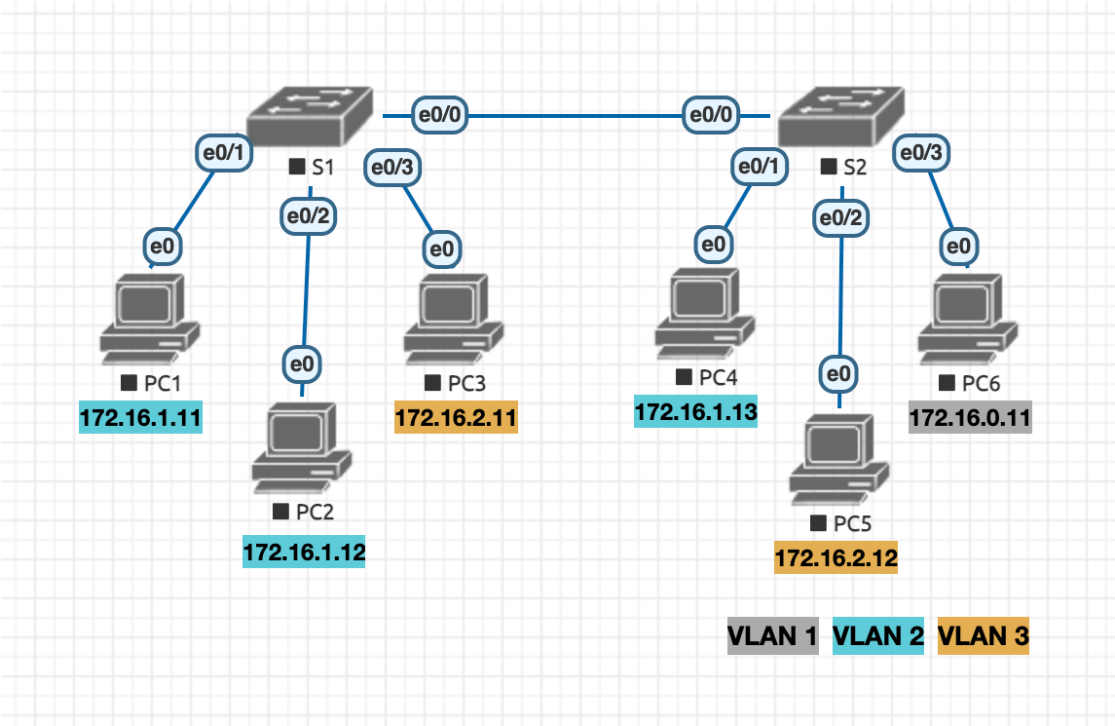
Labo 2 – VLAN

Marcos Rubinstein & Théo Mirabile

1 Mise en place du réseau

Pour commencer, créer un réseau ayant la topologie suivante :



1.1 Indications

- Pour les switches, créez des nœuds de type `Cisco IOL` en utilisant l'image `i86bi-linux-l2-ipbasek9-15.1g.bin`. Utilisez l'icône `Switch.png`.
- Pour les PCs, créez des nœuds de type `Linux` en utilisant l'image `linux-tinycore-6.4`. Utilisez l'icône `Desktop.png`.
- Pour configurer l'adresse IP des PCs, ouvrez le `Control Panel` dans la barre du bas, puis cliquez sur `Network`.
- Pour sauvegarder vos configurations sur les PCs, vous pouvez utiliser « filetool.sh -b » pour enregistrer et vous pouvez récupérer la configuration en utilisant la même commande avec l'option -r au lieu de -b
- Pour afficher l'adresse IP d'un PC, ouvrez le Terminal puis utilisez la commande `ifconfig`.

- Pour entrer en mode de configuration sur un switch, utilisez la commande `enable` puis `configure terminal`.

2 Introduction aux VLANs

La création de réseaux virtuels permet de séparer des groupes de stations liées physiquement au sein d'un même réseau. Par séparer, il faut comprendre que seules les stations appartenant au même VLAN pourront échanger de l'information. On parle alors de topologie logique, car l'appartenance des stations à un même VLAN ne dépend pas directement de leur emplacement physiquement sur le réseau.

Nous étudierons la configuration de VLANs par port sur un switch ainsi que l'interconnexion de VLANs à travers plusieurs switches, à l'aide du « VLAN tagging » avec le protocole IEEE 802.1Q.

