Rapport du projet intégré S4

Sujet

« Implémentation et design du réseau IP »

Préparé par :

-JABBARI Youssef

Sous la direction de :

- M. Mohammed EL KOUTBI
- M. Mostafa BELKASMI

Année Universitaire 2017-2018

INTRODUCTION

Le sujet qui m'a été affecté était la réalisation d'un design et implémentation d'un réseau IP d'un bâtiment qui se compose de 3 étages, dont chacun se constitue de 8 salles. Chaque salle dispose de 2 prises RJ45 et est de 72m de longueur et de 36m de largeur.
Pour ce faire, on va commencer tout d'abord par définir le câblage de la société en choisissant le type de câble le plus convenable à mon étude de cas, on calcule également une estimation globale du prix du câble ainsi que des Switchs et routeurs qu'on va exploiter dans notre architecture. Puis, on va présenter l'architecture LAN et WAN de notre projet. En définitive, on va aborder la sécurité de notre réseau.

Sommaire

CHAPITRE 1 : Câblage du bâtiment

-Etude comparative de câblage :

a. Paire torsadée

Il existe plusieurs types des paires torsadées :
- **Paire torsadée non blindée (UTP ou U/UTP)**
- **Paire torsadée écrantée (FTP ou F/UTP)**
- **Paire torsadée blindée (STP ou U/FTP)**
- **Paire torsadée doublement écrantée (FFTP ou F/FTP)**
- **Paire torsadée doublement blindée (SSTP ou S/FTP)**

➔L'UTP catégorie 5 est la mieux adaptée et la plus utilisée de nos jours puisqu'elle a une bonne fréquence, et présente une meilleure économie d'énergie.

b. Fibre optique

Il existe différents types de câble optique, divisé essentiellement en deux genres:
- **Les câbles à structure serrée (Monomode)**
- **Les câbles à structure libre (Multimode)**

➔On a choisi la fibre optique multimode car on a un déport moyenne distance utilisé pour les réseaux Gigabits jusqu'à 10Gb/s.

-Câblage du bâtiment :

a. Câblage horizontal

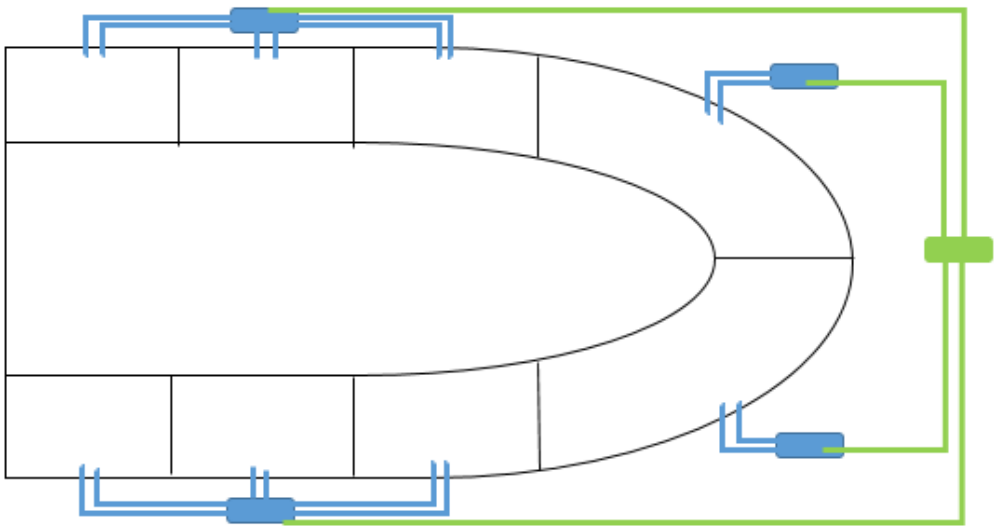


Figure 1: cablage horizontal

La longueur du câble par étage à utiliser est donc :
- UTP : [(**72*4) + (2*4)] * 2 = 592m**
-Fibre : **[(85 + (170 + 72 + 36)] * 2 = 726m**

Donc pour tout le bâtiment il me faudra :
- UTP : **592*3 = 1776m**
-Fibre : **726*3 = 2178m**

Le cout donc pour ce câblage est :
- UTP : **1776 *5,5 = 9768DH**
-Fibre : **2178*180 = 392 040DH**

b. Câblage verticale

On a 3 étages et on suppose que le switch fédérateur va être déposé au deuxième étage

Le câblage se fera avec de la fibre optique.

