TP6 : VTP (VLAN Trunking Protocol)

NB : Utiliser « cisco » pour tous les mots de passe.

Objectifs du TP :

1. Comprendre et configurer le VTP sur un réseau Cisco.
2. Pratiquer la création et la gestion des VLANs en utilisant le VTP.
3. Sécuriser le domaine VTP avec un mot de passe.
4. Vérifier la propagation des VLANs à travers le réseau.
5. Comprendre les différents modes VTP et leur fonctionnement.

Important / Documentation :

Capturez toutes les étapes et configurations dans un document Word avec des captures d'écran.

Documentez toute procédure de dépannage et les solutions appliquées.

Cours

1. VTP (VLAN Trunking Protocol)

- **Définition** : VTP est un protocole Cisco qui facilite la gestion des VLANs dans un réseau en propulsant automatiquement les modifications de VLAN à travers tous les switches d'un domaine VTP.
- **Modes VTP** :
    - **Serveur** : Peut créer, modifier, et supprimer des VLANs pour tout le domaine VTP.
    - **Client** : Reçoit les mises à jour de VLAN du serveur VTP mais ne peut pas créer, modifier ou supprimer des VLANs.
    - **Transparent** : Ne participe pas à VTP mais transfère les mises à jour VTP à travers le switch. Peut créer des VLANs locaux qui ne sont pas propagés.

- **Commandes Essentielles pour la Configuration**
    - **VTP Domain** : Définir ou changer le nom du domaine VTP :

      vtp domain [nom_du_domaine]
    - **VTP Mode** : Configurer le mode VTP (server, client, transparent) :

      vtp mode [server | client | transparent]
    - **VTP Password** : Définir un mot de passe VTP pour sécuriser le domaine :

      vtp password [mot_de_passe]

Rappel

1. VLAN (Virtual Local Area Network)

- **Définition** : Un VLAN est un sous-réseau qui peut regrouper des ensembles de périphériques réseau même s'ils ne sont pas connectés au même commutateur physique. Cela permet de créer des segments de réseau logiques, indépendants de l'emplacement physique.
- **Avantages des VLANs** :
    - **Sécurité** : Isolation des segments de réseau pour sécuriser les données sensibles.
    - **Gestion** : Simplifie l'administration réseau en regroupant des utilisateurs ayant des besoins similaires.
    - **Performance** : Réduit le domaine de diffusion, limitant ainsi le trafic inutile.

2. Trunks et Encapsulation Dot1Q

- **Définition** : Un trunk est une connexion entre deux switches ou entre un switch et un routeur qui transporte le trafic de plusieurs VLANs.
- **Encapsulation Dot1Q** :
    - **IEEE 802.1Q (Dot1Q)** est une norme de marquage VLAN qui insère un tag de 4 octets dans la trame Ethernet. Ce tag identifie le VLAN auquel appartient chaque trame.
    - **VLAN Natif** : Dans une configuration Dot1Q, le VLAN natif est le VLAN non marqué. Par défaut, c'est VLAN 1, mais il peut être modifié pour des raisons de sécurité.

3. Routage inter-VLAN

- **Définition** : Permet aux VLANs différents de communiquer entre eux via un routeur ou un switch de couche 3 (multicouche).
- **Méthodes de Routage inter-VLAN** :
    - **Routage avec un Routeur Physique (Router-on-a-Stick)** : Utilise une interface physique sur le routeur subdivisée en sous-interfaces, chacune correspondant à un VLAN.
    - **Switch Multicouche (Layer 3 Switch)** : Utilise des interfaces virtuelles de routage (SVI, Switch Virtual Interface) pour chaque VLAN.
- **Configuration d'une Interface de Routage** :
    - Chaque sous-interface est configurée pour un VLAN spécifique avec la commande encapsulation dot1Q [VLAN_ID].

