Les VLAN

Dino Lopez Pacheco – dino.lopez@univ-cotedazur.fr

1 Introduction

Dans ce TP, nous allons explorer l'isolation et renforcement du partitionnement d'un réseau avec des Virtual LANs (VLANs). La configuration des VLAN est une tâche assez commune dans un réseau d'entreprise, où souvent, le réseau est divisé en un sous-réseau spécialement dédié aux postes de l'administration, un (ou plus) sous-réseau pour la partie cœur de métier, et peut-être aussi une partie DMZ.

Nos tests se feront en utilisant des switches virtuels de type OpenVSwitch, qui offre une implémentation su standard 802.1Q.

Lors de vos tests, faites des captures d'écran et utilisez-les pour répondre aux exercices.

2 L'isolation des réseaux avec des VLANs

Pour commencer, nous allons explorer comment les trames Ethernet sont modifiées lorsqu'elles sont taggés avec une en-tête 802.1Q.

1. Téléchargez le fichier vlan-topo1.imn et déployez le réseau virtuel avec le logiciel CORE. Après le déploiement du réseau virtuel, aucun VLAN n'y est configuré.
2. Dans cette topologie, il y a 3 sous-réseaux.
    a. Déployez wireshark ou tcpdump sur « c2-10 » et « c2-20 »
    b. Depuis « c1-10 » exécutez une requête ARP vers « c2-10 » avec la commande « arping -c1 10.0.1.20 »
    c. Est-ce que « c2-10 » répond à la requête ARP ? est-ce que les autres clients voient passer la requête et/ou la réponse ? pourquoi ?

    Oui, « c2-10 » répond à la requête ARP. Oui, tous les autres clients du réseau lissent la requête ARP qui a été envoyé en mode broadcast. Vu que tous les sous-réseaux IP se partagent le même switch (et qu'un switch prend de décision de retransmission sur les adresses MAC de destination), il est normal que tous les clients voient passer les paquets dont l'adresse de destination au niveau MAC est l'adresse de broadcast.

3. Par défaut, en OpenVSwitch, tous les ports d'un switch sont configurés en mode trunk.
    a. Configurez le port « eth1 » et « eth2 » de « sw1 » en mode accès. Tous les paquets en provenance de « eth1 » et « eth2 » seront taggés avec les VLAN IDs 10 et 20 respectivement.
    b. Donnez les commandes que vous avez utilisez pour la configuration des ports « eth1 » et « eth2 » de « sw1 »
    c. Gardez les commandes dans un fichier nommé « conf-sw1.sh »

    Double click sur « sw1 », puis exécutez « ovs-vsctl set port eth1 tag=10 » et « ovs-vsctl set port eth2 tag=20 »

4. Déployez wireshark ou tcpdump sur « c1-10 », « c2-10 » et « c2-20 ». Depuis « c1-10 » exécutez une requête ARP vers « c2-10 » avec la commande « arping -c1 10.0.1.20 »
    a. Est-ce que « c2-10 » répond à la requête ARP ? Pourquoi ?

    Non. Notez que le trafic envoyé par « c1-10 » sera encapsulé dans le VLAN 10 et que « c2-10 » ne fait pas encore partie de ce VLAN. En conséquence, « c2-10 » n'a aucun

moyen de décapsuler le trafic enveloppé par le tag VLAN 10 et de répondre à la requête ARP.

b. Prouvez que les ports en mode accès fonctionnent correctement.

Si wireshark montre que les paquets sortant de « c1-10 » ne sont pas taggés, mais que « c2-10 » reçoit les messages avec un tag, cela prouve que notre *access port* fonctionne correctement.

c. Prouvez que les ports avec la configuration par défaut se comportent comme des ports de type trunk.

Si « c2-20 » et « c2-20 » reçoivent tous les messages depuis « c1-10 » et « c2-10 », taggés avec les VLANs 10 et 20 resp., ceci prouve que les ports d'attache de « c2-20 » et « c2-20 » possédant la configuration par défaut, se comportent bien comme un port trunk.

5. Configurez les VLANs au niveau du switch « sw2 », tel que montré par le dessin de la topologie.
   a. Les ports d'attache pour les clients « c2-* » sont de port d'accès.
   b. Prouvez que le trafic est isolé correctement grâce aux VLANs

Montrer par wireshark ou tcpdump qu'uniquement les membres d'un VLAN reçoivent le trafic en broadcast envoyé par l'un des client du VLAN.

c. Pourquoi cette fois-ci les arping fonctionnement correctement ?

Cette fois-ci, lors que les paquets sont retransmis par un *access port*, le tag VLAN est supprimé et les clients reçoivent les paquets tel qu'ils le verraient si aucune VLAN n'existait.

d. Gardez les commandes dans un fichier nommé « conf-sw2.sh »

6. Par sécurité, les administrateurs fréquemment limitent les VLAN IDs qui peuvent être transféré par un *trunk port* aux VLANs de confiance.
   a. Configurez le port « eth3 » de « sw1 » pour rester un port trunk mais qui ne retransfère que les paquets du VLAN 10.
   b. Prouvez que tout fonctionne comme attendu.
   c. Donnez les commandes que vous avez exécutez pour cet exercice et expliquez le déroulement de vos tests.