Il me faut pour le câblage vertical : **1 + (3*2) = 7m**
Le cout du câblage est donc : **7*180 = 1260DH**

Chapitre 2 : Architecture LAN

- Etude comparative des Switches/Routeurs

a. Etude comparative des switches

Il existe trois types de switchs :
- **Switch non administrative :** un switch non-administrable est un switch qu''il n'est pas possible de configurer, toute la programmation étant déjà intégrée,
- **Switch intelligent :** Il constitue le compromis entre un switch administrable et un modèle non-administrable.
- **Switch administrative** : proposent toutes les options que l'on peut actuellement proposer à un ingénieur réseau.

Le Switch **Cisco Catalyst 2960S** est le mieux adapté notre situation comme switch d'accès.
Le Switch **TP Link TL-SG5412F** sera choisi comme switch fédérateur et distributeur.

b. Etude comparative des routeurs

Il existe différent routeurs, ayant chacun ses propres caractéristiques.
On a choisi **Cisco CISCO888GW-GN-E-K9** comme routeur vu sa performance, ses caractéristiques qui s'adaptent à tous les protocoles et son prix adéquat.

c. Estimation globale de l'architecture réseau

Puisque on a besoin de douze switchs d'accès, donc le prix total des switchs est :
23 500*12 = 282000DH
On ajoute un switch principal et 3 distributeurs :
282 000+ 29 000*4 = 398 000*DH*
Puisque on a besoin de deux routeurs, donc le prix sera alors :

398 000 + 2 * 12 586.75 = 423 173.5
En se référant au chapitre précédant pour ajouter le prix du câblage, le cout global de cette architecture est de : **452 173.5 .5 + 9768 + 392 040 + 1260 = 826 241.5 *DH***

- Implémentation du wifi

Pour un implémenter un réseau wifi, il faut d'abord fixer le nombre de points d'accès.
On applique la formule de Pythagore pour déterminer le rayon du cercle et on prend la valeur entière de X.

On aura 7 points d'accès.

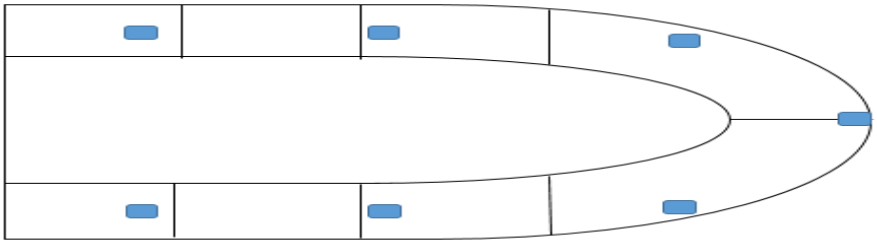


Figure 2: emplacement des points d'accès

-Architecture LAN

Mise en oeuvre du réseau local

La figure ci-dessous représente l'architecture LAN (sous paquet tracer) de notre bâtiment qui est composé de 4 étages, et pour la valeur de X étant égal à 36.