5. Vérifications et Dépannage

- **Vérifier les VLANs configurés sur un switch** : show vlan brief
- **Vérifier l'état des interfaces trunk** : show interfaces trunk
- **Vérifier la configuration VTP sur un switch** : show vtp status
- **Vérifier les interfaces configurées en tant que trunk** : show running-config interface [interface_id]

Topologie 1 :

Description :

- **Switch1** : VTP Server
- **Switch2** : VTP Transparent
- **Switch3** : VTP Client
- **Switch4** : VTP Transparent
- **Switch5** : VTP Client

Interconnexion :

- Switch1 (Serveur VTP) connecté via **G0/2** au Switch2 (Transparent) sur le port **G0/2**.
- Switch1 (Serveur VTP) connecté via **G0/1** au Switch4 (Transparent) sur le port **G0/1**.
- Switch2 (Transparent) connecté via **G0/1** au Switch3 (Client) sur le port **G0/1**.
- Switch4 (Transparent) connecté via **G0/2** au Switch5 (Client) sur le port **G0/1**.

Instructions pour Topologie 1 :

1. **Réalisez la topologie ci-dessus sur Cisco Packet Tracer en utilisant les modèles Cisco 2960 pour les switches.**
2. **Attribuez « SISR » comme nom de domaine VTP :**
   - **Switch1** (Serveur VTP) :

```
configure terminal
vtp domain SISR
vtp mode server
```

   -

```
Switch>ena
Switch>enable
Switch#conf
Switch#configure t
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vtp
Switch(config)#vtp dom
Switch(config)#vtp domain SISR
Changing VTP domain name from NULL to SISR
Switch(config)#vt
Switch(config)#vtp mo
Switch(config)#vtp mode se
Switch(config)#vtp mode server
Device mode already VTP SERVER.
Switch(config)#
```

   - et **Switch4** (Mode Transparent) :

```
configure terminal
vtp domain SISR
vtp mode transparent
```

   - **Switch3** et **Switch5** (Mode Client) :

```
configure terminal
vtp domain SISR
vtp mode client
```

3. **Configurer le mot de passe VTP pour sécuriser le domaine :**
   - **Sur tous les switches** :

```
configure terminal
vtp password cisco
```

Le mot de passe VTP « cisco » est utilisé pour sécuriser le domaine VTP « SISR ». Cela empêche les switches non autorisés d'envoyer des informations VTP sur le réseau.

4. **Créez un VLAN sur Switch1 et vérifiez sa propagation sur le domaine VTP :**
    - **Switch1** (Serveur VTP) :

```
configure terminal
vlan 10
name Marketing
```

    - **Vérification sur Switch3 (Client VTP)** :

```
show vlan brief
```

Lorsque le VLAN 10 est créé sur le switch VTP Serveur (Switch1), il doit se propager automatiquement aux switches en mode Client (Switch3 et Switch5). Les switches en mode Transparent (Switch2 et Switch4) ne doivent pas être affectés par ce changement.

5. **Essayez de créer un VLAN sur Switch2 (Transparent) et vérifiez sa propagation sur le domaine VTP :**
    - **Switch2** (Transparent VTP) :

```
configure terminal
vlan 20
name Sales
```

    - **Vérification** :

```
show vlan brief
```

Les VLANs créés sur les switches en mode Transparent ne sont pas propagés à d'autres switches. Ils n'affectent que le switch sur lequel ils sont configurés.

6. **Essayez de créer un VLAN sur Switch3 (Client VTP) :**
    - **Switch3** (Client VTP) :

```
configure terminal
vlan 30
name HR
```

La création de VLANs sur un switch VTP Client n'est pas possible. Les clients VTP reçoivent des mises à jour du serveur VTP mais ne peuvent pas créer ou supprimer des VLANs eux-mêmes.

```
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 30
VTP VLAN configuration not allowed when device is in CLIENT mode.
Switch(config)#name HR
                ^
% Invalid input detected at '^' marker.

Switch(config)#
```

Top

7. **Configurer et vérifier les trunks entre les switches pour la propagation des VLANs :**
    - Configurez les ports entre les switches en mode **trunk** pour transporter plusieurs VLANs.
    - Exemple de configuration de trunk sur **Switch1** :

```
configure terminal
interface range g0/1 - 2
switchport mode trunk
```

    - **Vérifiez les trunks sur chaque switch** :

```
show interfaces trunk
```

Les trunks permettent de transporter plusieurs VLANs entre les switches, assurant la propagation des VLANs à travers tout le réseau VTP.

