R109 – Initiation aux réseaux d’entreprise

Licence Pro Rob&IA

Nicolas MENDEZ – Laurent ROY

Objectifs

- **PARTIE 1 (sept-octobre) – 3h de cours ; 6h de TP**
  - Appréhender la structure et le fonctionnement d'un système informatique, Initiation à l'administration d'un OS Linux,
  - Comprendre les mécanismes permettant de communiquer avec l'extérieur, liens avec les réseaux informatiques.
- **PARTIE 2 (nov-déc-janv) – 10h de cours ; 14h de TP**
  - Apprendre les règles d'adressage IPv4 et comprendre le rôle d'une passerelle ,
  - Connaître la structure d'un réseau d'entreprise, Modèle OSI,
  - Protocoles ARP / IP / ICMP / TCP / UDP

Plan du cours

- **Première partie : Initiation aux systèmes informatiques Linux**
  1) Introduction à l'informatique. Principe d'un OS.
  2) Linux : Un bref historique
  3) Notion des principales commandes mkdir ; cd ; cp ; mv ; ps ; kill ...
  4) Gestion des utilisateurs et des droits
  5) Lien avec les réseaux informatiques

Plan du cours

- **Deuxième partie : Initiation aux réseaux d'entreprise**
  1) IPv4 ; configuration cartes réseaux ; rôle d'une passerelle,
  2) Modèles OSI
  3) Analyse de protocoles
     a) Couche 2 : Adresses MAC ; protocole ARP
     b) Couche 3 : protocoles IP, ICMP
     c) Couche 4 : protocoles TCP et UDP
  4) Topologie des réseaux

Cours Inversés

Protocole ARP

Son rôle ?

➔ Déterminer l'adresse physique de la machine si on connaît son adresse logique

A quoi ça sert ?

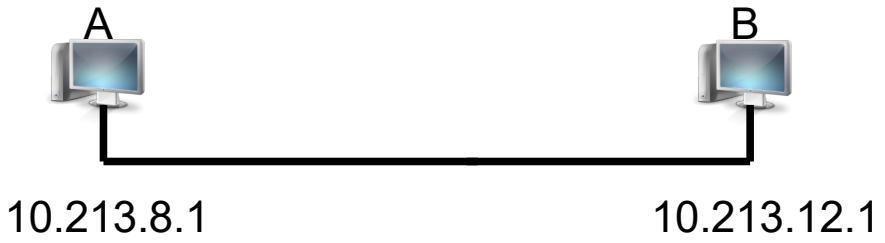
Scénario : la machine A veut envoyer un paquet IP à la machine B

Plusieurs cas

- Réseau point à point
- Réseau multi points

Protocole ARP : Cas réseau point à point

- Liaison PPP / HDLC / Frame Relay
- Liaison série... pas de suspens
- Le paquet IP est encapsulé dans une trame PPP et envoyé à l'autre extrémité du réseau



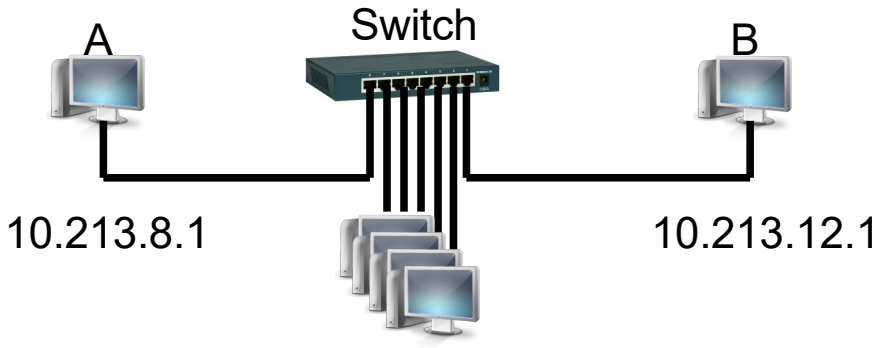
Protocole ARP : Cas réseau multipoints

Cas Ethernet

On doit encapsuler le paquet dans une trame Ethernet

Plusieurs machines sont reliées sur un même brin du réseau :
il faut **identifier** la bonne → **adressage**

