SAVOIRS	RESEAU	LE PROTOCOLE ARP

I. LE ROLE DU PROTOCOLE ARP

***ARP** : **A**ddress **R**esolution **P**rotocol*

Le protocole ARP permet de faire de la résolution d'adresse logique (adresse IP) en adresse physique (adresse MAC).
Ce protocole est indispensable pour que des équipements puissent communiquer sur un réseau local car, pour communiquer, les équipements doivent connaitre l'adresse MAC du destinataire.

À chaque trame placée sur un réseau doit correspondre une adresse MAC de destination. Quand un paquet est envoyé à la couche liaison de données pour être encapsulé dans une trame, le nœud désigne une table dans sa mémoire pour y trouver l'adresse de couche liaison de données qui est mappée à l'adresse IPv4 de destination. Cette table est appelée table ARP, ou cache ARP. La table ARP est stockée dans la mémoire vive (RAM) du périphérique.

Chaque entrée ou ligne de la table ARP comporte deux valeurs : une adresse IP et une adresse MAC. La relation entre les deux valeurs s'appelle une mise en correspondance : ce qui signifie simplement que si vous choisissez une adresse IP dans la table vous y trouverez l'adresse MAC correspondante. La table ARP garde en mémoire cache le mappage des périphériques du réseau local (LAN).

Pour lancer la procédure, un nœud émetteur tente de trouver l'adresse MAC associée à une adresse IPv4 de destination, dans la table ARP. Si ce mappage est dans la mémoire cache de la table, le nœud utilise l'adresse MAC comme destination MAC dans la trame qui encapsule le paquet IPv4. La trame est ensuite codée sur le support réseau.

II. MISE A JOUR DE LA TABLE ARP

La table ARP est mise à jour de manière dynamique.

Un périphérique dispose de deux méthodes pour obtenir des adresses MAC :

- La première consiste à surveiller le trafic sur le segment du réseau local. Quand un nœud reçoit des trames en provenance du support, il enregistre les adresses IP source et MAC dans la table ARP sous forme de mappage. Au fur et à mesure que les trames sont transmises sur le réseau, le périphérique remplit la table ARP de paires d'adresses.

- La seconde méthode permettant à un périphérique d'obtenir une paire d'adresses consiste à diffuser une requête ARP. Le protocole ARP envoie un message de diffusion de couche 2 à tous les périphériques du LAN Ethernet. La trame contient un paquet de requête ARP comportant l'adresse IP de l'hôte de destination. Lorsqu'un nœud reçoit la trame et identifie sa propre adresse IP, il répond en envoyant un paquet réponse ARP à l'expéditeur, sous la forme d'une trame monodiffusion (à une seule adresse MAC). Cette réponse permet de créer une nouvelle entrée dans la table ARP.

III. CREATION DE LA TRAME

Que fait un nœud lorsqu'il doit créer une trame et que le cache ARP ne contient pas la correspondance entre une adresse IP et l'adresse MAC de destination ?

Quand le protocole ARP reçoit une requête de mappage entre une adresse IPv4 et une adresse MAC, il recherche le mappage stocké en mémoire cache dans sa table ARP. S'il ne trouve pas d'entrée, l'encapsulation du paquet IPv4 échoue, et les processus de la couche 2 informent le protocole ARP qu'un mappage est nécessaire.

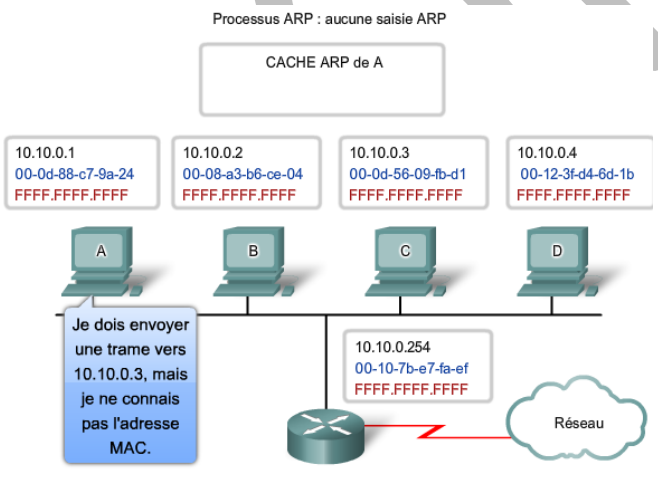
Les processus ARP envoient alors un paquet de requête ARP pour trouver l'adresse MAC du périphérique de destination sur le réseau local. Si le périphérique qui reçoit la requête possède l'adresse IP de destination, il répond à l'aide d'une réponse ARP. Une entrée est créée dans la table ARP. Les paquets à destination de cette adresse IPv4 peuvent à présent être encapsulés dans des trames.

