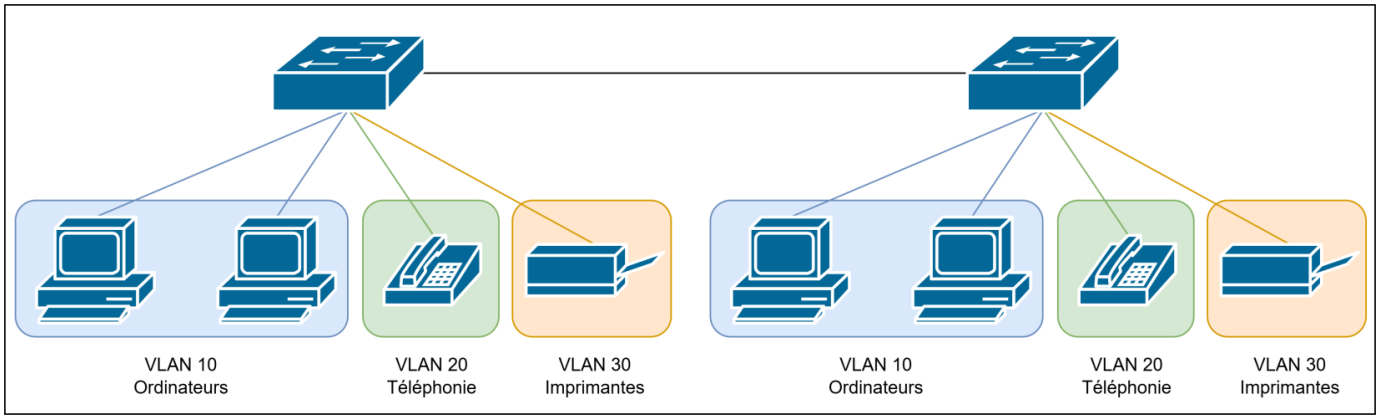
Réseaux locaux virtuels

Introduction

Lors de la conception d'un réseau, il est bonne pratique de segmenter un réseau en fonction de différents besoins. Qu'il s'agisse d'isoler chaque département d'une entreprise ou de segmenter un réseau par type d'appareils pour appliquer des règles de filtrage de trafic différentes en fonction du besoin, il sera nécessaire de segmenter le réseau à la couche de liaison de données pour éviter que quelqu'un change simplement son adresse IP pour accéder à des ressources différentes.



Dans une configuration telle que celle affichée dans le schéma ci-haut, il serait possible de bloquer l'accès à Internet pour les imprimantes et les téléphones, de prioriser le trafic des téléphones pour assurer une qualité d'appel ainsi que de les isoler puisqu'un téléphone IP ne devrait pas nécessiter d'accès à une imprimante. On pourrait aussi penser à ajouter un VLAN pour l'accès aux appareils de mise en réseau auquel seulement les postes de travail des techniciens pourraient accéder.

Quoi qu'il soit possible de segmenter un réseau physique en plusieurs domaines de diffusion par la création de différents ponts d'interfaces sur chaque routeur ou commutateur, ceci nécessiterait un lien physique par pont entre chaque appareil. C'est ici que le concept de réseaux locaux virtuels entre en jeu. Ceux-ci permettent de diviser un un commutateur ou un pont en plusieurs "bulles" réseau et de conserver ce trafic traversant un lien unique entre deux appareils correctement segmenté en ajoutant une étiquette à chaque trame ethernet transmise entre deux commutateurs.

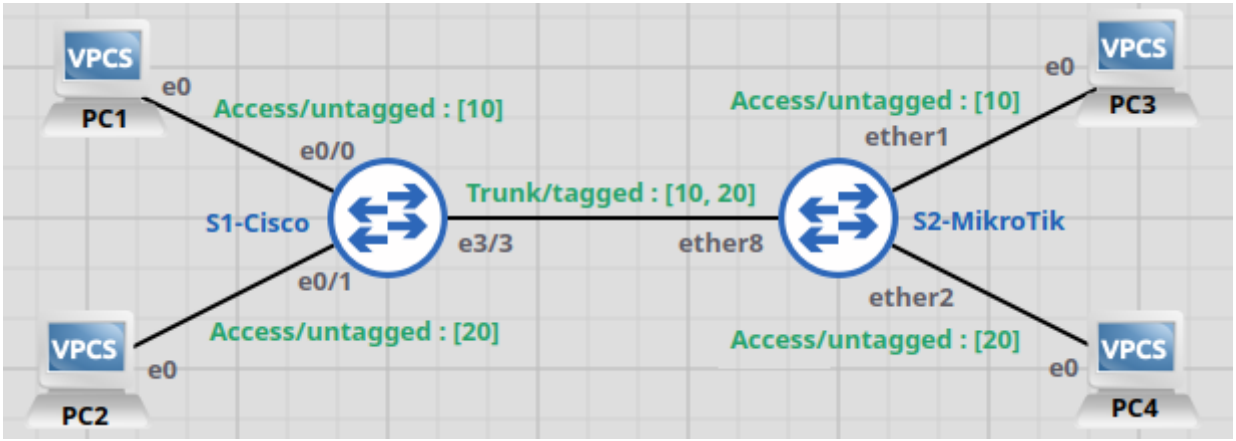
Différents manufacturiers ont différentes appellations pour ce mécanisme. Cisco à titre d'exemple appelle les liens entre différents appareils permettant le transport de plusieurs VLANs simultanément des "trunks" et décrit les ports donnant accès à un certain VLAN sans nécessiter d'étiquette entre l'appareil ou les appareils liés à une interface et le commutateur comme étant en mode "access". MikroTik parlera plutôt de "tagged" lorsque le trafic d'un VLAN doit être étiquetté sur le lien concerné et "untagged" sur un lien donnant accès à un VLAN sans nécessiter d'étiquette.

