Commutation

Acheminement de données par adresse MAC (couche 2 du modèle OSI) au sein de domaines de diffusion et segmentation de domaines de diffusion par réseaux locaux virtuels.

- Trames ethernet
- Domaines de diffusion (Broadcast)
- Pontage (bridging)
- Réseaux locaux virtuels

Trames ethernet

Introduction

Toute communication réseau/ethernet est composé de bits acheminés que ce soit par fréquences radio, lumière ou plus communément par signal électrique. Ces communications doivent être destinés à une adresse représentant un hôte réseau. Les protocoles les plus communs utilisent des adresses IP pour déterminer l'itinéraire à emprunter pour rejoindre une destination. Plusieurs appareils se situent généralement entre l'expéditeur et le destinataire. Qu'il s'agisse de routeurs, de commutateurs ou de points d'accès, chaque appareil situé entre les interlocuteurs doit être en mesure d'acheminer la donnée sans perdre l'information identifiant la destination finale de la communication.

Ces bits sont donc tout d'abord destinés à une adresse MAC pour être acheminés au sein d'un domaine de diffusion qui est l'étendue à laquelle serait acheminée une communication s'adressant à l'ensemble d'un réseau local. Les commutateurs, ponts et points d'accès utilisent donc cette information pour choisir où transférer la communication.

Ces trames ethernet ne possèdent pas de délai d'expiration et ne seront donc jamais émises à une adresse MAC inexistante au sein d'un réseau et en cas de boucle de commutation, il est possible qu'une trame diffusée (broadcast) surcharge éventuellement votre réseau. Le protocole spanning-tree peut être mis en place pour éviter une telle situation.

Cette structure est représentée théoriquement par le modèle OSI et peut être observée dans une capture de trafic avec tcpdump ou Wireshark.

Fonctionnement

Diffusion (Broadcast)

Un broadcast est destiné à l'ensemble des adresses MAC au sein du domaine de diffusion et peut être identifié comme étant destiné à l'adresse MAC de diffusion (FF:FF:FF:FF:FF:FF). Lorsqu'une diffusion entre dans un commutateur, elle sera retransmise par l'ensemble des ports du commutateur ou du bridge appartenant au même domaine de diffusion (voir VLANs pour la segmentation de domaines de diffusion).

Protocoles de couche 2

Certains protocoles tels que Profinet, spanning-tree ou ARP sont destinés uniquement à des adresses MAC. Pour ces communications, la section IPv4 ou IPv6 sera inexistante. Ces protocoles fontionnent soit par diffusion (broadcast) ou par des adresses MAC de destination forcées dans la configuration des appareils.

Destination locale

La capture suivante est divisée entre quatre sections. La première représente les données brutes transmises sur l'interface, la deuxième représente les adresses MAC de source et de destination de la communication. Ceci est ce qui décrit la trame ethernet. Cette trame contient ensuite un paquet IP représenté dans la section suivante identifiant les adresses IP de source et de destination.

```
Frame 78: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: 00:50:79:66:68:02, Dst: 00:50:79:66:68:05
    Destination: 00:50:79:66:68:05
    Source: 00:50:79:66:68:02
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.255.3, Dst: 192.168.255.6
Internet Control Message Protocol
```

L'adresse MAC de destination est généralement déterminée à l'aide du protocole ARP en fonction de l'adresse IP de destination. Si cette adresse IP est située dans un réseau directement connecté à un appareil selon la table de routage de l'expéditeur, celui-ci effectuera une requête ARP et utilisera l'adresse MAC correspondante à l'adresse IP pour composer son message. Si aucun appareil ne répond à cette requête ARP, le message ne pourra pas être composé et ne sera donc pas émis.

Destination externe

Si l'adresse IP de destination est située derrière un routeur selon la table de routage de l'émetteur, l'adresse MAC de la passerelle plutôt que celle de l'adresse IP de destination sera demandée et la trame sera acheminée au routeur par son adresse MAC.

Dans l'exemple suivant, on peut observer que l'adresse MAC de destination (fa:49:b6:ff:50:30) est la même, que le paquet soit destiné au routeur ou destiné à une adresse IP située de l'autre côté du routeur.