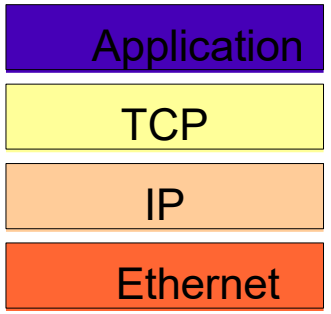
Il faut déterminer l'adresse MAC du destinataire

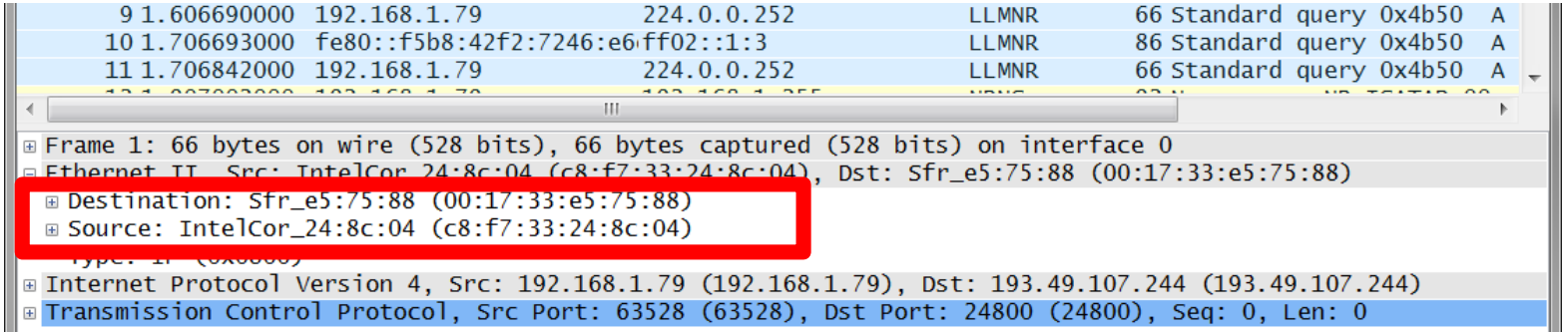


Protocole ARP : Construction du message

Rappel sur les couches Leurs besoins

- IP : les adresses IP
- Ethernet : les adresses MAC





Protocole ARP : problème à résoudre

Si on ne sait pas remplir les PCI …

- On ne peut pas envoyer le message

→ Il faut **résoudre** l'adresse MAC de la destination

= **Trouver une @ MAC qui correspond à une @ IP**

Remarque : Seulement dans IPv4. Disparaît en IPv6 ARP (remplacé par NDP neighbor Discovery Protocol)

Protocole ARP : Généralités sur ARP

- Protocole de niveau 3
- Se situe à l'interface entre les couches 2 et 3
- Défini par la RFC 826

Comment récupérer l'@ MAC d'une machine si on ne peut pas émettre de trame sans @ MAC ?

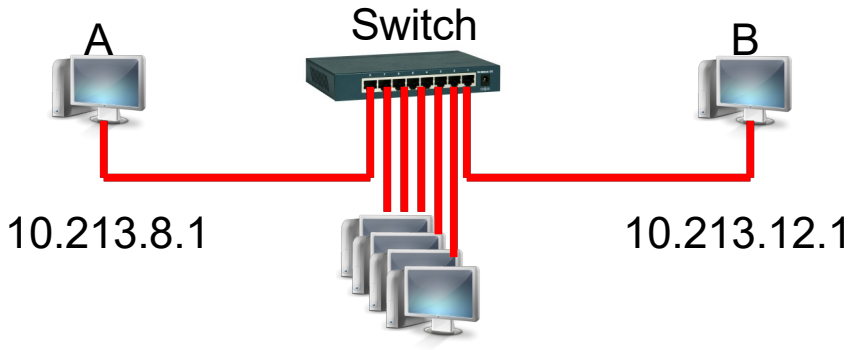
→ Utilisation de la diffusion : Adresse MAC diffusion FF:FF:FF:FF:FF:FF