Topologie 2 :

Description :

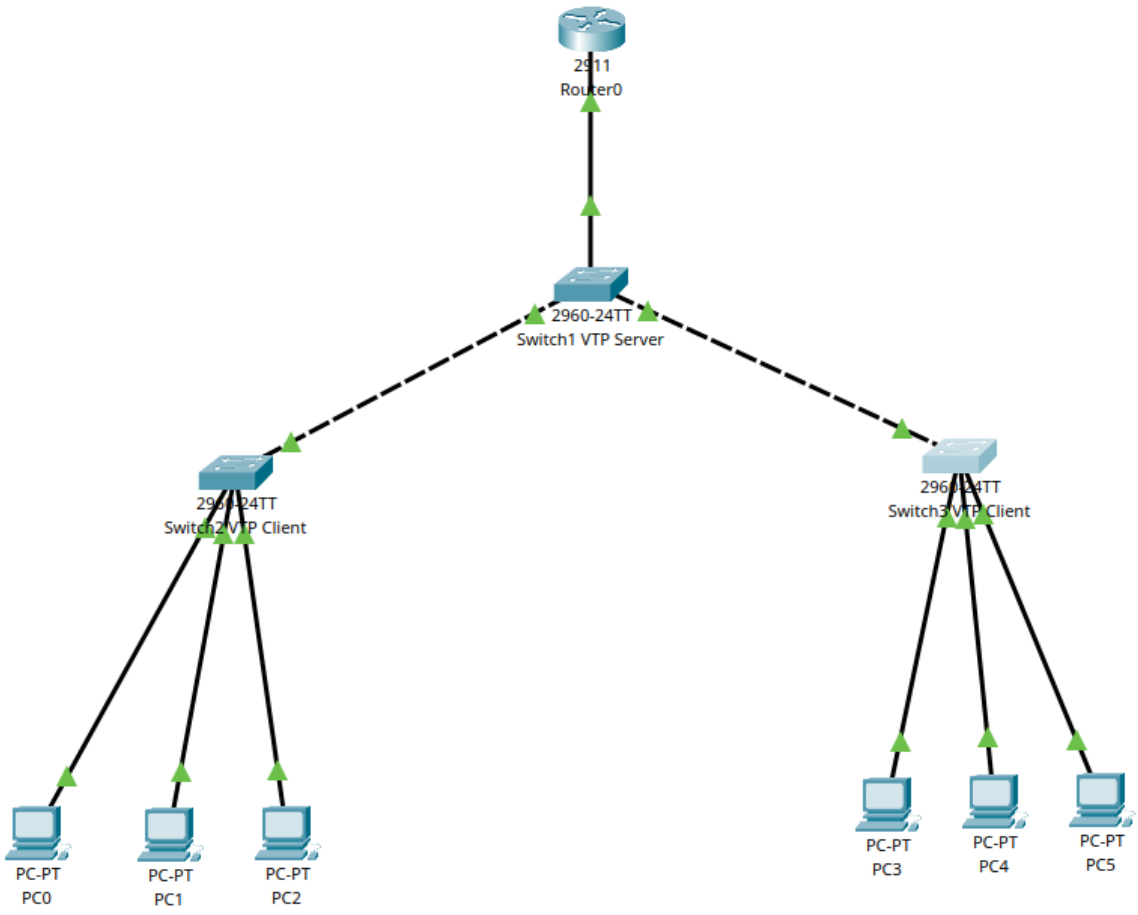
- **Switch1** : VTP Server
- **Switch2** et **Switch3** : VTP Clients
- **Routeur1** : Interconnexion pour le routage inter-VLAN

Ordinateurs :

- **PC1** à **PC6** connectés aux switches en mode Client VTP, appartenant à différents VLANs (10, 20, 30).

Interconnexion :

- Switch1 (Serveur VTP) connecté via **G0/1** au Switch2 (Client VTP) sur le port **G0/1**.
- Switch1 (Serveur VTP) connecté via **G0/2** au Switch3 (Client VTP) sur le port **G0/2**.
- Switch1 (Serveur VTP) connecté via **G0/3** au **Routeur1** sur le port **G0/0.10**, **G0/0.20**, **G0/0.30** pour le routage inter-VLAN.