Paquet destiné au routeur (10.60.9.1) :

```
Frame 23986: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
\Device\NPF_{8CA5DE3B-06FD-4657-A2E1-67C2BC69E370}, id 0
Ethernet II, Src: MicroStarINT_35:f2:9a (d8:cb:8a:35:f2:9a), Dst: fa:49:b6:ff:50:30
(fa:49:b6:ff:50:30)
    Destination: fa:49:b6:ff:50:30 (fa:49:b6:ff:50:30)
    Source: MicroStarINT_35:f2:9a (d8:cb:8a:35:f2:9a)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 10.60.9.69, Dst: 10.60.9.1
Internet Control Message Protocol
```

Paquet destiné au serveur DNS de google (8.8.8.8) :

```
Frame 276184: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
\Device\NPF_{8CA5DE3B-06FD-4657-A2E1-67C2BC69E370}, id 0
Ethernet II, Src: MicroStarINT_35:f2:9a (d8:cb:8a:35:f2:9a), Dst: fa:49:b6:ff:50:30
(fa:49:b6:ff:50:30)
    Destination: fa:49:b6:ff:50:30 (fa:49:b6:ff:50:30)
    Source: MicroStarINT_35:f2:9a (d8:cb:8a:35:f2:9a)
    Type: IPv4 (0x0800)
    [Stream index: 0]
Internet Protocol Version 4, Src: 10.60.9.69, Dst: 8.8.8.8
Internet Control Message Protocol
```

Paquet destiné à l'adresse IP d'un autre appareil au sein du même réseau IP :

```
Frame 485596: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface
\Device\NPF_{8CA5DE3B-06FD-4657-A2E1-67C2BC69E370}, id 0
Ethernet II, Src: MicroStarINT_35:f2:9a (d8:cb:8a:35:f2:9a), Dst: Google_55:87:1a
(38:8b:59:55:87:1a)
    Destination: Google_55:87:1a (38:8b:59:55:87:1a)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: MicroStarINT_35:f2:9a (d8:cb:8a:35:f2:9a)
    Type: IPv4 (0x0800)
    [Stream index: 3]
Internet Protocol Version 4, Src: 10.60.9.69, Dst: 10.60.9.54
Internet Control Message Protocol
```

Table de routage de la l'émetteur :

