

Lab- Analyse de trames

les séquences hexadécimales ci-dessous représentent deux trames Ethernet capturées par un logiciel de capture de trames. En vous basant sur le format d'une trame Ethernet et des paquets arp fourni en annexe.. vous devez :

1. identifier les adresses sources et de destination MAC et IP.
2. interpréter le reste des champs des deux trames
3. déterminer l'objectif de cet échange de trames.

PS : Ne pas prendre en compte le préambule le délimiteur et le FCS de trame lors de l'analyse.

Trame 1

```
ff ff ff ff ff ff 00 60 08 61 04 7b 08 06 00 01 08 00 06 04 00 01 00
60 08 61 04 7b 0a 0a 9f 02 00 00 00 00 00 00 0a 0a 01 01
```

Trame 2

```
00 60 08 61 04 7b 00 01 02 af f5 e2 08 06 00 01 08 00 06 04 00 02 00
01 02 af f5 e2 0a 0a 01 01 00 60 08 61 04 7b 0a 0a 9f 02 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

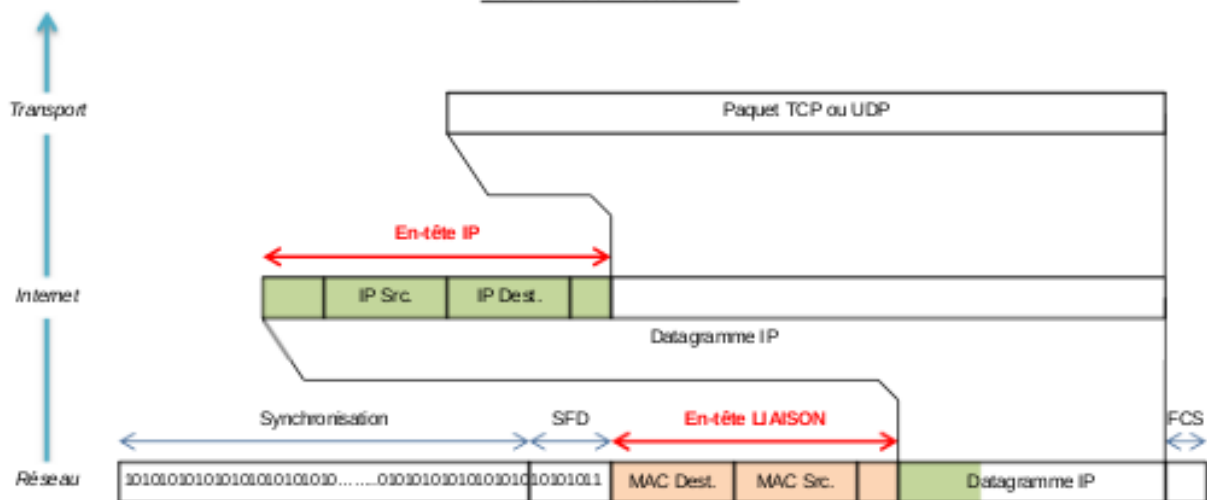
ANNEXES

Structure d'une frame Ethernet II

1 Structure générale.

C'est la frame que l'on rencontre dans la plupart des réseaux locaux actuels.

Schéma de la structure



Ce sont ces informations qui circulent sur le réseau

2 Trame ETHERNET II

AA = 10101010

AB = 10101011



Préambule : (7 octets) Permet la synchronisation des horloges de transmission. Il s'agit d'une suite de 1 et de 0 soit 7 octets à la valeur 0xAA

SFD : (1 octet) "Starting Frame Delimiter". Il s'agit d'un octet à la valeur 0xAB. Il doit être reçu en entier pour Valider le début de la trame.

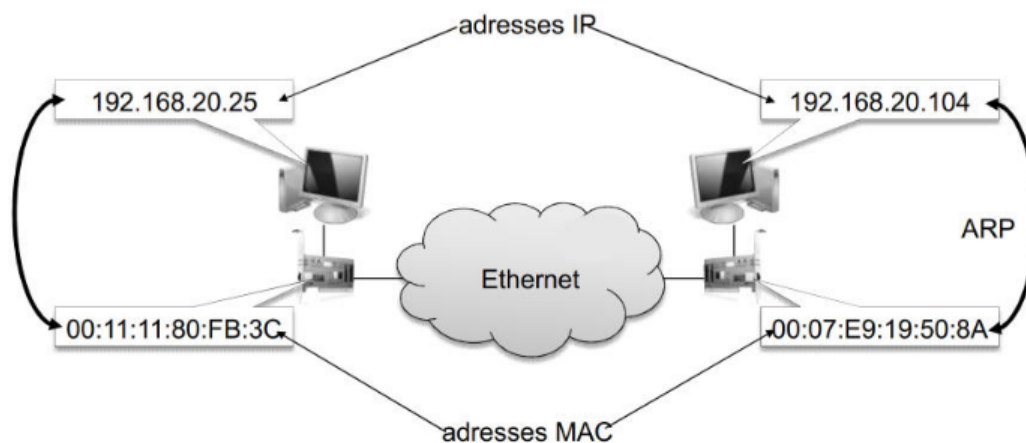
En-tête : (14 octets) - Adresse MAC du destinataire (6 octets)
- Adresse MAC de l'émetteur (6 octets)
- EtherType (Type de protocole) (2 octets)

Exemples de valeurs du champ EtherType →

FCS : (4 octets) Frame Check Sequence.
Ensemble d'octets permettant de vérifier que la réception s'est effectuée sans erreur.

EtherType	Protocole
0x0800	IPv4
0x0806	ARP
0x809B	AppleTalk
0x8035	RARP
0x86DD	IPv6

Les paquets ARP



Lorsqu'un hôte A souhaite émettre une trame à destination de l'hôte B dont il connaît l'adresse IP, il effectue au préalable une requête ARP en broadcast. Cette requête est de type « quelle est l'adresse MAC correspondant à l'adresse IP *adresseIP* ? Répondez à *monAdresseIP* ».

Toutes les hôtes vont recevoir la requête. L'hôte B qui possède cette adresse IP sera le seul à répondre en envoyant à la machine émettrice A une réponse ARP du type « je suis *adresseIP*, mon adresse MAC est *adresseMAC* ».

L'hôte A initialise alors sa table cache ARP (conservée en mémoire) en utilisant la réponse fournie. Les entrées dans cette table expirent après une temporisation donnée. Le cache ARP est consulté par un hôte juste avant l'envoi d'une requête ARP ; si la réponse se trouve dans le cache, la requête n'est pas effectuée.

