Laboratoire

rÉSEAUX LOCAUX VIRTUELS vlan

6 mars 2022

<Étudiant / classe>

<Étudiant / classe>

Objectifs du laboratoire

Ce laboratoire étudie les améliorations de la sécurité et des performances dans un LAN grâce aux VLAN.

Les objectifs de ce laboratoire sont:

* Comprendre les risques de sécurité dans un LAN commuté
* Comprendre le fonctionnement des VLAN
* Savoir configurer le trunking VLAN avec IEEE 802.1Q sous Cisco

Prérequis

Ce laboratoire demande des connaissances théoriques sur les réseaux locaux virtuels VLAN, présentées dans le chapitre « Couche liaison ». Il demande également des connaissances concernant la configuration de switches sous Cisco.

Rendu

Rapport dû une semaine après la fin du laboratoire. Ce laboratoire se fait sur deux semaines.

Questions théoriques

Répondez aux questions suivantes en utilisant le support du cours, Chapitre « Couche Liaison ».

Questions I

* Donnez deux avantages de l'utilisation de VLAN (2p)
* Pour chacune des propositions suivantes, marquez vraie ou faux en rapport avec l'appartenance à un VLAN, en supposant que chaque membre d'un VLAN est connecté à son propre port du switch (2p)

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.

* Quelle est la fonction du protocole 802.1Q (VLAN tagging) ? (2p)

* Une école d’ingénieurs à deux VLAN : un VLAN ‘professeur-e-s’ et un VLAN ‘étudiant-e-s’. Comment est-il possible qu’un étudiant envoie un e-mail à un professeur ? (1p)
* Décrivez brièvement le principe des VLAN par port. (2p)
* Donnez deux inconvénients des VLAN par port. (2p)

Pratique

***Première partie***

# Réseau

L'Illustration 1 montre le réseau que nous allons utiliser pour nos expériences. Utilisez la commande ip pour configurer les adresses des 5 machines selon la tabelle sous la figure..

La table ci-dessous montre l'appartenance des machines aux VLAN.

Illustration 1: Réseau de test pour VLAN

|  |
| --- |
| VLAN 2 |
| Pc1 | 172.16.1.11/16 |
| Pc2  | 172.16.1.12/16 |
| Pc5 | 172.16.1.14/16 |
| VLAN 3 |
| Pc3 | 172.16.2.11/16 |
| Intrus (VLAN2)  |
| Pc4 | 172.16.1.13/16 |

Dans l'état initial, aucune configuration n'a été faite. Configurez les adresses IP. Les pc doivent être capables de se pinger entre eux.

# Sécurité LAN

Nous avons déjà appris qu'un switch augmente la sécurité dans les réseaux locaux par rapport à un hub. Après l'apprentissage de la topologie du réseau, un switch est capable de n'envoyer une trame que sur le port qui va vers le destinataire de la trame.

Bien que cela représente une amélioration considérable de la sécurité LAN, il reste encore beaucoup de possibilités pour un intrus se trouvant dans le réseau d'influencer le comportement des switches. Il peut ainsi effectuer des attaques de déni de service ou de « passeur de seau » (man-in-the-middle).

## 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, pc4, peut 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 il redirige le trafic destiné à pc2 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, et voilà le résultat voulu.

* Depuis pc4, manipulez les caches ARP de pc1 et pc2 avec la commande suivante (en une seule ligne) :

pc4> sudo ip 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

Consultez la table ARP de pc1 et de pc2 pour en vérifier le contenu. Il se peut que le contenu s'efface rapidement. Ré-effectuez la manipulation jusqu'à obtenir la MAC de pc4 dans la table de pc1 et pc2. Joignez des captures d'écran.

Questions III

* Quel est le nom de l'attaque décrite ci-dessus ?

## Broadcast

A part les problèmes de sécurité, les trames de diffusion peuvent présenter un autre ennui dans un LAN switché. Les broadcasts sont typiquement générés par des serveurs, pour annoncer un service, par des clients, pour découvrir un service, par les protocoles de réseau pour s'adapter aux changements de configuration (STP, routage), mais aussi par le protocole ARP.

Pour illustrer cela,

* relancez une capture entre le switch 2 et pc4.
* Ensuite, depuis pc1, pinguez une adresse 172.16.1.x inexistante.

Joignez une capture d'écran de la capture wireshark.

Pc4 reçoit des requêtes ARP, envoyées en diffusion. Comme pc1 et pc4 sont connectés à des switches différents, il est clair que ces messages inondent le réseau entier et doivent être traités par chacune des machines du réseau.

Si l'on s'imagine le nombre de trames de diffusion générées par un LAN avec plusieurs milliers de stations, on comprend facilement l'intérêt de limiter la portée des messages de diffusion au stricte nécessaire.

***Deuxième partie***

# Les réseaux locaux virtuels

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.