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0        10.60.9.1       10.60.9.69    281
         10.60.9.0    255.255.255.0         On-link        10.60.9.69    281
        10.60.9.69  255.255.255.255         On-link        10.60.9.69    281
       10.60.9.255  255.255.255.255         On-link        10.60.9.69    281
```

Destination inexistante

Si l'adresse IP de destination n'est pas située dans la table de routage de l'émetteur ou qu'aucune réponse ARP n'est reçue pour la destination locale, l'envoi sera abandonné puisqu'il sera impossible de déterminer l'adresse MAC de destination.

Domaines de diffusion (Broadcast)

Un domaine de diffusion est la portée d'un réseau à travers laquelle deux hôtes peuvent communiquer directement ensemble à la couche de liaison de données. Au sein de cette bulle, deux hôtes devront généralement se situer dans le même sous-réseau IP afin d'être en mesure de s'identifier mutuellement dans leurs tables ARP pour composer les trames ethernet destinées à l'adresse MAC de destination. Il est possible d'héberger plusieurs sous-réseaux IP dans un seul domaine de diffusion mais dû à l'ensemble des protocoles opérant à la couche de liaison de données (particulièrement DHCP), il est préférable de se limiter à un réseau IP par domaine de diffusion.

Les sous-réseaux IP qui seront identifiés comme directement connectés à une interface dans la table de routage d'un hôte sont considérés comme les sous-réseaux auxquels un hôte pourra communiquer directement par adresse MAC de destination plutôt que par adresse IP. L'hôte consultera ainsi sa table de routage et sa table ARP pour déterminer à qui acheminer son trafic.

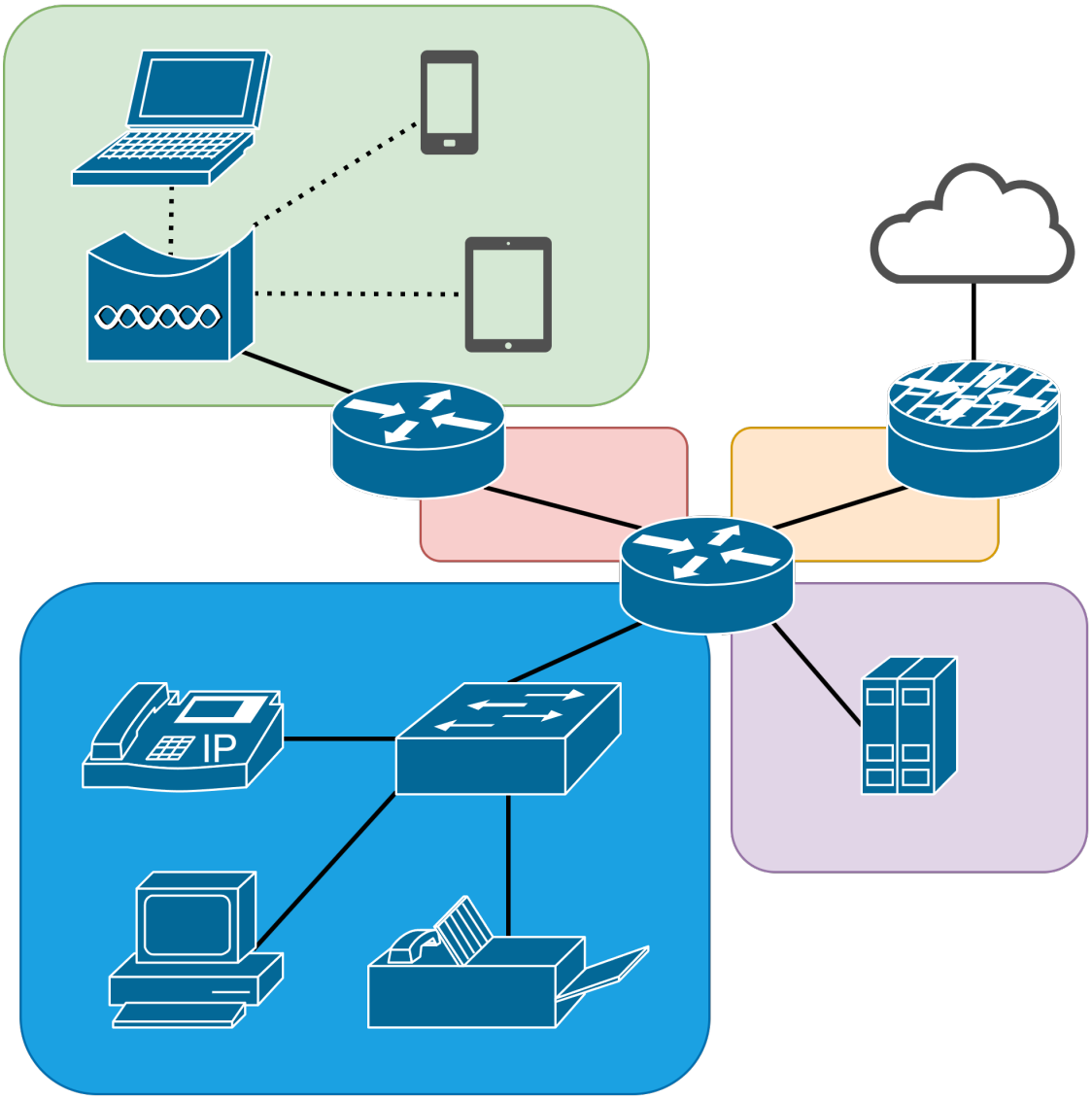
Il faut comprendre qu'au sein d'un domaine de diffusion, on doit observer le contenu des trames ethernet plutôt que des paquets IP et que les communications sont destinées aux adresses MAC (Contrôle d'Accès au Média) des hôtes. Cette adresse identifie de façon unique une interface pouvant communiquer avec le réseau à la couche de liaison de données. Chaque interface d'un appareil réseau doit avoir une adresse MAC unique. Un routeur possède une adresse MAC unique sur chaque interface, chaque pont, chaque VLAN et chaque interface de rebouclage (loopback). Chaque pont ou switch possède une table associant les adresses MAC observées aux interfaces par lesquelles du trafic originant de cette adresse. C'est à cette liste que se réfèrent ces appareils pour décider où acheminer une communication.