Cible toutes les machines sur un même brin du réseau

Protocole ARP : Fonctionnement

A envoie une trame Ethernet en diffusion

- MAC source : MAC_A
- MAC destination :**FF:FF:FF:FF:FF:FF**



Contenant une requête ARP

- IP source : IP_A
- IP destination : IP_B

Protocole ARP : Fonctionnement

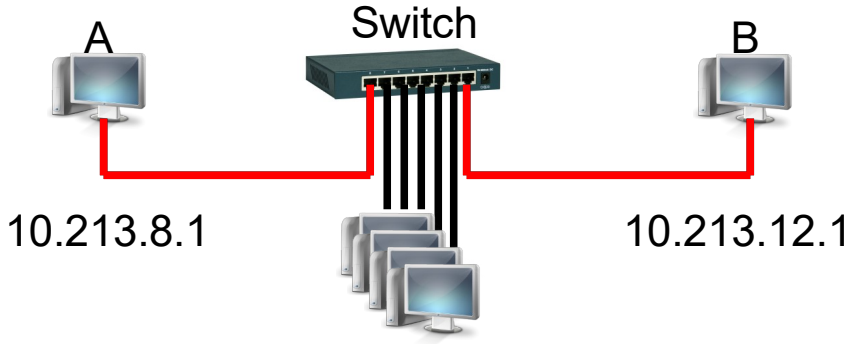
Optionnel : mise à jour du cache ARP en B (MAC de A)

