0/1.

End user computers are assigned to VLANs 10, 20, 30, 40, 50 and 60. Thanks to segmentation to VLAN, user traffic is sent to the distribution layer without being spread across the other access switches in campus.

As we can see on the Cmd-List 3 from running configuration files of any switches access layer , the VLAN names and their numbers, and the port which attached with it.

```
VLAN Name                       Status    Ports
---- ------------------------------ --------- -------------------------------
1    default                    active    Et0/3, Et1/0, Et1/1, Et1/2
                                          Et1/3, Et2/0, Et2/1, Et2/2
10   VLAN0010                   active    Et3/3
20   VLAN0020                   active    Et3/2
30   VLAN0030                   active    Et3/1
40   VLAN0040                   active
50   VLAN0050                   active
60   VLAN0060                   active
```

Cmd-List 3 : VLANs signed on the switches.

Part 2 : Distribution and core layer

The distribution layer consists of two multilayer switches Dist-1 and Dist-2. The core layer consists of the switches Core-1 and Core-2. These are the Cisco vIOS-l2 Qemu appliances on qcow2 disks. and they have assigned 256 MB memory by GNS3**.**

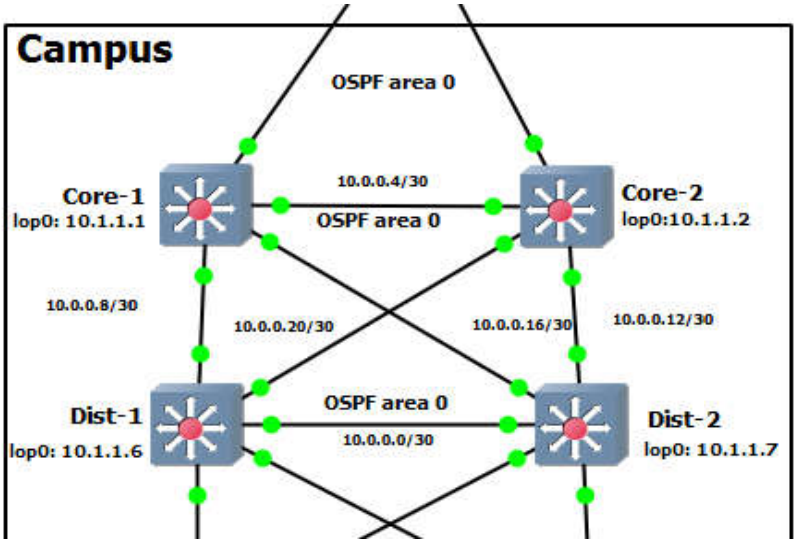


Figure 3.3 : Distribution and Core Layers of Enterprise Campus Network.

The distribution switches route traffic between end user VLANs and they connect the lower layer network to a Core layer. The interfaces toward the Access layer are layer 2 (switchports)**.** The layer 3 (routed) interfaces connect both distribution switches to each

other and to the Core switches. The layer 3 (routed) interfaces connect both distribution switches to each other and to the Core switches.

On the Cmd-List 4 and 5 illustration from running configuration file define that the cases of ports between distribution switches are no switchport, and given an IP addresses for both switches,

```
interface Ethernet0/2
 no switchport
 ip address 10.0.0.1 255.255.255.252
!
```

```
interface Ethernet0/2
 no switchport
 ip address 10.0.0.2 255.255.255.252
!
```

Cmd-List 4 : Configuration L3 link Dist-1. **Cmd-List 5:** Configurtation L3 link Dist-2.

The OSPF routing protocol is running on the distribution switches**.**

The Cmd-List 6 it's a configuration of OSPF protocol , started with activation the disregard the updated into specific interfaces or VLANs , then defining the subnets that are directly connected on every single switch.

```
router ospf 1
 passive-interface Ethernet0/0
 passive-interface Ethernet1/0
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan40
 passive-interface Vlan50
 passive-interface Vlan60
network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.20 0.0.0.3 area 0
 network 10.1.1.6 0.0.0.0 area 0
```

Cmd-List 6 : OSPF Configuration Protocol.

```
network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
network 192.168.60.0 0.0.0.255 area 0
```

Suit of Cmd-List 6.

The core layer is connected to the lower distribution layer with l3 P2P links configured with the IP addresses from the subnet 10.0.0.0/24. The core switches connect distribution and access layers to Cisco Adaptive Security Virtual Appliance (ASAv) configured with the IP addresses from the subnet 172.16.0.0/24.

Cmd-List 7 and 8 illustrate that the interfaces are connected layer three links, no switchport which mean we have to use the IP addresses.

```
interface Ethernet0/3
 no switchport
 ip address 10.0.0.10 255.255.255.252
```

Cmd-List 7 : Link Core-1 to ASA.

```
interface Ethernet0/3
 no switchport
 ip address 10.0.0.14 255.255.255.252
```

Cmd-List 8 : Link Core-2 to ASA.

Part 3 : Cisco ASA

The device is a Cisco Adaptive Security Virtual Appliance (ASAv) version 9.8 installed on qcow2 Qemu disk. The CiscoASAv9.8 provides traffic filtering and inspection services for the campus network and Data Center . It also connects the campus network and DC to the edge router. The recommended RAM size for ASAv instance is 2048 MB.

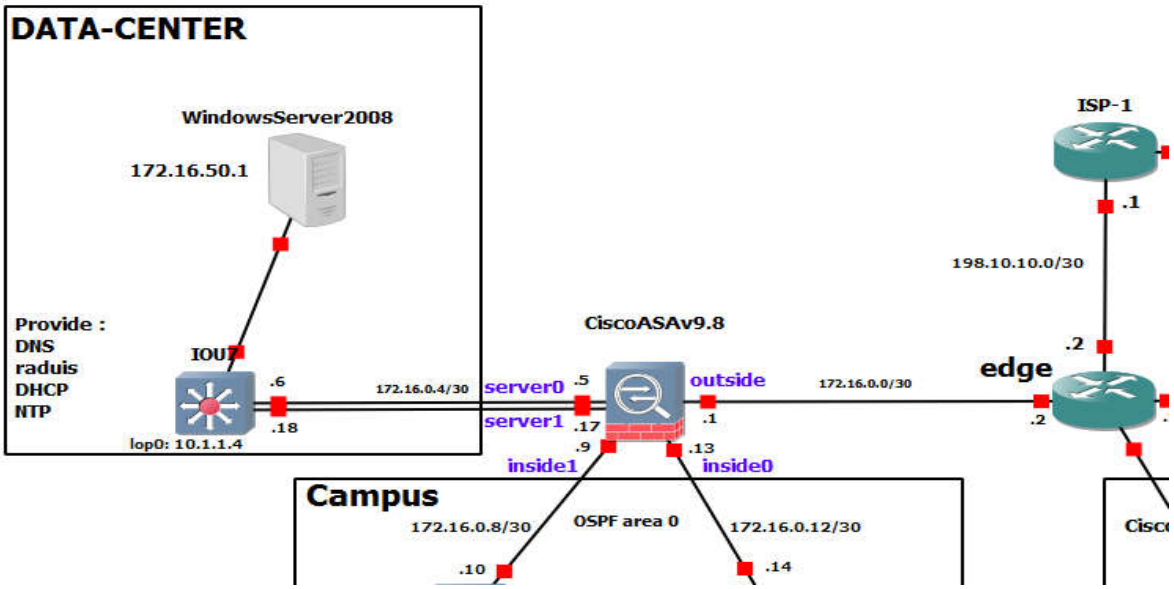


Figure 3.4 : CiscoASAv9.8**,** Campus, DATA-CENTRE and edge Connection.

The links connecting CiscoASAv9.8 to the Core switches are configured with the interface name INSIDE0 and INSIDE1.

Cmd-List 9 from the running configuration file of firewall that define the security-levels of the interfaces, and which zone it belong (inside) and IP addresses.

```
interface GigabitEthernet0/0
 nameif INSIDE0
 security-level 100
 zone-member inside_zone
 ip address 172.16.0.13 255.255.255.252
!
interface GigabitEthernet0/1
 nameif INSIDE1
 security-level 100
 zone-member inside_zone
 ip address 172.16.0.9 255.255.255.252
```

Cmd-List 9 : INSIDE Interfaces.

They have assigned a security level 100. The links connecting CiscoASAv9.8 to the DATA-CENTER are configured with the interface name SERVER0 and SERVER1.