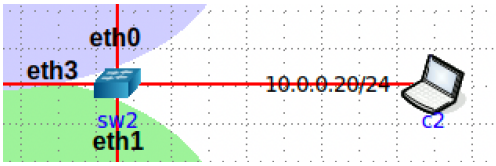
La commande est « ovs-vsctl set port eth3 trunks=10 ». Si on fait un ping entre « c1-10 » et « c2-10 » ça marche, mais un ping entre « c1-20 » et « c2-20 » ne fonctionne plus.

7. Configurez le port « eth3 » de « sw1 » pour transférer uniquement les paquets des VLAN 10 et 20.
   a. Prouvez que votre configuration fonctionne correctement
   b. Gardez toutes les commandes de configuration de sw1 dans un fichier nommé « conf-sw1.sh »
8. Arrêtez le réseau de test

3 Le VLAN natif

9. Avant de lancer le réseau de test, ajoutez un client au réseau et connectez-le à « sw2 ».
   a. Nommé le client « c2 ».

b. Par l'interface CORE, effacez les adresses IPv4 et IPv6 que vous auriez sur les interfaces de « sw1 ». Toujours avec CORE, donnez l'adresse 10.0.0.20/24 à « c2 ». Voici à quoi ressemble la partie modifiée de la topologie



10. Déployez le réseau de test et
    a. Rechargez à nouveau la configuration de la section 2, en exécutant les fichiers « conf-sw1.sh » et « conf-sw2.sh » sur « sw1 » et « sw2 » respectivement.
    b. Vérifiez que vous avez bien récupérez la configuration des ports VLAN en accès.
11. Faites un arping depuis « c1-10 » vers « c2-10 »
    a. Normalement, « c1 » voit passer votre requête. Pourquoi ?

    Oui, il voit passer la requête, dont la trame est taggé, parce qu'il s'agit d'un lien *trunk* laissant passer tous les VLANs

12. Exécutez la commande « ovs-vsctl set port eth0 vlan_mode=access » sur « sw1 ».
    a. Est-ce que « c1 » voit passer votre requête cette fois-ci ? Pourquoi ?

    Non, maintenant que le port est en mode « access », il ne laisse sortir que les trames correspondant au VLAN auquel le port d'accès appartient.

13. Faites un arping depuis « c1 » vers « c2 »
    a. Est-ce que l'arping fonctionne ? est-ce que le trafic est taggé ? expliquez vos observations

    L'arping ne devrait pas fonctionner car nous avons configures nos liens trunk pour ne retransmettre que des paquets taggés.

    b. Ceci n'est pas une pratique courante ni très conseillé, mais comment faire si jamais on souhaite qu'entre nos switches, le trafic entre c1 et c2 ne soit pas taggé, tout en faisant marcher correctement les arping ?

    Il faut déclarer les ports connectés aux clients en mode « access » et les ports entre les switches en mode « native-untagged ». il faut choisir cependant une valeur de tag pour les ports access et native-untagged, qu'on n'utilisera que pour le *native VLAN* préféremment.

14. Arrêtez le réseau.

4 La communication inter-VLAN

15. Téléchargez et déployez le réseau « vlan-topo1-router-2l.imn »
    a. Lancez le déploiement du réseau et rechargez la configuration des VLANs grâces aux fichiers « conf-sw1.sh » et « conf-sw2.sh »
    b. Configurez le réseau pour interconnecter les VLAN 10 et 20 avec la technique des liens multiples.
    c. Vous n'avez pas besoin de configurer quoi que ce soit sur le routeur pour exécuter le routage. Le routage se fera automatiquement lorsqu'il recevra des paquets d'un sous-réseau allant vers l'autre.
    d. Expliquez et montrez vos manips.

La solution est assez simple : l'interface du routeur avec adresse 10.0.1.1 doit être connecté à un « *access port* » du VLAN 10. Connectez l'interface du routeur avec adresse 10.0.2.1 à un « *access port* » du VLAN 20. Le reste se fait automatiquement et le ping ou arping doivent fonctionner.

16. Arrêtez le réseau.
17. Téléchargez et déployez le réseau « vlan-topo1-router-1l.imn »
    a. Lancez le déploiement du réseau et rechargez la configuration des VLANs grâces aux fichiers « conf-sw1.sh » et « conf-sw2.sh »
18. Renforcement de la sécurité du réseau grâce aux VLANs
    a. Configurez l'interface eth0 de sw1 en mode accès. Le trafic sera taggé avec l'ID 999
    b. Faites en sorte que les switches ne s'échangent par les liens trunk que le trafic des VLAN 10, 20 et 999.

Sur « sw1 » :
ovs-vsctl set port eth0 tag=999
ovs-vsctl set port eth3 trunks=10,20,999
Faire "sw2" en toute autonomie.

19. Configurez le réseau pour activer la communication inter-LAN en utilisant la technique d'un seul lien + 1 routeur.
    a. Expliquez et montrez vos manips.

La clé ici c'est de recevoir tout le trafic taggé, mais de créer des sous-interface qui feront le travail de décapsulation des trames. Si on met une sous-interface dans le VLAN 10, il faut configurer cette interface avec l'adresse passerelle attendu par le client (ie. 10.0.1.1 pour VLAN 10). En termes des commandes, il faut exécuter sur R1 :

```
ip link add link eth0 name eth0.10 type vlan id 10
ip a a 10.0.1.1/24 dev eth0.10
ip link set eth0.10 up; # activation de l'interface
```

Ensuite, faire de même pour les VLANs 20 et 999. Ensuite, les pings entre les réseaux doivent fonctionner correctement