Questions

1. Donnez deux avantages concrets de l'utilisation des VLANs.

2. Pour chaque affirmation, spécifiez si elle est vraie ou fausse :

a) Tous les membres d'un même VLAN sont dans le même domaine de broadcast.
b) Tous les membres d'un même VLAN sont dans le même domaine de collision.
c) Tous les membres d'un même VLAN doivent être connectés physiquement au même switch.
d) Tous les membres d'un même VLAN requièrent la capacité de travailler dans le mode full-duplex.

3. Quelle est la fonction du protocole 802.1Q (VLAN tagging) ?

4. Une école d'ingénieurs dispose de deux VLANs : un VLAN 'professeur-e-s' et un VLAN 'étudiant-e-s'. Comment est-il possible qu'étudiant accède au même serveur que son professeur ?

5. Décrivez brièvement le principe des VLAN par port.

6. Donnez deux inconvénients des VLAN par port.

2.1 Configuration des ports *access*

Sur un switch qui implémente les VLANs, on distingue des ports d'accès et des ports « *trunk* ». Un port d'accès va vers une station d'utilisateur, qui n'est typiquement pas capable de gérer l'encapsulation avec 802.1Q. Ces ports acceptent et envoient uniquement des trames sans VLAN tag 802.1Q.

Les ports « *trunk* » servent à étendre les VLAN à travers plusieurs switches. Ils seront étudiés plus tard.

Dans une première étape, nous aimerions configurer les ports d'accès du switch S1 avec deux VLAN:

- VLAN 2 comprenant les ports `e0/1` et `e0/2`
- VLAN 3 comprenant le port `e0/3`

Le VLAN 1 ayant souvent une signification particulière (notamment pour Cisco), nos VLAN sont numérotés à partir de 2.

Voici les commandes nécessaires pour effectuer cette configuration sur un switch Cisco:

```
S1#vlan database
S1(vlan)#vlan 2
S1(vlan)#vlan 3
S1(vlan)#exit
S1#config terminal
S1(config)#interface e0/1
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
S1(config)#interface e0/2
S1(config-if)#switchport access vlan 2
S1(config-if)#exit
S1(config)#interface e0/3
S1(config-if)#switchport access vlan 3
S1(config-if)#exit
```

Questions

7. Utiliser les commandes fournies précédemment pour configurer le switch S1.

8. Adapter ces mêmes commandes pour configurer le switch S2.
   Indiquer les commandes utilisées dans votre rapport.

9. Testez la configuration sur S1. Depuis PC1, effectuez un ping sur une adresse *IP* `172.16.1.x` inexistante. Quels PCs reçoivent la requête ARP ? *Conclusion ?*

2.2 Configuration des ports *trunk*

Pour l'instant la communication des PCs à travers les deux switches n'est pas possible. Nous allons maintenant relier les deux switches par l'intermédiaire d'un trunk VLAN. Lorsqu'une trame est envoyée d'un switch à l'autre, elle doit être marquée avec l'appartenance à un VLAN, pour que le switch récepteur puisse la traiter correctement. L'encapsulation avec le protocole 802.1Q permet cela.

Voici les commandes nécessaires pour effectuer cette configuration sur S1 :

```
S1(config)#interface e0/0
S1(config-if)#switchport trunk encapsulation dot1q
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk allowed vlan remove 4-1001
S1(config-if)#exit
```

Ces commandes mettent les interfaces entre les deux switches en mode 'trunk', sélectionnent le tagging avec 802.1Q ('dot1q'), et n'autorisent que les VLAN 1 à 3 à traverser ce trunk.

Questions

10. Configurez le second switch en suivant la même logique.

11. Testez la configuration. Depuis *PC11*, envoyez un ping sur une adresse `172.16.1.x` inexistante. Qui reçoit la requête ARP ?

12. Analysez les trames échangées entre les deux switches.

a) Indiquez l'emplacement et le format du 'VLAN tag' 802.1Q dans une trame Ethernet.
b) Quel champ identifie le VLAN d'une trame ?
c) Comparez deux trames de deux VLAN différentes pour vérifier vos propos.
Attention : souvenez-vous que l'encapsulation 802.1Q n'a pas lieu sur tout le réseau.