On Cmd-List 10 bellow, show the different between the configuration of Cmd-List 9, which display the security levels of servers zone 50 , and their IP addresses.

```
interface GigabitEthernet0/3
 nameif SERVER0
 security-level 50
 zone-member server-zone
 ip address 172.16.0.5 255.255.255.252
!
interface GigabitEthernet0/4
 nameif SERVER1
 security-level 50
 zone-member server-zone
 ip address 172.16.0.17 255.255.255.252
```

Cmd-List 10 : SERVER Interfaces.

They have assigned a security level 50. The link connecting the CiscoASAv9.8 to the edge router is configured with the interface name OUTSIDE and it has assigned a security level 0. Cmd-list 11 illustrate the configuration of outside interface g0/2.

```
interface GigabitEthernet0/2
 nameif OUTSIDE
 security-level 0
 ip address 172.16.0.1 255.255.255.252
!
```

Cmd-List 11 : OUTSIDE Interface.

Thanks to the security levels concept, TCP and UDP traffic from the hosts connected to the inside interfaces (level 100) can reach hosts in DC, behind the server interfaces (level 50) or hosts in the Internet behind the outside interface (level 0). The same is valid for traffic sent from DC to the Internet. In this case, network traffic takes a path from the server interface (level 50) to the outside (level 0) interface and back.

If we need to allow traffic initialized from host connected to the outside interface (level 0) to enter the interfaces with a higher level (100 or 50, in our case), we have to configure an access-list (ACL). The ACL must explicitly allow particular network traffic (e.g. TCP, UDP or ICMP) to enter the outside interface.

Default Static Route Configuration

We need to configure a default static route in order to reach hosts in the Internet. This route will be later redistributed to the OSPF process. the configuration bellow.

```
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.0.2 1
!
```

Cmd-List 12 : Default Route.

Objects and Object Groups Configuration

Using objects and object groups are reusable components that help to maintain configuration. We can modify an object in one place and have it be reflected in all other places that are referencing it. On Cmd-List 13 scopes of object network.

```
object network vlanS_172.16.50
 subnet 172.16.50.0 255.255.255.0
object network google_dns1
 host 8.8.8.8
object network google_dns2
 host 8.8.4.4
object network server1
 host 172.16.50.1
```

Cmd-List 13 : Sample from Object Network.

Management Protocol Configuration

- ICMP ECHO request and echo reply messages on inside interfaces, Allow management (192.168.40.0/24), server (172.16.50.0/24) subnets to ping the ASA inside interfaces.
- Allow SSH access to INSIDE0 and INSIDE1 interfaces.

Cmd-List 14 it is just a scope from the configuration file that define the permit of ICMP protocol for spicific subnets into ASA firewall

```
icmp permit 192.168.40.0 255.255.255.0 INSIDE0
icmp permit 10.1.1.0 255.255.255.0 INSIDE0
icmp permit 192.168.40.0 255.255.255.0 INSIDE1
icmp permit 10.1.1.0 255.255.255.0 INSIDE1
icmp permit 172.16.50.0 255.255.255.0 SERVER0
icmp permit 172.16.50.0 255.255.255.0 SERVER1
```

Cmd-List 14 : ICMP ECHO.

The next Cmd-list for SSH configuration to allow specific subnet such us VLAN 40 from the INSIDE of firewall, and we defined the timeout of using session of SSH which is 60 minute before the close, and the type of hashing to key-exchange.

```
ssh stricthostkeycheck
ssh 192.168.40.0 255.255.255.0 INSIDE0
ssh 192.168.40.0 255.255.255.0 INSIDE1
ssh timeout 60
ssh key-exchange group dh-group1-sha1
console timeout 0
```

Cmd-List 15 : SSH protocol.

OSPF Protocol and Authentication Configuration

The OSPF routing protocol ensures that connectivity is between campus and DC. The static default route pointing to edge is redistributed to OSPF process, we defined that by defual-information originate commend as shown in Cmd-List 16.

```
router ospf 1
 network 172.16.0.4 255.255.255.252 area 0
 network 172.16.0.8 255.255.255.252 area 0
 network 172.16.0.12 255.255.255.252 area 0
 network 172.16.0.16 255.255.255.252 area 0
 log-adj-changes
 default-information originate
```

Cmd-List 16 : OSPF protocol.

Zone Configuration

The CiscoASAv9.8 installs only one route to the subnet: 192.168.x.0/24 even they are two paths to these routes available. The first path is via Core-1 (172.16.0.10) and the second path is via Core-2 (172.16.0.14). It is because ECMP is not supported across multiple interfaces, so we cannot define a route to the same destination on a different interface. However, with zones, we can have up to 8 equal cost static or dynamic routes across up to 8 interfaces within a zone. To achieve ECMP via two different interfaces, we will create a zone inside_zone and assign Gi0/0 and it Gi0/1 to this zone. and we will create zone server_zone for Gi0/3 and Gi/04.

Access Lists (ACLs) Configuration

Access List out-to-ins

- Permit ICMP Echo Reply packets with the source IP address 8.8.8.8 and 8.8.4.4 to end user subnets 192.168.x.0/24. The ACL allows users to check connectivity to Google public DNS with the ping command.

- Permit DNS request/reply from 8.8.8.8 and 8.8.4.4 from/to Server - 172.16.50.1
- Permit NTP request from edge (10.1.1.5) to Server1.
- Apply ACL out-to-ins to the interface Outside in inbound direction.

Access List dc-to-ins_out

- Permit hosts in subnet (172.16.50.0/24) to send traffic to any IP address, the destination TCP port 80 (http),443 (https) and 53 (DNS).
- Permit hosts in subnet (172.16.50.0/24) to send traffic to any IP address, the destination UDP port 123 (NTP) and 53 (DNS).
- Permit hosts in subnet (172.16.50.0/24) to send to ICMP Echo Request (ping) to any IP address to the IP addresses 8.8.8.8 and 8.8.4.4
- Permit hosts in mgmt VLAN40 (192.168.40.0/24) to ping Server1.
- Apply ACL dc-to-ins to the interfaces SERVER0 and SERVER1 in inbound direction.

Each acces-list on Cmd-List 17 has a name first, then defined by the type extended , and the policies like permit or deny, then we need to determine any protocol we want to apply this policies and finally the concerned by this policies (the concerned has been put on objects).

```
access-list out-to-ins extended permit icmp object-group google_dns object-group end_vlans echo-reply
access-list out-to-ins extended permit icmp any object vlanS_172.16.50 echo-reply
access-list out-to-ins extended permit icmp any object loopbaks echo-reply
access-list out-to-ins extended permit udp object vios-l3 object server1 eq ntp
access-list out-to-ins extended permit udp object vios-l3 object server1 eq syslog
access-list out-to-ins extended permit udp object-group google_dns object server1 eq domain
access-list out-to-ins extended permit icmp any object-group mgmt echo-reply
access-list dc-to-ins_out extended permit tcp object vlanS_172.16.50 any object-group server1_tcp_out
```

Cmd-List 17 : ACL Collections.

```
access-list dc-to-ins_out extended permit udp object vlanS_172.16.50 any object-group server1_udp_out

access-list dc-to-ins_out extended permit icmp object vlanS_172.16.50 object-group google_dns echo

access-list dc-to-ins_out extended permit icmp object vlanS_172.16.50 object vlan40_192.168.40 echo-reply

access-list dc-to-ins_out extended permit udp object-group end_vlans object server1 eq ntp

access-list OUTSIDE_cryptomap extended permit ip object host_192.168.40.2 object host_192.168.70.2

access-list OUTSIDE_cryptomap_1 extended permit ip object host_192.168.40.2 object host_192.168.70.2
```

Suit of Cmd-List 17.

Also we need to apply this access list on an appropriate interfaces such OUTSIDE and SERVER0,1 interfaces.

```
access-group out-to-ins in interface OUTSIDE

access-group dc-to-ins_out in interface SERVER0

access-group dc-to-ins_out in interface SERVER1
```

Cmd-List 18 : ACL Apply interfaces.

Part 4 : data center

Data center consists of the two devices WindowsServer2008 and the Switch-Server. a single switch and the server is far away from any known DC network design. it's hard to emulate a real data center scaled large-size consist of thousands of servers. For this reason we only share the configuration of the Cisco L3 switch that is located in our DC. The switch is running Cisco vIOS-L2, version and it has assigned 256MB RAM by GNS3, and The server is running on VMware.