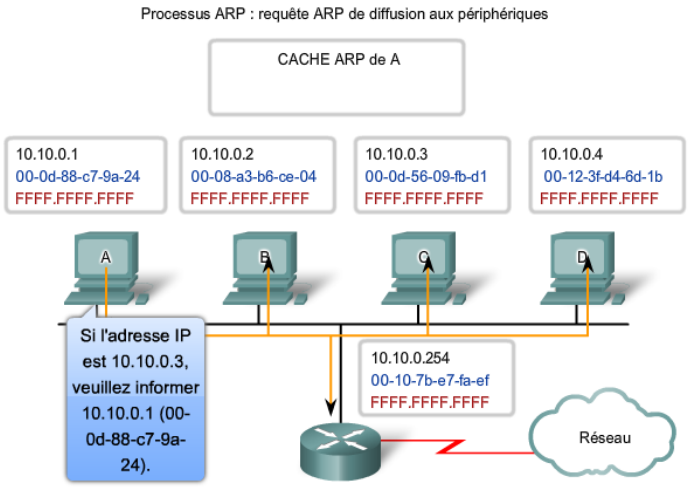
Si aucun périphérique ne répond à la requête ARP, le paquet est abandonné car il est impossible de créer une trame. L'échec de l'encapsulation est signalé aux couches supérieures du périphérique. Dans le cas d'un périphérique intermédiaire, comme un routeur, les couches supérieures peuvent choisir de répondre à l'hôte source en générant une erreur dans un paquet ICMPv4.

Procédure de résolution d'adresse logique en adresse physique :

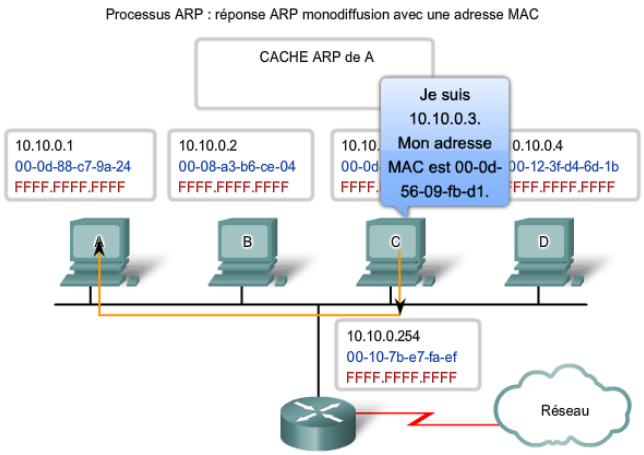
Etape 1 : 10.10.0.1 cherche qui est 10.10.0.3

Etape 2 : Envoyer une trame de broadcast en demandant qui est 10.10.0.3. Il envoie par la même occasion son adresse MAC

