

I. Modèle OSI et Ethernet

Le modèle OSI permet de standardiser les protocoles.

Couche physique : Transmet les bits sur un canal sous forme électrique (0 ou 1).

Couche de liaison : Simule une liaison parfaite en détectant et corrigeant les erreurs de transmission. Découpe les séquences en paquets. Régularise le flux.

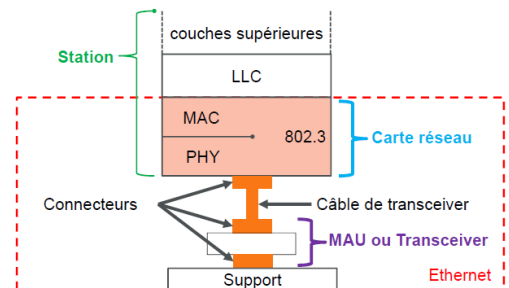
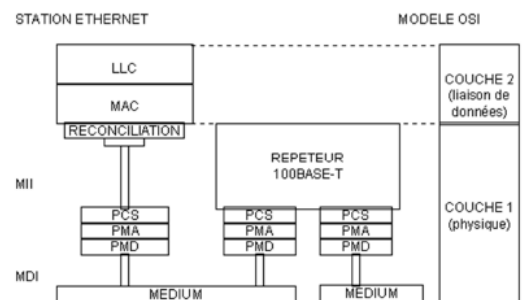
« Pour Le Réseau Tout Se Passe Automatiquement »

7. Application
6. Présentation
5. Session
4. Transport
3. Réseau
2. Liaison
1. Physique

II. Architecture Ethernet

L'architecture Ethernet se base sur diverses normes IEEE 802.xx. Elles standardisent le déploiement (802, 802.3), la gestion (802.1), ou les protocoles des réseaux (802.2, 802.10).

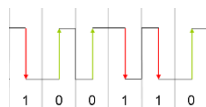
- **LLC (Logical Link Control) :**
Contrôle d'erreur
- **DTE : Data Terminal Equipment (carte réseau)**
 - **MAC (Media Access Control) :** Gestion trames et contrôle d'accès au média
 - **PHY (Physical Signaling Layer)**
 - Assemblage des trames (encapsulation des données) et détection d'erreurs
 - Contrôle de l'accès aux médias
- **MAU (Medium Access Unit) (= DCE = Transceiver) :**
interface d'accès au support physique
- **PCS (Physical Coding Sublayer) :**
Codage physique des signaux sur le câble
- **PMA (Physical Medium Attachment) :**
Connexion sur le câble
- **PMD (Physical Medium Dependent) :**
Définit la « connectique » et l'interface physique de connexion sur le câble



III. Accès au support

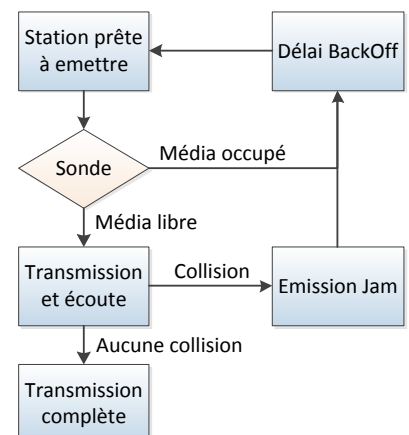
1. Codage de l'information : codage Manchester

- Front montant : 1
- Front descendant : 0



2. Types d'accès

- **Accès par élection (centralisé ou distribué) :**
Token Ring
- **Accès par compétition (résolution de collision) :**
CSMA/CD (Carrier Sense Multiple Access with Collision Detection) voir ci-contre



IV. Format de trame

Préambule	SOF Start Of Frame	Adresse destinataire	Adresse source	Type / Longueur	Données	FCS Frame Check Sequence
7 octets	1	6	6	2	46-1500	4
10101010	10101011					

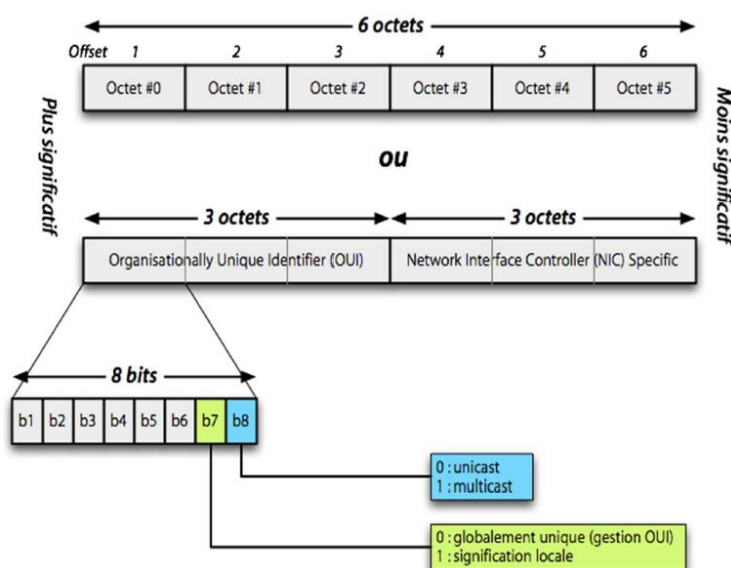
- Préambule : Syncho des horloges par suite de 0 et 1.
- Adresses : MAC sur 6 octets (ou broadcast FF:FF:FF:FF:FF:FF = tout le monde)

