PVLAN

Objectif : mettre en place des vlan privées

Ce TD n'est pas compatible Packet Tracer

Le VLAN privé a toujours un VLAN principal. Dans le VLAN principal, vous trouverez le port promiscous.

DDans le VLAN principal, vous rencontrerez un ou plusieurs VLAN secondaires. Il en existe deux types:
VLAN de **communauté**: tous les ports du VLAN de communauté peuvent communiquer entre eux et avec le port proche.
VLAN **isolé**: tous les ports du VLAN isolé ne peuvent pas communiquer entre eux, mais ils peuvent communiquer avec le port promiscous.

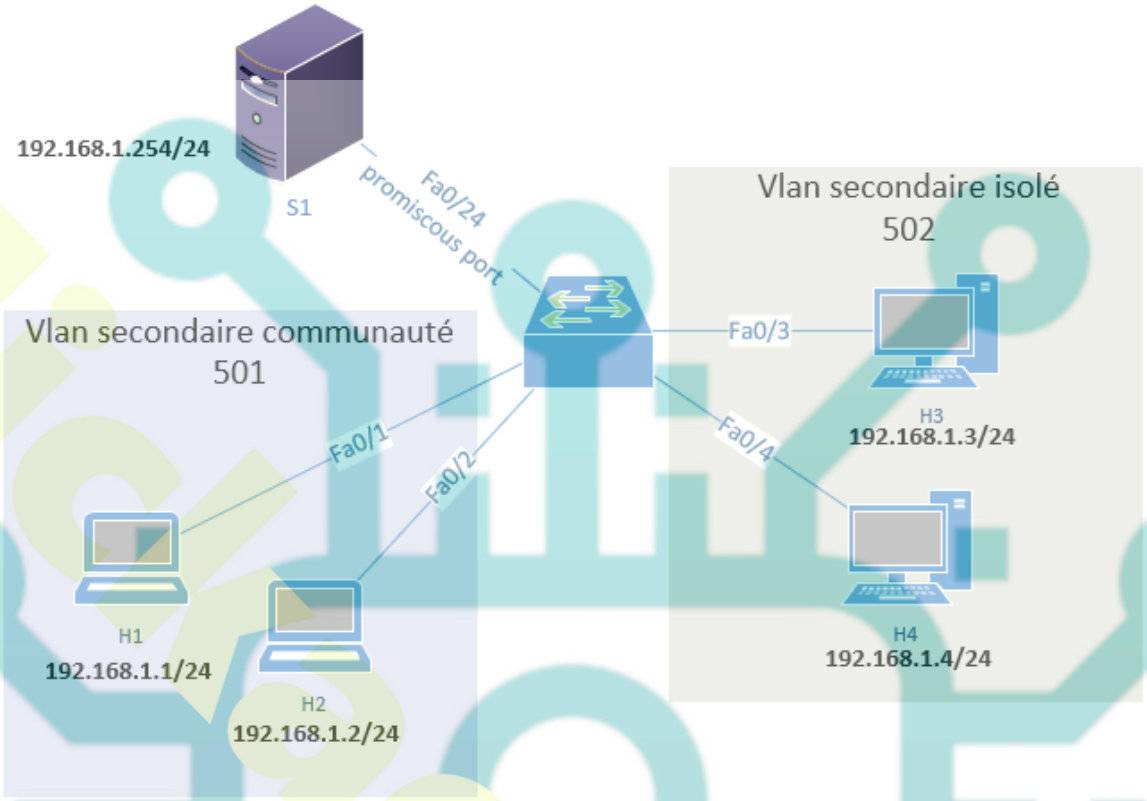

Schéma de du TD

Le réseau local virtuel principal porte le numéro 500.
Le VLAN de la communauté secondaire porte le numéro 501.
Le VLAN isolé secondaire porte le numéro 502.

- H1 et H2 sont dans le vlan communauté et doivent pouvoir se joindre, ainsi que le serveur connecté au port promiscous.
- H3 et H4 sont dans le VLAN isolé et ne peuvent communiquer qu'avec le serveur sur le port promiscous.
- Le serveur devrait pouvoir atteindre tous les ports.

