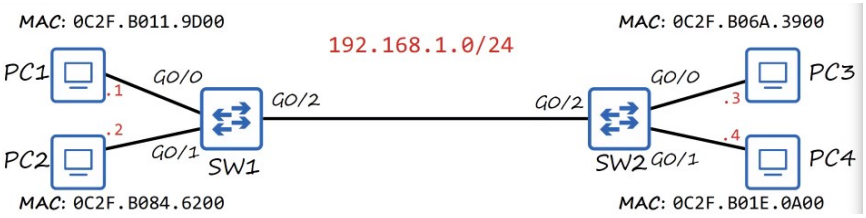
Cours 6 : Ethernet LAN Switching

Dans ce cours nous allons apprendre comment fonctionne le réseau localemement dans un LAN (Local Area Network). Le préambule et le SFD ne sont pas considérés comme faisant partie de l'entête Ethernet.
De plus la taille de l'entête Ethernet avec le trailer est de 18 bytes (6 + 6 + 2 + 4)
Il y a aussi une taille minimal pour un frame Ethernet (Entête + Payload + Trailer) qui est de 64 bytes.
Les 64 bytes – 18 bytes (header + taille du trailer) = 46 bytes
La taille minimal pour la taille d'un payload (paquet) est de 46 bytes.
Si le payload est de moins de 46 bytes d'autres bytes sont ajoutés.
Par exemple si l'on a 34 byte de paquet + 12 byte de padding = 46 bytes.

Dans le schéma suivant nous allons assigner des adresses IP aux différents PC sur l'adresse réseau : 192.168.1.0/24



Lorsqu'un appareil veut communiquer avec un autre appareil il n'inclut pas seulement son adresse MAC comme on a pu le voir dans le cours précédent.
Dans l'entête sera inclus l'adresse IP source, l'adresse IP de destination, l'adresse MAC source mais le PC1 ne connais actuellement pas l'adresse MAC de destination.
Lorsque l'on veut envoyer une donnée c'est l'adresse IP qui est indiqué.
Imaginons que le PC1 veut envoyer une donnée vers le PC3, pour se faire il doit tout d'abord découvrir l'adresse MAC du PC correspondant à la destination. Pour se faire il va utiliser le protocole ARP (Address resolution Protocol) qui va découvrir les adresses MAC présente sur le réseau.

- ARP est l'acronyme de « Address Resolution Protocol »
- il est utilisé pour découvrir la couche 2 (l'adresse MAC) à partir d'une adresse de couche 3 connu (l'adresse IP)
- Le protocole consiste en 2 messages : la requête ARP et la réponse ARP.
- La requête ARP est envoyé en Broadcast (envoyé à tous les hôtes sur le réseau)
- La réponse ARP est envoyé en Unicast (envoyé seulement à un seule hôte, celui qui envoie la requête)

L'adresse utilisé en Broadcast pour connaître les adresse MAC est : FFFF.FFFF.FFFF
PC1 envoie la requête ARP au SW1, le SW1 ajoute l'adresse à la table d'adresse MAC, de cette manière l'adresse MAC est apprise dynamiquement. La requête ARP est envoyé au interface, le PC2 reçoit la requête mais puisque la requête ne lui est pas adressé il n'accepte pas la requête.
Le SW2 reçoit aussi la requête et ajoute l'adresse MAC du PC1 à sa table d'adresse MAC.
Le SW2 redistribue la requête sur ses interfaces, le PC4 reçoit la requête mais ne l'accepte pas, le PC3 accepte la requête puisque c'est son adresse IP qui correspond à la requête.
Une fois la requête reçu le PC3 va renvoyer une réponse au PC1 en Unicast pour confirmer la réception. La réponse va s'ajouter aux table d'adresse MAC du SW2 et du SW1, la réponse est ensuite reçu pas le PC1.

