ENSIAS

جامعة محمد الخامس
Université Mohammed V


Cabling & WiFi, LAN Architecture, WAN architecture, NAT/PAT/DHCP and Security.

# Project:

## Design and implement IP networks

framed by
Abdellatif Kobbane

realized by
Heiballa Abdellahi

**IOSM 2019/2020**

## *Special thanks*

It is with the greatest pleasure that i express my deep gratitude to all people who contributed, directly or indirectly, to the accomplishment of this work.

To our parents who have always learned that the quest for knowing is the essence of existence.

I mainly address our supervisors Mr. Kobbane  Abdellatif, I would like to express our deep gratitude for the help they have given us throughout this work.

I also want to send our most sincere thanks to the entire ENSIAS teaching staff, for all the efforts they make in order to prepare and ensure quality training.

# Abstract

This document is the core of my work regarding our network project.

The essential objective of this document is to design and implement IP network of a company.

During my work, the first mission was to realize comparative analysis to look for the most suitable type of cable to construct an adequate network for the whole company building. Then, i realize also a comparative study to choose the right switch and router to set up the LAN architecture building located in Casablanca, then the WAN architecture that is located between Casablanca and Rabat, and Finally I reinforced my architecture using multiple security protocols, all this work is represented with PACKET TRACER software.



Keywords: cabling, LAN, WAN, security, PACKET TRACER…

# Table of Contents

# Table of Contents

# Chapter I: Estimation of internal interconnection and WIFI charges

## Introduction

To succeed in such a project, it is necessary to make a detailed study about the loads of the implementation of an internal connection. This study involves a lot of knowledge of prediction and abstraction on the one hand and exact calculation on the other hand by taking into consideration the overall architecture of the company and the way in which the machines are dispersed into services such as end machines (workstations) and interconnect equipment (switches and routers).

Among the work of a network engineer is to provide a strategy for cabling the equipment involved, thus involving the decision-making aspect and the various risks in order to be able to reach in the end to an economic, effective and relevant decision.

An enterprise has two building one at Casablanca and the second at Rabat.

The Casablanca building has **9 flours** with **8 rooms** each as depicted in the following figure:

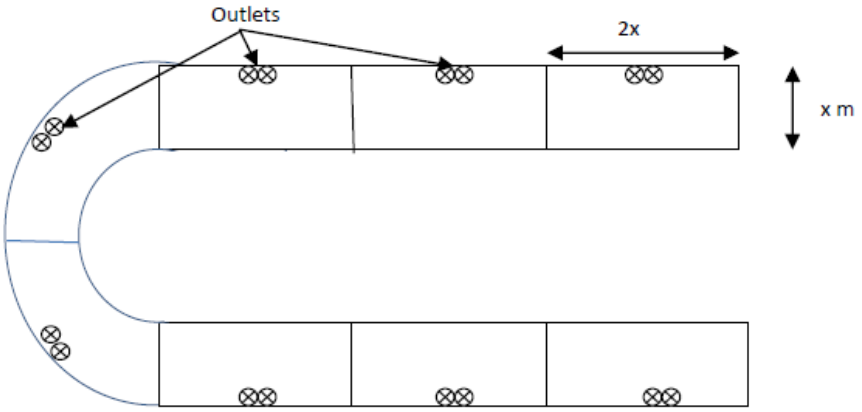



*Figure 1 Casablanca building.*

### Casa Headquarters:

The headquarters of Casablanca is  located in a building of 9 floors, each floor is composed of 8 rooms, the surface of each room is 29x58= 1682 $m^2$ .

### Rabat Headquarters:

In Rabat, the network contains twenty computers belonging to the 10.29.132.0 / 27 network.

- The main switch as a VTP server and the others as VTP clients.

- The main switch is the STP root bridge.

## Work to do :

Market research on the Casablanca building installation.

Configuration of the DNS (149.0.0.3 /29) and WEB (149.0.0.4 /29) servers between the internal routers and Casablanca.

Configuration of the default static routes on routers Rabat and Casablanca Configuration of the PAT service on the routers Rabat and Casablanca Configuration of a DHCP server on the internal router to serve all the VLANs of Casablanca.

## The security strategy:

Limit ssh access on switches and routers to the Administrator's portable administrator (10.29.1.100 /24).

Deny floor2-VLAN access to the Internet.

On the Casablanca Router, open only DNS and Web Services for future communications from the Internet.

Configure a VPN tunnel between the Rabat and Casablanca sites, use AES for encryption and SHA2 for authentication.

Internet can be seen as 3 routers (EST, CORE and WEST) connected by leased lines and configured by OSPF.

Casa-EST: 149.0.1.0 / 30.

EST-CORE: 149.0.2.0 / 3.

CORE-WEST: 149.0.3.0 / 30.

and WEST-Rabat: 149.0.4.0 / 30.