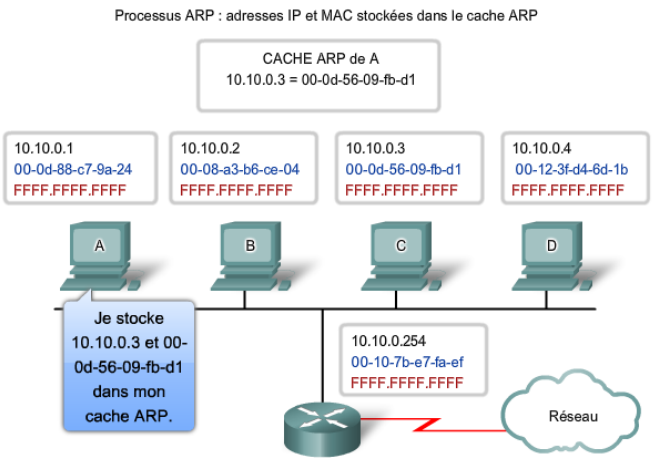


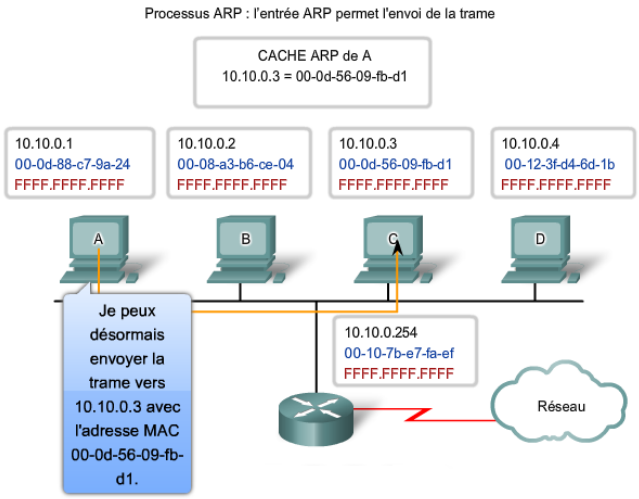


Etape 3 : La machine 10.10.0.3 répond en envoyant son adresse MAC.



Etape 4 : 10.10.0.1 stocke dans son cache ARP l'adresse MAC de 10.10.0.3.





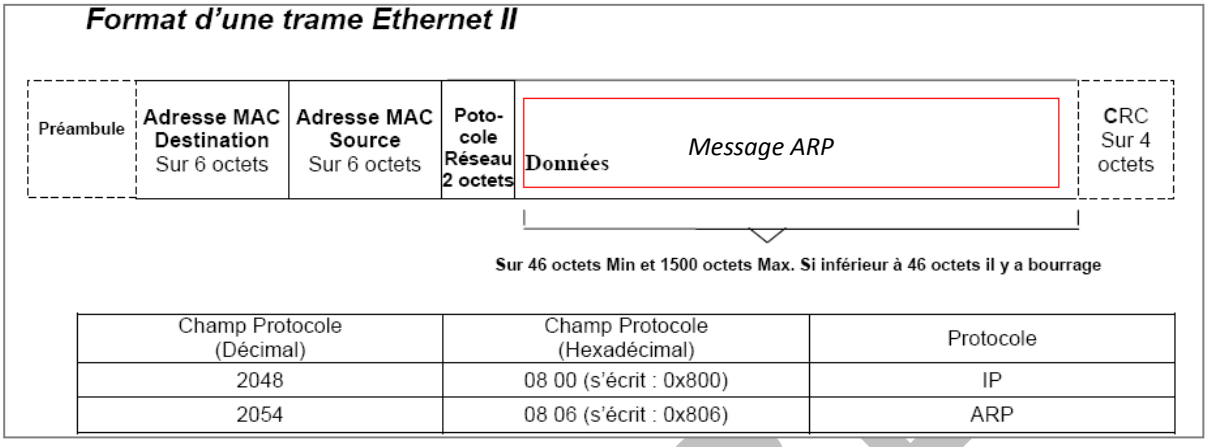
Etape 5 : 10.10.0.1 peut envoyer un message à 10.10.0.3

<u>Visualisation d'un cache ARP :</u>

```
C:\> arp -a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamique
  172.16.255.254        00-0c-85-cf-66-40     dynamique
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interface : 172.16.1.1 --- 0x60004
  Adresse Internet      Adresse physique      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamique
C:\>
```

IV. CONSTITUTION DE LA TRAME ARP

- Structure générale de la trame ARP :



Champ Protocole (Décimal)	Champ Protocole (Hexadécimal)	Protocole
2048	08 00 (s'écrit : 0x800)	IP
2054	08 06 (s'écrit : 0x806)	ARP