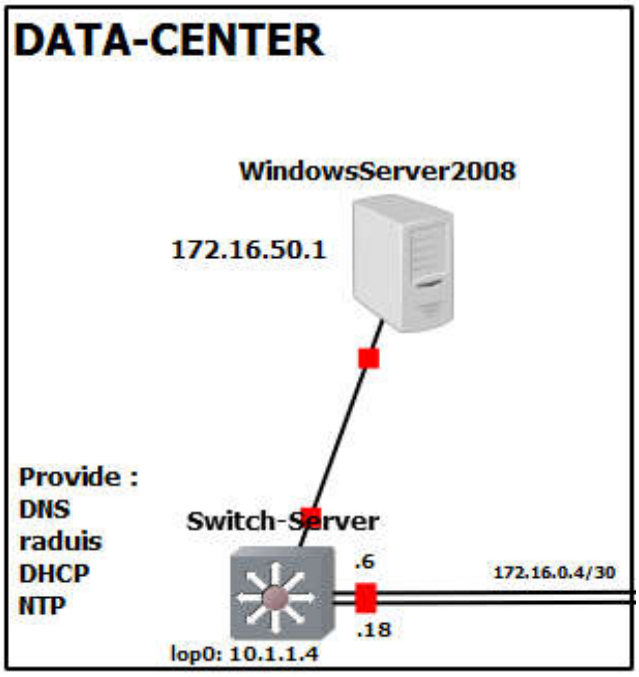


Figure 3.5 : Data Center.

Switch-Server Configuration

- The switch is connected with point-to-point layer3 links to the CiscoASAv9.8**.**
- The OSPF routing protocol**.**
- The switch is acting as default gateway with the IP address 172.16.50.254/24. This IP address is configured on the WindowsServer2008 under IPv4 configuration.
- The switch is synchronizes its time with the WindwosServer2008 using NTP**.**

```
ntp server 172.16.50.1
```

Cmd-List 19 : NTP protocol.

Server Configuration

As Server Data Center of enterprise campus network must provide domain name servers to the local users of the company and network management application such us Active Directory, and we need to synchronize the time of our network by using NTP service. Moreover, we need DHCP server to provide end users with an IP addresses Dynamics. The list 18 below reduce the functions are provided by server data center :

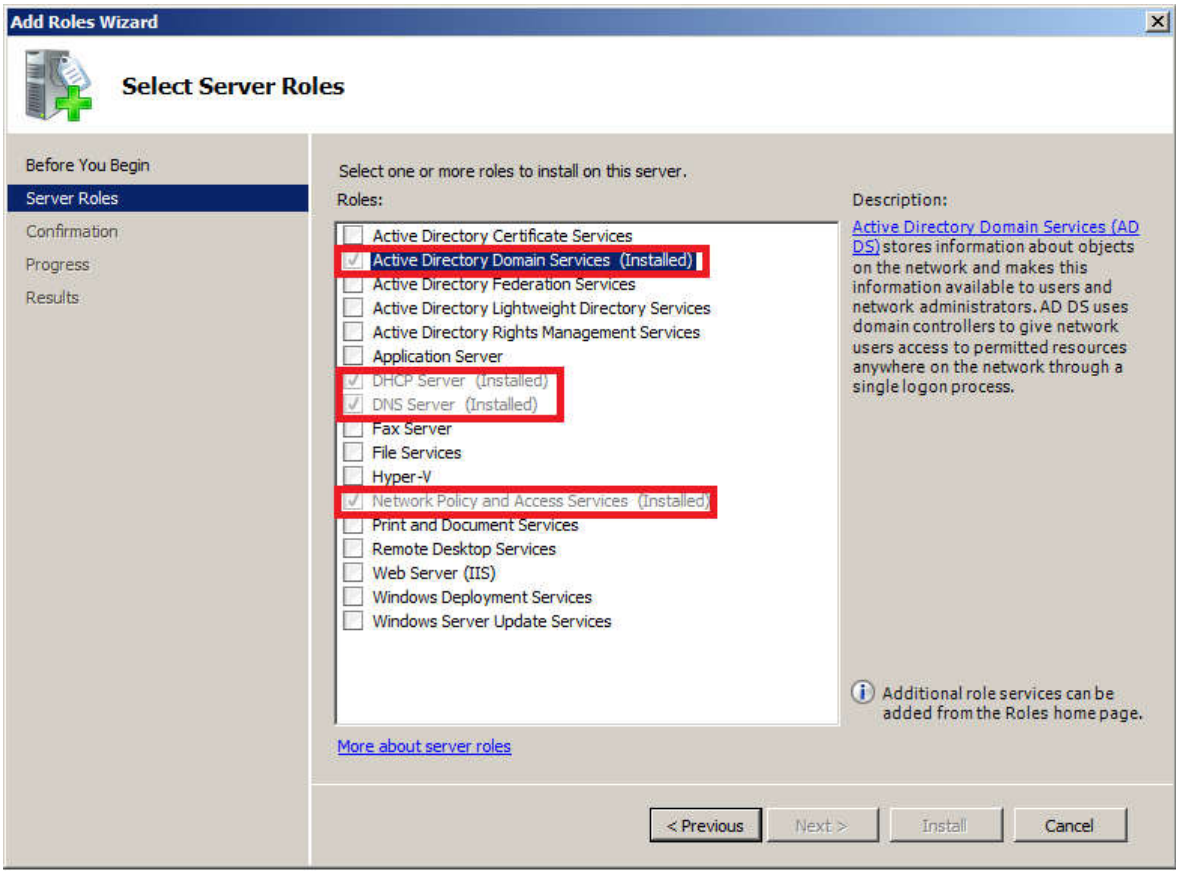


Figure 3.6 : Server Roles.

Network policy and Access Serveres installed to provide network professionals with RADIUS Server , which allow all devices of the company to check authenticate when the administrator wants to access into this devices to troubleshoot or change some policies.

RADIUS Server is a protocol that was originally designed to authenticate remote users to a dial-in access server. When a user tries to authenticate, the device sends a message to the **RADIUS** server. [18]

But because of limitation of ASAv system we used on this lab, we cannot make configuration for RADUIS server on our project, we just mention the functionality and wait for a new version might provide us with RADUIS server for free.

Part 5 : Edge Router and ISPs

We are going to explain the configuration of the edge router edge and configuration of ISP routers. These routers has been installed as dynamips to emulate the hardware of the Cisco 7200 by directly booting an actual Cisco IOS software image into the emulator. they are running IOS Version 15.2(4)S6. and they have assigned 512MB RAM by GNS3.

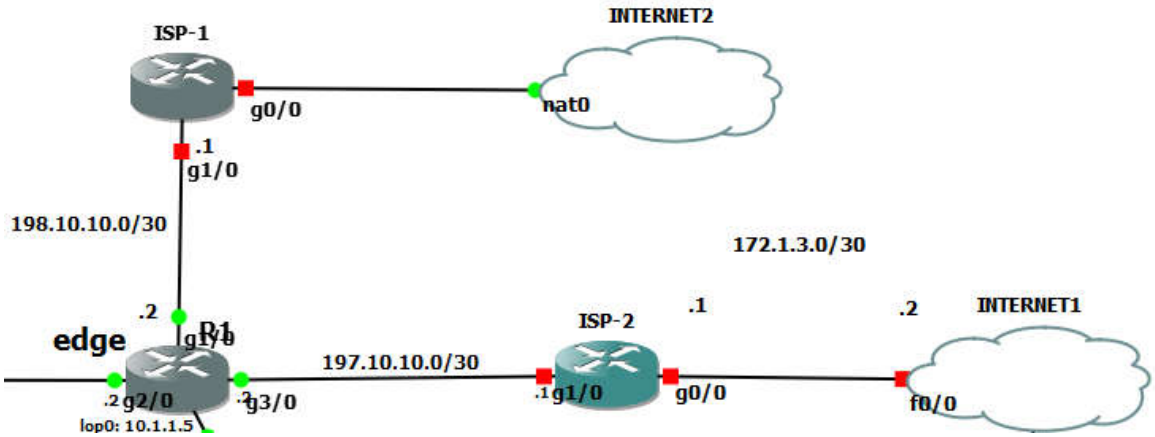


Figure 3.7 : Company Connection to the Internet via edge router.

The company has assigned the prefix 195.1.1.0/24. Devices located in DMZ have assigned the prefix 195.1.1.128/25. The prefix 195.1.1.0/25 is assigned for devices hidden behind NAT. NAT is configured on edge router**.** translating campus and data center subnets to the subnet 195.1.1.128/25. The router is connected to the upstream providers via their Ethernet ports g1/0 and g3/0.

