TPs Réseau Avancés

Selim Lakhdar < selim.lakhdar@etudiant.univ-lille1.fr >

TP1 : Configuration d’équipements réseau

1- Connexion au switch : cables droits

2- Configuration telnet :

```
    >enable
    #configure terminal
    (config)# line vty 0
    (config-line)# password bonjour
    (config-line)# transport input telnet
    (config-line)# end
    #configure terminale
    (config)# interface vlan1
    (config-if)# ip address 192.168.1.254 255.255.255.0
    (config-if)# exit
    (config)# end
```

3- Configuration ssh :

```
    >enable
```

```
#configure terminal
#hostname SB4
#ip domaine-name lille
#crypto key generate rsa
(config)# line vty 0
(config-line)# login local
(config-line)# transport input ssh
(config-line)# end
#configure terminale
(config)# interface vlan1
(config-if)# ip address 192.168.1.254 255.255.255.0
(config-if)# exit
(config)# end
```

4- tftp

```
ssh root@192.168.1.254
copy system:running-config tftp
```

TP2 : LAN

1. Commutation

1. `sudo ifconfig enp2s0 up 192.168.1.2`

   C ne reçoit pas les messages ICMP envoyés en unicast de **A** vers **B**.

   Il les reçoit après que **B** ce soit déconnecté.

C reçoit des requêtes de "Who has … " pour retrouver la destination.
==> Requêtes broadcast pour reconstituer l'adresse physique. (de B)

2. @MAC-C = 30:B5:C2:04:FA:F3
   le switch change de port aléatoirement entre **B** et **C**.
   À intervalle régulier la table CAM change (le port change)
   Les deux clients reçoivent les ping de **A** désormais. (Il n'y a plus de différence entre **B** et **C**, les deux reçoivent en même temps)

   `mac address-table static 30b5.c205.0d80 vlan 1 interface Gi1/0/6`
   `mac address-table static 30b5.c205.0d80 vlan 1 interface Gi1/0/10`

3. Les adresses mac de **A**, **B** et **S1** sont associés au même port sur **S2**.
   A et **B** peuvent se pinger

2. Sécurisation des ports

1. Après avoir sécuriser le port, **B** ne peut plus ping **A**, et **C** ne peut pas ping **B**.
   Le *mode sticky* permet de sauvegarder les anciennes associations et de détecter un changement de port (adresse).

   ```
   configure terminal
   ```

```
interface Gi1/0/1
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
```

2. Sécurisation des ports active mais fastidieuse (configurer pour chaque port, et le changer à chaque changement de port)

3. configure terminal
   interface range Gi1/0/1-24
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security mac-address sticky

3. Boucle de communication

1. Les ping sont retransmis en boucle (spam), car aucun des deux switches ne reconnait l'adresse, et espère la trouver en redirigeant la requête vers une interface connue

2. Lors de la recherche d'un hôte inconnue, la requête parcours le réseau. (risque de boucle)

3. Au minimum il faut filtrer les deux ports d'un même switch (où ils bouclent)

4. Le *sotrm-control* peut bloquer un trafic légitime lors de la mise en prod dans un réseau important.

```
configure terminal
interface Gi1/0/1
storm-control broadcast level 15
end
```

4. Bridge linux

```
    sudo ifconfig enp1s0 up 0.0.0.0
    sudo ifconfig enp3s0 up 0.0.0.0
    sudo brctl addbr A
    sudo brctl addif A enp1s0
    sudo brctl addif A enp3s0
    sudo ifconfig A up 192.168.1.1
```

5. Arbre recouvrant

1. **S2** est le pont racine.
2. Les *messages STP* sont transmis chaque **2 secondes**
3. *Les ports qui émettent* : *0/1 0/2* de **S2** et *eth0* de **A** et **B.**

   Les ports qui reçoivent : *0/1, 0/2* de **S1** et *eth1* de **A** et **B**.
4. Destination: Spanning-tree-(for-bridges)*00 (01:80:c2:00:00:00)*

   C’est un *MAC MULTICAST*

   Elles ne sont pas diffusées sur l’ensemble du domaine de diffusion.

5.1. Choix du pont racine

1. Le pont root sera le pont avec la plus petite priorité

```
configure terminal
spanning-tree vlan 1 priority 4096
end
```

2. Si les priorités sont égales. le nœud qui a l'@ MAC la plus petite est choisit comme **root**, grâce au *bridge id*

3. On préfère mettre (fixer) en root le nœud le plus gros du réseau.

5.2. Choix des ports racines

1. Election du pont Root
2. Choix des ports Root
3. Choix de ports désignés

Les ports non désignés sont mis en blocking.

Etats des ports :

- Blocking
- Listening
- Learning
- Forwarding

7. VLAN

1. Pour le VLAN 2 :

```
configure terminal
vlan 2
name atelier
ex
interface range Gi1/0/1-2
switchport mode access
switchport access vlan 2
```

   Pour le VLAN 3 :

```
configure terminal
vlan 3
name direction
ex
interface range Gi1/0/3-4
switchport mode access
switchport access vlan 3
```

   A reçoit de **B** uniquement, **C** reçoit de **D** uniquement.

