École Nationale Supérieure
d'Informatique et d'Analyse
des Systèmes

Ingénierie web et informatique mobile

Rapport du projet intégré S4 1ère Partie

Conception et Implémentation des réseaux IP

Réalisé par :
Aymen CHLA
Youssef FARABY

Encadré par :
M. Mohammed EL KOUTBI
M. Mostafa BELKASMI

Année Universitaire 2017 - 2018

Remerciements

Tout d'abord, on tient à exprimer nos vifs remerciements et notre profonde gratitude à toute personne ayant contribué, de près ou de loin, à la réalisation de ce projet et ayant fait de cette période un moment très profitable.

On tient particulièrement à remercier nos encadrants M. Mohammed EL KOUTBI et M. Mostafa BELKASMI, pour leur guide et leurs conseils, ainsi que pour leur encadrement durant toutes les phases de réalisation de ce projet.

Nos remerciements vont aussi aux membres du jury, qui nous ont fait l'honneur d'accepter de juger notre travail.

On tient à exprimer les purs sentiments de reconnaissance et de sincères remerciements à nos familles, qui nous ont soutenus moralement durant la réalisation du projet et qui ont favorisé son aboutissement.

Résumé

Le présent document synthétise notre travail effectué durant le deuxième semestre de la deuxième année au titre du projet fédérateur S4, qui s'intitule «Conception et Implémentation des réseaux IP ».

Ce projet a pour mission de réaliser une étude globale de l'architecture réseau d'une société qui se compose d'un siège situer à Casablanca et d'une filiale à Rabat. Dans un premier temps notre travail consistait en une étude comparative pour les types de câbles et dispositives les mieux adapté en terme de coût et de performance pour construire l'architecture réseau la plus adapté pour cette société. Par la suite nous avons mis en place une architecture LAN du réseau du siège en utilsant le logiciel de simulation PACKET TRACER.Ainsi nous avons entamer sur l'implémentation de l'architecture WAN pour permetre la communication entre le siège et la filiale. Finalement on a renforcer la sécurité de notre architecture en utilisant plusieurs protocoles.

Abstract

This document summarizes our work done during the second second year under the unifying project S4, entitled «Design and Implementation of IP Networks».

This project's mission is to carry out a global study of the network architecture of a company consisting of a head office located in Casablanca and a subsidiary in Rabat. At first our work consisted of a comparative study for the types of cables and devices best suited in terms of cost and performance to build the most suitable network architecture for this company. Subsequently we implemented a LAN architecture of the headquarters network using the PACKET TRACER simulation software. So we start on the implementation of the WAN architecture to allow communication between the headquarters and the subsidiary. Finally we have to strengthen the security of our architecture using multiple protocols.

Abbreviations

ACL Access Control List
DHCP Dynamic Host Configuration Protocol
DMZ Demilitarized Zone
DNS Domain Name System
LAN Local Area Network
NAT Network Address Translation
OSPF Open Shortest Path First
PAT Port Address Translation
PPP Point-to-Point Protocol
SSH Secure shell
STP Spanning Tree Protocol
UTP Unshielded Twisted Pair
VLAN Virtual Local Area Network
VPN Virtual Private Network
VTP VLAN Trunking Protocol
WAN Wide Area Network

Table des figures

1.1 Catégories de cables 11
1.2 Câblage horizontal 11
1.3 Fibre monomodes et multimodes 13
1.4 Comparaison monomodes et multimodes 13
1.5 Point d'accès 14

2.1 Architecture LAN 16
2.2 vlan 17
2.3 VTP serveur 17
2.4 VTP client 17
2.5 Configuration du protocole STP 18
2.6 DHCP sur le routeur du siège 19
2.7 DHCP sur le routeur de la filiale 19

3.1 Architecture WAN 20
3.2 Connexion au serveur WEB et DNS 21
3.3 Translations d'adresses 21

4.1 ACL VLAN 2 22
4.2 ACL Internet 23
4.3 SSH activer 23
4.4 ACL accès SSH 23
4.5 Connexion via SSH 24
4.6 Tunnel VPN 25
4.7 ACL du NAT 26
4.8 Ping vers Internet 26
4.9 Ping vers le LAN de Rabat 26

Table des matières

Remerciements **2**

Résumé **3**

Abstract **4**

Introduction générale **9**

1 Câblage du bâtiment et points d'accès **10**
1.1 Câblage horizontale : pair torsadé 10
1.1.1 Etude Comparative 10
1.1.2 Estimation du coût 12
1.2 Câblage vertical : fibre optique 13
1.2.1 Etude Comparative 13
1.3 Points d'accès 14
1.4 Conclusion 15