La configuration de VLAN privés nécessite de changer le mode VTP en transparent.

```
SW1(config)#vtp mode transparent
```

Commençons par la configuration du VLAN de communauté. Tout d'abord, on créé le VLAN 501 et on indique au commutateur qu'il s'agit d'un VLAN de communauté. Ensuite, on créé le VLAN 500 et on le configure en tant que VLAN principal. Puis, on indique au commutateur que le VLAN 501 est un VLAN secondaire.

```
SW1(config)#vlan 501
SW1(config-vlan)#private-vlan community
SW1(config-vlan)#vlan 500
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#private-vlan association add 501
```

Les interfaces fa0 / 1 et fa0 / 2 sont connectées à H1 et H2 et appartiennent au VLAN 501 de communauté. Au niveau de l'interface, on doit informer le commutateur que ce sont des ports hôte . On utilise la commande switchport private-vlan host-association pour indiquer au commutateur que le VLAN 500 est le VLAN principal et que 501 est le VLAN secondaire.

```
SW1(config)#interface range fa0/1 – 2
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 500 501
```

On configure le port promiscuous sur le port fa0/24 en tapant la commande switchport mode private-vlan switchport mode. On dois également mapper les VLAN à l'aide de la commande de mappage switchport private-vlan.

```
SW1(config)#interface fa0/24
SW1(config-if)#switchport mode private-vlan promiscuous
SW1(config-if)#switchport private-vlan mapping 500 501
```

Nous pouvons vérifier notre configuration en consultant les informations de switchport. L'interface fa0/2 a la même configuration que fa0/1.

```
SW1#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
```

Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: 500 (VLAN0500) 501 (VLAN0501)
Administrative private-vlan mapping: none

Voici les informations sur le switchport pour fa0 / 24 (notre port promiscuous). Vous pouvez voir les informations de mappage.

SW1#show interface fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 500 (VLAN0500) 501 (VLAN0501)

La commande suivante nous donne des informations précieuses. Vous pouvez voir que le VLAN 500 est le VLAN principal et que 501 est le VLAN secondaire. Il nous dit aussi si le VLAN est une communauté ou un VLAN isolé des ports.

SW1#**show vlan private-vlan**
Primary Secondary Type Ports
500 501 community Fa0/1, Fa0/2, Fa0/24

La commande suivante nous donne des indications sur le type de vlan

```
SW1#show vlan private-vlan type
Vlan Type
---- -----------
500 primary
501 community
```

- **Test des connexions**

```
H1>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
```

H1 est capable d'atteindre H2.

```
H1>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
```

H1 peut également atteindre le serveur derrière le port promiscuous.

```
S1>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
```

Le serveur peut atteindre H2. Le VLAN communautaire semble être opérationnel.

Continuons avec la configuration du VLAN isolé.
La configuration est identique à celle du VLAN de communauté, mais cette fois-ci, on utilise la commande private vlan isolated. N'oubliez pas d'ajouter l'association entre le VLAN principal et secondaire à l'aide de la commande private-vlan association add. La commande private-vlan primary n'est pas utilise car saisie auparavant, je l'affiche simplement pour que la configuration reste complète.

```
SW1(config)#vlan 502
SW1(config-vlan)#private-vlan isolated
SW1(config-vlan)#vlan 500
SW1(config-vlan)#private-vlan primary
SW1(config-vlan)#private-vlan association add 502
```

Cette partie est identique à la configuration du VLAN de communauté, mais on configure les interfaces fa0/3 et fa0/4 qui sont connectées à H3 et H4.

```
SW1(config)#interface range fa0/3 – 4
SW1(config-if-range)#switchport mode private-vlan host
SW1(config-if-range)#switchport private-vlan host-association 500 502
```

Nous avons déjà configuré le port fa0/24 en tant que port promiscuité, mais je le montre ici aussi pour que la configuration reste complète. On a maintenant besoin de créer un mappage supplémentaire entre VLAN 500 (principal) et VLAN 502 (secondaire).

```
SW1(config)#interface fa0/24
SW1(config-if)#switchport mode private-vlan promiscuous
SW1(config-if)#switchport private-vlan mapping 500 502
```

- **Vérification**

```
SW1#show interfaces fa0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: down
Administrative Trunking Encapsulation: negotiate
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

```
Administrative private-vlan host-association: 500 (VLAN0500) 502
(VLAN0502)
Administrative private-vlan mapping: none
```

- nous pouvons voir l'association hôte entre le VLAN 500 et le 502.

```
SW1#show interfaces fastEthernet 0/4 switchport | include host-as
Administrative private-vlan host-association: 500 (VLAN0500) 502
(VLAN0502)
```

- **On vérifie le port promiscous**

```
SW1#show interfaces fa0/24 switchport
Name: Fa0/24
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 500 (VLAN0500) 501 (VLAN0501)
502(VLAN0502)
```

- **On vérifie les vlan**

```
SW1#show vlan private-vlan
Primary Secondary Type Ports
------- --------- ---------------- ----------------------------
------------
-
500 501 community Fa0/1, Fa0/2, Fa0/24
500 502 isolated Fa0/3, Fa0/4, Fa0/24
```

SW1#show vlan private-vlan type
Vlan Type
—- ————————
500 primary
501 community
502 isolated

- **On teste les connexions**

```
H3>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
```

H3 peut joindre le promiscuous port.

```
H4>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time<1ms TTL=128
```

H4 également.

```
H3>ping 192.168.1.4
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.4:
Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
```

H3 ne peut pas joindre H4 ce qui est normal.