Jumbo Frame permet de transférer des packets de 1518 à 9000 octets. (sur réseaux Gbits)

V. Méthodes de diffusion de trames sur un réseau

- **Unicast** : un vers un
- **Broadcast** : un vers tous
- **Multicast** : un vers groupe

VI. Adressage MAC : XX:XX:XX:XX:XX:XX



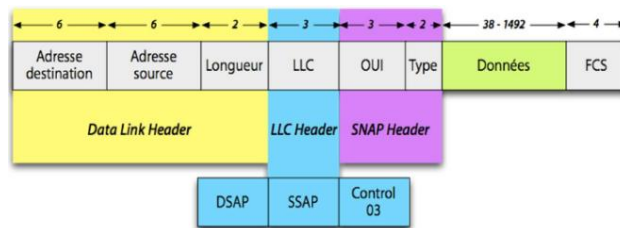
VII. Matériel Ethernet

- **Multirépéteurs (Niveau 1) / Multitransceivers** (Entre niveaux 1 et 2)
- **Pont Ethernet** : (Niveau 2) Répéteur de trames. Relie deux réseaux Ethernet.
 - **Spanning Tree** : évite les boucles sur un réseau avec ponts.
 - **Ethernet learning bridge** : écoute les réseaux pour faire une table d'adresse. Ne fait passer les trames que si nécessaire et si valides. Possibilité de filtrage.
- **Ethernet commuté (switching)** : réseau en étoile. Plusieurs interfaces E/S toutes reliées.
 - **Flooding** : Une trame vers adresse inconnue envoyée sur tous les ports
 - **Store and Forward Switching** : comme les ponts. Obligatoire si vitesses asymétriques. Vérifie la validité des trames. Possibilité de filtrage.
 - **Cut Through Switching** : Trame renvoyée dès que l'adresse est lue. Pas de vérif.

VIII. LLC : Logical Link Control

Contrôle d'erreur et contrôle de flux. Fiabilise MAC.

- LLC1 : mode datagramme (non connecté, non fiable)
- LLC2 : mode connecté (type HDLC)
- LLC3 : mode non connecté, avec acquittement



En tête LLC :

- **DSAP / SSAP** : Destination / Source Service Access Point (protocole destinataire et émetteur)
- **Control** : UI (Unnumbered Info (gestion de liaison)) / I (Info) / S (Supervision (flux d'erreur))

SNAP : Subnetwork Attachment Protocol : permet de spécifier bcp de protocoles.

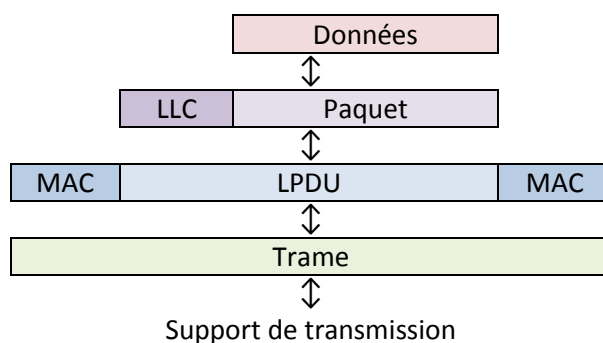
IX. Synthèse de transmission de trame

Emission :

- Lecture les données et l'adresse de destination venant de LLC
- Fabrication la trame
- Attente l'indication de média libre de PHY avant émission la trame
- Si collision indiqué par PHY, traitement, sinon indication de succès à LLC

Réception :

- Lecture de trame et décodage de l'adresse de destination (vérif si celle de la station)
- Vérification CRC et longueur de trame et envoi d'état de réception à LLC
- Communication des données et adresse source à LLC.



X. Virtualisation Ethernet (VLAN)

Permet de **séparer un réseau Ethernet physique en plusieurs réseaux virtuels**. Se configure en assignant divers ports d'un **switch** selon des réseaux différents. Un port configuré pour un réseau ne peut communiquer qu'avec les ports configurés pour ce même réseau.

On peut avoir un port « **trunk** » pour faire passer les trames de **tous les VLAN**, par exemple pour relier deux switches. Si elles passent par un trunk, les trames sont marquées, sinon elles ne le sont pas.

1 IP par VLAN.

XI. Sécurité

1. Couche physique

- **Les risques :**
 - Ecoute de la communication
 - Interception
 - Multiplicité des supports
- **Attaque :** Accéder physiquement au réseau
- **Défense :** Eliminer les possibilités de connexion
- **Solutions :**
 - Limiter l'accès aux salles réseaux
 - Chasser les petits switch de bureau et les points d'accès wifi « sauvage »
 - Chasser les prises actives (débrancher ou désactiver les prises)
 - Wifi (Chiffrer les communications, éloigner des zones publiques, protéger la connexion au réseau)

2. Couche de liaison

- **Les risques :**
 - « Man in the middle »
 - VLAN hopping (changement de VLAN)
 - Attaque contre le switch (MAC flooding)
 - Perturbation de services tels que le DHCP
- **Les attaques :**
 - MAC flooding : saturation de la table MAC
 - Utilisation d'un serveur DHCP pirate pour rediriger la communication vers soi
 - Former des paquets pour changer de VLAN
 - Usurper une adresse MAC
- **Solutions :**
 - Limiter le nombre d'adresses MAC utilisables sur un port de commutateur.
 - Couper un port en cas d'anomalie
 - Spécifier le port qui doit relayer le DHCP
 - Autoriser la connexion d'un PC après authentification (serveur Radius)
 - Surveiller les couples Adresse MAC - IP