2 Architecture LAN **16**
2.1 Mise en oeuvre du réseau local 16
2.2 Protocoles 17
2.2.1 VLAN 17
2.2.2 STP 18
2.2.3 DHCP 18
2.3 Conclusion 19

3 Architecture WAN **20**
3.1 Architecture DMZ 21
3.2 PAT 21
3.3 Conclusion 21

4 Sécurité Réseaux **22**
4.1 Acces Control List (ACL) 22
4.2 SSH 23
4.3 Configuration du Tunnel VPN 24
4.4 Conclusion générale 27

Bibliographie/Webographie **28**

Introduction générale

Pour assurer une architecture réseau avec une bonne qualité de service, fiabilité, sécurité et avec un coût minimale nous avons réaliser ce projet dans plusieurs étapes. Notre cas d'étude est une société dans la filiale est situé à Rabat et le siège à Casablanca. Ce dernier est un batiment qui se composent de 4 étages, chaque étage continent huit salles et chaque salle à deux prises RJ45 «au milieu de la salle », la hauteur est de 3 mètre avec une surfae de 16*32 m^2. Ce rapport décrit donc l'essentiel du travail réalisé lors de ce projet. Il comporte quatre chapitres, le premier chapitre concerne le câblage de notre bâtiment et l'estimation globale du prix, le deuxième chapitre concerne l'architecture réseau locale. Quant au troisième chapitre. On va se focaliser sur la partie WAN, finalement le dernier chapitre, le plus important, emportera sur la sécurisation de notre réseau.

Chapitre 1

Câblage du bâtiment et points d'accès

Notre cas d'étude est une société dans la filiale est situé à Rabat et le siège à Casablanca. Ce dernier est un batiment qui se composent de 4 étages, chaque étage continent huit salles et chaque salle à deux prises RJ45 «au milieu de la salle », la hauteur est de 3 mètre avec une surfae de 16*32 m^2.

1.1 Câblage horizontale : pair torsadé

1.1.1 Etude Comparative

Etude Comparative des différentes catégories de cables

- **cat 1 :** applications de téléphonie bande passante 300-3400 hz
- **cat 2 :** applications jusqu'à 1 Mb/s
- **cat 3 :** applications type ethernet 10 Mb/s sur 100 mètres
- **cat 4 :** applications type token-ring 16 Mb/s
- **cat 5 :** applications type ethernet 100 Mb/s sur 100 mètres
- **cat 5e :** applications type ethernet 2,5 Gb/s sur 100 mètres (10 Gb/s sur 30 mètres)
- **cat 6 :** applications type ethernet 5 Gb/s sur 100 mètres (10 Gb/s sur 55 mètres)
- **cat 6a :** applications type ethernet 10 Gb/s sur 100 mètres
- **cat 7 :** applications type ethernet 100 gb/s

Speed	Compatible Cable
10G	CAT6a (100m)
	CAT6 (55m)
	CAT5e (30m)
5G	CAT6 (100m)
	CAT5e (30m)
2.5G	CAT5e (100m)
1G	CAT5e (100m)
100M	CAT5 (100m)

FIGURE 1.1 – Catégories de cables

- Entre les switchs de distributions et les switchs d'accès **l'UTP catégorie 6a** est la mieux adapté et la plus utilisé dans nos jours puisqu'elle a une bonne fréquence, et présente une meilleure économie d'énergie.
- Entre les switchs d'accès et les terminaux **l'UTP catégorie 5** est la mieux adapté puisque elle a moins de débit que l'UTP 6a est garenti un bon débit.

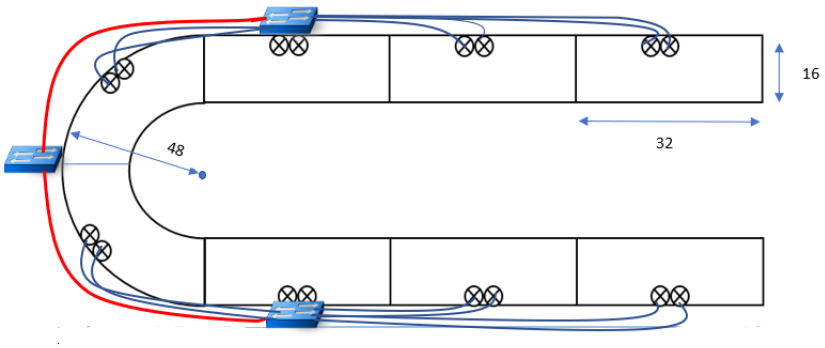


FIGURE 1.2 – Câblage horizontal

On a opté pour une architecture de 3 niveaux :
- Un switch fédérateur qui lie entres les étages du batiment.
- un switch de distribution pour chaque étage.
- Deux switch d'accès pour chaque étage pour lier tout les terminaux.

