mission 1

Loic kebabla
Sadek Mousaceb
Franck vetri

Mission 1– Implémentation de l'infrastructure physique.

Etape 1 🔹 **1. Réaliser le schéma physique**

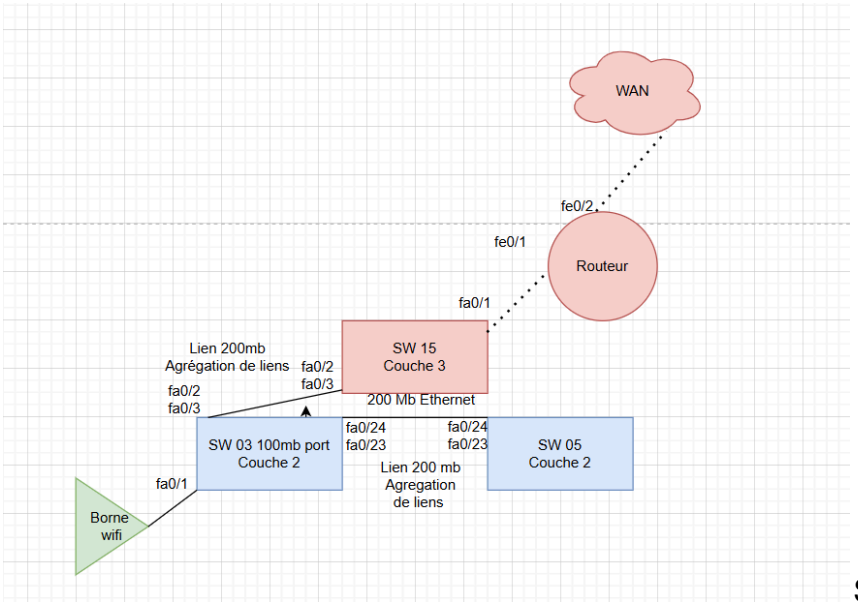
Matériel :

- 1 commutateur niveau 3
- 2 commutateurs niveau 2
- 1 borne Wi-Fi reliée au switch 0/3
- 1 routeur vers **Internet**
- 1 routeur « **AGENCY (C2900)** » vers le WAN/

Connexions :

- L3 ↔ L2(1) : **200 mb**
- L2(1) ↔ L2(2) : **200 Mbps**
- L3 ↔ Routeur Internet
- L3 ↔ Routeur

Etape 2 🔹 2. Réaliser le schéma physique



S

Étape 3 🔹 3. Configurer les accès consoles bonnes pratiques

-Configuration du mot de passe enable sur les switch et routeur (cisco)
- sauvegarde de la conf (copy run startconfig)
-description des liens

Étape 4 : Configuration du protocole de prévention des boucles (Spanning Tree)

Afin d'éviter les boucles de niveau 2 dans le réseau et d'assurer une topologie stable, nous configurons le protocole Spanning Tree Protocol (STP) en mode PVST (Per-VLAN Spanning Tree).

Commandes de configuration

```
enable
configure terminal
spanning-tree mode pvst
spanning-tree vlan 10
```

Le PVST est un mode du Spanning Tree Protocol (STP) qui permet de gérer la prévention des boucles séparément pour chaque VLAN.

Au lieu d'avoir un seul arbre STP pour tout le switch, le PVST crée une instance STP par VLAN.

Étape 5 : Configuration de la sécurité des ports (Port Security)

Pour renforcer la **sécurité du réseau local**, nous configurons la fonctionnalité **Port Security** sur l'ensemble des commutateurs.

```
enable
configure terminal
interface range fa0/10 - 24
 switchport mode access
 switchport port-security
 switchport port-security maximum 50
 switchport port-security violation restrict
```

Les ports **FastEthernet fa0/10 à fa0/24** sont :

- configurés en mode access
- protégés contre les connexions non autorisées

- capables de bloquer les excès de connexions sans couper le service

Mission 2

Mission 2 Intégration des réseaux virtuels.

Centralisation et déploiement des réseaux (VLANs)

Objectif : Configurer les réseaux de façon centralisée pour les déployer sur toute l'infrastructure.

Pour répondre à cet objectif, on utilise généralement le protocole **VTP (VLAN Trunking Protocol)**. Le Switch 03 (par exemple) sera le serveur, et les autres les clients.

```
cli
conf t
# Sur le switch server
vtp domain
vtp mode server
vtp password cisco
vlan 10


# Sur les Switche Clients (SW-05, SW-15)
vtp domain
vtp mode client
vtp password cisco
```

Ces commandes servent à configurer le **VTP (VLAN Trunking Protocol)** afin de **centraliser la gestion des VLANs** dans un domaine réseau.
Grâce à VTP, les VLANs créés sur un switch **serveur** sont automatiquement **propagés** vers les switches **clients**, évitant une configuration manuelle répétitive.