Au sein d'un domaine de diffusion, il est possible d'acheminer une copie du trafic à une destination unique (unicast), à plusieurs destinations (multicast) et à tous les hôtes situés dans le réseau IP ou domaine de diffusion (broadcast). Acheminer le trafic à plusieurs destinations permet d'optimiser la bande passante d'un réseau en évitant de devoir répéter la même information pour chaque hôte demandant l'information.

Advenant le cas où une information devrait être acheminée à l'extérieur d'un domaine de diffusion (ex. Internet), il faudra acheminer ce trafic à une passerelle (ex. un router) pour permettre au trafic d'être transféré d'un domaine de diffusion à un autre jusqu'à la livraison de la donnée à sa destination.

Dans l'exemple suivant, chaque encadré représenterait un domaine de diffusion de ce réseau. En haut à gauche, tous les appareils sans-fil seraient regroupés dans une même bulle et pourraient se contacter directement sans l'intermédiaire d'un routeur mais le routeur sera nécessaire pour contacter l'extérieur de leur réseau. La bulle en bas à gauche est le même concept mais plutôt que

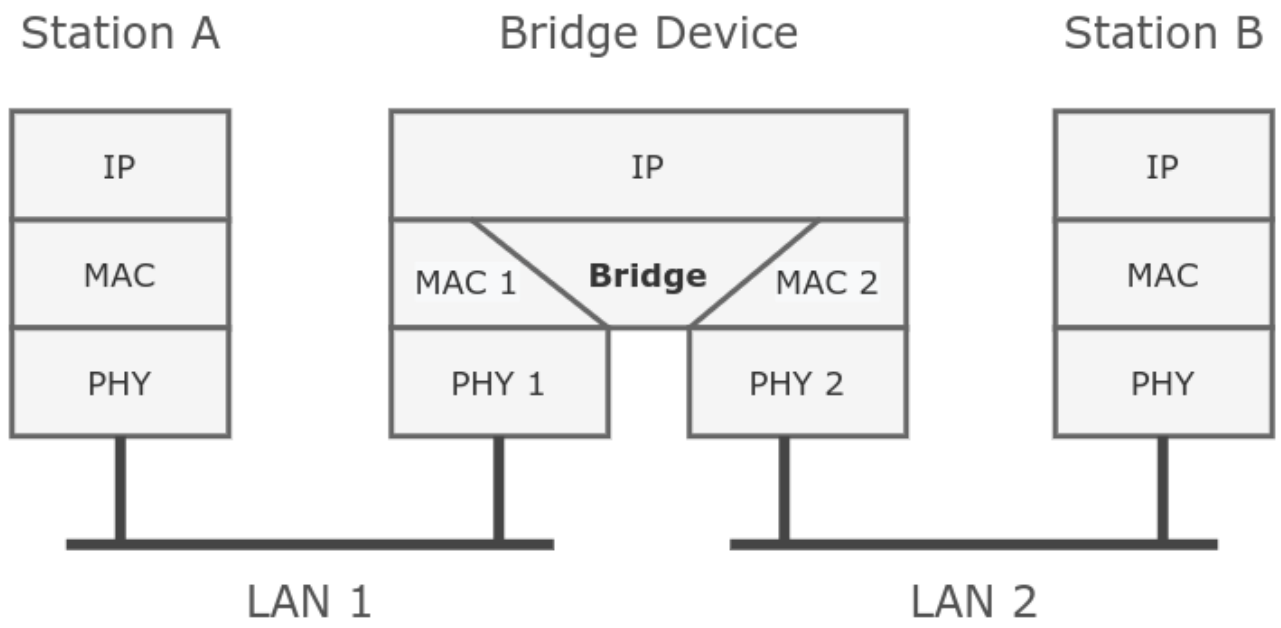
d'être regroupés ensemble par un point d'accès sans-fil, le domaine de diffusion est étendu par un commutateur.



Pontage (bridging)

Pour permettre de regrouper plusieurs appareils au sein d'un seul domaine de diffusion, il est nécessaire de relier plusieurs interfaces d'un appareil de mise en réseau (switch, routeur, pare-feu, etc.) dans un même domaine de diffusion. Qu'il s'agisse d'un hôte muni de plusieurs interfaces réseau, d'un point d'accès sans-fil, d'un routeur ou d'un commutateur, ponter deux interfaces ou plus permet de transmettre un broadcast à travers l'appareil pour en joindre un autre.

Dans le schéma suivant, l'appareil sur lequel un pont est configuré a seulement deux interfaces qui y sont reliées mais plus d'interfaces pourraient y être ajoutées au besoin.