La figure 1.2 décrit la manière dont nous avont concu le câblage pour chaque étage.

1.1.2 Estimation du coût

La surface de la chambre circulaire est 16m*76m (2*pi*r/4=76m) La surface de la chambre réctangulaire est 16*32 m^2 La longueur du câble par étage à utilsé est donc :

- Du switch de distribution vers les switchs d'accès : 184m
- Du switch d'accès vers les outlets : 604m

Pour tout le bâtiment il faut 184m de câble UTP 6a : **184*6 = 1104 MAD**.
Pour tout le bâtiment il faut 604m de câble UTP 5 : **604*5 = 3020 MAD**.
Le coût total pour le câblage horizontale est : **4124 MAD**

1.2 Câblage vertical : fibre optique

1.2.1 Etude Comparative

Les jarretières optiques sont composées généralement de deux fibres optiques protégées par une gaine et équipées à chaque extrémité d'un connecteur optique. Il existe deux type de fibres optiques : les fibres monomodes et les fibres multimodes.
Fibre monomodes : Les fibres monomodes sont utilisées pour des débits élevées ou pour de longues distances.
Fibre multimodes : les fibres multimodes sont moins chers que les monomodes et sont utilisées sur des distances plus modestes.

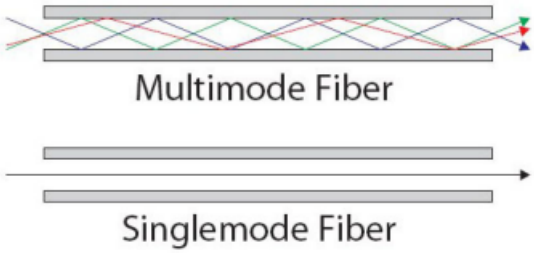


FIGURE 1.3 – Fibre monomodes et multimodes

- La fibre multimode à une bande passante limitée et ne dois pas dépasser des distance de 5Km.
- La fibre monomode à une très grande bande passante et est utilisée pour des distances supérieures à 5Km.
- La fibre multimode à un coeur plus grand par rapport à la fibre monomode.
- Plusieurs longueurs d'onde lumineuse circule dans la fibre multimode tandis qu'une seule onde lumineuse traverse la fibre monomode.

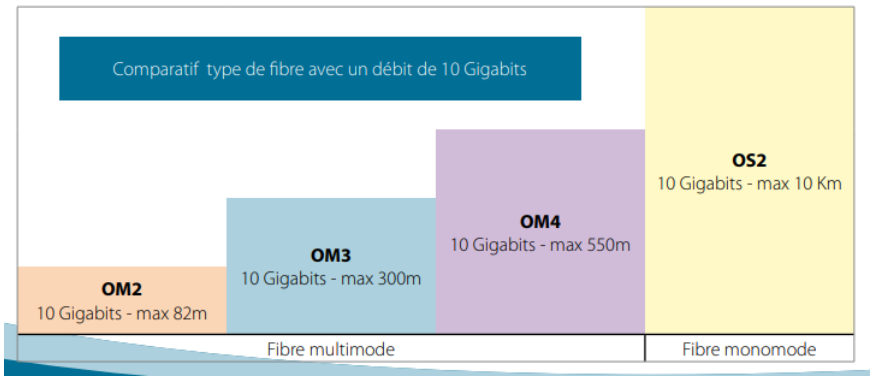
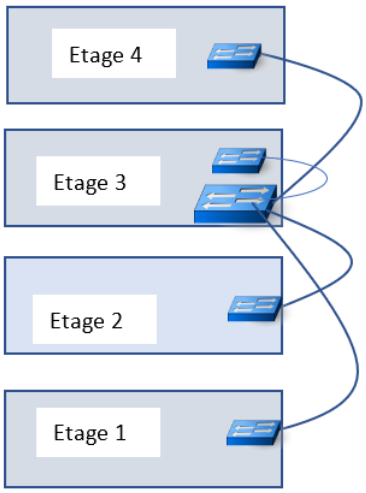


FIGURE 1.4 – Comparaison monomodes et multimodes

On a choisi **la fibre optique multi-mode OM3** car on a un déport moyenne distance utilisé pour les réseaux Gigabits jusqu'à 10Gb/s.

Pour la fibre optique sachant que la hauteur d'un étage est de 3m et le switch fédérateur est positionné dans le 2 ème étage il nous faut : 13m.