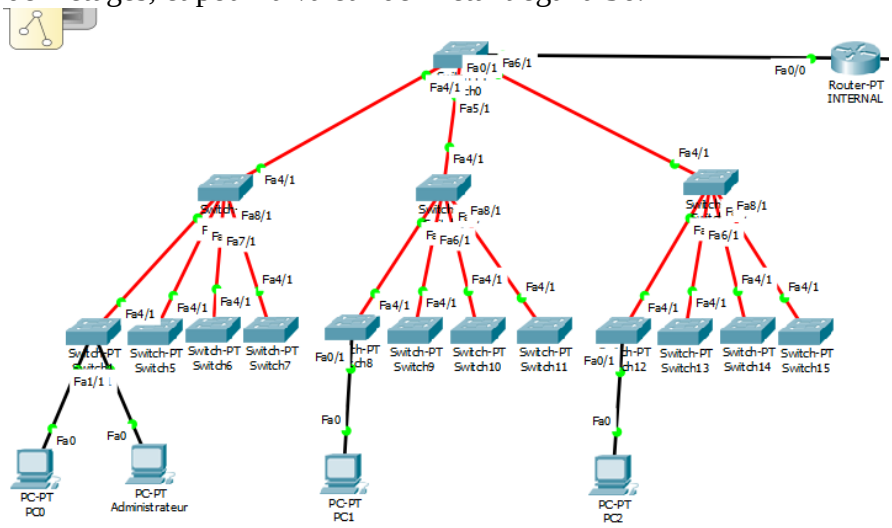


Figure 3:architecture LAN

Routage Inter-Vlan

Le switch fédérateur est configuré comme VTP server et considéré comme étant la racine primaire de tous les VLANS, alors que les autres switchs sont des VTP clients.

```
FEDERATEUR#show vtp status
VTP Version                     : 2
Configuration Revision          : 3
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Server
VTP Domain Name                 : ensias
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x03 0xD0 0x31 0x83 0x28 0x8B
0x47 0xCD
Configuration last modified by 0.0.0.0 at 3-1-93 00:04:02
Local updater ID is 10.36.1.50 on interface Vl136 (lowest
numbered VLAN interface found)
```

```
Switch#show vtp status
VTP Version                     : 2
Configuration Revision          : 3
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
VTP Operating Mode              : Client
VTP Domain Name                 : ensias
VTP Pruning Mode                : Disabled
VTP V2 Mode                     : Disabled
VTP Traps Generation            : Disabled
MD5 digest                      : 0x03 0xD0 0x31 0x83 0x28 0x8B
0x47 0xCD
Configuration last modified by 0.0.0.0 at 3-1-93 00:04:02
```

Mise en Place des Vlans

Dans notre cas, on a configuré le routage inter-vlan entre le routeur Internal et les différents switchs de chaque étage. On a donc eu recours à 3 Vlans :

- Vlan 136
- Vlan 236
- Vlan 336

```
VLAN Name                              Status    Ports
---- --------------------------------- ---------
--------------------------------
1    default                           active    Fa2/1, Fa3/1,
Fa5/1
136  vlan-flour1                       active    Fa0/1, Fa1/1
236  vlan-flour2                       active
336  vlan-flour3                       active
```

Attribution des ports aux VLANs :

```
interface FastEthernet0/1
 switchport access vlan 136
 switchport mode access
```

Pour configurer le routage inter-VLAN on a :

-Configurer un port multi-VLAN sur le switch à l'aide de la commande switchport mode trunk

-Créer autant de sous-interfaces que de VLANs sur le routeur :

```
interface FastEthernet0/0.1
 encapsulation dot1Q 136
 ip address 10.36.1.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.2
 encapsulation dot1Q 236
 ip address 10.36.2.1 255.255.255.0
 ip access-group VLAN2 in
 ip nat inside
!
interface FastEthernet0/0.3
 encapsulation dot1Q 336
 ip address 10.36.3.1 255.255.255.0
 ip nat inside
```

Mise en place de l'OSPF

Dans notre cas, la mise en place du routage OSPF a été mise en place dans le câblage constituant la zone Internet, soit entre les différents routeurs : EST, CORE et WEST.