On peut utiliser la commande `arp -a` pour voir la table ARP (Windows, MacOS, Linux)

- L'adresse Internet est l'adresse IP (l'adresse de couche 3)
- L'adresse Physique est l'adresse MAC (l'adresse de couche 2)
- Si le Type est en statique cela signifie que c'est une entrée par défaut.
- Si le Tyoe est en dynamic cela signifie qu'il est appris par ARP

```
C:\Users\user>arp -a

Interface: 169.254.146.29 --- 0x9
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.167 --- 0xd
  Internet Address      Physical Address      Type
  192.168.0.1           98-da-c4-dd-a8-e4     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Il est possible d'utiliser un logiciel pour simuler le réseau appelé GNS3 mais aussi un logiciel Cisco appelé Packet Tracer plus simple d'utilisation.

A présent que l'adresse du PC1 est connu il est possible de tester la connexion en lançant une requête ping.
Le ping est très utile il est utilisé pour tester la connectivité.
- Il mesure le temps que la requête prend pour être réceptionné
- Il utilise deux messages : Une requête Echo ICMP, Une réponse Echo ICMP

C'est similaire au requêtes et réponses ARP
- La commande pour utiliser ping est : `ping (ip address)`

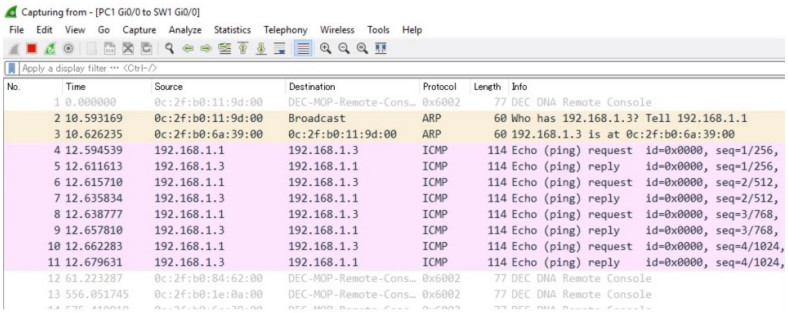
voici la capture d'écran d'une requête ping :

```
PC1#
PC1#ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 20/20/22 ms
PC1#
```

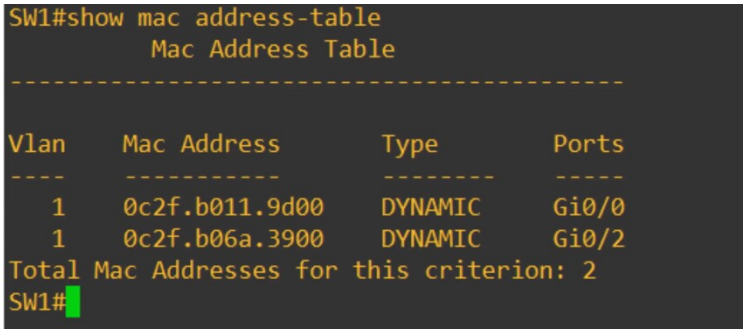
Pourquoi la y a t-il une requête qui n'a pas fonctionné sur les 5 envoyé ?
C'est parce que la première requête était une requête ARP pour connaître l'adresse MAC
La commande pour voir la table ARP sur le switch est `show arp`

```
PC1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.1.1              -  0c2f.b011.9d00  ARPA   GigabitEthernet0/0
Internet  192.168.1.3             34  0c2f.b06a.3900  ARPA   GigabitEthernet0/0
PC1#
```

Voici une capture d'écran sur Wireshark sur laquelle on peut voir la requête ARP envoyé avec la réponse ARP.



Voici à présent la commande pour voir la table d'adresse MAC sur un Switch Cisco :
`SW1#show mac address-table`



Comme on peut le voir il y a la section Vlan pour indiquer le numéro de Vlan, l'adresse MAC, le type, et le numéro de port/interface

Les adresses MAC se retirent automatiquement après 5 minutes d'inactivité c'est aussi appelé « aging ».
Il est aussi possible de supprimer manuellement l'adresse MAC de la table en utilisant la commande :
`SW1#clear mac address-table dynamic`
ou bien si l'on veut supprimer une seule adresse MAC :
`SW1#clear mac address-table dynamic address 0c2f.b011.9d00`
Il est aussi possible de supprimer les adresses MAC se trouvant sur une seule interface :
`SW1#clear mac address-table dynamic interface Gi0/0`