Cmd-List 20 from configuration file that define the activation of protocol NAT and the pool of IP addresses that we need to translate, exactly on the router edge.

```
ip nat pool 1 195.1.1.1 195.1.1.127 netmask 255.255.255.128
ip nat inside source list 1 pool 1 overload
```

Cmd-List 20 : Nat Pool.

Sure we need to determine the interface that we are going to apply the NAT on it, for example here, we have g0/0, g1/0 and g2/0, as shown on Cmd-List 21.

```
interface GigabitEthernet0/0
 ip address 195.1.1.129 255.255.255.252
 ip nat outside
!
interface GigabitEthernet1/0
 ip address 198.10.10.2 255.255.255.252
 ip nat outside
!
interface GigabitEthernet2/0
 ip address 172.16.0.2 255.255.255.252
 ip nat inside
!
interface GigabitEthernet3/0
 ip address 197.10.10.2 255.255.255.252
 ip nat outside
```

Cmd-List 21 : EDGE Interfaces**.**

The entire prefix 195.1.1.0/24 is advertised to the both ISPs via BGP routing protocol. When one of the ISP goes down, the incoming traffic to the prefix 195.1.1.0/24 is not no affected. The outgoing traffic from the edge router to the Internet is primary sent to ISP-1. If the ISP-1 goes down, traffic is sent via ISP-2.

The router ISP-1 are bridged to the interface NAT by GNS3 cloud via their interface g0/0. The interface in NIC(network interface card) presented in my laptop. The NIC is connected to the huawei router that connects home network to the Internet. The routers ISP-1 receive the IP addresses on the ports g0/0 from DHCP server running on huawei router, as shown on Cmd-list 22.

```
interface GigabitEthernet0/0
 description Link to Simulated Internet
 ip address dhcp
 ip nat outside
```

Cmd-List 22 : DHCP for interface e0/0 from ISP-1.

part 6 : DMZ

Demilitarized Zone (DMZ) Our DMZ consists of three devices CiscoASAv9.8-DMZ, a multilayer switch Switch-DMZ and WindowsServer2008-DMZ All the devices in DMZ are run by Qemu, except the WindowsServer2008-DMZ was installed on VMware. We used The same server and firewall and switch that used on data center.

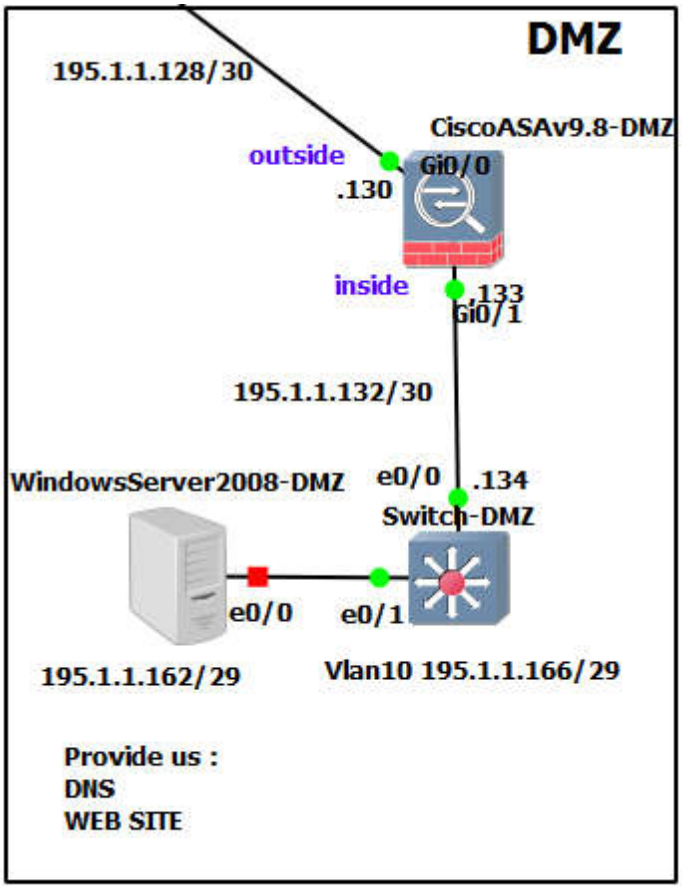


Figure 3.8 : Demilitarized Zone - DMZ.

server deployed in DMZ has configured with the IP addresses 195.1.1.161/29. The server is assigned to VLAN10 on the switch Switch-DMZ. The subnet reserved for devices in VLAN10 is 195.1.1.160/29 with the default gateway IP address 196.1.1.166.

Firewall

IP Addresses and Security Levels

The switch is an access switch that connects servers to the network. The switch is connected to CiscoASAv9.8-DMZ G0/1 interface. The security level configured on the interface is set to 100. The security level for the interface G0/0 is set to 0. The interface G0/0 connects the firewall to the device edge. Thanks to this security level configuration, all devices inside DMZ can initialize connection to the Internet. However, hosts in the Internet cannot initialize connection to devices in DMZ. To allow connection initialized from outside to inside for a particular network traffic, the appropriate access-list must be configured on firewall.

Cmd-List 23 is a scope of file configuration that define the security level on inside and the outside of firewall DMZ.

```
interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 195.1.1.130 255.255.255.252
!
interface GigabitEthernet0/1
 nameif INSIDE
 security-level 100
 ip address 195.1.1.133 255.255.255.252
```

Cmd-List 23 : Security level interfaces.

Static Routes

Configure a static default route pointing toward the router edge (195.1.1.129), and configure a static route pointing to devices inside DMZ toward the switch-DMZ (195.1.1.134), shown on Cmd-List 24.

```
route OUTSIDE 0.0.0.0 0.0.0.0 195.1.1.129 1
route INSIDE 195.1.1.160 255.255.255.224 195.1.1.134 1
route INSIDE 195.1.1.192 255.255.255.192 195.1.1.134 1
```

Cmd-List 24 : Static Routes.

Objects and Object Group

Define object-groups and objects network type exactly as we did before on Cisco ASA firewall of campus network, to be reusable components that help to maintain configuration.

Access Lists out-to-ins

- Allow SSH access from 195.1.1.0/24 to 195.1.1.0/24 through CiscoASAv9.8-DMZ. It allows to manage devices in DMZ from the campus network and data center.
- Allow ICMP ECHO Reply from Google 8.8.8.8 and 8.8.4.4**.**
- Allow access from the Internet to web server 195.1.1.161 port 80, 443.
- Allow DNS requests from 195.1.1.129 edge to DNS server 195.1.1.161 port 53**.**
- Apply the access-list out-to-ins in incoming direction to the outside interface.

SSH Access

Allow SSH access to OUTSIDE interfaces from subnet 195.1.1.0/25.

Traffic Inspection

As website server host a lot of visitors, we need to control the untrusted host using http protocol, So there are specific commends en firewall to inspect the traffic http from malicious code injected.

In Cmd-List 25 bellow, we just display the command configuration of traffic inspection for http protocol.

```
ciscoasa# sh running-config policy-map
!
policy-map type inspect http http_map
 parameters
  protocol-violation action drop-connection log
policy-map type inspect dns migrated_dns_map_1
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns migrated_dns_map_1
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
```

Cmd-List 25 : List of Inspected Protocols.

Switch-DMZ Configuration

The interface e0/0 is connected to firewall and it is configured as a routed interface. and it is configured as a routed interface. The interface e0/1 is configured as the switchport with VLAN10. It connects the server to the network. **Server**

In server windows 2008 installed Active Directory to manage the services, and automatically DNS server had been installed, then to prepare a website there are another feature should installed with Active directory to create and manage a website which is IIS web server package used for hosting website.

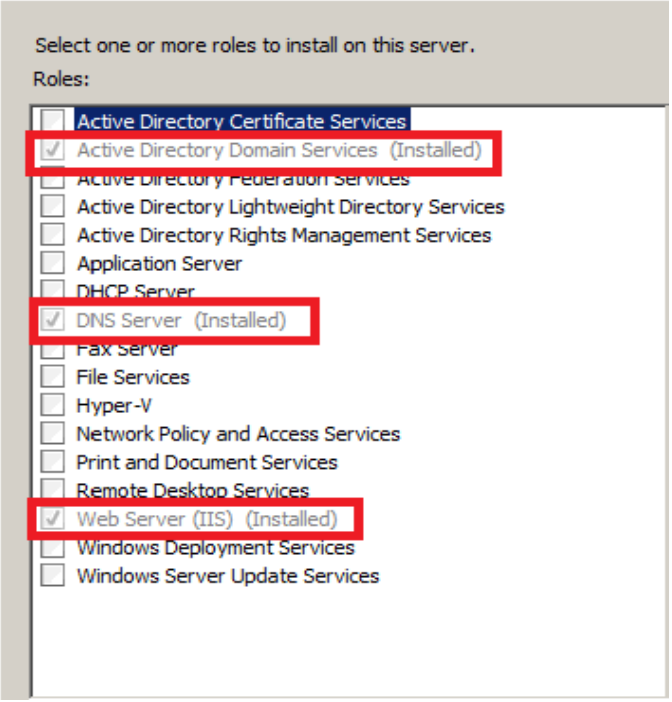


Figure 3.9 : Server Roles DMZ

part 7 : Branch A

We could consider Branch A as a Campus network, basically it has the same devices except a server farm, Our object in establishing this branch is just to represent one of WAN technology called VPN, and provide the company with another branch hopefully to expend its activities.