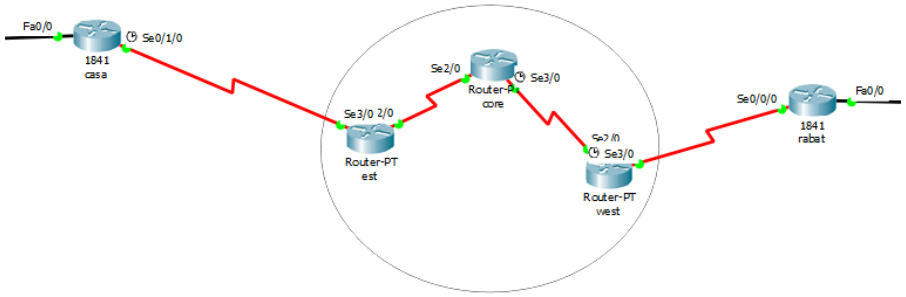


Figure 4: zone internet

Pour configurer le routage OSPF, on a eu recours à la commande suivante :
routageospf 1
network @adresse_reseau @wildcard area 0 .

Pour vérifier le fonctionnement du protocole OSPF, utilisons la commande show ip ospf. Cette commande permet d'afficher les informations concernant le routage OSPF.

```
core#show ip ospf
 Routing Process "ospf 1" with ID 156.0.3.1
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 2
        Area has no authentication
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 3. Checksum Sum 0x01d59b
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Chapitre 3: Architecture WAN

-Configuration DNS et WEB

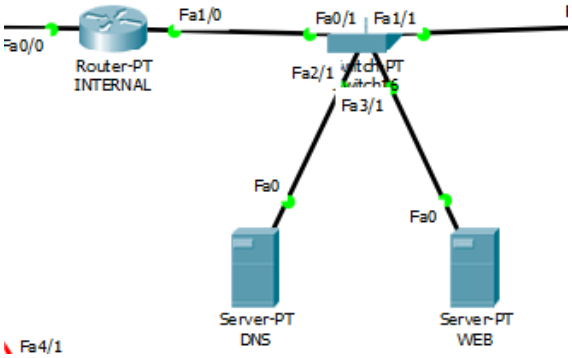


Figure 5: DNS et WEB

On a pris deux serveurs, et on a configuré l'un d'entre eux comme serveur DNS et ceci en lui affectant l'adresse 156.0.0.3 255.255.255.248, et l'autre comme serveur WEB en lui affectant l'adresse suivante 156.0.0.4 255.255.255.248 .

Pour vérifier si le serveur web fonctionne on a accéder au Web Browser depuis un PC du réseau de l'entreprise et la page ci-dessous s'affichera.

Figure 6: web browser

- Configuration du NAT :

Tout d'abord on va utiliser la commande **ipnatinside** pour spécifier l'interface interne et la commande **ipnatoutside** pour spécifier l'interface externe.

Ensuite on a définit une liste d'accès standard (ACL) autorisant les adresses qui doivent être traduites comme suit :

```
access-list 1 permit 10.36.0.0 0.0.255.255
```

Il ne reste plus qu'à configurer le NAT.

```
ip nat inside source list NAT_SSH interface FastEthernet1/0
overload
```

[ACL du NAT modifiée pour le protocole SSH]

- Configuration du DHCP

```
ip dhcp pool VLAN1
 network 10.36.1.0 255.255.255.0
 default-router 10.36.1.1
 dns-server 156.0.0.3
ip dhcp pool VLAN2
 network 10.36.2.0 255.255.255.0
 default-router 10.36.2.1
 dns-server 156.0.0.3
ip dhcp pool VLAN3
 network 10.36.3.0 255.255.255.0
 default-router 10.36.3.1
 dns-server 156.0.0.3
```

Chapitre 4 : Sécurité des réseaux

- Configuration des ACLs

Une ACL sur un routeur filtrant, est une liste d'adresses ou de ports autorisés ou interdits par le dispositif de filtrage.

ACL 1: Interdire le VLAN2 de tout accès vers Internet.

