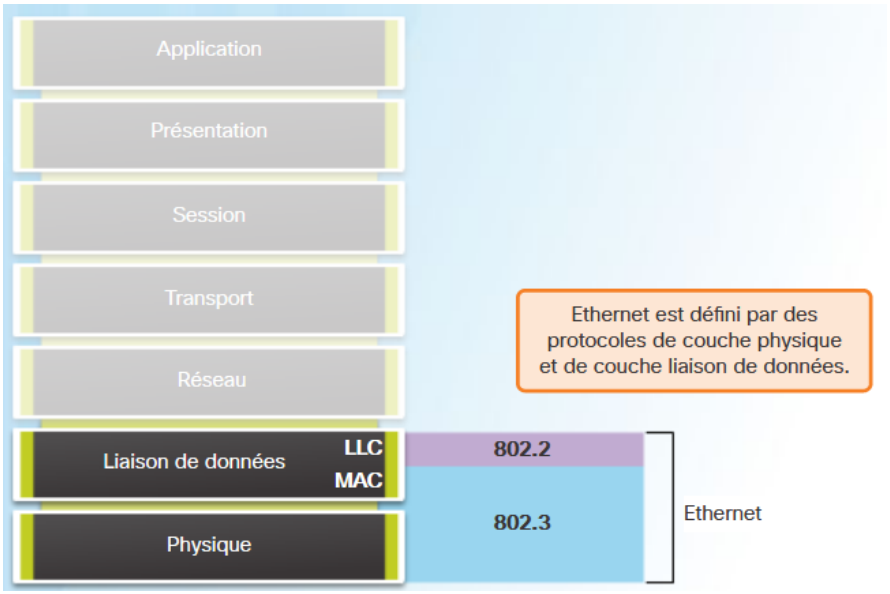
Chapitre 5 : Ethernet

Ethernet est la technologie **LAN la plus utilisée aujourd'hui**. Elle se positionne sur la couche liaison de données et prend en charge des bandes passantes de 10, 100, 1.000, 10.000, 40.000 et 100.000 MBit/s. Cette norme définit un protocole de la couche 2 et 3 et se divise en deux sous-couches :

- **LLC** (**sous couche de liaison logique**) qui gère la communication entre les couches **supérieures et inferieures**. Cette couche est **tout à fait logicielle** et indépendante du matériel.
  .
- **MAC** La sous-couche inferieure, elle est mise en œuvre au niveau matériel des cartes réseau de la machine.

Ethernet fut créé en 1973 et n'a cessé d'évoluer pour augmenter sa bande passante et devenir plus flexible.



1 Sous-couche MAC

Cette sous couche à deux objectifs : encapsuler les données et contrôler l'accès au support.
Cette sous couche en charge de l'encapsulation gère :

- **La délimitation des trames** permettant la synchronisation de l'émetteur avec le récepteur
- **L'adressage** physique de la trame
- **Détection des erreurs**

La sous couche gère aussi l'accès au support et vérifie ainsi la disponibilité de celui-ci et les éventuelles collisions.

La structure d'une trame Ethernet est la suivante :

La trame Ethernet se présente comme suit, sa taille peut varier entre 64 et 1.518 octets et toute trame plus petite ou plus grande sera interprétée comme un fragment de collision.

Préambule	Adresse de destination	Adresse source	Type	Données	Contrôle de trame
8 octets	6 octets	6 octets	2 octets	46 à 1500 octets	4 octets

- **Préambule** Délimiteur de trame (SFD) utilisé pour synchroniser l'émetteur avec le récepteur
- **Adresse MAC de destination** L'identifiant physique du destinataire permettant une monodiffusion, multidiffusion ou une diffusion
- **Adresse MAC source** L'identifiant d'origine de la trame
- **EtherType** Un champ identifiant le protocole de la source précédente
- **Données** Les données encapsulés de la couche supérieur
- **Fin de trame (FCS)** Permettant de détecter les erreurs de trame et de la terminer

Si la trame est incomplète au niveau d'un commutateur, celle-ci **est abandonnée.**

La taille minimale d'une trame Ethernet est de **64 octets** et la taille maximale est de **1518 octets**. Une trame de collision ou **Runt** est inférieure à 64 octets

Exemple : Quelques types de protocoles :

- 0x800 pour IPv4
- 0x86DD pour IPv6
- 0x806 pour ARP

2 Adresse MAC

La base hexadécimale est utilisée pour les adresses MAC. Il se présente comme un système de nombre de 0 À 9 et de A à F :

Équivalents décimaux et binaires des caractères hexadécimaux 0 à F

Décimal	Binaire	Hexadécimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

On représente une adresse MAC en regroupant les caractères hexadécimaux par paire et en les séparant par des - ou des : ou bien par le regroupement par 4 et la séparation par des points.

