Compte rendu du Projet 2 - BTS SIO SISR : Evolution de l'infrastructure réseau de TiersLieux86

1.Objectif général

L'entreprise TiersLieux86, basée à Chasseneuil, souhaite améliorer la robustesse et la performance de son infrastructure réseau. Cette évolution intervient suite à une première phase où un client externe (ValorElec) avait été intégré. Le projet vise à ajouter la tolérance aux pannes, la supervision centralisée, le routage inter-VLAN et la sécurité du réseau via des ACL.

2. Matériel utilisé :

- Un switch manageable Cisco (2960)
- Un routeur Cisco (1941)
- Des PC clients sous Windows
- Une machine virtuelle Debian 12 (serveur Web dans la DMZ)

3. Topologie physique

- 1 routeur principal (routChass)
- 2 routeurs en redondance (HSRP)
- 1 switch central (Multiplayer Switch)
- 5 switches d'étage/bâtiment
- Des serveurs (Web, DNS, Syslog, TFTP, NTP)
- Des clients internes + 1 PC internaute
- 5 Access Points

4. Plan d'adressage IP

Les VLANs ont été définis comme suit :

VLAN	Nom	Réseau	Passerelle
10	Administration	192.168.10.0/24	192.168.10.1
20	DMZ	192.168.20.0/24	192.168.20.1

30	Wifi visiteurs	192.168.30.0/24	192.168.30.1
40	ValorElec	192.168.40.0/24	192.168.40.1
50	Esporting	192.168.50.0/24	192.168.50.1
60	Accès Public Filaire	192.168.60.0/24	192.168.60.1
70	Administration réseau	192.168.70.0/24	192.168.70.1
Ext	Internet/NAT	62.244.71.0/24	62.244.71.201

5. Services déployés

- **NTP** : Synchronisation de tous les équipements au serveur NTP
- **TFTP** : Sauvegarde centralisée des configurations
- **Syslog** : Centralisation des logs
- **DNS** : résolution interne (ex : www.monsite.local)
- **Web** : site interne et public via NAT

5.1 – Serveur Web Apache2 dans la DMZ

- Installation d'un serveur Web Apache2 sur une machine virtuelle Debian 12.
- Configuration d'une IP statique sur la VM : 192.168.30.100.
- Positionnement de la VM dans le VLAN 30 (DMZ) via le port Fa0/2 du switch.
- Routage inter-VLAN activé sur le routeur pour permettre la communication entre VLAN 30 (DMZ) et VLAN 60 (poste client).

6. Routage inter-VLAN

Configuré via sous-interfaces sur le routeur routChass (dot1Q).

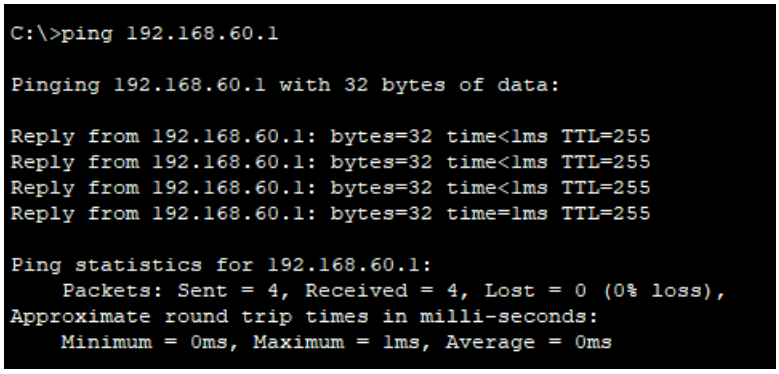
7. Sécurité et supervision

- **ACL** : blocage des accès entre VLAN 10 et VLAN 20

- **Port security** : activé sur les ports d'accès
- **RSTP** : protocole spanning-tree rapide
- **HSRP** : redondance des routeurs
- **EtherChannel** : agrégation de liens

8. Tests effectués

Test 1 – Ping vers la passerelle du VLAN 60
Objectif : Vérifier que le poste client (X1) peut joindre la passerelle de son VLAN.
Depuis : Laptop X1
Vers : Routeur RoutChass (interface Fa0/0.60)
Commande : ping 192.168.60.1



Conclusion : Le routage inter-VLAN est opérationnel pour le VLAN 60.