Résultat final

- Le VLAN **10 –** est créé **une seule fois** sur le switch qualifié comme serveur
- Il est automatiquement disponible sur **SW-05 et SW-15**
- La gestion des VLANs est **centralisée, sécurisée et cohérente**

---

2. Redondance et Agrégation de liens

Configuration du Groupe 1 (Lien SW-03 ↔ SW-15)

Cli
Sur SW-03 et SW-15
conf t
interface range fa0/2 - 3
 channel-group 1 mode active
 switchport mode trunk

Configuration du Groupe 2 (Lien SW-03 ↔ SW-05)

cli
Sur SW-03 et SW-05
conf t
interface range fa0/23 - 24
 channel-group 2 mode active
 switchport mode trunk

---

3. Sécurisation des ports "Poste de Travail"

Objectif : Mettre en place les bonnes pratiques et sécuriser les accès utilisateurs.

On applique ici la limitation d'adresses MAC et la protection contre les erreurs sur les ports d'accès.

Ports concernés :

- **SW-15 :** fa0/4-24
- **SW-03 :** fa0/4-22
- **SW-05 :** fa0/1-22

Commande à appliquer sur chaque switch pour les plages d'interfaces correspondantes
Enable
Conf t
interface range 0/4-24
 switchport mode access
 switchport access vlan 10

 # Sécurité des ports
Enable
conf t
 switchport port-security
 switchport port-security maximum 50
 switchport port-security violation restrict

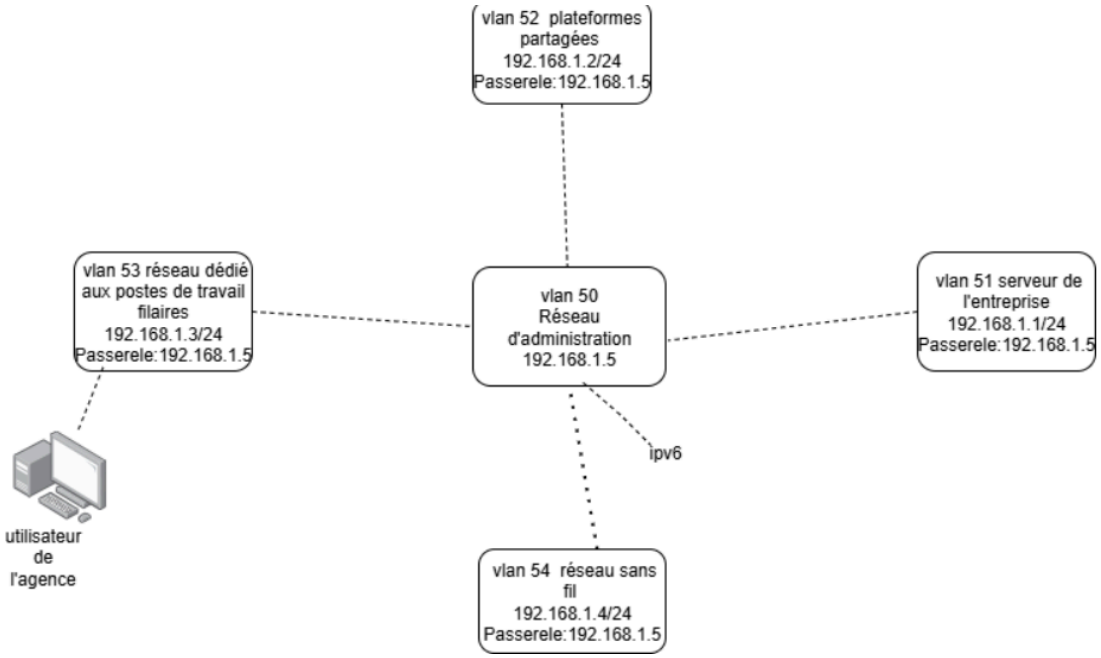
Ces commandes permettent de :

- **Sécuriser les ports d’accès**
- **Limiter le nombre d’équipements connectés 50 en l'occurrence**
- **Réagir proprement aux tentatives d’accès non autorisées**
- **Automatiser les adresses mac**

Mission 3

Mission 3 – Définition de l’adressage logique

Mise en oeuvre du schémas logique



Mise en place des ip sur les vlan 50,51,52,53,54