   (A et B) et *(C et D)*

2. Les VLAN permettent d’isoler les ports du switch qui lui sont

associées.

3. Sur **S1** et **S2** :

   Pour le VLAN 2 :

```
configure terminal
vlan 2
name atelier
ex
interface Gi1/0/1
switchport mode access
switchport access vlan 2
interface Gi1/0/3
switchport mode access
switchport access vlan 2
```

   Pour le VLAN 3 :

```
configure terminal
vlan 3
name direction
ex
interface Gi1/0/2
switchport mode access
switchport access vlan 3
interface  Gi1/0/4
switchport mode access
```

```
switchport access vlan 3
```

8. Trunk

```
configure terminal
interface Gi1/0/3
switchport nonegotiate
switchport mode trunk
switchport trunk allowed vlan 2-3
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
```

2. On remarque un vlan ID qui permet de différencier les différents vlan.
   On remarque aussi l’encapsulation de la trame avec le protocole 802.1Q.
3. 12 bits => 4096 VLAN
4. Les paquets ne peuvent pas être interprétés, si deux protocoles différents sont déployer de chaque coté du trunk.

```
switchport trunk encapsulation dot1Q
```

```
 switchport trunk native vlan 2
```

Les deux vlan sont toujours isolés.

On ne peut avoir qu’un Vlan natif par trunk.

On remarque qu’il n’y a plus d’encapsulation 802.1Q pour les

trames du vlan 2.

6. Les trames sont ré envoyées.

   Dans une grande structure, même si un VLAN ne comporte aucun utilisateur, les requêtes lui seront quand même envoyées

9. Surveillance des ports

```
configure terminal
monitor session 1 source interface Gi1/0/3
monitor session 1 destination interface Gi1/0/4 encapsulation
 dot1q
```

10. VTP

```
configure terminal
vtp domain TOTO
vtp mode server
```

Le trunk transmet les trames envoyées par le VLAN 3.

Les paquets VTP sont transmis sur le trunk.

Seul le serveur VTP peut créer des VLAN.

```
VLAN Trunking Protocol
    Version: 0x02
    Code: Subset Advertisement (0x02)
    Sequence Number: 1
```

```
    Management Domain Length: 4
    Management Domain: TOTO
    Configuration Revision Number: 8
    VLAN Information
        VLAN Information Length: 20
        Status: 0x00
        VLAN Type: Ethernet (0x01)
        VLAN Name Length: 7
        ISL VLAN ID: 0x0001
        MTU Size: 1500
        802.10 Index: 0x000186a1
        VLAN Name: default
    VLAN Information
        VLAN Information Length: 20
        Status: 0x00
        VLAN Type: Ethernet (0x01)
        VLAN Name Length: 7
        ISL VLAN ID: 0x0002
        MTU Size: 1500
        802.10 Index: 0x000186a2
        VLAN Name: atelier
    VLAN Information
        VLAN Information Length: 20
        Status: 0x00
        VLAN Type: Ethernet (0x01)
        VLAN Name Length: 6
        ISL VLAN ID: 0x0003
        MTU Size: 1500
```

```
        802.10 Index: 0x000186a3
        VLAN Name: access
```

2. Un switch peut basculer en mode serveur et avoir les droits d'ajout de VLAN.
   Ceci peut entraîner des failles de sécurités; qu'un client devienne serveur et modifie le réseau.

3. L'inter-compatibilité entre les différentes machines. On ne peut pas garantir que l'autre machine communique de la même façon.

11. Routage inter-vlan

Sur le routeur :

```
configure terminal
interface Gi0/1
no shutdown
end
configure terminal
interface Gi0/1.2
encapsulation dot1Q 2
ip address 192.168.10.254
end
interface Gi0/1.3
encapsulation dot1Q 3
ip address 192.168.11.254
```

```
end
configure terminal
ip routing
end
```

Sur le switch :

```
configure terminal
interface Gi1/0/5
switchport mode trunk
switchport trunk allowed vlan 2-3
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 3
```

Sur les clients du VLAN 2 :

```
sudo route add -net 192.168.11.0 netmask 255.255.255.0 gw 192
.168.10.254
```

Sur les clients du VLAN 3 :

```
sudo route add -net 192.168.10.0 netmask 255.255.255.0 gw 192
.168.11.254
```

Les trames 802.1Q sont retransmissent d’un réseau à un autre (retransmissent grâce à un routeur).

12. Trunk et serveur

```
vconfig add enp2s0 2
vconfig add enp2s0 3
```

```
switchport trunk allowed vlan 2-3
```

3. Les requêtes VTP sont reçu par le poste.

   L'ajout du VLAN sur **S1** n'a pas été pris en compte sur **S2**.

   On ne peut pas ajouter de vlan sur **S2** (il n'est pas ajouté).

```
 flash:vlan.dat
```

   Dans la running config

13. Agrégation des liens

```
Interface range Gi1/0/3-5
channel-group 1 mode on
```