Test 2 – Ping vers le serveur Web dans la DMZ
Objectif : Vérifier que le poste client peut communiquer avec le serveur hébergé dans la DMZ.
Depuis : Laptop X1
Vers : SrvWebDMZ
Commande : ping 192.168.30.100

```
C:\>ping 192.168.30.100

Pinging 192.168.30.100 with 32 bytes of data:

Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127
Reply from 192.168.30.100: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.30.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

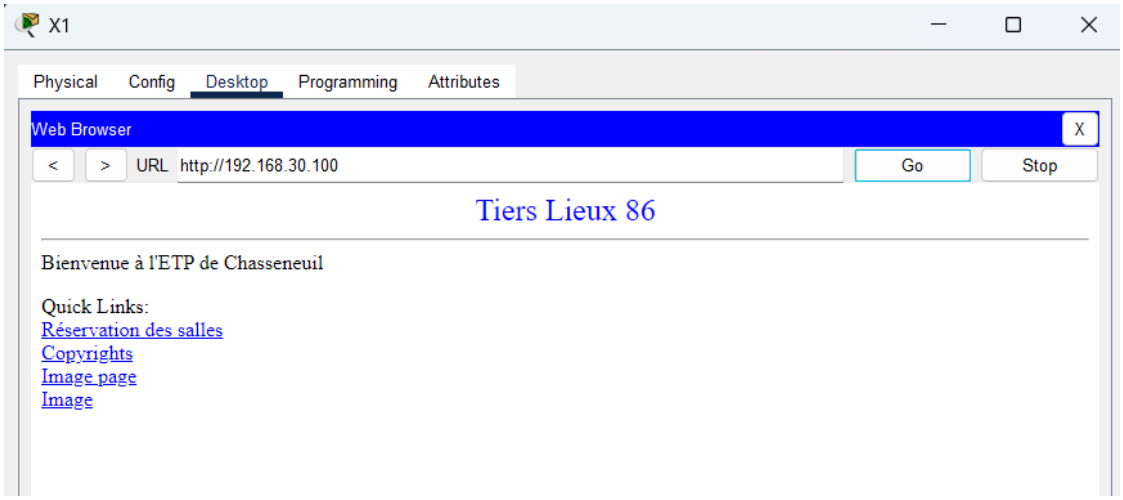
Conclusion : La connectivité entre le VLAN 60 et la DMZ est fonctionnelle.

Test 3 – Accès HTTP au site simulé de l'ETP

Objectif : Vérifier l'accessibilité du serveur web hébergé dans la DMZ via HTTP.

Depuis : Laptop X1

URL testée : http://192.168.30.100



Conclusion : Le service HTTP est opérationnel sur le serveur Web de la DMZ.

Test 4 – Ping vers le serveur DHCP (réseau interne)

Objectif : Vérifier que le poste X1 ne peut pas atteindre le serveur du réseau interne en raison des règles ACL.

Depuis : Laptop X1

Vers : SrvIntraDHCP

Commande : ping 192.168.10.1

```
C:\>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Conclusion : L'ACL appliquée au niveau du routeur empêche l'accès au VLAN 10 depuis le VLAN 60.

Test 5 – Blocage d'accès au VLAN 10 depuis le VLAN 60

Objectif : Vérifier que le poste client ne peut pas accéder au serveur DNS situé dans le VLAN 10, conformément aux règles de sécurité.
Depuis : Laptop X1 (VLAN 60)
Vers : SrvDNS (IP : 192.168.10.11, VLAN 10)
Commande :ping 192.168.10.11

```
C:\>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:

Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.
Reply from 192.168.60.1: Destination host unreachable.

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Conclusion : L'ACL appliquée sur le routeur bloque bien les communications du VLAN 60 vers le VLAN 10. La politique de sécurité est respectée et le filtrage inter-VLAN est fonctionnel.

Test 6 – Vérification de l'adresse MAC du Laptop X1 dans la table du switch

Objectif : Vérifier que le switch connecté au Laptop X1 via l'Access Point apprend correctement son adresse MAC.

Depuis : Switch Switch_Etage
Commande :show mac address-table

```
Switch_Etage>show mac address-table
          Mac Address Table
-------------------------------------------