La machine B renvoie une trame Ethernet

- MAC source : MAC_B
- MAC dest : MAC_A

Contenant une réponse ARP

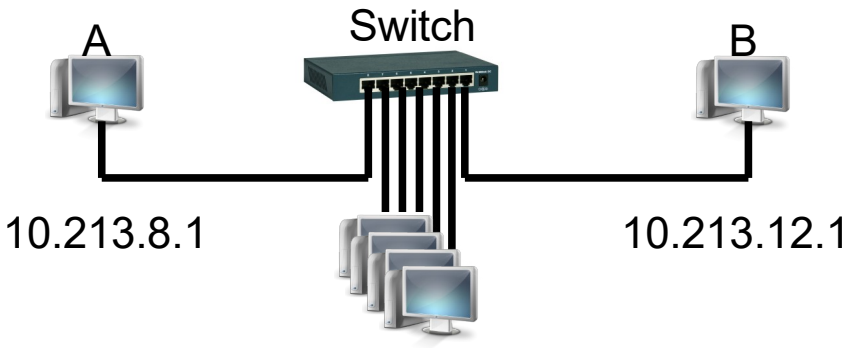
- IP source : IP_B
- IP dest : IP_A



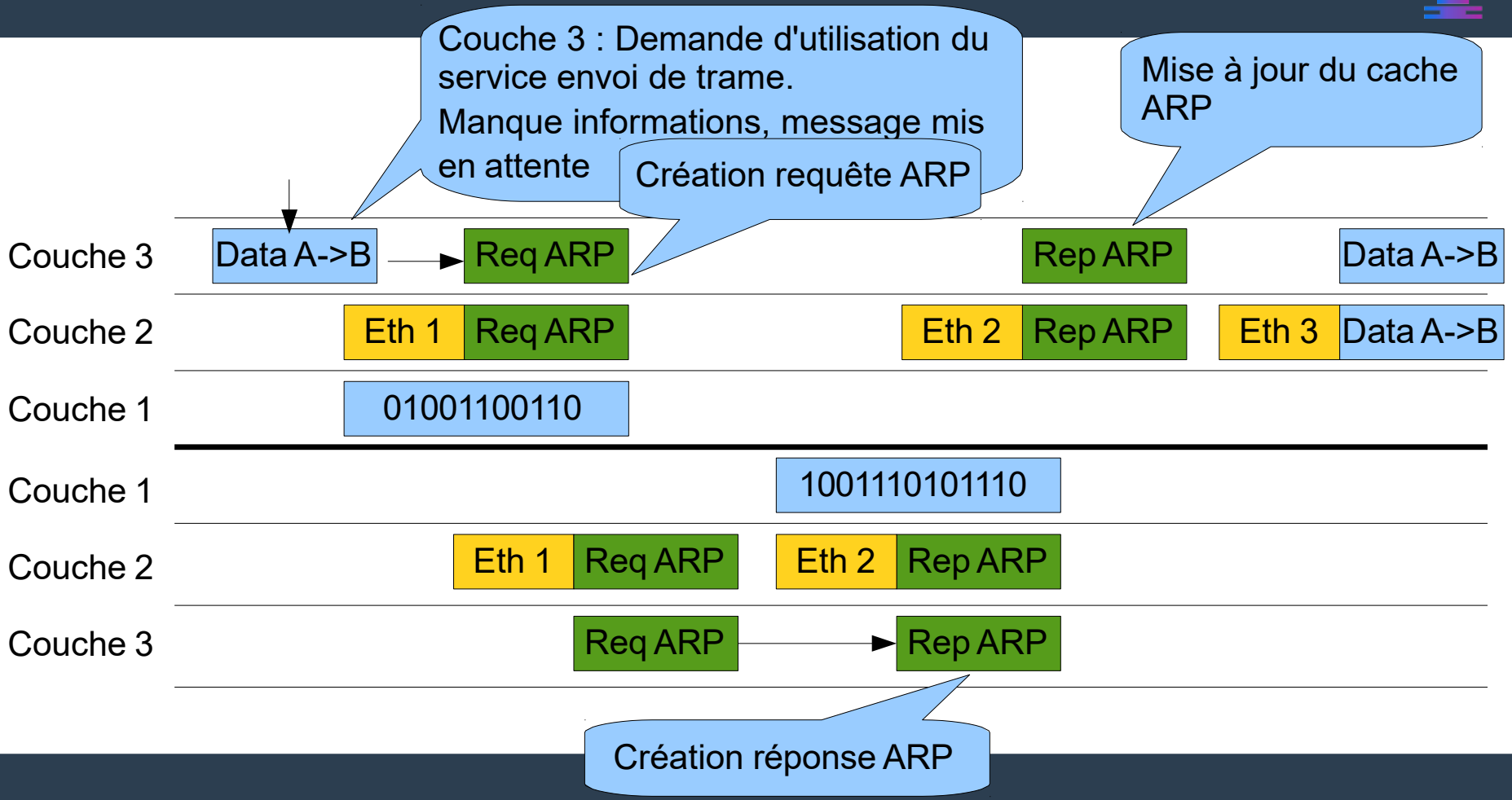
Protocole ARP : Fonctionnement

→ Mise à jour du cache ARP en A (MAC de B)

→ Les machines A et B sont prêtes pour discuter



Protocole ARP : Synoptique de l'envoi d'une trame vers une machine inconnue



Protocole ARP : Analyse

- Capture de trame ARP : Requête ARP

No.	Time	Source	Destination	Protocol	Length	Info
15202	9.274705000	Sfr_e5:75:88	IntelCor_24:8c:04	ARP	42	Who has 192.168.1.79? Tell 192.168.1.1
15203	9.274732000	IntelCor_24:8c:04	Sfr_e5:75:88	ARP	42	192.168.1.79 is at c8:f7:33:24:8c:04
15204	9.276465000	69.4.231.52	192.168.1.79	HTTP	1506	Continuation or non-HTTP traffic

```
Frame 15202: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: Sfr_e5:75:88 (00:17:33:e5:75:88), Dst: IntelCor_24:8c:04 (c8:f7:33:24:8c:04)
  Destination: IntelCor_24:8c:04 (c8:f7:33:24:8c:04)
  Source: Sfr_e5:75:88 (00:17:33:e5:75:88)
  Type: ARP (0x0806)
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Sfr_e5:75:88 (00:17:33:e5:75:88)
  Sender IP address: 192.168.1.1 (192.168.1.1)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.79 (192.168.1.79)
```

```
0000  c8 f7 33 24 8c 04 00 17  33 e5 75 88 08 06 00 01   ..3$.... 3.u.....
0010  08 00 06 04 00 01 00 17  33 e5 75 88 c0 a8 01 01   ........ 3.u.....
0020  00 00 00 00 00 00 c0 a8  01 4f                     ........ .O
```