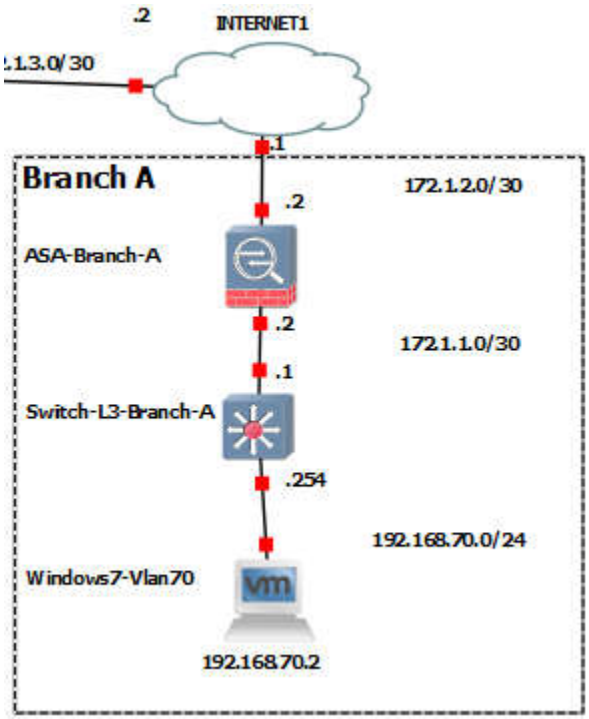


Figure 3.10 : Branch A (Remote-site).

This branch contains Vlan70 represented by windows7, it consider as a VLAN management that has connection directly to the official branch through internet by using VPN tunneling. The configuration it's just basic configuration for both devices, switch layer three and the firewall.

3.3.4 Protection Policies And Security Network

We followed methods to secure the company from any possible threat, Either inside or outside the company. connection of branches or between devices entre the campus may be attacked by several types of attacks. So we had started by securing management plan and data plan. Moreover, implementing VPN site-to-site to secure the connection through internet between our branches.

3.3.4.1 Securing Management Plane

In this part we are going to ensure the traffic that an administrator uses between enterprise campus devices are save by using :

- Secure Shell SSH protocol as remote management protocol to monitor or configure the devices safely.[19]

below we have an example from our project representing access from group management Vlan40 by SSH protocol to Ciscoasa firewall :

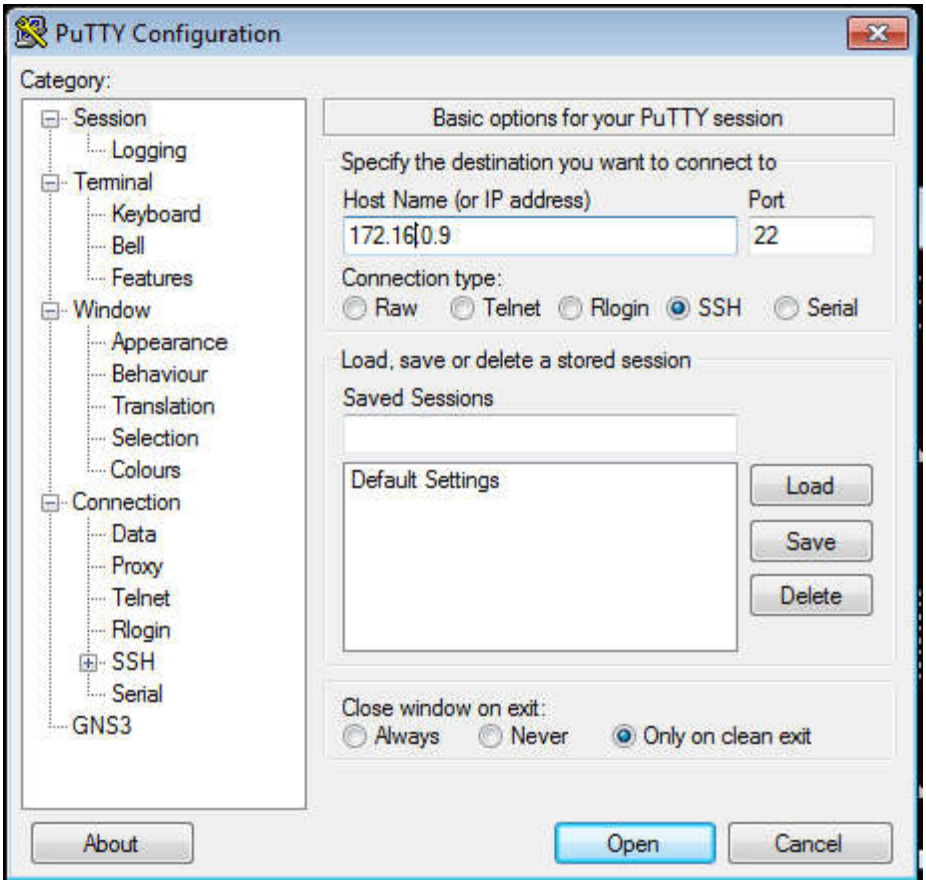


Figure 3.11 : Using Putty to access by SSH.

Click Open and the next picture will be the official shell which would ask you about username to login and the password :

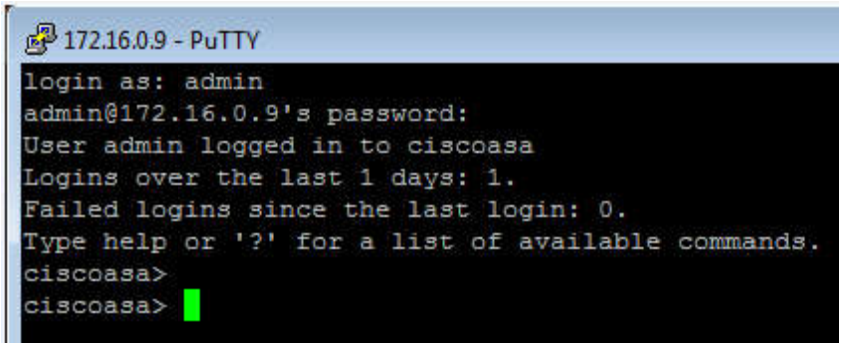


Figure 3.12 : Commend line firewall opened by SSH putty.

- Using AAA Authentication Authorization Accounting framework to perform authorization with security server RADUIS, Which this service has been installed on server of data center.[19]
- Syslog has been installed on server data center for network devices to send event message into it. Any devices belong to network has been configured to send syslog message. for example, a router might send messages about users logging on to console sessions, while a web-server might log access-denied events. [20]

Example from our project represent an event happened When we wanted to log into enable mode in the firewall with incorrect logging :

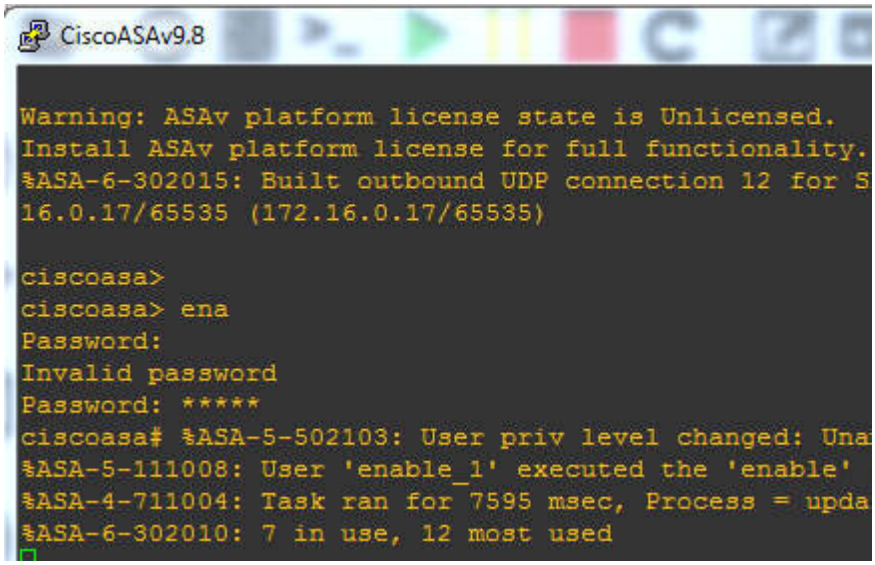


Figure 3.13 : Shown a mistake when logging enable.