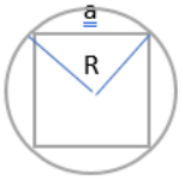
Le coût total pour la fibre optique est : 13*180=2340 MAD



1.3 Points d'accès

Un point d'accès est un dispositif qui permet aux périphériques sans fil de se connecter à un réseau câble ou un réseau internet à l'aide connexion radio.

Les points d'accès utilisés dans la société on un rayon de r = 70m selon la loi de Pythagore $a^2 = r^2+r^2$ Donc a=98.99, on prend a=100.
On aura besoin de 3 points d'accès pour chaque étage positionné selon le schéma suivant :



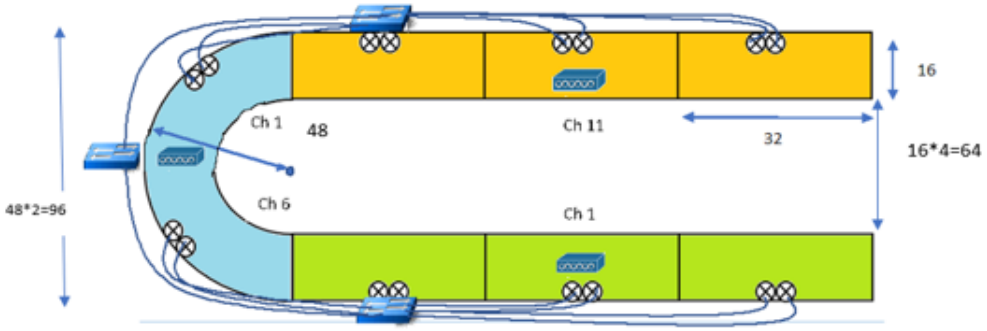


FIGURE 1.5 – Point d'accès

1.4 Conclusion

Les types de câblages les mieux adaptés à notre situation
sont l'UTP catégorie 6a et l'UTP 5 pour le câblage horizontal et la fibre optique multimode OM3 pour le câblage vertical. Pour câbler l'immeuble, nous avons besoins de 13m verticalement, alors que pour câbler les étages d'un immeuble nous avons besoin de 788m avec un prix total de : **6464 MAD**.

Chapitre 2

Architecture LAN

2.1 Mise en oeuvre du réseau local

L'architecture réseau hiérarchique est la plus utilisé de nos jours, ceci est dû à plusieurs avantages parmi lesquels la scalibilité, la redondance, la performance, la sécurité et maintenabilité.
Un modèle de conception hiérarchique est recommandé car il est plus facile à gérer et à développer, et les problèmes sont résolus plus rapidement.

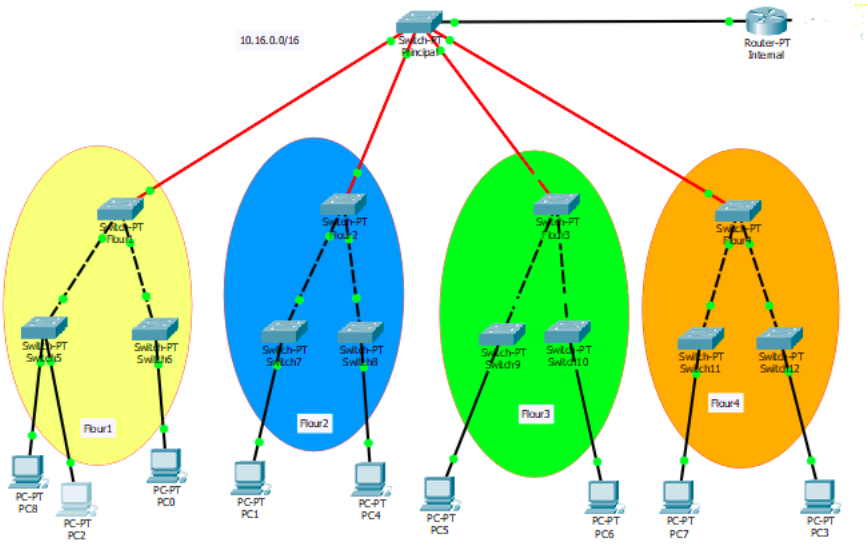


FIGURE 2.1 – Architecture LAN

2.2 Protocoles

2.2.1 VLAN

Le VLAN regroupe, de façon logique et indépendante, un ensemble de machines informatiques. On peut en retrouver plusieurs coexistant simultanément sur un même commutateur réseau. Pour notre cas le batiment du siège est subdiviser en 4 vlans, un VLAN pour chaque étage. Pour administrer et configurer les VLANs nous avons utilisé le protocole VTP il permet d'ajouter, renommer ou supprimer un ou plusieurs vlans sur le seul switch maître et dans un domaine Vtp.