Configuring PPP with CHAP on all leased lines

## Market study:

Casablanca headquarters contains 9 floors of the same dimensions (29x58 m2)

## Size of the floor:

Our local (floor) contains eight rooms with a length 58m and a width of 29m,

and with a height of 3m

The total surface of the floor is

203 * 116 = 23,548 m2

The total surface of the 8 rooms is

6*(29*58)+2*(pi * 58^2-(pi * 29^2))

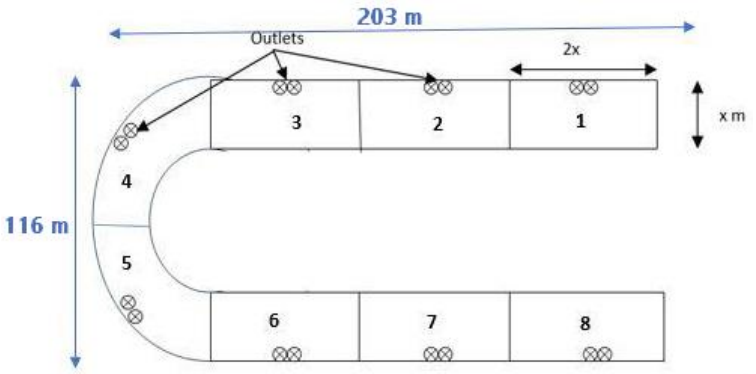
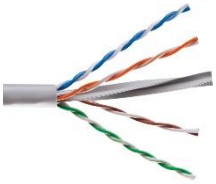



*Figure 2 building dimensions.*

## Wiring and supports:



**Category 6 U / UTP cabling:**

The proposed pre-wiring architecture complies with the environmental standards and standards of Category 6 and guaranteed performance.

## Solution:

The solution I found is that I will connect each RJ45 output with a dedicated switch for each floor. to ensure the connection of the complete topology of the building later with the help of the backbone switch, which will be implemented in the first floor.

## Category 6 U / UTP cabling:

The proposed pre-wiring architecture complies with norms and standards related to the category 6 environment and guaranteed performance.

| **Flow rates** | **Compatible cable** |
|---|---|
| 10 Gb / s | CAT6a (100 m) |
| | CAT6 (55 m) |
| | CAT5e (30 m) |
| 5 Gb / s | CAT6 (100 m) |
| | CAT5e (30 m) |
| 2.5 Gb / s | CAT5e (100 m) |
| 1 Gb / s | CAT5e (100 m) |

## Result:

As long as the longest cable of a stage does not exceed 100 m and CAT6 can pass up to 5Gb/s  for cables that do not exceed 100 m, then it is appropriate for this case

The length of the cable UTP cat 6 per floor:

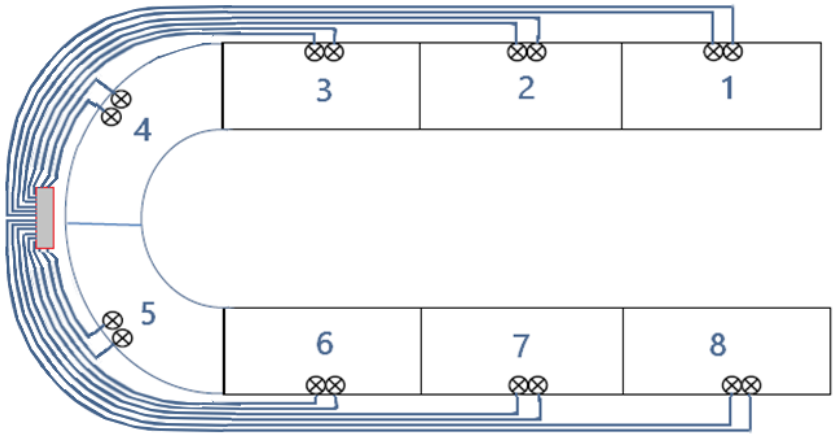



*Figure 3 cabling solution.*

## The length of the UTP cat 6 cable per stage:

| **room** | **Length** |
|---|---|
| 1 & 8 | (29+58+58+(pi*58/2)) *4 +8 =952 m |
| 2&7 | (29+58+(pi*58/2) *4 +8 = 459 m |
| 3&6 | (29+(pi*58/2)) *4+8 =488 m |
| 4&5 | (pi*58/4)*4+8=190 m |
| **Total** | 2089m=2100m |

**Vertical**:Associate to each floor a Switch (16 ports) to connect them to the backbone switch which will be found in the 1st floor via the optical fiber chosen before.

**Length of fiber needed**: 27+24+21+18+15+12+9+6+3=135 m

Cost of the fiber: 135x170.00 = **22950.00dh**

**PLASTIC CHUTE 80x50mm**

The chute must comply with NF C 68-1 02 standards. The chute will be used for the routing of computer cables.

**The total languor of the chutes per floor is:**

(pi*58/2)*2+(58+58+29)*2+3=475m

This item is paid by the linear meter including supply, installation, mounting accessories, inside corners, outside corners, bypasses, end caps, joints - staples, any partition bores and any other installation requirements.

**Outlets**

must be female RJ45 type and conform to the ANSI / TIA / EIA 568 B 2.10 category 6 standard.

This socket should be unmarked, wired as a computer socket (on the two pairs).

The modules for the sockets must be U / UTP type Cat6, with self-attaching,

The number of takes per floor is 16 .