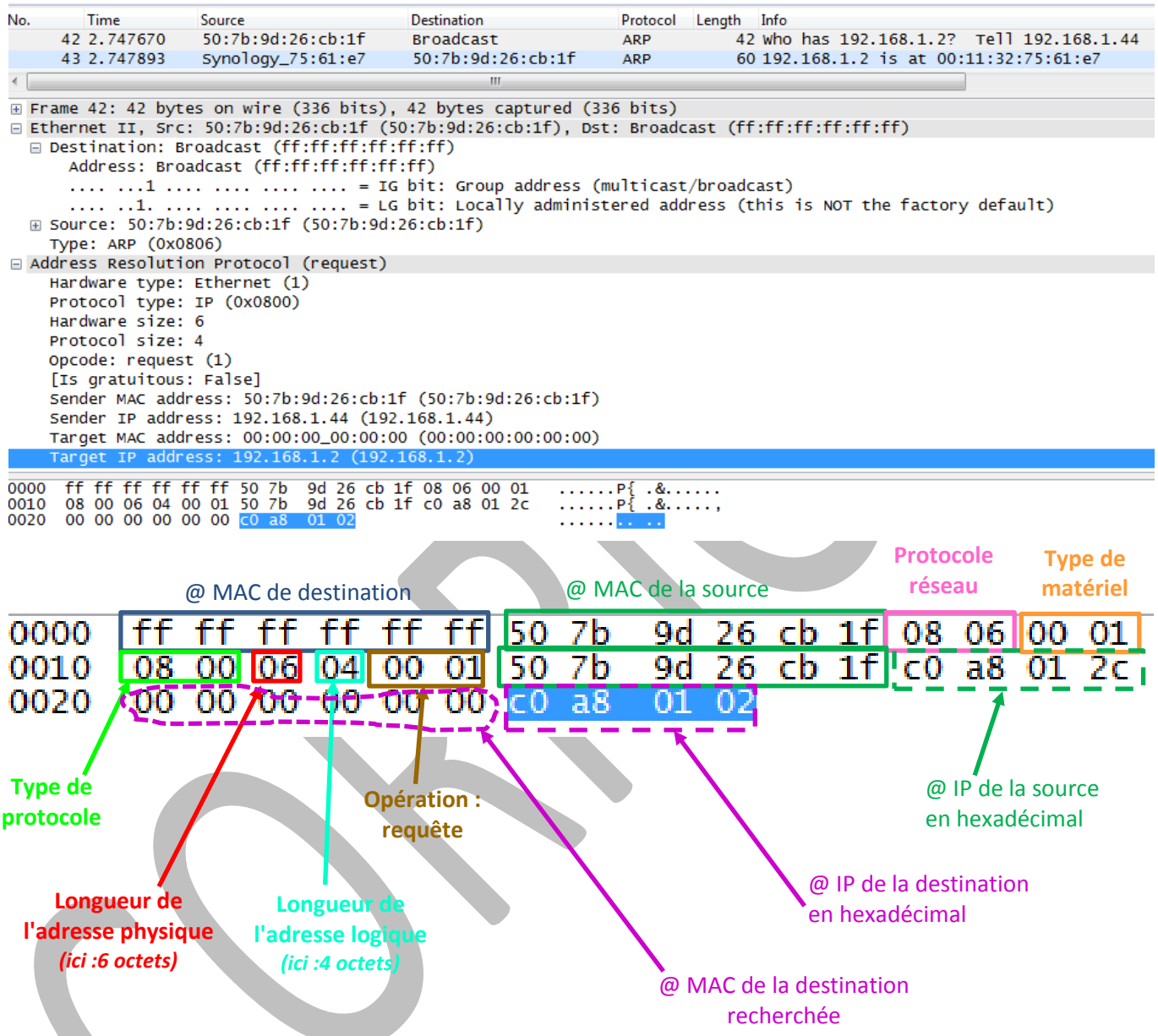
- La structure d'un message ARP est le suivant :

	Bits 0 – 7	**Bits 8 – 15**	**Bits 16 – 23**	**Bits 24 – 31**
0	Type de matériel (*Hardware type*)		Type de protocole (*Protocol type*)	
32	Longueur de l'adresse physique (*Hardware Address Length*)	Longueur de l'adresse logique (*Protocol Address Length*)	Operation	
64	Adresse physique de l'émetteur (*Sender Hardware Address*) – Adresse MAC source			
96				
112	Adresse réseau de l'émetteur (*Sender Protocol Address*) – Adresse IP de source			
144	Adresse physique du destinataire (*Target Hardware Address*) – Adresse MAC destination			
176				
192	Adresse réseau du destinataire (*Target Protocol Address*) – Adresse IP de destination			

V. ETUDE DE TRAMES ARP CAPTUREES A L'AIDE DE WIRESHARK :

A. Requête ARP :

Pour étudier la composition d'une trame ARP, nous allons l'exemple suivant :



Le 13ème et 14ème octet (0806) permettent de définir que le paquet encapsulé dans la trame est un paquet de type ARP.
Les 21ème et 22ème octets permettent de définir que c'est une requête ARP car le code est à 00 01