Protocole ARP : Analyse

- Capture de trame ARP : Réponse ARP

No.	Time	Source	Destination	Protocol	Length	Info
15202	9.274705000	Sfr_e5:75:88	IntelCor_24:8c:04	ARP	42	Who has 192.168.1.79? Tell 192.168.1.1
15203	9.274732000	IntelCor_24:8c:04	Sfr_e5:75:88	ARP	42	192.168.1.79 is at c8:f7:33:24:8c:04
15204	9.276465000	69.4.231.52	192.168.1.79	HTTP	1506	Continuation or non-HTTP traffic

```
⊞ Frame 15203: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
⊟ Ethernet II, Src: IntelCor_24:8c:04 (c8:f7:33:24:8c:04), Dst: Sfr_e5:75:88 (00:17:33:e5:75:88)
  ⊞ Destination: Sfr_e5:75:88 (00:17:33:e5:75:88)
  ⊞ Source: IntelCor_24:8c:04 (c8:f7:33:24:8c:04)
    Type: ARP (0x0806)
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_24:8c:04 (c8:f7:33:24:8c:04)
    Sender IP address: 192.168.1.79 (192.168.1.79)
    Target MAC address: Sfr_e5:75:88 (00:17:33:e5:75:88)
    Target IP address: 192.168.1.1 (192.168.1.1)
```

```
0000  00 17 33 e5 75 88 c8 f7  33 24 8c 04 08 06 00 01   ..3.u... 3$......
0010  08 00 06 04 00 02 c8 f7  33 24 8c 04 c0 a8 01 4f   ........ 3$.....O
0020  00 17 33 e5 75 88 c0 a8  01 01                     ..3.u... ..
```

Protocole ARP : Analyse

- Encapsulé dans une trame (Ethernet)

Pré	Mac dest	Mac src	0x0806	ARP	CRC

- Format du PCI ARP :
  - Taille inconnue car dépend des adresses
  - requêtes et les réponses ont le même format : le champ Opération vaut 1 s'il s'agit d'une requête ou 2 s'il s'agit d'une réponse

	Bits 0-7	Bits 8-15	Bits 16-31
0	Hardware type		Protocol type
32	Hardware address length	Protocol address length	Operation
64	Sender Hardware Address		
?	Sender Protocol Address		
?	Target Hardware Address		
?	Target Protocol Address		

Protocole ARP : Analyse

- **Hardware type (2 octets)**
  - Caractérise le protocole de la couche liaison
  - Chez nous : 0001 = Ethernet (il en existe d'autres)
- **Protocole type (2 octets)**
  - Caractérise le protocole de la couche réseau
  - Chez nous : 0800 = IP
- **Hardware Address Length (1 octet)**
  - Taille des adresses de niveau 2 : 6 octets (Ethernet)
- **Protocol Address Length (1 octet)**
  - Taille des adresses de niveau 3 : 4 octets (IP)

Protocole ARP : Analyse

- **Operation (2 octets)**
  - Type de message : 01 requête, 02 réponse
- **Sender Hardware Address**
  - Adresse de niveau 2 de l'émetteur (adresse MAC)
- **Sender Protocol Address**
  - Adresse de niveau 3 de l'émetteur (adresse IP)
- **Target Hardware Address**
  - Adresse de niveau 2 de l'émetteur (adresse MAC)
- **Target Protocol Address**
  - Adresse de niveau 3 de l'émetteur (adresse IP)