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa1/1, Fa2/1, Fa3/1
116  Vlan-Flour1                      active
216  Vlan-Flour2                      active
316  Vlan-Flour3                      active
416  Vlan-Flour4                      active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

FIGURE 2.2 – vlan

La figure si-dessus représente les VLANs associés aux différents étages.

```
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Server
VTP Domain Name                 : ensias
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x36 0x65 0xA7 0x2A 0x40 0x9B 0x58 0x7C
Configuration last modified by 0.0.0.0 at 3-1-93 00:01:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

FIGURE 2.3 – VTP serveur

```
Flour2#show vtp status
VTP Version                     : 2
Configuration Revision          : 0
Maximum VLANs supported locally : 255
Number of existing VLANs        : 9
VTP Operating Mode              : Client
VTP Domain Name                 : ensias
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x36 0x65 0xA7 0x2A 0x40 0x9B 0x58 0x7C
Configuration last modified by 0.0.0.0 at 3-1-93 00:01:00
```

FIGURE 2.4 – VTP client

Les figures si-dessus représentent la configuration du protocole VTP, le switch fédérateur étant le serveur VTP et les switchs de distributions et d'accès représentent les clients VTP.

2.2.2 STP

Afin d'assurer qu'il n'y a pas de boucles dans un contexte de liaisons redondantes (convergentes) entre des matériels de couche 2 et de les bloquer et les détruire si besoin. Les réseaux doivent avoir un unique chemin entre 2 points. Un bon réseau doit aussi inclure une redondance des matériels pour fournir un chemin alternatif en cas de panne. C'est la STP détecte et désactive des boucles de réseau en fournissant un mécanisme de liens de backup. Il permet de faire en sorte que des matériels compatibles avec le standard ne fournissent qu'un seul chemin entre deux stations d'extrémité.

```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: Vlan-Flour1 Vlan-Flour2 Vlan-Flour3 Vlan-Flour4
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is disabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                    0         0        0          5          5
VLAN0116                    0         0        0          5          5
VLAN0216                    0         0        0          5          5
VLAN0316                    0         0        0          5          5
VLAN0416                    0         0        0          5          5

---------------------- -------- --------- -------- ---------- ----------
5 vlans                     0         0        0         25         25
```

FIGURE 2.5 – Configuration du protocole STP

La figure si-dessus représente la configuration du protocole STP dans le switch fédérateur. Pour avons configurer le protocole STP pour tout les VLANs.

2.2.3 DHCP

Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement sa configuration principalement, sa configuration réseau (adresse IP, passerelle par défaut, adresse serveur DNS).

Nous avons configurer un pool pour chaque réseau notamment pour les Vlans du siège et le LAN de la filiale.

```
ip dhcp excluded-address 10.16.1.1
ip dhcp excluded-address 10.16.2.1
ip dhcp excluded-address 10.16.3.1
ip dhcp excluded-address 10.16.4.1
!
ip dhcp pool Flour1
 network 10.16.1.0 255.255.255.0
 default-router 10.16.1.1
 dns-server 136.0.0.3
ip dhcp pool Flour2
 network 10.16.2.0 255.255.255.0
 default-router 10.16.2.1
 dns-server 136.0.0.3
ip dhcp pool Flour3
 network 10.16.3.0 255.255.255.0
 default-router 10.16.3.1
 dns-server 136.0.0.3
ip dhcp pool Flour4
 network 10.16.4.0 255.255.255.0
 default-router 10.16.4.1
 dns-server 136.0.0.3
```

FIGURE 2.6 – DHCP sur le routeur du siège

La figure si-dessus représente la configuration du protocole DHCP sur le routeur internal du siège.