**6U BREWING BOX**

The cabinet must be swiveling with a minimum capacity of 6 Units, and it must meet the

Minimum requirements: Depth: 60 cm; width: 60 cm; The box must be equipped with:

✓ Swiveling side panels removable from the inside without tools

✓ Curved reversible door in screen-printed safety glass;

✓ Key lock;

✓ Full cable entry plates at the top and bottom;

✓ Each floor must have a brewing box 6u

**FIBER OPTIC CABLE «Multimode»**

The optical fiber proposed must be of the OM3 class Multimode type, supporting high data transmission speeds (10 GBits / s). It is used as the main element of distribution cabling in fiber optic data or telecommunication systems.

Physical Characteristics:

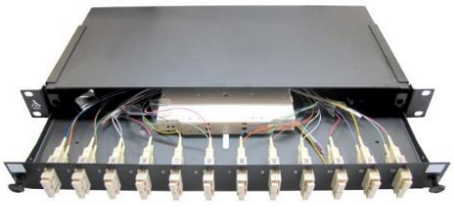
Nb of fibers: 4 strands.

DIA Heart coating: 50/125 µm.

DIA Ext. Cable: 6 mm.

Breaking load: 15000 N / 100 mm.

Protection: int / ext.



**OPTICAL DRAWER 4 ports**

The optical drawer installed in the computer cabinets will be a sliding optical drawer that complies with the international ISO 11801 standards. The drawer must be equipped with the connectors required to connect two multi-mode OM3 class optical fiber cables, each of 4-core.

The use of optical fiber mainly offers 3 problems:

✓ A high price of installation.

✓ A complexity of implementation: multitude of connectors, fragility.

✓ The high cost of active equipment.

Fiber has the following advantages over copper.

The distance: the copper is limited to 100 m, the fiber reaches several hundred meters and several kilometers according to the technical choices.

## Result:

The fiber is not recommended in our case, it is better to use UTP CAT6 or CAT6e instead of optical fiber.

## Network equipment:

**Cisco SG500X-24P Access Switch**

The Cisco SG500X Switches are part of a range of Ethernet stackable Managed Switches, which offers all the advanced capabilities you need to support a more demanding network environment at an affordable price. These switches provide 2-port Gigabit Ethernet connectivity with optional 10 Gigabit uplinks,The switch meets the following technical specifications:

Chassis type: Rack mountable - 1U (19).

Administration functions: SNMP, RMON, WEB, CLI.

Ports:

24 ports RJ45 PoE + 10/100/1000 Mbit / s (up to 30.8 W) with automatic detection.

2 dedicated 10G SFP + ports.

DiffServ

Security Architecture:

Radius authentication support.

SSL and SSH support.

**The Switch 2950-24**

The Cisco 2950 Switch is for Dedicated Floor Switching Fixed 10/100/1000 Mbps Ethernet, delivering exceptional performance, flexibility, and manageability, combined with unparalleled investment protection. This range of 10/100/1000 autosensing switches offer many advanced quality of service features(QoS) and multicast flow processing. The Web Management Interface provides easy-to-use administrative functions through the Cisco Cluster Management Suite) and integrated Cisco IOS software. The Catalyst 2950T-24 Gigabit on copper, with two high-speed uplinks 10/ 100/1000, offers small and medium-sized businesses an ideal solution for migrating from Fast Ethernet to Gigabit Ethernet while using existing Category 5 copper cabling. The Catalyst 2950 switch range is made up of 9 different models that combine all the needs for 10/100 ports from 12 to 48 ports, and the needs for 100FX, Gigabit copper, and Gigabit fiber ports.

The wireless access point

The Wireless Access Point can be used to build or expand an N-based wireless broadband network or to connect multiple Ethernet-enabled devices such as game consoles, media players, printers, or wireless devices to a wireless network. storage.

The access point meets the following technical specifications:

Interface: An Ethernet 10/100 M (RJ45) port .

Wi-Fi standards: IEEE 802.11n.

**Scopes and flows**

The 802.11a, 802.11b, and 802.11g standards, known as "physical standards," are revisions of the 802.11 standard and provide modes of operation that provide different rates for different ranges.

| Standard | Frequency | Data Rate[1] | Range | Type |
|---|---|---|---|---|
| 802.11a | 5 GHz | 54 Mbps | 120m | LAN |
| 802.11b | 2.4 GHz | 11 Mbps | 140m | LAN |
| 802.11g | 2.4 GHz | 54 Mbps | 140m | LAN |
| 802.11n | 2.4/5 GHz | 248 Mbps[2] | 250m | LAN |

The Wi-Fi solution in business requires to ask the following questions:

• **Scaling**: How many users will need to connect to Wi-Fi?

• **Usage**: What use of Wi-Fi will be made? Simple Internet connection or connection to potentially bandwidth-intensive applications?

• **Coverage**: What is the area to cover in Wi-Fi?

• **Security**: what level of security do I want to put in place? For example, are there differentiated access classes between visitors (Internet access only) and employees (access to the internal computer network)?

**Result:**

In the building Casablanca you must use an access point Wifi N (802.11n).

## Wifi solution:

The IEEE 802.11n standard achieves a theoretical throughput of up to 240 Mbit/s over

each of the usable frequency bands (2.4 GHz and 5 GHz). This is the recommended standard by the specifications for the installation of the wireless network in the enterprise.

this standard is 70 m for the 2.4 GHz frequency band.

Explanatory diagram of the coverage area of a WIFI access point that uses the standard.