```
ip access-list extended VLAN2
 permit ip 10.36.0.0 0.0.255.255 10.36.0.0 0.0.255.255
```

La figure ci-dessous montre le refus d'accès à internet d'un ordinateur qui appartient au deuxième étage.

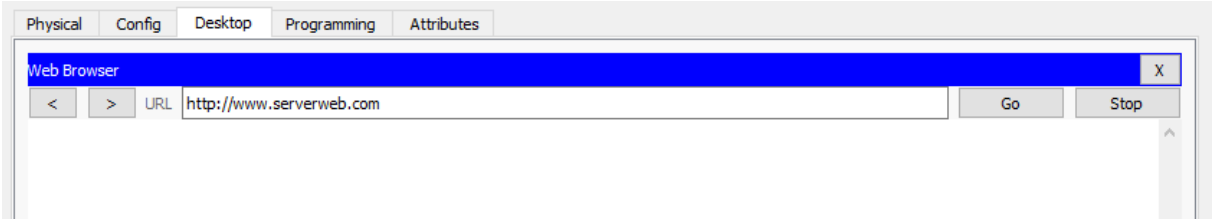


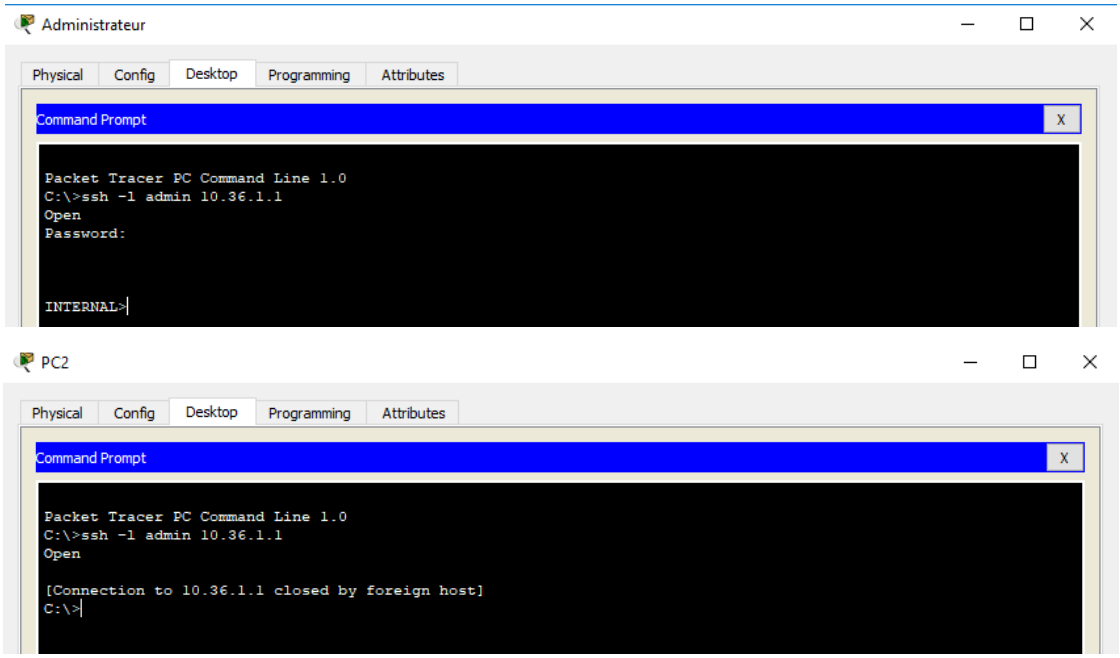
Figure 7: refus d'acces a internet

ACL 2 : Autoriser l'accès depuis Internet vers la DMZ juste pour les services DNS et WEB.

Ceci a été réalisé grâce aux commandes suivantes :