```
ip dhcp excluded-address 10.16.136.1
!
ip dhcp pool rabat
 network 10.16.136.0 255.255.255.224
 default-router 10.16.136.1
 dns-server 136.0.1.5
```

FIGURE 2.7 – DHCP sur le routeur de la filiale

La figure si-dessus représente la configuration du protocole DHCP sur le routeur de la filiale.

2.3 Conclusion

Dans ce chapitre nous avons présenté l'architecture LAN basée sur un modèle hiérarechique de 3 niveaux en implémentant les trois protocoles VTP, STP et DCHP. Les besoins de l'entreprise exige une interconnection réseau avec le monde extérieur autrement dis Internet ainsi que la filiale situer à Rabat. Dans le chapitre suivant nous allons répondre à ces besoins avec une architecture WAN.

Chapitre 3

Architecture WAN

Ce chapitre décrit l'architecture WAN qui inclut le type de routage utilisé entre le bâtiment de Casablanca «Siège »et Rabat «Filiale », la configuration des serveurs WEB et DNS et finalement la translation des adresses via le NAT.

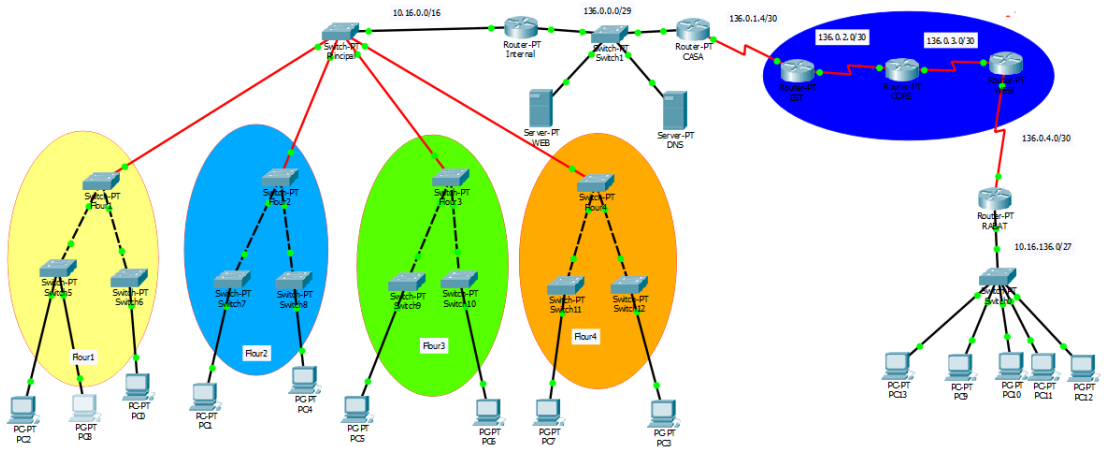


FIGURE 3.1 – Architecture WAN

Nous avons considéré internet comme étant trois routeur [EST, CORE et WEST] liés par des lignes séries et configurés avec le protocole OSPF.
Nous avons configuré le protocole PPP dans les lignes séries avec l'option CHAP entre les Routeurs Casa et EST, Rabat et WEST puisqu'elle représente une forte authentification.

3.1 Architecture DMZ

Une zone démilitarisée ou DMZ est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.
On a rajouté deux serveurs : DNS et WEB relié par un switch qui se place entre les deux routeurs de Casablanca et Internal.

FIGURE 3.2 – Connexion au serveur WEB et DNS

3.2 PAT

Le PAT est la technique basée sur le NAT dynamique. Il Effectue une translation des ports IP entre un réseau interne privé ou intranet et une Adresse IP sur internet. Tout simplement Le PAT est un Nat dynamique + une translation d'adresse basée sur les Ports. Nous avons utilsé le PAT sur les routeurs Internal et Rabat.

```
internal#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 136.0.0.1:1024    10.16.3.2:1        136.0.4.2:1        136.0.4.2:1024
icmp 136.0.0.1:1025    10.16.1.3:1        136.0.4.2:1        136.0.4.2:1025
icmp 136.0.0.1:1       10.16.4.3:1        136.0.3.2:1        136.0.3.2:1
icmp 136.0.0.1:2       10.16.4.3:2        136.0.2.1:2        136.0.2.1:2
```

FIGURE 3.3 – Translations d'adresses

3.3 Conclusion

Nous avons utilisé le PAT pour traduire l'adresse réseau privée en réseau public pour permettre au LAN de sortir à l'internet, nous avons configurer un serveur WEB et un serveur DNS sur une DMZ et nous avons configurer le protocole PPP avec CHAP sur les lignes séries.
Dans le chapitre suivant nous allons introduire quelques aspects de sécurité.

Chapitre 4

Sécurité Réseaux

Ce chapitre décrit les techniques employées pour garantir une bonne sécurité de notre architecture réseau.

4.1 Acces Control List (ACL)

Pour limiter l'accès à internet pour le VLAN-flour2 on a utilisé l'Access liste suivante :

```
ip access-list extended VLAN2
 permit ip any 10.16.0.0 0.0.7.255
 permit tcp any host 136.0.0.4 eq www
 permit tcp any host 136.0.0.4 eq 443
 permit tcp any host 136.0.0.3 eq domain
 permit udp any host 136.0.0.3 eq domain
```

FIGURE 4.1 – ACL VLAN 2

La figure si-dessus représente l'ACL utilsé pour interdire le VLAN 2 d'accéder à internet, la première ligne pour autoriser la communication entre les VLANs et le reste pour autoriser le VLAN 2 d'accèder au DMZ.

Pour autorisez l'accès depuis Internet vers la DMZ juste pour les services DNS et WEB nous avons utilisé l'ACL suivante :