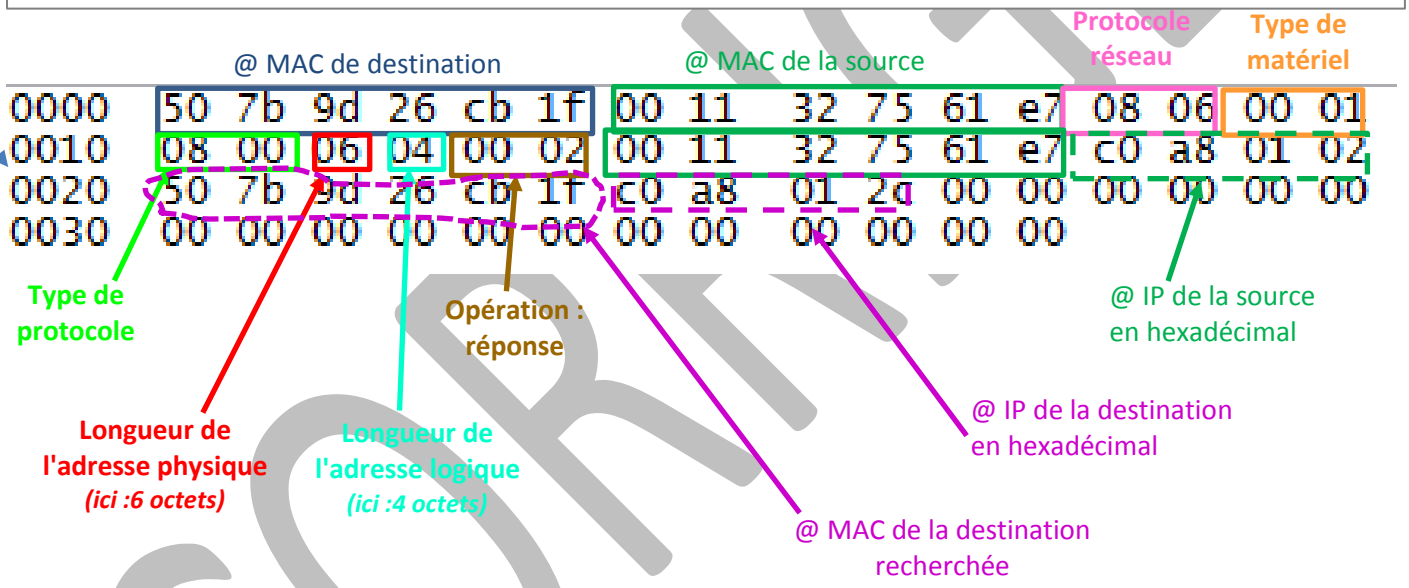
L'équipement possédant l'adresse MAC **50 :7b :9d :26 :cb :1f** et l'adresse IP **$(C0\ A8\ 01\ 2c)_{16}$ soit $(192.168.1.44)_{10}$** cherche à connaitre l''adresse MAC **(00 00 00 00)** de l'équipement qui possèdent l'adresse IP $(C0\ A8\ 01\ 02)_{16}$ soit **$(192.168.1.2)_{10}$**

B. Réponse ARP :

```
No.     Time        Source                Destination           Protocol Length Info
     42 2.747670    50:7b:9d:26:cb:1f     Broadcast             ARP          42 Who has 192.168.1.2?  Tell 192.168.1.44
     43 2.747893    Synology_75:61:e7     50:7b:9d:26:cb:1f     ARP          60 192.168.1.2 is at 00:11:32:75:61:e7

⊞ Frame 43: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
⊟ Ethernet II, Src: Synology_75:61:e7 (00:11:32:75:61:e7), Dst: 50:7b:9d:26:cb:1f (50:7b:9d:26:cb:1f)
  ⊟ Destination: 50:7b:9d:26:cb:1f (50:7b:9d:26:cb:1f)
      Address: 50:7b:9d:26:cb:1f (50:7b:9d:26:cb:1f)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
  ⊟ Source: Synology_75:61:e7 (00:11:32:75:61:e7)
      Address: Synology_75:61:e7 (00:11:32:75:61:e7)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000000000
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: False]

0000  50 7b 9d 26 cb 1f 00 11  32 75 61 e7 08 06 00 01   P{.&.... 2ua.....
0010  08 00 06 04 00 02 00 11  32 75 61 e7 c0 a8 01 02   ........ 2ua.....
0020  50 7b 9d 26 cb 1f c0 a8  01 2c 00 00 00 00 00 00   P{.&.... .,......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```



Le 13ème et 14ème octet (08 06) permettent de définir que le paquet encapsulé dans la trame est un paquet de type ARP.
Les 21ème et 22ème octets permettent de définir que c'est une réponse ARP car le code est à 00 02

L'équipement qui possède l'adresse IP 192.168.1.2 répond qu'il possède l'adresse MAC 00:11:32:75:61:e7 à l'équipement qui possède l'adresse IP 192.168.1.44;
C'est ce dernier qui avait effectué la requête ARP.