

Réseaux 1 – TP5

Vlan et Trunking

Objectifs :

A l'issue de la phase d'expérimentation vous devrez être capable :

- De créer des vlan(s).
- D'assigner une adresse IP à un vlan.
- D'étendre un Vlan sur plusieurs commutateurs.
- De vérifier « l'étanchéité » des vlan(s).
- De mettre en œuvre des mots de passes (telnet et mode enable).
- D'effacer une configuration et des vlan(s).

Documents complémentaires :

Toutes les documentations sur le commutateur CISCO est disponible via le lien suivant en précisant le modèle du commutateur en main : <https://www.cisco.com/c/en/us/support/switches/index.html>

Organisation de la séance :

Les étudiants seront divisés en groupes (Selon le nombre des commutateurs disponibles). Chaque groupe est doté au minimum du matériel suivant :

- 1 commutateur (CISCO),
- 1 câble port-série,
- 2 adaptateurs USB-Ethernet,
- 2 câbles RJ45 (chaque groupe doit avoir une couleur unique) et
- 2 ordinateurs de la salle.
- 1 câbles RJ45 partagé entre 2 groupes.

Le TP se déroule sur 2 heures. Le texte ci-dessous décrit une série de réalisations à effectuer en se répartissant les tâches.

Compte Rendu :

Aucun compte rendu n'est demandé pour ce TP, mais n'hésitez pas à prendre des notes.

Réseau local virtuel VLAN :

Un (VLAN, Virtual Local Area Network) est un sous-réseau de niveau 2, qui peut partager le même réseau avec d'autres VLANs. Les commutateurs sont chargés d'isoler chaque VLAN, ce qui est utile pour sécuriser les échanges. Le protocole 802.1q est utilisé pour marquer les trames Ethernet et

indiquer le VLAN auquel elles appartiennent. Les VLAN peuvent être définis par port ou par adresse MAC. Pour communiquer entre eux, deux VLANs doivent être reliés par un routeur (niveau 3). Le niveau de sécurité n'est cependant pas idéal, certaines attaques permettent de passer d'un VLAN à l'autre.

Réalisations

La figure au tableau décrit la configuration de base du réseau à construire sur la salle.

1. Configuration de base

1. Reprenez la dernière configuration du TP4 en utilisant pour chaque machine virtuelle une adresse IP qui reprend le dernier chiffre du numéro de l'ordinateur dans le dernier octet de l'adresse IP 192.168.1.**X**. Testez que les machines virtuelles connectées au commutateur peuvent communiquer entre elles en utilisant la commande suivante :

Terminal>**ping l'autre_adresse_ip_de_la_machine_virtuelle**

Pour visualiser la table d'adressage utilisée par le commutateur, lancez la commande suivante dans le terminal port série et vérifiez les ports associés aux adresses MAC des deux machines virtuelles aux ports physiques du commutateur :

Switch#**show mac address-table dynamic**

Connectez votre commutateur avec le commutateur d'un autre groupe qui soit proche de vous, et testez la connexion avec la commande *ping* en utilisant les adresses IP configurées dans l'autre groupe.

2. Accès et authentification

Comme nous l'avons déjà vu, la connexion au commutateur s'effectue par le port série « console » ou bien à distance en utilisant les lignes virtuelles (appelées vty). Dans ce qui suit, nous allons créer au minimum un mot de passe pour l'accès aux différents terminaux (console et virtuel) et un autre pour l'accès au mode privilégié (enable). Avant d'entamer cette configuration, on note que par défaut les mots de passe apparaissent en clair quand on affiche le fichier de configuration. Nous allons donc lancer le service de chiffrement « encryption-password » en premier, par conséquent les mots de passe apparaîtront alors chiffrés quand on affiche la configuration du commutateur.

2.a) Chiffrement des mots de passe :

Switch(config)#**service password-encryption**

2.b) Ajoutez un mot de passe pour l'accès via la port série console :

Passez en mode configuration globale :

Switch#**configure terminal**

Passez à la ligne console :

Switch(config)#**line console 0**

Utilisez le mot de passe « tprezo » pour l'accès via le port console :

Switch(config-line)#**password tprezo**

Activez la vérification du mot de passe :

Switch(config-line)#**login**

```
Switch(config-line)#exit
```

2.c) Ajoutez un mot de passe pour l'accès à distance via telnet :

Spécifiez le nombre maximum de connexions aux quelles on est limité pour l'accès au commutateur à distance, ici jusqu'à 4 ports :

```
Switch(config)#line vty 0 4
```

Utilisez le même mot de passe « tprezo » pour l'accès à distance, vous pourriez le changer pour tester une connexion *telnet* via la machine virtuelle après avoir configuré l'adresse IP du vlan par défaut 1 (voir section 3).

```
Switch(config-line)#password tprezo
```

```
Switch(config-line)#login
```

```
Switch(config-line)#exit
```

2.d) Ajoutez un mot de passe pour avoir accès au mode privilégié :

```
Switch(config)#enable password cisco
```

Pour tester ces différentes configurations, configurez l'adresse du vlan 1 (par défaut) en utilisant la commande suivante, changez le **X** en utilisant le dernier chiffre du numéro de l'ordinateur connecter au commutateur via le port série :

```
Switch(config-if)#ip address 192.168.1.9X 255.255.255.0
```

Accédez à la configuration du commutateur de l'autre groupe. S'il vous propose un mot de passe à saisir, utilisez les mots de passe mentionnés dans l'énoncé.