802.11n:

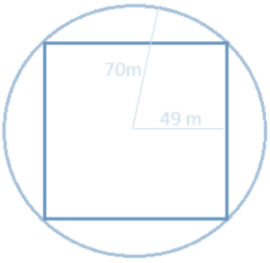



*Figure 4 coverage area of 802.11n.*

Based on the diagram above I can cover an entire floor by wifi using two wifi access points only:

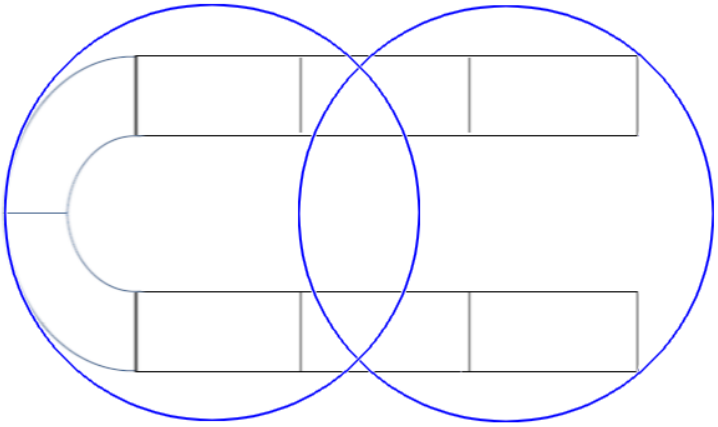


*Figure 5 floor coverage.*

**Cisco 1841 Router**

The Cisco 1841 router with the following benefits:

Fast transmission for simultaneous services at T1 / E1 WAN network speeds,

Better investment protection due to its performance and enhanced modularity, Better investment protection thanks to its enhanced modularity, Support existing or new modules.

Other Feature:

Connectivity Technology: Wired Chassis.

Type: Modular Data Link.

Protocol: Ethernet, Fast Ethernet.

Network / Transport Protocol: IPSec.

## Security programs

Encryption algorithm: DES, Triple DES, SSL, 128 bit AES, 192 bit AES, 256 bit AES.

Méthode d'authentification : SSH et Telnet.

**Purchase order:**

| Num | Designation | quality | U price | HT Total |
|---|---|---|---|---|
| 1 | TRANSMISSION CABLE | 18,900 m | 12,00 | 226800.00 |
| 2 | PLASTIC CHU 80x50 | 4,275 m | 50,00 | 38475.00 |
| 3 | OUTLETS | 144 | 30,00 | 4320.00 |
| 4 | 16U BREWING BOX | 1 | 8,000.00 | 8000.00 |
| 5 | 6U BREWING BOX | 9 | 3000,00 | 27000.00 |
| 6 | "Cisco 3560" Federator Switch | 1 | 45000,00 | 45000.00 |
| 7 | Cisco 2960 Access Switch | 9 | 25000.00 | 225000.00 |
| 8 | The wireless access point | 1 | 2000.00 | 2000.00 |
| 9 | Cisco router | 9 | 12000.00 | 108000.00 |
| 10 | Server | 9 | 10000.00 | 90000,00 |
| The configuration | | | 10000.00 | 10000.00 |
| **Total HT** | | | | **784595,00** |
| **T.V.A (20%)** | | | | **156919,00** |
| **Total Price** | | | | **941514,00** |

# Chapter I: VLANs

An end-to-end switched architecture provides the ability to segment the network into multiple virtual or logical LANs (workgroups within the network).

## VTP configuration

At the backbone switch I will configure the VTP in server mode, and the access switches in client mode.

For switching, used a hierarchical model with two levels (Core and Access levels  Considering each flour as an independent VLAN:

- VLAN name: Vlan-Flour1, VLAN numer:129, VLAN Network Address: 10.29.1.0/24.

- VLAN name: Vlan-Flour2, VLAN numer:229, VLAN Network Address: 10.29.2.0/24.

- VLAN name: Vlan-Flour3, VLAN numer:329, VLAN Network Address: 10.29.3.0/24.

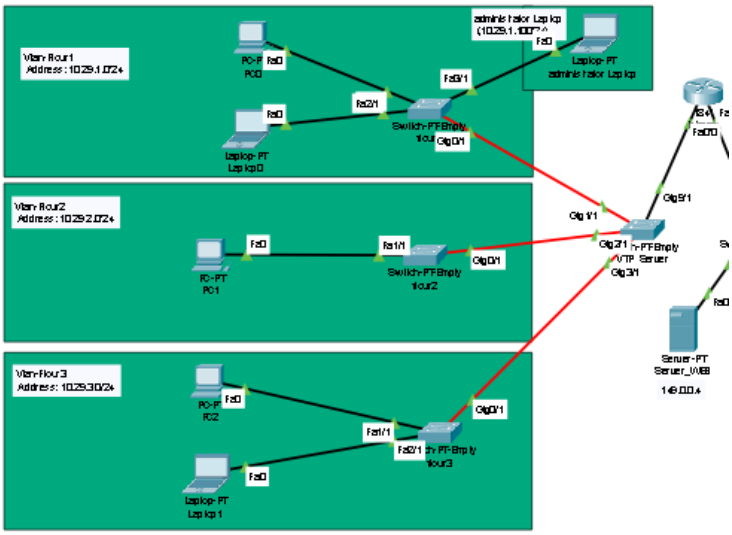


*Figure 6 LAN interconnection diagram.*

VTP or VLAN Trunking Protocol is a level 2 protocol used to configure and administer VLANs.

