

## 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 Switches 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**
-