```
casa#show access-lists
Extended IP access list ACL_INTERNET
    10 permit tcp any host 136.0.0.4 eq www (5 match(es))
    20 permit tcp any host 136.0.0.4 eq 443
    30 permit tcp any host 136.0.0.3 eq domain
    40 permit udp any host 136.0.0.3 eq domain (1 match(es))
    50 permit tcp any any established
```

FIGURE 4.2 – ACL Internet

Les trois première ligne autorise l'accès depuis internet vers la DMZ pour les services DNS et WEB, alors que la dernière ligne autorise l'accès si seulement si la connexion est déjà établie depuis le LAN.

4.2 SSH

Secure Shell (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés. Il devient donc impossible d'utiliser un sniffer pour voir ce que fait l'utilisateur. Pour notre cas nous avons limité l'accès ssh pour les switchs et les routeurs Internal, Casa et Rabat. Seule l'administrateur pourra y accéder à distance.

```
casa#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

FIGURE 4.3 – SSH activer

Voici l'ACL utilisé pour autoriser l'accès juste pour l'administrateur :

```
switch-core(config)#access-list 23 permit 10.16.4.2
switch-core(config)#line vty 0 4
switch-core(config-line)#ac
switch-core(config-line)#access-class 23 in
switch-core(config-line)#exit
```

FIGURE 4.4 – ACL accès SSH

La figure si-dessous montre une connexion à distance via SSH depuis la machine de l'administrateur :

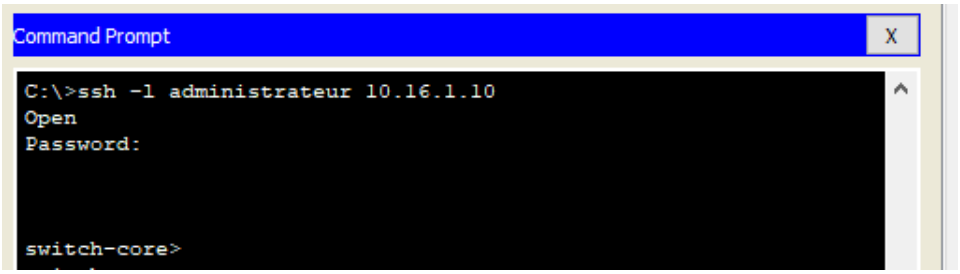


FIGURE 4.5 – Connexion via SSH

4.3 Configuration du Tunnel VPN

Un VPN (Virtual Private Network) est un réseau virtuel s'appuyant sur un autre réseau comme Internet. Il permet de faire transiter des informations, entre les différents membres de ce VPN, le tout de manière sécurisée.
On peut considérer qu'une connexion VPN revient à se connecter en réseau local mais en utilisant Internet. On peut ainsi communiquer avec les machines de ce réseau en prenant comme adresse de destination, l'adresse IP local de la machine que l'on veut atteindre.
Il existe plusieurs types de VPN fonctionnant sur différentes couches réseau, mais on a choisi IPSEC tunnel vu puisqu'il est plus efficace que les autres types en termes de performance, car contre il est très contraignant au niveau de la mise en place.

Pour vérifier que le VPN fonctionne sur nos routeurs de Casa et Rabat, on vérifie les informations retournées par la commande suivante :

```
casa#sh crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: VPNMAP, local addr 136.0.1.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.16.0.0/255.255.248.0/0/0)
   remote  ident (addr/mask/prot/port): (10.16.136.0/255.255.255.224/0/0)
   current_peer 136.0.4.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 0
   #pkts decaps: 4, #pkts decrypt: 4, #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.: 136.0.1.5, remote crypto endpt.:136.0.4.2
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x13E3484F(333662287)

     inbound esp sas:
      spi: 0x6B4F4EA7(1800359591)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2007, flow_id: FPGA:1, crypto map: VPNMAP
        sa timing: remaining key lifetime (k/sec): (4525504/3485)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x13E3484F(333662287)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2008, flow_id: FPGA:1, crypto map: VPNMAP
        sa timing: remaining key lifetime (k/sec): (4525504/3485)
```

FIGURE 4.6 – Tunnel VPN

Nous éditons l'ACL du NAT déjà existante qui s'appelle LAN pour interdire la translation d'adresse vers le LAN distant. De cette façon aucune adresse IP source à destination de RABAT ne sera changée. Néanmoins si la destination est autre que RABAT, les adresses IP sources seront translatées.

```
Extended IP access list LAN
    10 deny ip 10.16.0.0 0.0.7.255 10.16.136.0 0.0.0.31 (13
match(es))
    20 permit ip 10.16.0.0 0.0.7.255 any (6 match(es))
```