As a result security we will get an event, selected by red color about this point on Kiwi Syslog service manager , shown on figure 3.14.

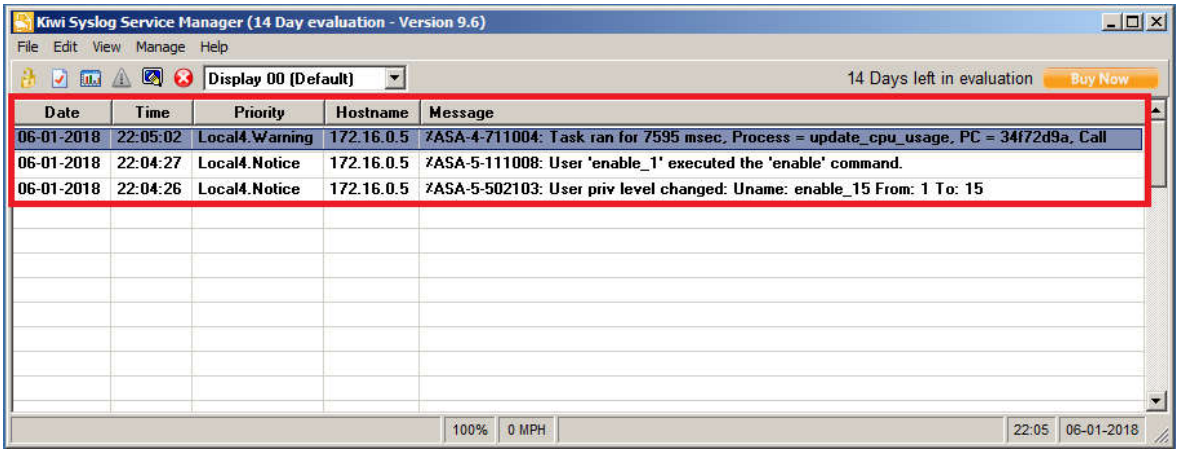


Figure 3.14 : kiwi Syslog service.

3.3.4.2 Securing Data Plane

The most important in this part is securing protocols and traffic that the network devices use on their own, such a routing protocol can dynamically learn and share routing information that the router can then use to maintain an update routing table, which mean one failure occurs in the control plan, the router might not be able to share or correctly learn dynamic routing information. [19]

The following steps bellows explain the protocols or methods are used to secure the data plan :

- Securing routing protocol OSPF with using password authentication between L3 switches and firewall and routers.

by authentication using MD5 hashing on interfaces :

```
Dist-1(config)#int e0/2
Dist-1(config-if)#ip ospf authentication message-digest
Dist-1(config-if)#ip ospf message-digest-key 1 md5 Mypassword
Dist-1(config-if)#ip ospf network point-to-point
```

Cmd-List 26 : Authentication OSPF.

Then about the traffic that is being forwarded through the network devices between clients and servers, any single failure in data plan could effects the ability of company's services or could possibly break down the network.

- Access control lists (ACL)
- VLANs and Spanning Tree Protocol (STP)
- Using Zone-Bazed Firewall

3.3.4.3 Implementing VPN Using Cisco ASA With ASDM

Depending on Cisco Adaptive Security Device Manager (ASDM) is graphic user interface (GUI) tool used to manage Cisco ASA. We had created a VPN tunneling between local site (Campus) and Remote site (Branch A).

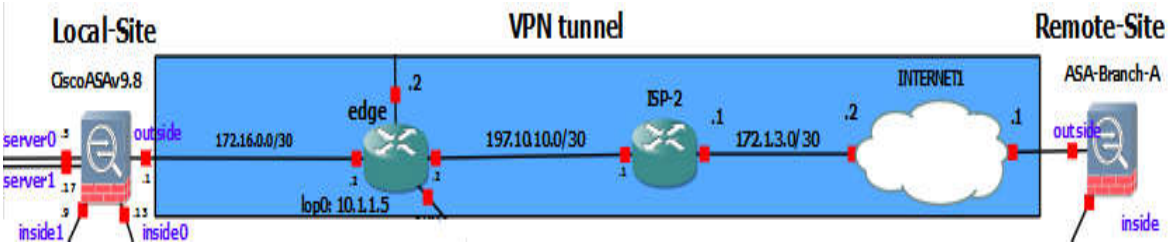


Figure 3.15 : VPN Tunnel Site-to-Site.

The steps to implement VPN Site-to-Site :

- From local site or remote site we have the same steps, So we need to know the peer IP address for each site.
- Then we identified the Access list that has to protect through VPN connection it could be VLANs or specific hosts instead of Object Networks. In our case we chose Host from VLAN40 local site and Host from VLAN70 remote site.
- Select the pre-shared key to authenticate this device with the peer.
- Configure the source interface for the traffic on the ASA. The ASDM automatically creates the Network Address Translation (NAT) rule based on the ASA version and pushes it with the rest of the configuration in the final step.

Configuration a VPN Site-to-Site from VLAN40 monitoring with the following settings :

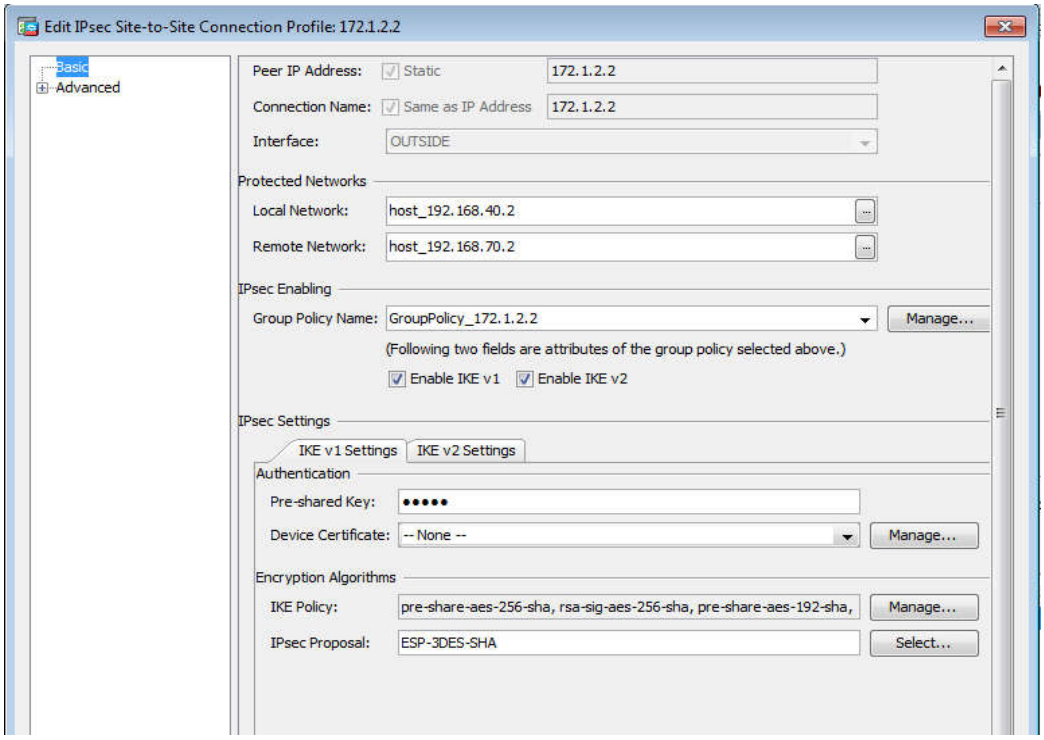


Figure 3.16 :ASDM setting from VLAN40.