Instructions pour Topologie 2 :

1. **Réalisez la topologie ci-dessus sur Cisco Packet Tracer en utilisant les modèles Cisco 2960 pour les switches et Cisco 2911 pour le routeur.**
2. **Attribuez « SISR » comme nom de domaine VTP et configurez chaque switch avec les modes appropriés :**
    - **Switch1** (Serveur VTP) : Configurer le switch1 en mode serveur sur le nom de domaine SISR avec le mot de passe Cisco.

```
interface FastEthernet0/1
switchport mode trunk
switchport trunk allowed vlan all
no shutdown
```

    - **Switch2** et **Switch3** (Client VTP) : Configurer le switch2 et 3 en mode client sur le nom de domaine SISR avec le mot de passe Cisco.

```
interface FastEthernet0/2
switchport mode trunk
switchport trunk allowed vlan all
no shutdown
```

```
interface FastEthernet0/1
switchport mode trunk
switchport trunk allowed vlan all
no shutdown
```

```
interface FastEthernet0/2
switchport mode trunk
switchport trunk allowed vlan all
no shutdown
```

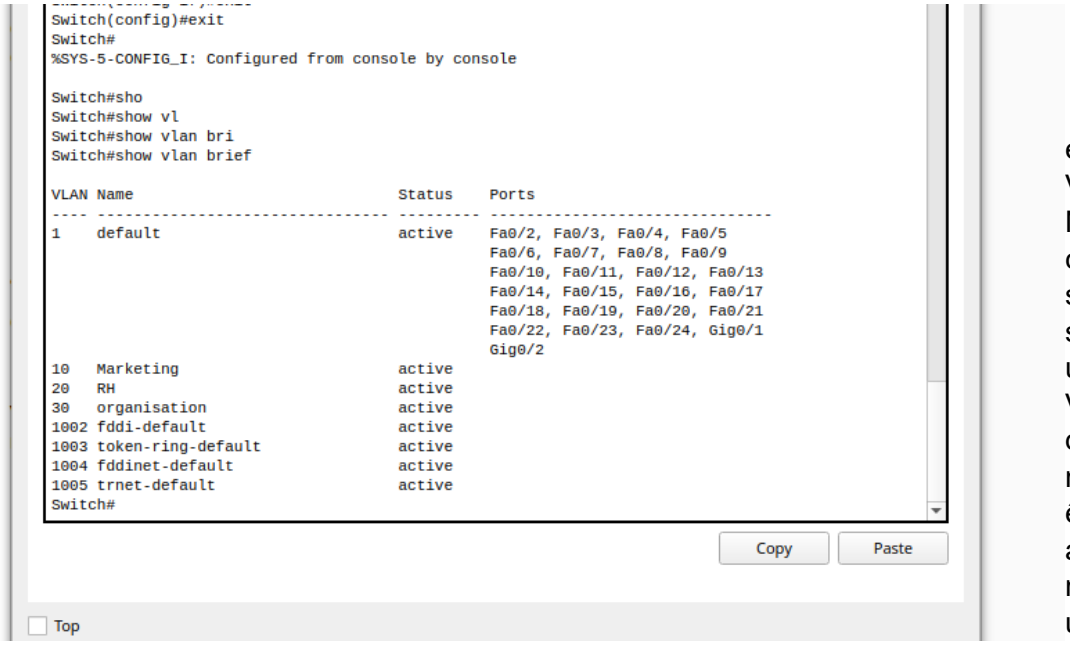
3. **Créer les VLANs sur le Serveur VTP (Switch1) et vérifier leur propagation aux Clients :**
    - **Switch1** (Serveur VTP) :

```
vlan 10
name VLAN10
exit

vlan 20
name VLAN20
exit

vlan 30
name VLAN30
exit
```

    - **Vérification sur Switch2 et Switch3** :



Les VLANs créés sur le serveur VTP doivent être automatiquement propagés aux switches en mode client.

4. **Configurer le routage inter-VLAN sur le Routeur1 :**
    - **Routeur1** :
5. **Vérifiez la connectivité entre les PC de différents VLANs pour s'assurer que le routage inter-VLAN fonctionne correctement.**