Exemple :

00-05-9A-3C-78-00
00:05:9A:3C:78:00
0005.9A3C.7800

Une adresse MAC est constituée de deux parties de 24 Bits, l'une définie par la IEEE et propre a chaque constructeur et une autre laissée au choix du constructeur. Ainsi, on est assuré qu'une adresse MAC **est unique au niveau mondial**. Ce système est appelé ***OUI* pour Organizationally Unique Identifier**.

Le plus souvent l'adresse MAC est gravée dans la mémoire morte de la carte réseau, elle est ainsi dite rémanente (BIA). On peut toutefois la changer logiciellement dans le système d'exploitation. Lors du démarrage, cette adresse est stockée dans la mémoire vive pour être utilisée.

Quand un paquet atteint la carte réseau, la carte réseau compare l'adresse MAC de destination par rapport a celle stockée en mémoire vive et interprète le paquet s'il est la destination.

Les commutateurs utilisent deux types de méthodes pour transférer les trames vers le port associé :

- **Cut-Through** : Achemine la trame avant qu'elle **ne soit complètement lue** et ne contrôle pas les erreurs ; dans la variante fast-forward, les donnes sont immédiatement transmises et cela peut poser certains problèmes mais permet un fort débit ; La seconde variant Fragment-free consiste à stocker les 64 premier octets avant de conclure à un port vers lequel communiquer et procéder à un petit check des erreurs de trames
- **Store and Forward** : **Enregistre la trame dans la mémoire** et pendant que la trame est en train d'être enregistrée, le commutateur décide du port vers lequel acheminer la trame et procède à un test de redondance cyclique (**CRC**) en analysant l'en-queue de la trame pour **vérifier que la trame et valide** pour ne pas engorger le réseau de données invalides.

Pour permettre une bonne transmission, les commutateurs sont munis de mémoire tampons pouvant être de deux types :

- **Axé sur les ports** Les trames sont stockées dans les files d'attente associés à chaque port entrant et sortant ; les donnes sont transmises dès que le port se libère
- **Mémoire partagée** Un seul mémoire reprend toutes les trames et le port de destination est alloué dynamiquement

Le protocole Ethernet peut fonctionner en semi-duplex ou en duplex intégral. Lors d'une connexion sur un commutateur ou un autre périphérique, les deux périphériques échangent des informations pour choisir le moyen de transmission en fonction du système offrant la meilleure bande passante. Si on ne s'accorde pas on risque beaucoup de collisions sur le canal provenant du système en semi-duplex.

Un autre point sur lequel s'accorder est le type de câble utilisé. Pour éviter une configuration, on utilise le **système Auto-MDIX** permettant, par de multiples échanges entre commutateur et autre périphérique de conclure au type de câble utilisé et ainsi de modifier les configurations en conséquence.

3 ARP (Address Resolution Protocol)

Si l'adresse IP de destination n'appartiens pas au réseau actuel, la machine l'envoie automatiquement à la passerelle, une machine de couche 3 permettant de faire la liaison avec un réseau distant.

Pour associer une adresse IP aux adresses MAC le long du chemin on utilise le protocole ARP permettant de résoudre les adresses MAC et de tenir une table de mappage.

Pour résoudre les adresse MAC à partir de l'adresse IP d'un périphérique, il consulte la table de mappage contenu dans sa mémoire vive. Si l'adresse MAC correspondante n'est pas présente, il envoie une requête ARP sur le réseau.

Une requête ARP contient dans son corps, soit l'adresse IP cible soit l'adresse MAC cible dont il faut compléter le couple. Et la trame Ethernet de ce type de requête contient en en-tête :

- **L'adresse MAC de diffusion** permettant à chacun de répondre **(FFFF.FFFF.FFF)**
- **L'adresse MAC source** de la machine émettrice
- **Le type de trame** soit 0x806 dans le cas d'une requête ARP

Après cette requête seul la machine correspondant à l'IP renseignée dans le corps répond avec l'adresse IP de l'expéditeur et son adresse MAC. Et s'accompagne d'une trame Ethernet standard de monodiffusion avec le type ARP. Dès que le périphérique émetteur reçoit la réponse il l'ajout à sa table de mappage et envoie la trame prévue.

Les entrées de la table de mappage sont rapidement effacées si elles ne sont pas utilisées depuis un certain temps mais cela dépend du système d'exploitation.

Pour afficher la table de mappage on peut utiliser la commande `show ip arp` sur les appareils Cisco ou `arp -a` sur windows 7.

Si de nombreuses demandes ARP sont diffusés en même temps sur un réseau à faible bande passante cela peut inonder le réseau, mais ce genre de perte de performances reste minimes.

Dans la table d'adresse mac enregistrées par le commutateur, on trouve les adresses source **des trames entrantes de la couche 2**.

La table ARP d'un commutateur mappe une adresse de **couche 3 à une adresse de couche 2 dans le réseau local.**

Certains pirates peuvent se faire passer pour un autre périphérique en **répondant à certaines requêtes ARP** qui ne lui sont pas destinées et ainsi empoisonner la table de mappage du périphérique (**USURPATION**). De plus une **multitude de requêtes ARP peuvent ralentir le réseau**.