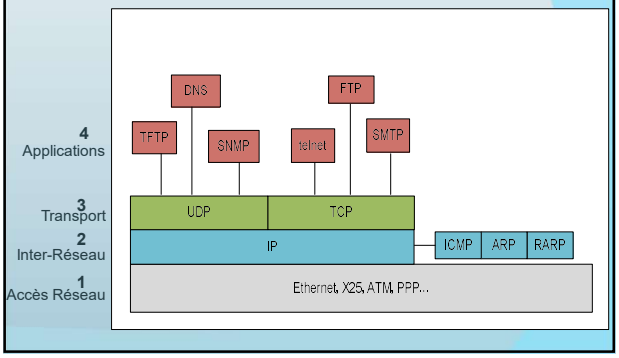
Address Resolution Protocol

(RFC 826)

Rappel



Problématique

- L'adressage universel employé par IPv4 n'a pas de sens pour la couche inférieur du modèle TCP/IP (1 – accès réseau)
- La norme Ethernet (ou IEEE) impose un identifiant unique pour chaque interface construite et commercialisée
- Une machine doit savoir « lire » son adresse physique pour la mettre à disposition du protocole de dialogue
- Pour transmettre des données sur un réseau physique, un hôte doit connaître ou apprendre une adresse physique de destination

L'adresse Medium Access Control

- Elles sont délivrées par l'IEEE (Institute of Electrical and Electronics Enginers)
- Codée sur 6 octets dont 3 pour le constructeur et 3 pour le rang de l'interface (environ 16M de plages d'adresses pour autant d'identifiants d'interface)

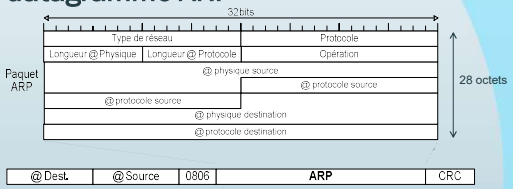
Exemple d'adresse physique en représentation hexadécimale :

08:00:09:35:d5:0b	08:00:09 est attribué à la firme Hewlett-Packard 35:d5:0b est l'adresse de la carte

D'autres constructeurs, capturés au hasard des réseaux :

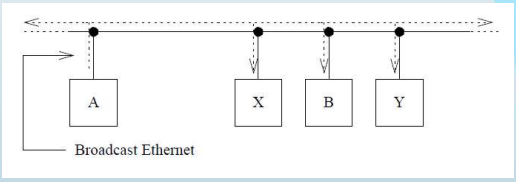
00:11:24	Apple Computer
00:00:0C	Cisco Systems, Inc.
00:06:5B	Dell Computer Corp.
08:00:20	Sun Microsystems
AA:00:04	Digital Equipment Corporation
00:10:5A	3Com Corporation
...	...

Le datagramme ARP



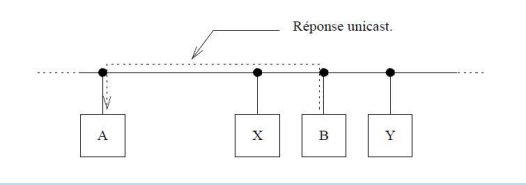
- Type de réseau pour définir le format des adresses physiques (1 pour Ethernet)
- Protocole pour définir le format des adresses logiques (0800 = IP)
- Longueur pour la taille en octets des adresses physiques et logiques (6o @MAC, 4o @IPv4)
- Opération précise le contenu du message (1: requête ARP, 2: réponse ARP, 3: requête RARP, 4: réponse RARP)
- Les champs suivants sont explicites

Requête ARP



- L'interface A (192.168.0.1) demande à toutes les machines LAN (FF:FF:FF:FF:FF:FF) « qui possède l'@ IPv4 192.168.0.2 ? »
- Toutes les machines « écoutent » le réseau et renseignent leurs tables ARP avec l'@IP et l'@MAC de A

Réponse ARP



- L'interface B (192.168.0.2) envoie à l'interface A son @MAC
- Si B ne répond pas, A repose la question indéfiniment
- Une table ARP gérée par le système d'exploitation mémorise les correspondances @IP / @MAC (environ 20mn de TTL réinitialisé à chaque échange fructueux)
- En cas « d'échec ICMP », la ligne est supprimée de la table

Table ARP

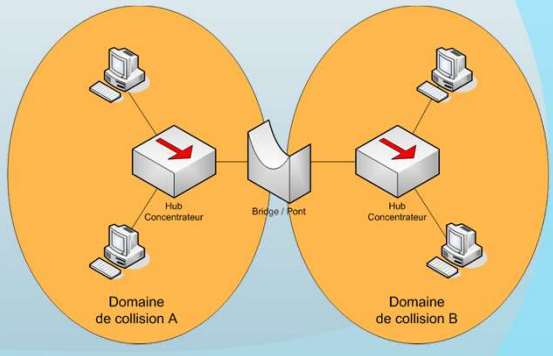
```
$ arp -a
soupirs.chezmoi.fr  (192.168.192.10) at 8:0:9:85:76:9c
espoirs.chezmoi.fr  (192.168.192.11) at 8:0:9:85:76:bd
plethore.chezmoi.fr (192.168.192.12) at 8:0:9:a:f9:aa
byzance.chezmoi.fr  (192.168.192.13) at 8:0:9:a:f9:bc
ramidus.chezmoi.fr  (192.168.192.14) at 0:4f:49:1:28:22 permanent
desiree.chezmoi.fr  (192.168.192.33) at 8:0:9:70:44:52
pythie.chezmoi.fr   (192.168.192.34) at 0:20:af:2f:8f:f1
ramidus.chezmoi.fr  (192.168.192.35) at 0:4f:49:1:36:50 permanent
gateway.chezmoi.fr  (192.168.192.36) at 0:60:8c:81:d5:1b
```