13. Combien de VLANs différents peuvent être gérés avec l'encapsulation 802.1Q ?

14. L'encapsulation 802.1Q est-elle également utilisée sur les ports *access* ?

15. Quelle est la longueur maximum d'une trame avec 802.1Q ?

a) Justifiez avec une capture Wireshark et comparez le résultat avec les trames sans 802.1Q.
Grâce à l'option -s du ping, envoyez une trame d'une taille supérieure à 2000 bytes.
La longueur de la trame affichée sur Wireshark (on wire) ne prend pas compte du CRC (+ 4bytes).
b) Expliquez comment un ping avec une payload plus grande que le maximum peut nous permettre de déterminer de manière rigoureuse la taille maximum d'une trame. (*question bonus*)

3 Sécurité des VLANs

3.1 ARP spoofing

Dans cette partie, nous allons introduire l'ARP spoofing. Il s'agit d'une technique pour effectuer une attaque sur un réseau local. Imaginons que PC1 veut établir une connexion avec PC2. Il va envoyer une requête ARP pour connaître l'adresse MAC qui correspond à l'adresse IP de PC2 et la stocker dans son cache ARP.

Un intrus, que l'on pourrait représenter par PC4, pourrait faire ceci :

1. Il apprend l'adresse MAC de PC2
2. Il manipule le cache ARP de PC1 pour associer l'adresse IP de PC2 à sa propre adresse MAC. Ainsi, tout le trafic destiné à PC2 est redirigé vers lui-même.
3. Il relaie ensuite toutes les trames interceptées à la vraie adresse MAC de PC2.

En exécutant ces opérations pour les deux sens, de PC1 à PC2 et de PC2 à PC1, l'intrus PC4 est capable d'intercepter toutes les données échangées.

Mais comment faire pour manipuler le cache ARP de PC1 et PC2 ?

Plusieurs outils existent pour forger des messages ARP et ainsi associer l'adresse IP d'une victime à l'adresse MAC de l'intrus. Mais il est possible d'obtenir le même effet avec de simples pings. Pour usurper l'identité de PC2, il suffit pour PC4 de changer brièvement son adresse IP à celle de PC2 et envoyer un ping à PC1. PC1 va mettre à jour son cache ARP avec l'adresse MAC de PC4, et on obtient le résultat voulu.

16. Depuis PC4, manipulez les caches ARP de PC1 et PC2 avec la commande suivante (en une seule ligne) :

```
sudo ifconfig eth0 172.16.1.12; (ping -c 1 172.16.1.11);
sudo ifconfig eth0 172.16.1.11; (ping -c 1 172.16.1.12);
sudo ifconfig eth0 172.16.1.13
```

17. Consultez la table ARP de PC1 et de PC2 pour en vérifier le contenu, à l'aide de la commande `arp -a`.
    Il se peut que le contenu s'efface rapidement. Refaites la manipulation jusqu'à obtenir la MAC de PC4 dans la table de PC1 et PC2. Joignez des captures d'écran.

3.2 Attaque « Man-in-the-middle »

Les expériences précédentes ont déjà montré que les trames de diffusion restent à l'intérieur d'un VLAN, ce qui signifie une réduction du trafic broadcast dans le réseau. Certaines attaques peuvent être prévenues ainsi mais il y a aussi moyen de contourner cette protection dans certains cas.

18. Est-ce qu'un attaquant est capable d'effectuer une attaque *man-in-the-middle* avec la segmentation en VLANs s'il veut s'attaquer à un VLAN différent du sien ?

3.3 Attaque « VLAN hopping »

Malheureusement, certaines implémentations des VLANs ont des failles qu'un acteur malveillant pourrait exploiter. Une attaque possible se nomme *VLAN hopping*.

19. Renseignez-vous et décrivez en quoi consiste le VLAN hopping.

20. Quelles attaques (écoute clandestine, déni de service) peuvent être menées avec cette méthode ?

21. Proposez une approche pour empêcher cette attaque.

4 Recherche d'information et compréhension détaillée

22. Faites maintenant un ping depuis PC4 vers PC1 et capturez simultanément avec Wireshark à l'interface e0/0 de PC1 et e0/0 de PC4.

    Utilisez le filtre de capture ARP dans les deux captures. Dans un des deux interfaces, vous devriez voir seulement les requêtes ARP tandis que dans l'autre, vous devriez voir les requêtes et aussi les réponses ARP. Expliquez la raison. Pour ce faire, vous pouvez par exemple observer avec Wireshark le trajet parcouru par les requêtes ARP ainsi que celui des réponses ARP pour comprendre les différences entre les deux interfaces.

23. Faites un ping de PC1 vers PC6.
    Est-ce que le ping passe ? Si oui, pourquoi ?