Empêchez votre commutateur pour qu'il soit configuré par l'autre groupe qui est connecté à vous.

3. Configuration des réseaux virtuels

Gardez dans l'esprit que les interfaces 100Mbps/s sont nommées FastEthernet, les interfaces 1Gbit/s sont nommées GigabitEthernet. Les numéros des ports du commutateur ont la syntaxe suivante: 0/1, 0/2, ..., 0/48.

3.a) VLAN

Pour configurer un réseau virtuel vlan, nous utilisons la commande suivante pour le vlan 2. Le vlan 2 n'est qu'un titre d'exemple :

```
Switch(config)#vlan 2
```

Vous pourriez donner un nom à ce vlan, par exemple vlan2test

```
Switch(config-vlan)#name vlan2test
```

```
Switch(config-vlan)#end
```

Pour vérifier les caractéristiques de ce vlan, utilisez la commande suivante :

```
Switch#show vlan name vlan2test
```

Pour associer un port à un vlan, nous utilisons la suite des commandes suivantes :

Entrez l'interface à ajouter au VLAN, exemple fastEthernet 0/2 :

```
Switch(config)#interface fastEthernet 0/2
```

Définissez le mode d'adhésion au réseau local virtuel pour ce port, ici port d'accès de couche 2.

```
Switch(config-if)#switchport mode access
```

Attribuez le port à un VLAN. Les ID de VLAN valides sont compris entre 1 et 4094.

```
Switch(config-if)#switchport access vlan 2
```

```
Switch(config-if)#end
```

Utilisez la commande suivante pour vérifier le vlan associé au port, ici FastEthernet 0/2.

```
Switch#show interfaces FastEthernet 0/2 status
```

Pour configurer un port, notamment la vitesse, le mode et même donner une description, vous allez chercher vous même les bonnes commandes à utiliser pour suivre la configuration donnée dans le tableau ci-dessous. Utilisez les commandes suivantes pour avoir de l'aide :

```
Switch(config)#interface fastEthernet 0/2
```

```
Switch(config-if)#?
```

| Port | Vitesse | Duplex | Vlan | Description |
|------|---------|--------|------|-------------|
| 1 | 10 | half | 1 | |
| 2 | 10 | half | 1 | |
| 3 | 100 | full | 1 | Poste1 |
| 4 | 100 | full | 1 | - |
| 5 | 100 | full | 2 | - |
| 6 | 100 | full | 2 | Poste2 |
| 7 | 10 | half | 2 | - |
| 8 | 10 | half | 2 | - |
| 9 | 100 | full | 6 | - |
| 10 | 100 | full | 6 | - |
| 11 | 100 | full | 6 | - |

Connectez le vlan 2 de votre groupe avec le vlan 2 de l'autre groupe. Vous allez remarquer qu'il faudrait réserver un port associé au même vlan pour qu'on puisse connecter à l'autre vlan. Si nous avons beaucoup de vlans, que fait-on nous s'il n'y a plus de ports ? Ce problème est résolu dans la section 3.b.

Avant d'aller à la réalisation 3.b, connectez votre vlan 2 avec le vlan 6 de l'autre groupe, vérifiez la connexion avec les machines de l'autre groupe via commande *ping*. Que remarquez-vous ? Donnez des explications.

3.b) Trunk

Une ligne de réseau est une liaison point-à-point entre une ou plusieurs interfaces de commutateur Ethernet et un autre périphérique réseau, tel qu'un routeur ou un autre commutateur. Les lignes réseau Ethernet acheminent le trafic de plusieurs VLAN sur une seule liaison et vous pouvez étendre les VLAN sur un réseau entier. Ce mécanisme est pris en charge dans le protocole IEEE 802.1Q qui est implémenté dans le commutateur. Autrement dit, nous pouvons définir un VLAN sur plusieurs commutateurs (ou équipements).

Vous pouvez configurer un *trunk* (jonction) sur un port Ethernet. Utilisez les commandes suivantes pour configurer un trunk, ici on prend le port FastEthernet 0/20 comme un port de jointure. Puis, ajoutez les ids des vlans que vous voulez fusionner avec le commutateur de l'autre groupe (2 et 6).

```
Switch(config)#interface fastEthernet 0/20
```

```
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if)#switchport trunk allowed vlan add id_vlan
```

Paramétrez les commutateurs en rajoutant le port trunk avec la configuration suivante :

| Port | Vitesse | Duplex | Vlan | Description |
|------|---------|--------|-------|---------------------|
| 12 | 100 | full | trunk | Lien interswitch |

Testez la connectivité entre les stations appartenant au même vlan et différents vlans, que remarquez-vous ?

Proposez et testez d'autres configurations !