The VTP protocol allows you to manage vlan (add, rename or delete) on a single switch (the server) this is the unifying switch in our case, which will propagate this configuration to all other switches (clients).

Here is what follows the statue of the VTP protocol in the company:

**The VTP configuration of the unifying switch:**

```
VTP_Server>en
VTP_Server#sh vtp st
VTP Version                     : 2
Configuration Revision          : 47
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x06 0x97 0xDC 0x89 0x65 0x27 0xDA
0x03
Configuration last modified by 0.0.0.0 at 3-1-93 05:09:27
Local updater ID is 10.29.1.3 on interface Vl129 (lowest numbered
VLAN interface found)
```

*Figure 7 VTP server configuration.*

**The configuration of the other switches:**

```
Switch>en
Switch#sh vtp st
VTP Version                     : 2
Configuration Revision          : 47
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : cisco
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x06 0x97 0xDC 0x89 0x65 0x27 0xDA
0x03
Configuration last modified by 0.0.0.0 at 3-1-93 05:09:27
Switch#
```

*Figure 8 clients switch configuration.*

## The STP protocol:

The Spanning Tree Protocol (STP) is a layer 2 protocol that operates on bridges and switches. The specification for the STP protocol is IEEE 802.1D. The objective main of the STP protocol is to make sure that you don't create loops when you have redundant paths in your network since loops are fatal for the network. To force the unifying switch to be the Root bridge, it must be assigned the lowest priority.

```
VTP_Server#show sp
VTP_Server#show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32769
              Address     0001.C74C.3C75
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32769  (priority 32768 sys-id-ext 1)
              Address     0001.C74C.3C75
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- --------
--------------------------------
Gi1/1            Desg FWD 4         128.2    P2p
Gi2/1            Desg FWD 4         128.3    P2p
Gi3/1            Desg FWD 4         128.4    P2p
Gi9/1            Desg FWD 19        128.10   Shr

VLAN0129
  Spanning tree enabled protocol ieee
```

*Figure 9 STP configuration on VTP server.*

## DHCP :

In order to maintain an automatic IP configuration, the internal router has been configured as being a DHCP server, its role is therefore to ensure the IP configuration of the stations of all VLANs while specifying the default gateway and DNS server for all machines.

DHCP configuration on the internal routers:

```
ip dhcp excluded-address 10.29.1.3 10.29.1.4
ip dhcp excluded-address 10.29.2.3 10.29.2.4
ip dhcp excluded-address 10.29.3.3 10.29.3.4
!
ip dhcp pool Vlan-Flour1
 network 10.29.1.0 255.255.255.0
 default-router 10.29.1.1
 dns-server 149.0.0.3
ip dhcp pool Vlan-Flour2
 network 10.29.2.0 255.255.255.0
 default-router 10.29.2.1
 dns-server 149.0.0.3
ip dhcp pool Vlan-Flour3
 network 10.29.3.0 255.255.255.0
 default-router 10.29.3.1
```

*Figure 10 DHCP configuration*

In the first flour, two routers are deployed in the cabinet, one (Internal) for inter-VLAN routing and the second (Casablanca) connecting the enterprise to internet. The network address between the two routers is 149.0.0.0/29. The IP address of the serial interface of the Casablanca to ISP is 149.0.1.5/30.

In Rabat, the network contains twenty PCs belonging to the network 10.29.149.0/27.

## The DMZ zone

The DMZ zone contains two DNS 149.0.0.3 and 149.0.0.4 Web servers.

For the test of the two servers I create a page of the address dns.casa.ma.

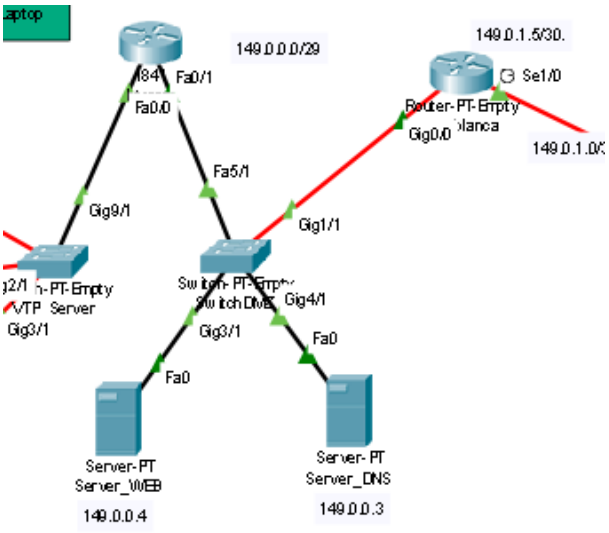



*Figure 11 dmz zone*

**PAT configured at router Casa**

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

# Chapter II: WAN

In this zone I have set the Internas 3 routers
(EST, CORE and WEST) linked by leased lines
and configured by OSPF.
Casa-EST: 149.0.1.0/30,
EST-CORE: 149.0.2.0/30;
CORE-WEST: 149.0.3.0/30
WEST-Rabat: 149.0.4.0/30.
Configure PPP with CHAP on all leased lines