Étiquetage de VLANs

Dans l'exemple suivant, les vPCs 1 et 3 sont situés dans le même VLAN (VLAN10) et les vPCs 2 et 4 sont dans un autre VLAN (VLAN20). Par conséquent, les vPCs identifiés par des nombres impairs ne peuvent pas rejoindre les vPCs identifiés par des nombres pairs même s'ils seraient situés dans le même sous-réseau IP car ils sont séparés dans des domaines de broadcasts distincts.

Les PC sont branchés dans des ports qu'on peut décrire comme étant des ports d'accès (ports donnant accès à un réseau). Ceci indique au commutateur que tout trafic entrant sans identifiant de VLAN par ce port sera assigné au VLAN configuré sur l'interface ainsi qu'indiquer au commutateur que toute communication de ce VLAN destiné à l'adresse MAC branchée derrière le port sera transmise par ce port en retirant l'étiquette de VLAN associée à la communication. Ceci permet de relier les hôtes au réseau sans nécessiter la configuration de l'identifiant de VLAN sur l'hôte.

Le lien entre les deux commutateurs peut être décrit comme un "trunk". La configuration de chaque commutateur indique que tout trafic associé aux VLANs spécifiés dans la configuration de l'interface. Ceci permet aux commutateurs d'identifier à quel VLAN une communication est destinée et l'acheminer seulement aux adresses MAC de ce VLAN.



Configuration S1:

```
interface Ethernet0/0
 switchport access vlan 10
 switchport mode access
end

interface Ethernet0/1
 switchport access vlan 20
 switchport mode access
end

interface Ethernet3/3
```

```
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20
 switchport mode trunk
end
```

Configuration S2:

```
/interface bridge
add name=LAN vlan-filtering=yes

/interface bridge port
add bridge=LAN interface=ether1 pvid=10
add bridge=LAN interface=ether2 pvid=20
add bridge=LAN interface=ether8

/interface bridge vlan
add bridge=LAN tagged=LAN,ether8 untagged=ether1 vlan-ids=10
add bridge=LAN tagged=LAN,ether8 untagged=ether2 vlan-ids=20
```

On peut observer dans les tables de commutation de nos switches que les adresses MAC des PC sont associées aux identifiants de VLANs configurés sur les ports de switch.

Table de commutation S1 :

```
S1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  10    0050.7966.6800    DYNAMIC     Et0/0
  10    0050.7966.6802    DYNAMIC     Et3/3
  20    0050.7966.6801    DYNAMIC     Et0/1
  20    0050.7966.6803    DYNAMIC     Et3/3
```

Table de commutation S2 :

```
[admin@S2] > /interface/bridge/host/print
Flags: D - DYNAMIC; L - LOCAL
Columns: MAC-ADDRESS, VID, ON-INTERFACE, BRIDGE
 #    MAC-ADDRESS        VID  ON-INTERFACE  BRIDGE
```

```
 6 D  00:50:79:66:68:00   10  ether8        LAN
 7 D  00:50:79:66:68:02   10  ether1        LAN
11 D  00:50:79:66:68:01   20  ether8        LAN
12 D  00:50:79:66:68:03   20  ether2        LAN
```

On peut aussi observer le mécanisme d'étiquetage de VLAN permettant aux commutateurs d'assigner le trafic aux bons VLANs. Suivons une requête ICMP (ping) entre PC1 et PC3.

PC1 -> S1 : Rien d'anormal ici, on y observe les adresses MAC et IP du PC1 comme source et celles de PC3 comme destination. Comme le port du commutateur est configuré pour donner accès au VLAN 10, cette communication sera assignée au VLAN 10.

```
Frame 49: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: 00:50:79:66:68:00, Dst: 00:50:79:66:68:02
Internet Protocol Version 4, Src: 10.0.10.10, Dst: 10.0.10.11
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

S1 -> S2 : En se fiant à sa table d'adresses MAC, le commutateur S1 sait qu'il peut contacter l'adresse MAC du PC3 (68:02) par son interface ether8 dans le VLAN 10. Comme sa configuration le stipule, il ajoutera donc l'identifiant du VLAN à la communication. On peut observer cet identifiant à la ligne 3 dans la capture suivante.

```
Frame 126: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface -, id 0
Ethernet II, Src: 00:50:79:66:68:00, Dst: 00:50:79:66:68:02
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 10
Internet Protocol Version 4, Src: 10.0.10.10, Dst: 10.0.10.11
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

S2 -> PC3 : Le commutateur S2 reçoit la communication et peut lire de l'étiquette ajoutée par S1 à la communication que ce message est destiné au VLAN 10. Comme le mentionne sa table de commutation, cette adresse MAC peut être rejointe à son port ether1. La configuration de l'interface ici est "untagged" et indique donc au commutateur de retérer l'étiquette de VLAN lorsque le message sera envoyé à PC3.

```
Frame 75: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: 00:50:79:66:68:00, Dst: 00:50:79:66:68:02
Internet Protocol Version 4, Src: 10.0.10.10, Dst: 10.0.10.11
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
```

> Projet GNS3 adapté à cette machine virtuelle incluant GNS3

Routage inter-VLAN

Pour circuler entre plusieurs VLANs, il est évidemment nécessaire de passer par un routeur.

Différentes méthodes et configurations sont empruntées à cet effet. Ces méthodes sont décrites ici

.

Revision #18
Created 2025-02-05 01:22:45 UTC by Alexandre Arsenault-Jetté
Updated 2025-07-11 01:03:39 UTC by Alexandre Arsenault-Jetté