Similar configuration to VPN Site-to-Site from VLAN70 monitoring :

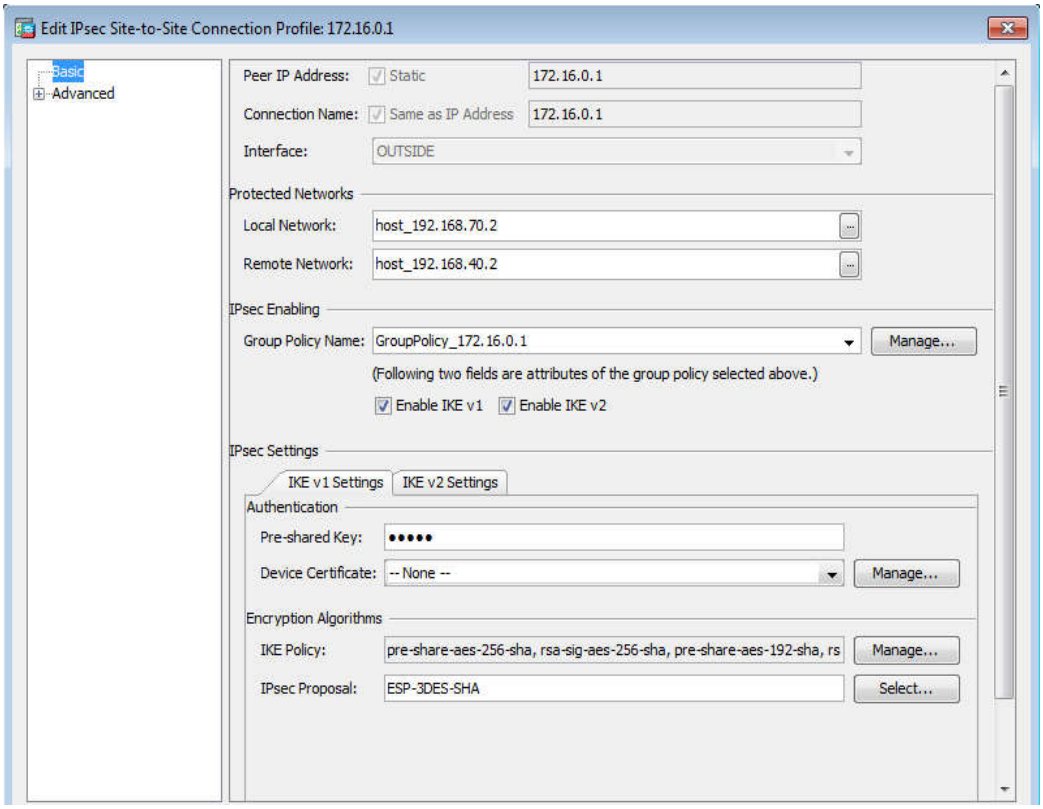


Figure 3.17 : ASDM setting from VLAN70.

3.4 Emulation Results

Connectivity between end users of campus and internet :

From host located in VLAN40, we attempt to ping into Google DNS with IP 8.8.8.8, we obtain successful replay as shown below :

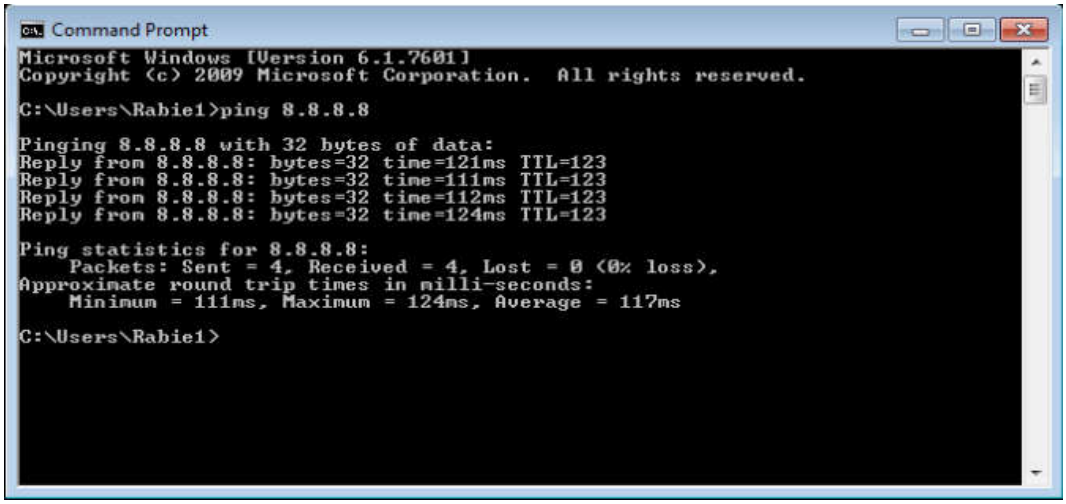


Figure 3.18 : ping to Google.

Accessing into Web Sever on DMZ :

In Web Server of DMZ we have a default web site has been configured by service IIS. So from the host located in VLAN40, and whatever VLAN are being that host we should access the server by http protocol and browsing the website (http://195.1.1.161/).

Figure 3.19 : Page Website.

Connectivity between two branches (Local-Site, Remote-Site)

With VPN tunneling we have got connection between two sites, we obtain successful replay, from PCs belongs to VLAN 40 ,70 with IP addresses 192.168.40.2 and 192.168.70.2 respectively, as shown below on command prompt of windows 7 :

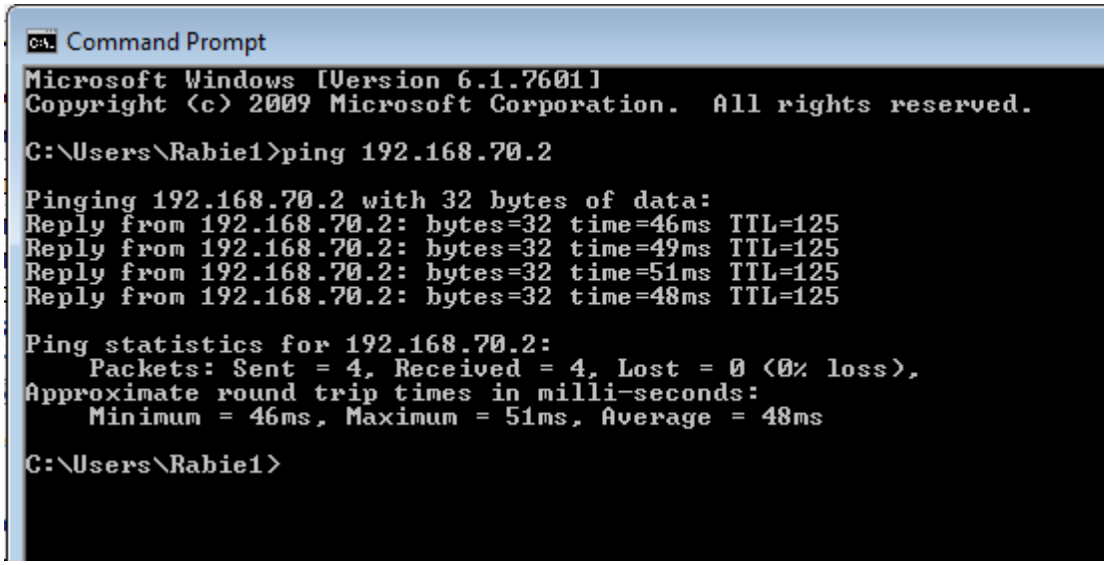


Figure 3.20 : Ping to the Remote-Stie.

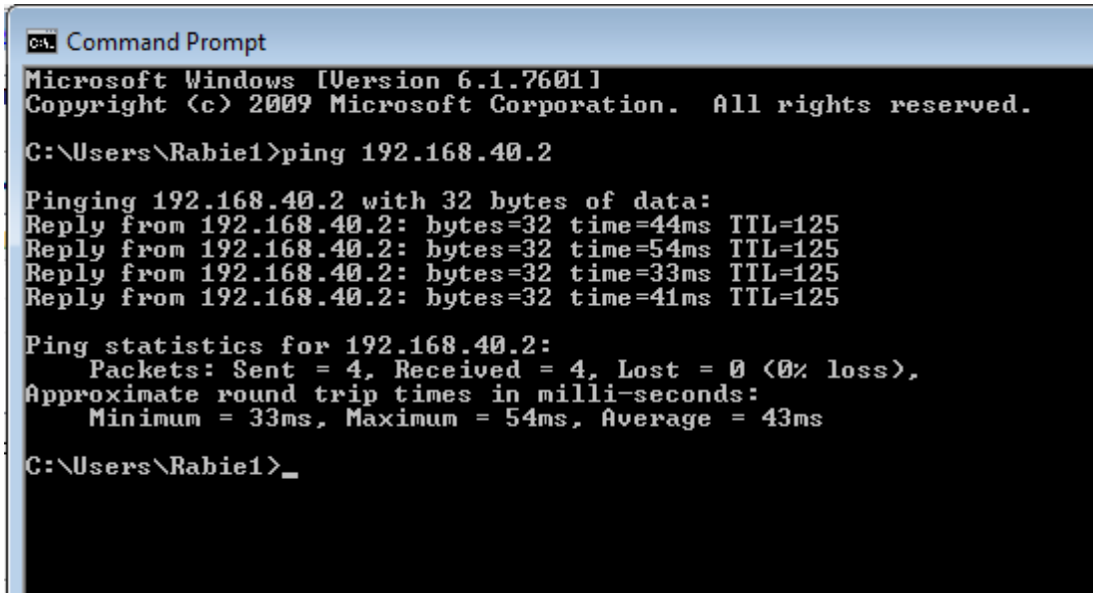


Figure 3.21 : Ping to the Local-Site.