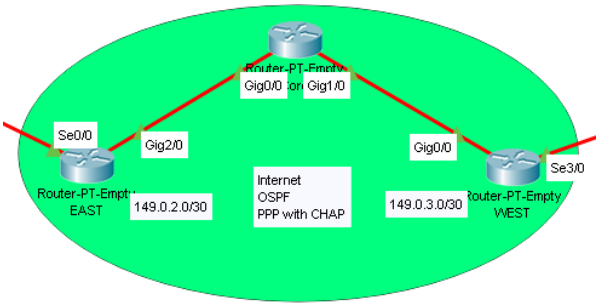



*Figure 12 wan architecture.*

## OSPF:

I have configured the OSPF protocol in all the routers that make up the ISP network.

OSPF allows the exact and complete connection of the network topology, it bases its decisions of routing on the minimal cost tree calculation and it uses the Dijikstra algorithm for the

determine based on a quantity called Metric.

The configuration of Core routers of the ISP network:

```
router ospf 1
 log-adjacency-changes
 redistribute static subnets
 network 149.0.0.0 0.0.0.7 area 0
 network 149.0.1.0 0.0.0.3 area 0
!
```

*Figure 13ofpf casablanca*

```
router ospf 1
 log-adjacency-changes
 network 10.29.149.0 0.0.0.31 area 0
 network 149.0.4.0 0.0.0.3 area 0
 default-information originate
!
```

*Figure 14 ospf rabat*

## The PPP protocol:

The PPP protocol (point to point) is the only authentication protocol in branch networks, this protocol was implemented on the routers with the CHAP authentication mechanism, this is a mechanism strong authentication compared to the PAP because it ensures the non-circulation of the password in the network.

Configuration of the Rabat router

```
interface Serial0/1/1
 ip address 149.0.4.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 ip nat outside
 clock rate 2000000
 crypto map CMAP
```

*Figure 15 PPP encapsulation on Rabat*

## PAT: Port address Translation

To maintain the secrecy of the internal network of each local of the company, I have chosen to configure the PAT (Port address Translation) protocol in the internal router and rabat to ensure that the company's internal networks remain private

the PAT protocol translates all internal addresses into a single public address which is that of the serial output to the outside.

```
Rabat#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 149.0.4.2:1024     10.29.149.10:1025  149.0.0.4:80       149.0.0.4:80
tcp 149.0.4.2:1025     10.29.149.3:1025   149.0.0.4:80       149.0.0.4:80
tcp 149.0.4.2:1034     10.29.149.3:1034   149.0.0.4:80       149.0.0.4:80
tcp 149.0.4.2:1035     10.29.149.3:1035   149.0.0.3:80       149.0.0.3:80
tcp 149.0.4.2:1036     10.29.149.3:1036   149.0.0.3:80       149.0.0.3:80
tcp 149.0.4.2:1037     10.29.149.3:1037   149.0.0.3:80       149.0.0.3:80
tcp 149.0.4.2:1038     10.29.149.3:1038   149.0.0.3:80       149.0.0.3:80
tcp 149.0.4.2:1039     10.29.149.3:1039   149.0.0.3:80       149.0.0.3:80
tcp 149.0.4.2:1040     10.29.149.3:1040   149.0.0.3:80       149.0.0.3:80
```

*Figure 16 The translation table of the rabat router.*

# Chapter III: Security

## Introduction:

Network-based security threats have caused a dramatic increase in theft identities and financial fraud. Spam, Viruses and Spyware cause significant problems for individuals and businesses.

A flaw of Security can irreparably damage the brand or reputation of a company.

In this chapter I will detail how I met the security criteria that appear in

the specifications to properly protect the company against these various risks.

## Telnet:

Telnet is a protocol allowing to emulate a remote terminal, it means that it allows to execute commands entered using the keyboard on a remote machine.

Only the Admin workstation that exists on the first floor of the Casa room is allowed to configure all the other cisco equipment that exists in the premises of the company.

(Casablanca, Rabat), through telnet.

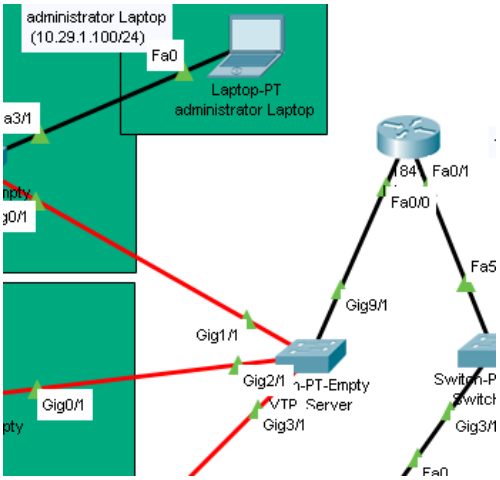



*Figure 17 The admin workstation.*

An ACL which allows this has been configured in all switches and routers:

```
access-list 14 permit host 10.29.1.100
access-list 14 deny any
!
!
!
!
!
!
line con 0
!
line aux 0
!
line vty 0 4
 access-class 14 in
 password cisco
 login
```

*Figure 18 ACL configuration.*

```
C:\>telnet 10.29.1.3
Trying 10.29.1.3 ...Open


User Access Verification

Password:
VTP_Server>
```

*Figure 19 Telnet check*

## Prohibit Vlan three from accessing the internet:

For security reasons, the third floor of the company's premises located at Casa is prohibited from accessing the Internet.