```
access-list 101 permit tcp any host 151.0.0.4 eq www
access-list 101 permit tcp any host 151.0.0.4 eq 443
access-list 101 permit tcp any host 151.0.0.3 eq www
access-list 101 permit udp any host 151.0.0.3 eq domain
```

ACL 3 : Limiter l'accès ssh aux Switchs et aux routeurs Internal, Casa.



- Configuration du tunnel VPN

Les VPN ont deux applications principales : la connectivité site-à-site et la connectivité à accès distant.

L'architecture globale du WAN est comme suit :

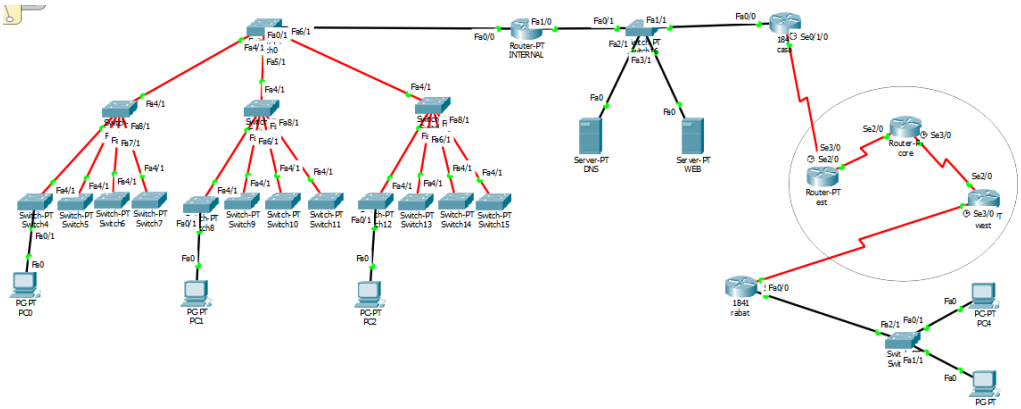


Figure 8: architecture WAN

On va commencer par la configuration du tunnel VPN entre CASA et RABAT en suivant les étapes suivantes :
On va s'occuper des stratégies de chiffrement avec ISAKMP (Internet Security Association and Key Management Protocol). Cette appliance fournie la sécurisation des paquets qui seront acheminés d'un bout à l'autre.
#crypto isakmp policy 10
#encryption aes
#authentication pre-share
#group 5
On précise ensuite la clé d'échange qui sera KEYVPN ainsi que la destination de l'hôte distant
#crypto isakmp key KEYVPN address 156.0.4.2
Ensuite on sélectionne la méthode de cryptage que l'on appelle CRYPSET
#crypto ipsec transform-set CRYPSET esp-aes esp-sha-hmac
ESP-AES est l'algorithme de cryptage et esp-sha-hmac est la méthode d'authentification. Il reste ensuite la configuration des ACLS.
Finalement, pour vérification on utilise la commande : sh crypto ipsec sa

```
interface: Serial0/1/0
    Crypto map tag: VPNMAP, local addr 156.0.1.5

   protected vrf: (none)
   local  ident (addr/mask/prot/port):
(10.36.0.0/255.255.0.0/0/0)
   remote  ident (addr/mask/prot/port):
(10.36.156.0/255.255.255.224/0/0)
   current_peer 156.0.4.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 0
   #pkts decaps: 1, #pkts decrypt: 1, #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.: 156.0.1.5, remote crypto endpt.:
156.0.4.2
```

Conclusion

On était amenés à réaliser une architecture réseau d'une société qui se compose de 3 étages, chacun contient 8 salles.
Dans un premier lieu, nous avons décidé le type de câblage convenable pour notre architecture, puis nous avons établi l'architecture LAN de notre projet tout en configurant les VLANS, le routage inter-vlan, calcul d'une estimation du cout global. Pour l'architecture WAN, on a configuré DNS et WEB afin d'accéder à internet. On a adapté le routage OSPF pour 5 routeurs. Ensuite, nous avons configuré le protocole NAT ainsi que la mise en place du serveur DHCP qui a pour but de générer des adresses ip automatiquement. Dans un dernier lieu, on a sécurisé notre architecture tout en appliquant des access-liste afin d'assurer l'authentification et nous avons renforcé notre sécurité par VPN en utilisant la cryptographie.
Ce projet nous a permis d'enrichir nos connaissances en tout ce qui est câblage, protocole que ce soit de commutation ou de routage, ainsi que d'avoir une idée sur la sécurité des réseaux.