TP4 : Compréhension et Pratique des VLANs et Trunks

Topologie à Réaliser :

1. **Ordinateurs :**
   - **PC1** : Connecté au **Switch1** (192.168.10.21/24) dans le VLAN 10
   - **PC2** : Connecté au **Switch1** (192.168.20.22/24) dans le VLAN 20
   - **PC3** : Connecté au **Switch1** (192.168.30.23/24) dans le VLAN 30
   - **PC4** : Connecté au **Switch2** (192.168.10.24/24) dans le VLAN 10
   - **PC5** : Connecté au **Switch2** (192.168.20.25/24) dans le VLAN 20
   - **PC6** : Connecté au **Switch2** (192.168.30.26/24) dans le VLAN 30
   - **Laptop1 Admin** : Connecté au **Switch1** (192.168.1.100/24)
2. **Interconnexion :**
   - **Switch1** connecté à l'interface G0/1 du **Switch2** via l'interface G0/1.

Exercices et Questions de Contrôle :

Partie 1 : Configuration des VLANs

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#VLAN 10
Switch(config-vlan)#name Personnel
Switch(config-vlan)#exit
Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#VLAN 20
Switch(config-vlan)#name Etudiants
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#VLAN 30
Switch(config-vlan)#name Professeurs
Switch(config-vlan)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#VLAN 99
Switch(config-vlan)#name Gestion
Switch(config-vlan)#int G0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 99
Switch(config-if)#int G0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#end
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
```

1. **Créer et Configurer les VLANs :**

- Créez les VLANs 10, 20, 30 sur **Switch1** et **Switch2**.
- Nommez-les "Personnel", "Etudiants" et "Professeurs" respectivement.
- Attribuez les VLANs aux ports appropriés sur chaque commutateur.

Questions :

- **Q1 :** Quelle est la commande pour créer un VLAN sur un commutateur Cisco et lui donner un nom spécifique ?

VLAN (numéro)
name (nom)

- **Q2 :** Comment vérifier que vos VLANs ont été créés et sont correctement configurés sur **Switch1** ?

show vlan brief

show vlan id (10, 20 ou 30)

- **Q3 :** Pourquoi est-il important de nommer les VLANs et de les attribuer correctement aux ports ?

nommer les VLAN et les attribuer correctement aux ports est essentiel pour la sécurité, la gestion efficace, et l'optimisation des performances du réseau.

2 Configurer une Interface de Gestion :

- Configurez une interface VLAN de gestion sur **Switch1** et **Switch2** en utilisant le VLAN 99.

Questions :

- **Q4 :** Quelle est la commande pour configurer une interface de gestion VLAN sur un commutateur ?

interface vlan <numéro_vlan>
ip address <adresse_ip> <masque_de_sous_reseau>
no shutdown

- **Q5 :** Pourquoi utilise-t-on généralement un VLAN séparé pour la gestion des commutateurs ?

un VLAN séparé pour la gestion des commutateurs améliore la sécurité, l'isolation du trafic, et la facilité de gestion, tout en réduisant les risques associés aux accès non autorisés.

Partie 2 : Configuration des Trunks et de la Sécurité des VLANs

```
Switch#en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range Fa0/1-24,G0/1-2
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#end
Switch#write memory
%SYS-5-CONFIG_I: Configured from console by console

Building configuration...
[OK]
Switch#
```

3 **Configurer les Trunks entre les Commutateurs :**

- Configurez les interfaces G0/1 sur **Switch1** et **Switch2** en mode trunk pour permettre le passage des VLANs entre eux.

Questions :

- **Q6 :** Quelle est la différence entre un port configuré en mode "access" et en mode "trunk" ?

Un port en mode "access" est assigné à un seul VLAN et transporte uniquement ce trafic. Un port en mode "trunk" peut transporter plusieurs VLANs simultanément, utilisant des étiquettes (tags) pour différencier le trafic.

- **Q7 :** Comment pouvez-vous vérifier les trunks configurés sur **Switch1** ?

show interfaces trunk

- **Q8 :** Pourquoi est-il important de configurer le VLAN natif lors de la configuration d'un trunk ?

Configurer le VLAN natif sur un trunk est important pour éviter les fuites de VLAN pour que le trafic non étiqueté soit associé au VLAN natif, évitant ainsi les conflits et assurer la compatibilité afin de garantir que les périphériques non VLAN-aware peuvent communiquer correctement.

4 **Sécurité des VLANs :**

- Configurez le **port security** sur tous les ports d'accès pour limiter le nombre d'adresses MAC apprises à 2 et configurez une action de restriction en cas de violation.

Questions :

- **Q9 :** Qu'est-ce que le **port security** et pourquoi est-il utilisé sur les commutateurs ?

Le port security limite les adresses MAC autorisées sur un port, empêchant ainsi les accès non autorisés et renforçant la sécurité du réseau.

- **Q10 :** Quelle commande permet de configurer le **port security** pour restreindre le nombre d'adresses MAC ?

switchport port-security maximum <nombremax>

Partie 3 : Vérification et Dépannage

5 **Vérification de la Connectivité :**

- Testez la connectivité entre les PC du même VLAN pour s'assurer que le trafic ne traverse pas les VLANs.

Questions :

- **Q11 :** Quelle commande utiliseriez-vous pour vérifier la connectivité entre deux PCs dans le même VLAN ?

ping <adresse_IP_du_PC_cible>

- **Q12 :** Si la connectivité au sein du même VLAN ne fonctionne pas, quelles étapes de dépannage devriez-vous suivre pour identifier le problème ?

Vérifier les câbles et les connexions physiques.

Confirmer que les PCs sont dans le même VLAN.

S’assurer que les ports sont actifs (show interface status).

Vérifier les configurations IP (adresse et masque).
Tester avec ping pour isoler le problème.

6 **Dépannage des VLANs :**

- Identifiez et corrigez toute erreur de configuration possible dans votre topologie.

Questions :

- **Q13 :** Quel outil ou commande Cisco Packet Tracer utiliseriez-vous pour capturer et analyser le trafic ARP ?

Utiliser l'outil de capture de paquets. Cliquer sur l'icône de l'outil (une loupe) dans le menu et sélectionner le port ou le périphérique pour analyser le trafic ARP.

- **Q14 :** Si un PC dans VLAN 10 ne peut pas communiquer avec un autre PC dans VLAN 10, que devriez-vous vérifier en premier ?

Vérifier d'abord les configurations IP des PCs, en s’assurant qu'ils sont dans le même sous-réseau (même VLAN 10) et que leurs adresses IP et masques de sous-réseau sont corrects.

Partie 4 : Sécurité et Bonnes Pratiques

7 **Configurer des Bonnes Pratiques de Sécurité sur les VLANs :**

- Désactivez tous les ports inutilisés sur les commutateurs.
- Assurez-vous que tous les ports de trunk ne négocient pas automatiquement le mode de trunking.

Questions :

- **Q15 :** Pourquoi est-il recommandé de désactiver les ports inutilisés sur les commutateurs ?

Il est recommandé de désactiver les ports inutilisés sur les commutateurs pour réduire les risques de sécurité, prévenir les accès non autorisés, et minimiser les collisions et le bruit sur le réseau.

- **Q16 :** Que signifie configurer un port trunk avec switchport nonegotiate et pourquoi est-ce important pour la sécurité ?

Configurer un port trunk avec « switchport nonegociate » empêche le port de négocier automatiquement le mode trunk avec d'autres périphériques. C'est important pour la sécurité car cela réduit le risque d'attaques via la négociation de trunking, comme le VLAN hopping.