Protocole ARP : Analyse

- Exemple :

```
    7 23.105646     Dell_02:b5:12       Dell_02:b4:fc       ARP         60 10.216.6.1 is at c8:4b:d6:02:b5:12
```

```
▾ Ethernet II, Src: Dell_02:b5:12 (c8:4b:d6:02:b5:12), Dst: Dell_02:b4:fc (c8:4b:d6:02:b4:fc)
  ▾ Destination: Dell_02:b4:fc (c8:4b:d6:02:b4:fc)
      Address: Dell_02:b4:fc (c8:4b:d6:02:b4:fc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▾ Source: Dell_02:b5:12 (c8:4b:d6:02:b5:12)
      Address: Dell_02:b5:12 (c8:4b:d6:02:b5:12)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Dell_02:b5:12 (c8:4b:d6:02:b5:12)
    Sender IP address: 10.216.6.1
    Target MAC address: Dell_02:b4:fc (c8:4b:d6:02:b4:fc)
    Target IP address: 10.216.5.1
```

```
0000  c8 4b d6 02 b4 fc c8 4b  d6 02 b5 12 08 06 00 01
0010  08 00 06 04 00 02 c8 4b  d6 02 b5 12 0a d8 06 01
0020  c8 4b d6 02 b4 fc 0a d8  05 01 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

Protocole ARP : Cache

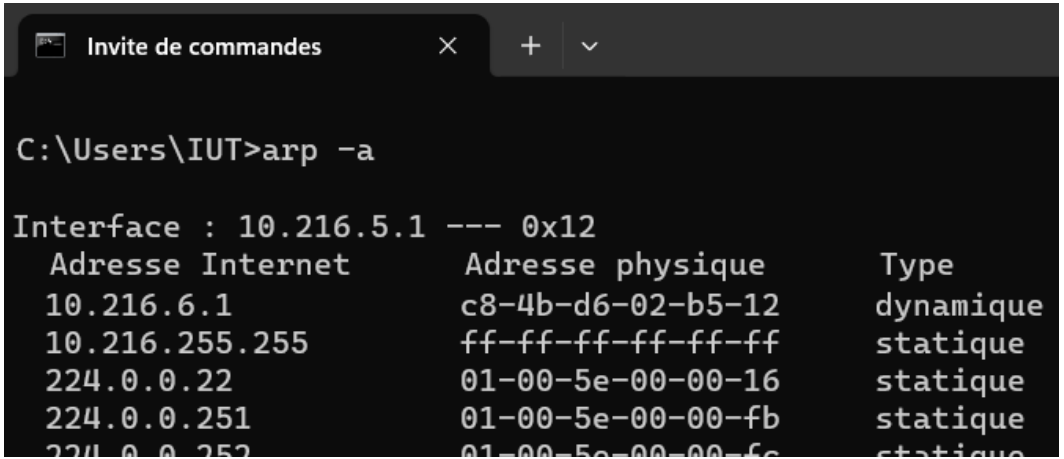
- Cache ARP ?
  - Fichier contenant les **paires @MAC / @IP**
- Comment le visualise-t-on ?
  - **arp -a** sous windows
  - **ip neigh** sous linux (ou cat /proc/net/arp)
- Différentes entrées dans le cache
  - Statique
  - Dynamique

Protocole ARP : Cache

- Sous Linux