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

   1    000a.416a.3d01    DYNAMIC     Gig0/1
   1    000a.f37b.d208    DYNAMIC     Gig0/1
  10    000a.416a.3d01    DYNAMIC     Gig0/1
  20    000a.416a.3d01    DYNAMIC     Gig0/1
  30    000a.416a.3d01    DYNAMIC     Gig0/1
  40    000a.416a.3d01    DYNAMIC     Gig0/1
  50    000a.416a.3d01    DYNAMIC     Gig0/1
  60    000a.416a.3d01    DYNAMIC     Gig0/1
  99    000a.416a.3d01    DYNAMIC     Gig0/1
```

Conclusion : L'adresse MAC du Laptop X1 apparaît bien dans la table du switch sur le port Gig0/1, associé au VLAN 60. Cela valide que la communication Wi-Fi du client est bien relayée au niveau de la couche 2 par le switch.

9. Vérifications de configuration

Des commandes de vérification ont été utilisées pour confirmer la bonne configuration des interfaces, des VLANs et des trunks sur les équipements réseau.

Commande – show ip interface brief (Routeur RoutChass)

Objectif : Vérifier que toutes les interfaces VLAN du routeur sont actives et correctement configurées.

Commande utilisée :

show ip interface brief

```
routChass#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.2.254   YES manual up                    up
FastEthernet0/0.60     192.168.60.1    YES manual up                    up
FastEthernet1/0        unassigned      YES manual up                    up
FastEthernet1/0.10     192.168.10.1    YES manual up                    up
FastEthernet1/0.20     172.16.2.254    YES manual up                    up
FastEthernet1/0.30     192.168.30.1    YES manual up                    up
FastEthernet1/0.99     192.168.99.1    YES manual up                    up
FastEthernet2/0        193.252.148.1   YES manual up                    up
```

Résultat attendu :
Les sous-interfaces du routeur (Fa0/0.10, Fa0/0.20, ..., Fa0/0.70) doivent toutes apparaître "up/up" et posséder les adresses IP des passerelles définies dans le plan d'adressage pour chaque VLAN.

Commande – show vlan brief (SwitchIntra et SwitchDMZ)

Objectif : Vérifier la création des VLANs et l'affectation correcte des ports en mode access.

Switch Intra :

```
Switch_Intra#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                 Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                 Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                 Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                 Fa0/22, Fa0/23, Gig0/2
10   ValorElec                         active    Fa0/24
20   Esporting                         active
30   Visiteurs_WIFI                    active
40   Visiteurs_FIL                     active
50   AdminBureaux                      active
60   DMZ                               active
99   AdminReseau                       active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Switch DMZ :

```
Switch_DMZ#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                 Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                 Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                 Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                 Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                 Gig0/1, Gig0/2
10   VLAN0010                          active    Fa0/4
20   VLAN0020                          active    Fa0/3
30   VLAN0030                          active    Fa0/2
40   VLAN0040                          active
50   VLAN0050                          active
60   VLAN0060                          active
99   VLAN0099                          active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

Résultat attendu :
Les VLANs 10, 20, 30, 40, 50, 60 et 70 doivent être actifs, et les ports doivent être correctement affectés (exemple : Fa0/2 en VLAN 30 pour le serveur Web, Fa0/3 en

VLAN 10 pour le serveur DNS, etc.).
Cette commande doit être exécutée sur les switches 2960-24TT switchIntra et 2960-24TT switchDMZ.

Commande – show interfaces trunk (switchIntra)

Objectif : Vérifier que les ports d'interconnexion entre les switches sont bien configurés en mode trunk, avec l'encapsulation IEEE 802.1Q.

```
Switch_Intra#show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Gig0/1      auto         n-802.1q       trunking      1

Port        Vlans allowed on trunk
Fa0/2       1-1005
Gig0/1      1-1005

Port        Vlans allowed and active in management domain
Fa0/2       1,10,20,30,40,50,60,99
Gig0/1      1,10,20,30,40,50,60,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       1,10,20,30,40,50,60,99
Gig0/1      1,10,20,30,40,50,60,99
```

Résultat attendu :
Le port Fa0/2 apparaît bien en mode trunk, avec l'encapsulation dot1q, et autorise la propagation des VLANs 10 à 70 entre les équipements réseau. Cela garantit que la segmentation logique circule correctement entre les switches.

10. Points forts du projet

- Mise en œuvre de la tolérance aux pannes (RSTP, HSRP)
- Supervision centralisée avec les services Syslog, TFTP et NTP
- Sécurité réseau via ACLs sur les accès sensibles
- Accès Internet fonctionnel grâce au NAT
- Infrastructure segmentée et évolutive

11. Conclusion

Le projet 2 répond aux besoins d'une infrastructure professionnelle sécurisée et supervisée. Les VLANs, le routage, les ACLs et les services sont pleinement opérationnels. Ce projet est prêt à être intégré dans le portfolio, section « Projet 2 ».