At the level of the internal router I configured the following ACL:

```
ip access-list extended Flour2
 deny tcp any any eq telnet
 permit ip 10.29.2.0 0.0.0.255 10.29.0.0 0.0.255.255
 deny ip 10.29.2.0 0.0.0.255 any
 permit ip 10.29.2.0 0.0.0.255 149.0.0.0 0.0.7.255
 permit ip any any
```

*Figure 20 flour 2 ACL.*

**The process is to :**

- ✓ prohibit telnet access to the outside.
- ✓ allow the 2nd floor to communicate with the other floors.
- ✓ prohibit valn-flour2 from going to any other destination.
- ✓ give permission to vlan-flour3 to access the dmz area.
- ✓ let other VLANs communicate with the outside freely.

This ACL is applied later in the interface closest to the source so it is

the internal interface of the internal router:

```
interface FastEthernet0/0.229
 encapsulation dot1Q 229
 ip address 10.29.2.1 255.255.255.0
 ip access-group Flour2 in
 ip nat inside
```

*Figure 21 ACL to internal interface.*

## Access to DNS and Web services:

For security reasons I have given access only to web and DNS services.

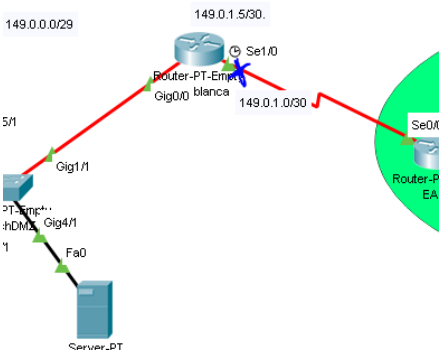
To ensure this I have configured the following ACL on the local external router located at Casa:

```
ip access-list extended webdns
 permit tcp any host 149.0.0.4 eq www
 permit tcp any host 149.0.0.3 eq domain
 permit udp any host 149.0.0.3 eq domain
 deny ip any host 149.0.0.3
 deny ip any host 149.0.0.4
 permit ip any any
 permit tcp any any eq telnet
```

Th process is :

- ✓ enable web service.
- ✓ enable secure web service.
- ✓ enable dns service.
- ✓ allow telnet return.
- ✓ maintain the connection of internal VLANs with the outside (the return of packets).

After creating the ACL, I applied it to the point closest to the source:




```
interface Serial1/0
 ip address 149.0.1.1 255.255.255.252
 ip access-group webdns in
 ip nat outside
 clock rate 2000000
```

*Figure 22 interface of Casablanca.*

*Figure 23 access to dns and web server.*

# Chapter IV: VPN

## Introduction :

The purpose of a Virtual Private Network (VPN) is to "provide users and administrators of the operating conditions, use and security through a public network identical to those available on a private network ". In other term, I want to group private networks, separated by a public network (internet) in

giving the user the illusion that they are not separate, while keeping the appearance

secure which was ensured by a logical cut to the internet.

The VPN is therefore only a concept, behind it, several implementations have seen the

day, depending on the use to be made of it, the level of security, the size of the network, etc ...

Several technical means can be used and coupled to implement VPNs:

encryption, authentication, integrity control and tunnels.

The tunnel is an essential component of VPNs; the problem is as follows:

wants to connect two private networks which are separated by a public network (internet) so

transparent to the user. The user will thus use virtual network interfaces and will have

the illusion of talking directly to the network that is, in fact, on the other side of the Internet.

## Prerequisite:

Before starting the configuration of the tunnels between the sites, it is first of all necessary to take into consideration that to succeed in establishing a tunnel, each router (outside the tunnel) must know the internal network of the other router (the other end of the tunnel).

So first of all it is necessary to modify the NAT ACL with regard to Rabat, here is the following ACL:

```
ip access-list extended NAT-TRAFIC
 deny ip 10.29.149.0 0.0.0.31 10.29.0.0 0.0.15.255
 permit ip 10.29.149.0 0.0.0.31 any
```

*Figure 24 Nat traffic in rabat.*

This ACL is then applied to NAT:

```
ip nat inside source list NAT-TRAFIC interface Serial0/1/1 overload
ip classless
```

*Figure 25 nat applicated in rabat.*

This is equivalent to saying to the Router: Do not translate IPs that want to communicate with the network on the other side of the tunnel (the DMZ Zone in this case). But for other destinations (other than the DMZ network) you can translate.