- Peut être consultée par la commande « arp -a » (unix et windows)
- Les entrées peuvent être dynamiques ou statiques
- Unix complète également la table avec les noms de domaine si possible

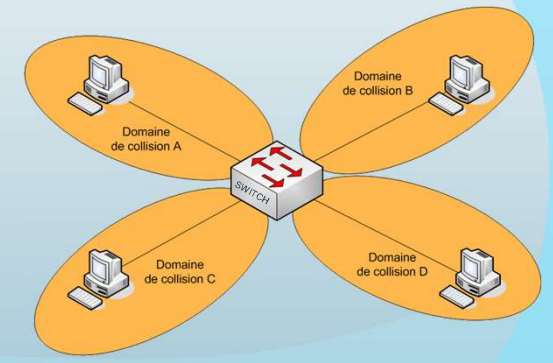
Proxy ARP

- Les proxy ou passerelles ARP permettent à des interfaces qui ne partagent pas le même support physique d'appartenir au même domaine de diffusion

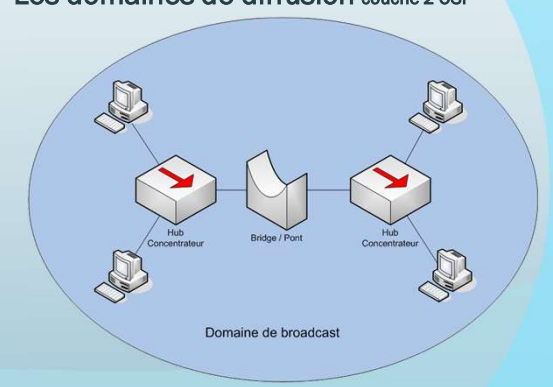
Les domaines de collision couche 1 OSI



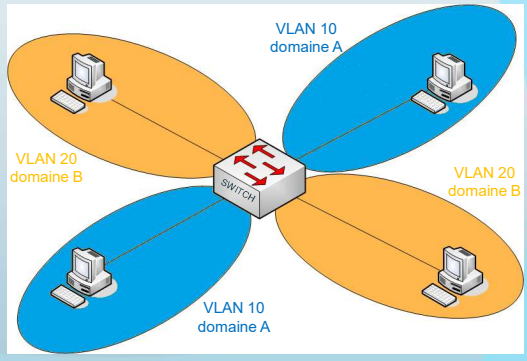
Les domaines de collision couche 1 OSI



Les domaines de diffusion couche 2 OSI



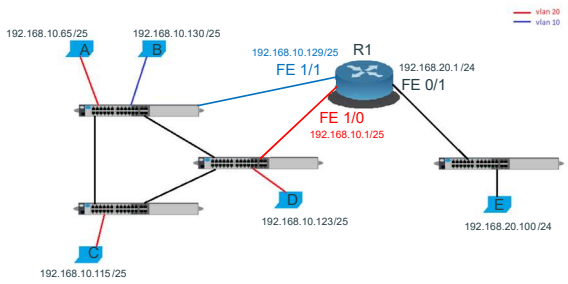
Les domaines de diffusion couche 2 OSI



Questions pratiques

- Comment vérifier que je suis seul à utiliser une @ IP ?
  Envoyer une requête ARP avec ma propre adresse IP (personne ne doit répondre).
- A qui est adressée ma requête ARP quand elle concerne l'interface d'un réseau logique (IPv4) différent du mien?
  A la passerelle IP (configurée ou par défaut).

Mise en situation



Donner à chaque adresse IP un masque en cohérence avec les vlans représentés

Protocole RARP
(Reverse Address Resolution Protocol)

- Sur la base d'ARP, ce protocole permet à des machines qui ne peuvent ou ne doivent pas mémoriser leurs adresses IP d'en obtenir une (en général par un serveur ARP)
- Technique ancienne, remplacée aujourd'hui par la technique DHCP

Quelques notions de Cyber Sécurité

- La force et la faiblesse du protocole ARP, c'est sa simplicité.
- La mémoire du protocole est réécrite à chaque nouvelle entrée.
- « L'exploitation » de ce protocole consiste à polluer le réseau par de fausses trames ARP encodées par le pirate.

MAC Flooding

- Par défaut, les commutateurs limitent la capacité d'écoute du réseau (sniffing).
- En cas de surcharge, certains commutateurs basculent en mode hub.
- On génère donc une très grande quantité de fausses réponses ARP pour saturer le commutateur et ainsi pouvoir écouter l'intégralité du réseau pendant un certain temps.
- Une architecture réseau sécurisée devra donc éviter ce type de commutateur ou simplement désactiver cette fonctionnalité le cas échéant.

Deny of Service (DoS)

- Une fois le réseau cartographié grâce éventuellement au MAC FLOODING on utilise les informations contre le réseau par différentes méthodes:
- Falsification d'identité d'un serveur
- Falsification d'identité d'une passerelle
- … et bien d'autres

Man in the Middle

- Plutôt que réduire un service à néant il peut être « intéressant » de détourner les informations sans se faire prendre.
- Le pirate usurpe l'identité du client et du serveur par exemple et configure sa machine en pseudo proxy ARP.

Sécurisation

- Ces méthodes, bien que basiques, sont encore aujourd'hui très efficaces sur un grand nombre de réseaux. Elles peuvent être la base d'attaques beaucoup plus complexes.
- Il est pourtant assez facile de les déjouer :
  - utilisation de caches ARP statiques (couteux)
  - utilisation d'équipements nativement protégés contre ces attaques bien connues.
  - sécurisation des échanges client / serveur au niveau transport ou applications (échanges de clés RSA….)