Il est possible d'assigner une adresse IP à un bridge pour permettre à l'appareil pontant les interfaces d'interagir avec les appareils au sein du réseau qu'il étend. Un bridge a par conséquent aussi une adresse MAC unique et c'est cette adresse MAC qui sera observée lorsqu'un appareil sera branché derrière un port "esclave" du pont.

Un routeur sans-fil domestique est généralement configuré avec une interface dotée d'un client DHCP faisant face au réseau étendu et d'un pont regroupant quatre interfaces ethernet et deux radios WiFi donnant accès au même réseau local pour permettre aux appareils au sein du réseau d'interagir ensemble. On pourrait ici penser à un iPad ecleart un Apple TV ou un ordinateur et une imprimante.

Un prolongateur de portée sans-fil est un appareil muni de deux interfaces WiFi, une se connectant à un point d'accès existant et une autre rediffusant un autre réseau sans-fil. Ces deux interfaces étant pontées, un appareil se connectant au réseau diffusé par le "prolongateur de portée" (qui est

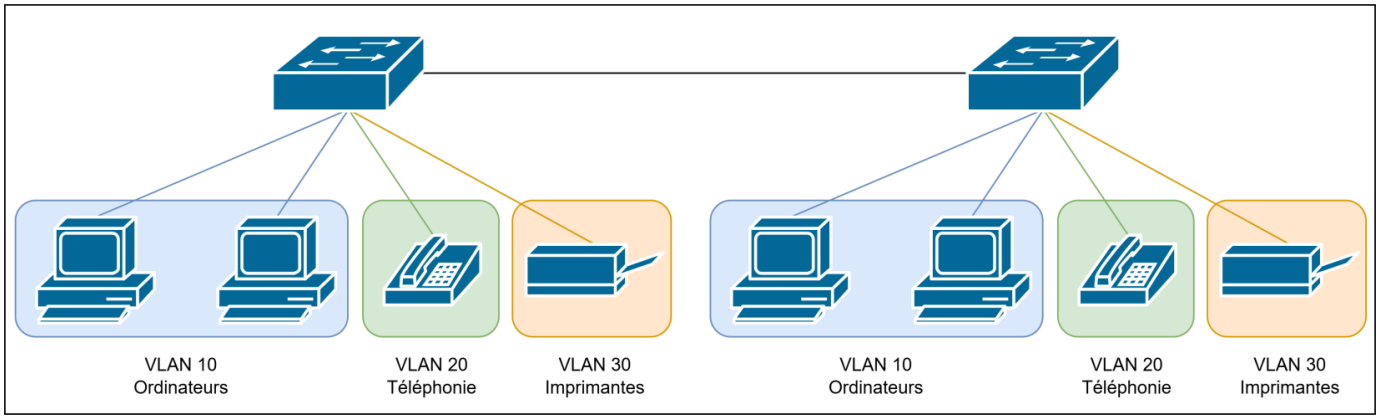
en réalité un pont sans-fil) se retrouve dans le même réseau que ceux reliés au réseau sans-fil principal.

Un commutateur est par défaut un appareil dont tous les ports font partie d'un seul pont. Il sert à étendre la portée d'un réseau unique, de permettre d'y relier plus d'appareils qui pourront communiquer ensemble sans l'entremise d'un routeur. Certains routeurs permettent aussi de ponter leurs interfaces. On peut penser ici à un appareil exécutant MikroTik RouterOS. Par défaut dans la majorité des modèles, les interfaces sont séparées mais il est possible de créer un pont et d'y relier plusieurs interfaces.

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.

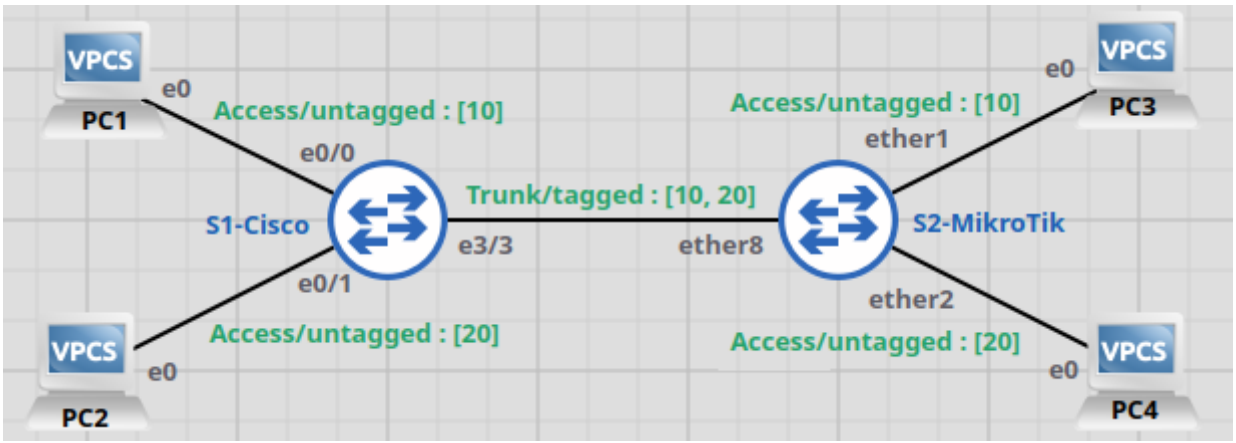
Différents manufacturiers ont différentes appellations pour ce mécanisme. Cisco à titre d'exemple appelle les liens entre différents appareils permettant le transport de plusieurs VLANs simultanément des "trunks" et décrit les ports donnant accès à un certain VLAN sans nécessiter d'étiquette entre l'appareil 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

.