FIGURE 4.7 – ACL du NAT

Translation d'adresse vers un LAN distant :

```
Router(config)#do show ip nat translation
Pro  Inside global     Inside local       Outside local
Outside global
icmp 136.0.0.1:5       10.16.1.4:5        136.0.2.2:5
136.0.2.2:5
icmp 136.0.0.1:6       10.16.1.4:6        136.0.4.2:6
136.0.4.2:6
```

FIGURE 4.8 – Ping vers Internet

Translation d'adresse vers le LAN de Rabat :

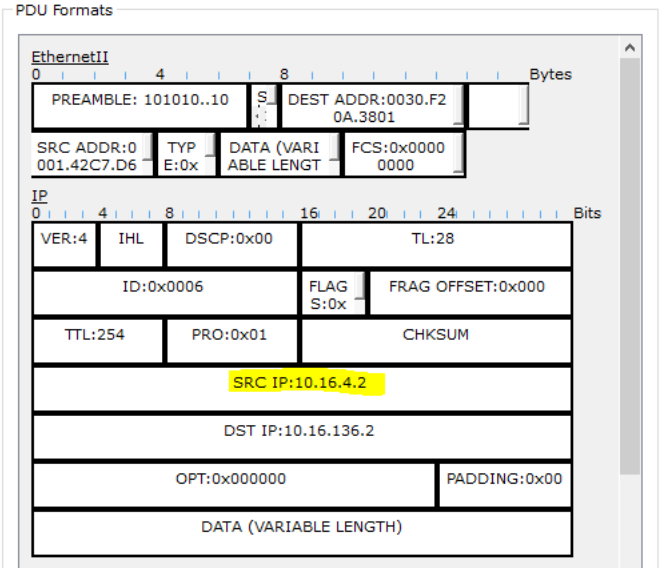


FIGURE 4.9 – Ping vers le LAN de Rabat

4.4 Conclusion générale

Ce projet avait pour but majeur la solidification et la mise en pratique de l'ensemble des compétences théoriques et techniques acquises durant la deuxième année filière IWIM. Il consistait à concevoir une architecture réseau complète d'un bâtiment d'une entreprise qui se compose de quatres étages dont chacun comporte huit salles. Tout d'abord nous avons commencer par identifié les besoins de notre architecture en terme d'équipements et de câblages ce qui nous a mener a faire une étude comparative des différents type de câbles non seulement en terme de performances mes aussi en terme de coût. L'architecture finalement choisis est une architecture hiérarechique de trois niveaux en utilisant pour le câblage vertical la fibre optique multimode OM3 et pour le câblage horizontal une pair torsadé catégorie UTP 6a et UTP 5.
Nous avons mis en oeuvre l'architecture LAN on créant un VLAN pour chacun des quatres étages on utilisant le protocole VTP, pour éliminer les boucles nous avons utilisé le protocole STP et finalement pour distribuer automatiquement la configuration de base à savoir l'adresse IP, le DNS et la passerelle nous avons utilisé le protocole DHCP.
On ce qui concerne l'architecture WAN nous avons commencer par configurer la DMZ qui contient un serveur WEB et DNS, nous avons considéré l'internet comme étant 3 routeur avec comme routage dynamique OSPF.On a configuré le PAT pour sortir via internet à l'aide d'une adresse publique.
Pour sécurisé notre réseau d'abord on utilisant une authentification avec CHAP entre les routeurs d'extrémités et internet, puis nous avons rajouter des ACL pour assurer l'identification et on a renforcé la sécurité en utilisant le VPN basé sur le cryptage AES et l'authentification SHA2, finalement pour autoriser l'administrateur de gérer à distance et de manière sécurisé les équipements réseaux nous avons utilisé le protocole SSH.
Ce projet nous a permis de se familiariser premièrement avec les différents concepts de câblages, ainsi que les différents protocoles de commutations et de routages, nous avons aussi pu s'enrichir encore plus dans le cryptage et l'authentification pour renforcer la sécurité de notre architecture réseau.

Bibliographie/Webographie

- **Cours :**
  [1] Mohammed EL KOUTBI, Technique de routages, 2016.
  [2] Mohammed EL KOUTBI, Technique de commutation, 2016.
  [3] Mostafa BELKASMI, Cryptographie, 2018.

- **Références :**
  [w1] Configuration NAT https ://www.ciscomadesimple.be/
  [w2] Définition des protocoles disponible http ://www.infonitec.com/
  [w3] Configuration VPN https ://ciscotracer.wordpress.com/2017/03/22/vpn-site-site/