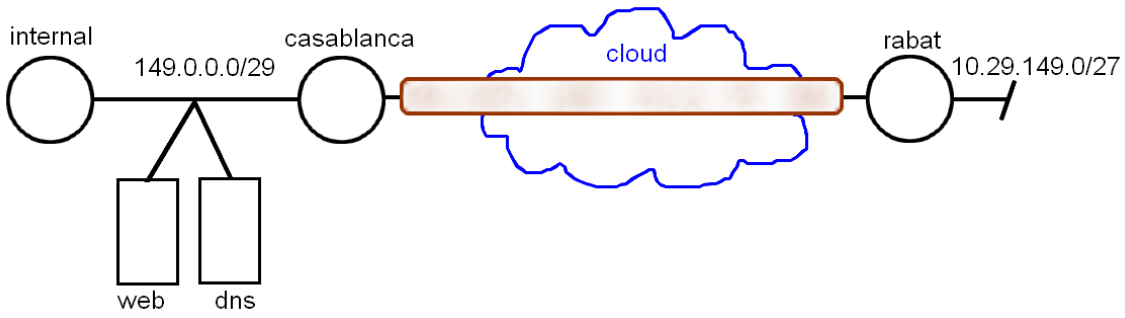



*Figure 26 The tunnel.*

## Protocol used:

IPSec (Internet Protocol Security) was designed to secure pass-through communications by

a tunnel between Casablanca and Rabat.

IPSec is not a replacement for IP but a complement. So, it incorporates essential notions of

security to the IP datagram which will ensure its authenticity, authentication and encryption. For

this makes extensive use of session keys.

IPSec is widely used for deploying VPN network across the Internet at small and large scale.

## Détails du protocole:

The internal mechanism of IPSec is complex. The fact that this protocol is highly configurable introduces concepts of management and configuration unknown to the IP world.

### IPSec flow management

#### *Security Policy*

An SP defines what must be treated on a flow. How I want to transform a package.

I used two different policies:

It will be indicated there for a given flow:

- ✓ The IP addresses of the sender and the receiver
- ✓ By which protocol it should be treated (ESP in our case);
- ✓ The IPSec mode to use (tunnel in our case);
- ✓ The sense of connection

#### *Security Association*

An SA defines how the packet will be treated according to its associated SP. They are just the

"realization" of the SP. It has all the properties of the link. Thus, it will be represented by a data structure which is called political.

in our case two policies have been deployed:

policy 1: between External and Remote1

- ✓ Encryption algorithm: AES
- ✓ Hash algorithm: SHA2
- ✓ Key exchange method: group 5

```
Rabat#sh crypto ipsec transform-set
Transform set 50: {    { esp-256-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },
```

*Figure 27 rabat ipsec.*

## IPSec mode:

Tunnel mode: This mode is used to encapsulate IP datagrams in IPSec. SA is applied over an IP tunnel. Thus, the original IP headers are not modified and an IPSec-specific header is created. This mode is often used to create tunnels between remote LAN networks. Indeed, it allows to connect two gateways being able to use IPSec without disturbing the IP traffic of the machines therefore not necessarily ready to use IPSec.

## IPSec key management:

ISAKMP (Internet Security Association and Key Management Protocol) allows negotiation, the establishment and removal of security associations (SA), thereby securing packages to be routed.

Here is the status of the VPN configuration on the External router:

```
Internal#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: CMAP, local addr 149.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.29.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port):
(10.29.149.0/255.255.255.224/0/0)
   current_peer 149.0.4.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 0
   #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 1, #recv errors 0

     local crypto endpt.: 149.0.0.1, remote crypto endpt.:149.0.4.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x0(0)

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:
```

*Figure 28 VPN configuration  on Internal.*

```
Internal#sh crypto map
Crypto Map CMAP 10 ipsec-isakmp
        Peer = 149.0.4.2
        Extended IP access list VPN-TRAFIC
            access-list VPN-TRAFIC deny ip 10.29.0.0 0.0.255.255 any
            access-list VPN-TRAFIC permit ip 10.29.0.0 0.0.255.255
10.29.149.0 0.0.0.31
        Current peer: 149.0.4.2
        Security association lifetime: 4608000 kilobytes/900 seconds
        PFS (Y/N): Y
        Transform sets={
                50,
        }
        Interfaces using crypto map CMAP:
                FastEthernet0/1
```

*Figure 29 crypto map Internal.*

```
Internal#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status

IPv6 Crypto ISAKMP SA
```

*Figure 30 SA crypto internal.*

# General conclusion

This project is a good opportunity to learn and put yourself in reality in front of challenges of implementing an IP network for us as engineers.

Throughout this project I have achieved many of the essential tasks during installing a network.

Firstly, I was concerned with designing an internal network architecture within the company, I carried out the internal wiring of the building while justifying the choice of location of the equipment and cables involved, I have implemented the corresponding LAN architecture by adapting the hierarchical model with PACKET TRACER software, I created three VLANs that each correspond to a floor, then an estimate of the overall cost was made following a deep and selective research in the equipment market in order to be able to give in the end almost can combine it costs the implementation of internal network while maintaining my economic solution (financial side) and efficacy (side technical).

Secondly, I configured the DNS and WEB servers after I simulated the architecture WAN under Packet Tracer so that you can subsequently configure the OSPF routing protocol on the routers that make up the ISP network, I then configured the PAT protocol to meet the requirements imposed by the specifications because certain networks must keep it private.

Thirdly, I approached the security aspect considering its importance and its necessity.

Authentication between some routers has been done using the PPP protocol.

I have also set up Access lists in order to meet the security criteria requested by the

specifications.

In the end, I was fortunate to tackle a more advanced security aspect, which is to implement the VPN.

to ensure more security by using encryption and hashing methods to strengthen authentication, integrity and confidentiality of the data exchanged.