```
test@ubuntuServer:~$ ip neigh
10.216.5.1 dev eth0 lladdr c8:4b:d6:02:b4:fc STALE
10.216.6.1 dev eth0 lladdr c8:4b:d6:02:b5:12 REACHABLE
```

- Sous windows



Protocole ARP : Cache

- Pourquoi un cache ?
  - → Pour éviter les résolutions à chaque paquet
- Pourquoi des entrées statiques ?
  - → Évite les requêtes en diffusion pour des machines souvent usitées
- Pourquoi entrées dynamiques ?
  - → Ne pas garder toutes les entrées inutilisées
  - → Permettre la mise à jour des adresses MAC (changement carte)

Décrit dans la RFC 826

Protocole ARP : Cache

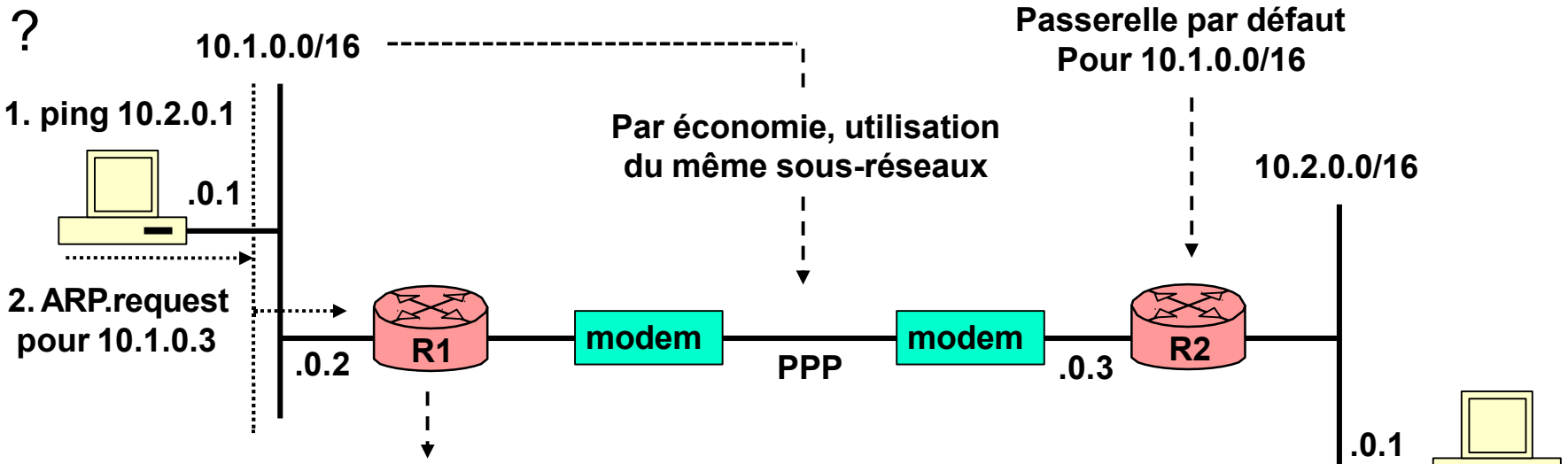
- **Timeout** → Après 3 tentatives ratées on arrête
- Les états possibles d'une entrée

cache state	meaning	action if used
permanent	never expires; never verified	reset use counter
noarp	normal expiration; never verified	reset use counter
reachable	normal expiration	reset use counter
stale	still usable; needs verification	reset use counter; change state to delay
delay	schedule ARP request; needs verification	reset use counter
probe	sending ARP request	reset use counter
incomplete	first ARP request sent	send ARP request
failed	no response received	send ARP request

Protocole ARP : Proxy

- Portée d'une requête ARP ?

→ Réseau local : **jusqu'au routeur** → Que se passe t-il si le réseau est divisé ?



Si Proxy ARP est activé sur R1, il répond en transmettant l'adresse MAC de .0.2 (sachant qu'il est connecté à .0.3 via une autre interface que l'interface par laquelle est arrivée la requête ARP)

Protocole ARP : ARP GRATUIT

- Question envoyée sans attendre de réponse
- Permet d'annoncer qu'une adresse IP est associée avec une adresse mac
- Utile pour savoir si une adresse IP est déjà utilisée (dans ce cas réponse)
  - → DHCP
- Permet la mise à jour des caches ARP

Protocole ARP : Vulnérabilités

Il existe des failles ...

– Usurpation d'adresse MAC (MAC Spoofing)
- On corrompt le cache ARP d'un switch (message forgé)

– Usurpation d'identité ARP (ARP spoofing)
- Répondre plus vite que le destinataire au requêtes ARP

– Cache poisoning
- Outil arp-sk
- Envoi de requête ARP unicast avec des valeurs choisies entraîne une mise à jour du cache faussé

Utilisation :

– Écoute / Interception / Man in the middle / Dénis de service

Protocole ARP : Parades

- Les systèmes de détection d'intrusions

– IDS : surveille les modification ARP (ArpWatch)

- Le cache ARP Statique

– Attention chez microsoft statique signifie qui n'expire pas … mais est modifiable

- Filtrage au niveau ARP

– Filtrage MAC / IP

- Sources :

– http://tools.ietf.org/html/rfc826

– http://linux-ip.net/html/ether-arp.html

Fin

Bibliographie :
COMBY F. : *Cours M1101 et M1104* , IUT RT Béziers
TANENBAUM A., WETHERALL, D. : *Réseaux 5ème éd.* Pearson
HÉROLD J.-F., GUILLOTIN O., ANAYA P. : *Informatique industrielle et réseaux en 20 fiches*, Dunod
LOHIER S., PRESENT D., *Transmissions et réseaux 2ème èd.* , Dunod