To prove that connectivity between two sites, we need to make sure that connection are encrypted by ISAKAMP, **ISAKMP** is the protocol that specifies the mechanics of the key exchange.

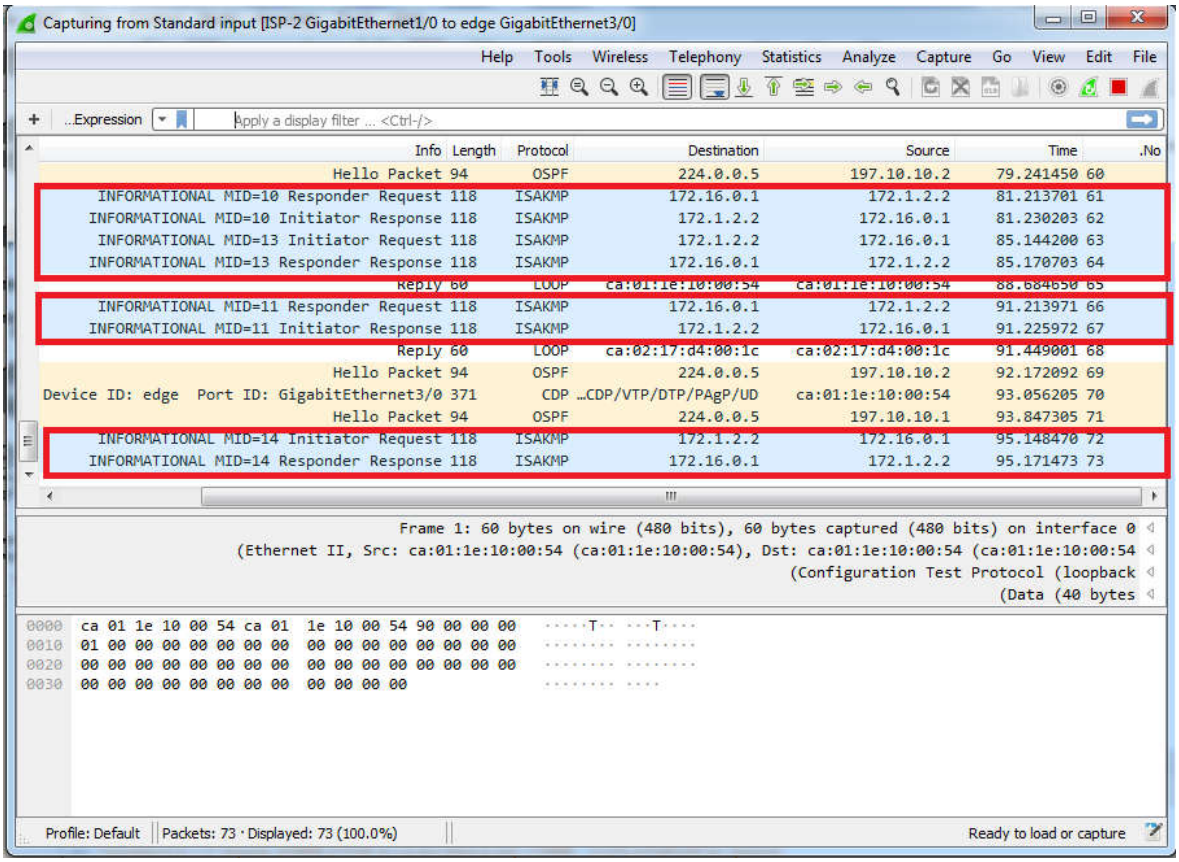


Figure 3.22 : Wireshark Capturing ISAKAMP.

We can see that red frame are captured by Wireshark analyzer, it contain the source and the destination that using ISAKAMP to exchange the key between themselves and start communicate safely.

The IP addresses are the outside interfaces of firewalls that provide VPN tunneling. Started with request ISAKMP from 172.16.0.1, just when we start pinging directly to the Remote-Site, then we have got response from 172.1.2.2. The similar result happened when we reverse the ping direction.

3.5 Conclusion

This chapter gave us an idea about the practice in the real work, with all difficulties we could face, a specially in configuration and adaptivity between different devices and different systems, the most hard work are being there. but with basics knowledge of

networking and spending hours of beating in this craft, we could build a great knowledge and we could handle the issues might happen. finally, we have to admit about the deficiencies exactly on the feeble resource that we used to build this whole network.

General Conclusion

General Conclusion

We were careful about our dissertation methodology and its content, and we can consider it as a first dissertation of this field at the university of Biskra discussed about most certifications valuable in networking, Cisco certified networking from associate until the expert (CCNA, CCNP, CCIE) and particular Cisco Certified Design (CCDA, CCDP).

We gave the subject great importance, because there is no company or any enterprise does not have a network, or any services and applications network tended to the end users. Moreover, For everyone has passion to be prepared for field of business or even to expand his information for academic preparation, this dissertation such an opportunity to evolve the students or any candidate for graduation to improve his network skills.

The networking technologies are developing day after day, and we could say develop of one month make the old technologies as a legacy. The large organization which were the responsible for the new devices has invented or a new technologies has released, make a direct impact into the fate of the future design of enterprise network, which mean as a student we have to follow this incredible growth evolution, with hope in order to create a new one.

Perspective

As a perspective around this dissertation, and after spending a lot of times practicing network configuration, we found some weaknesses around OSPF algorithm. We suggest for the candidates students to the next year, that take cares about this point. They have to determine the weaknesses and define it for development purposes. Moreover, as another perspective for candidates, they could make their studies about configuration by using programming language. For example, they could integrate the configuration of Cisco devices with python language, which is considered as a gateway to new technology SDN (Software Defined Network).

Bibliography

Bibliography

[1] 23/08/2016 https://www.networkcomputing.com/data-centers/campus-network-design-models/1685370612

[2] 09/05/2014 http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

[3] Wayne Lewis, 'LAN switching and wireless:CCNA exploration companion guide' Cisco Press, April 2008

[4] 2018/06/17 http://slideplayer.com/slide/10957395/

[5] https://en.ids-imaging.com/techtipps-detail/en_techtip-multicast.html

[6] Ron Gilster, 'CCNA for Dummies', IDG Books Worldwide-Inc , June 2009

[7] 02/06/2015 https://learningnetwork.cisco.com/thread/84956

[8] 2018/03/11 https://networklessons.com/spanning-tree/introduction-to-spanning-tree/

[9] 2018/04/20 https://networklessons.com/switching/introduction-to-vtp-vlan-trunking-protocol/

[10] 2018/03/25 https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ipv4-address-configuration-on-cisco-ios-catalyst-switch/

[11] 2018/06/17 https://www.ciscolive.com/global/on-demand-library/?search=BRKCRS-2031#/session/1467135308468001hKMQ

[12] Diane Teare, 'Designing for Cisco Internetwork Solutions (DESGN) ', Second Edition, Cisco Press, October 2007

[13] 18/05/2018 https://en.wikipedia.org/wiki/Graphical_Network_Simulator-3

[14] 23/06/2017 https://en.wikipedia.org/wiki/Dynamips

[15] 22/06/2018 https://en.wikipedia.org/wiki/Wireshark

[16] 26/06/2018 https://en.wikipedia.org/wiki/VMware

[17 13/06/2018 https://en.wikipedia.org/wiki/QEMU

[18] 2018/04/15 https://www.watchguard.com/help/docs/fireware/12/en-US/Content/en-US/authentication/radius_how_works_c.html

[19] Sikandar Shaik, 'CCNA Security (210-260) Lab Workbook' NOA solutions, Arcade,2nd & 3rd floor, 2016.

[20] 05/05/2018 https://www.networkmanagementsoftware.com/what-is-syslog/