## Configuration de VLAN sur un switch

Sur un switch VLAN, 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 sw\_lan\_A avec deux VLAN:

* VLAN 2 comprenant les ports fa0/1 et fa0/2
* VLAN 3 comprenant le port fa0/3

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

A titre d'illustration, regardons les commandes nécessaires si sw\_lan\_A était un switch Cisco:

sw\_lan\_A#**vlan database**

sw\_lan\_A(vlan)#**vlan 2**

sw\_lan\_A(vlan)#**vlan 3**

sw\_lan\_A(vlan)#**exit**

sw\_lan\_A#**config terminal**

sw\_lan\_A(config)#**interface fa0/1**

sw\_lan\_A(config-if)#**switchport access vlan 2**

sw\_lan\_A(config-if)#**exit**

sw\_lan\_A(config)#**interface fa0/2**

sw\_lan\_A(config-if)#**switchport access vlan 2**

sw\_lan\_A(config-if)#**exit**

sw\_lan\_A(config)#**interface fa0/3**

sw\_lan\_A(config-if)#**switchport access vlan 3**

sw\_lan\_A(config-if)#**exit**

sw\_lan\_A(config)#

Les quatre premières commandes créent les deux VLAN 2 et 3. Ensuite, chacune des interfaces est configurée comme port d'accès et assignée au VLAN correspondant.

Questions IV

* Effectuez une configuration analogue sur sw\_lan\_B. Configurez les VLAN 2 et 3 et attachez fa0/2 à vlan2 et fa0/1 à vlan3. Indiquez les commandes utilisées. (4p)
* Testez la configuration sur sw\_lan\_A. Depuis pc1, effectuez un ping sur une adresse 172.16.1.X inexistante. Quels PCs reçoivent la requête ARP? Conclusion ? (2p)

## VLAN trunking

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.

Encore une fois à titre d'illustration, regardons la configuration d'un switch Cisco :

sw\_lan\_A(config)#**interface fa 0/0**

sw\_lan\_A(config-if)#**switchport mode trunk**

sw\_lan\_A(config-if)#**switchport trunk encapsulation dot1q**

sw\_lan\_A(config-if)#**switchport trunk allowed vlan remove 4-1001**

sw\_lan\_A(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.

Configurez le second switch en suivant la même logique.

Questions V

* Testez la configuration. Depuis pc1, envoyez un ping sur une adresse 172.16.1.X inexistante. Qui reçoit la requête ARP ? (2p)

## Analyse de l'encapsulation 802.1Q

Questions VI

Analysez les trames échangées entre les deux switchs.

* Indiquez l'emplacement et le format du 'VLAN tag' 802.1Q dans une trame Ethernet. Quel champ identifie le VLAN d'une trame ? 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. (3p)
* Combien de VLAN différents peuvent être gérés avec cette encapsulation ? (1p)
* Cette encapsulation, est elle aussi utilisée sur les ports d'accès ? (1p)
* Quelle est la longueur maximum d'une trame avec 802.1Q ? Justifiez votre réponse avec une capture wireshark et comparez le résultat avec les trames sans 802.1Q. (3p)

***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).***

* Bonus : 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.
* Expliquez la différence d'encapsulation avec ISL au niveau de la trame.

## Cette partie est optionnelle et elle peut être réalisée à al fin si vous avez le temps. Passer donc à la Section 4. Sécurité

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.

###### Attaque « Man-in-the-middle »

Questions VII

* Est-ce qu'un attaquant est capable d'effectuer une attaque man-in-the-middle maintenant que le réseau est segmenté en vlan et qu'il veut s'attaquer à une vlan différente ?

###### Attaque de « VLAN hopping »

Malheureusement quelques implémentations de VLAN ont des failles qu'un utilisateur malveillant pourrait exploiter. Une attaque pouvant être menée est le VLAN hopping.

Questions VIII

* Renseignez-vous et décrivez en quoi consiste le VLAN hopping.
* Quelles attaques (écoute clandestine, déni de service) peuvent être orchestrées avec cette méthode ? (4p)
* Proposez une approche pour empêcher cette attaque. (2p)

# Routage entre VLAN

Dans une configuration correcte, les switchs VLAN empêchent toute communication entre VLAN différents. Mais souvent il est nécessaire de permettre certains types de trafic entre deux VLAN, par exemple pour pouvoir envoyer un e-mail à un utilisateur d'un autre VLAN.

Le passage entre les VLAN n'est possible qu'au niveau de la couche 3 du modèle OSI, donc à l'aide d'un routeur. Typiquement un firewall est actif sur un tel routeur pour restreindre les transferts entre VLANs.

Dans notre réseau, le router1 peut assumer ce rôle.

Questions IX

* Décrivez une méthode comment le router1, qui n'a qu'une seule interface réseau, peut router entre le VLAN 2 et le VLAN 3? (3p)