

Réseaux

Couche Réseau

Adresses

E. Jeandel

Résumé des épisodes précédents

- Comment un ensemble de machines, reliées physiquement entre elles, peuvent communiquer

Problématique

- Internet = Interconnexion de réseaux.
- Si une machine veut parler à une autre, elle doit
 - Savoir où elle est
 - Savoir comment la contacter

Aujourd'hui : première partie.

Problématique

- Attribuer une adresse à une machine
- savoir comment envoyer un message à une machine connaissant uniquement son adresse
- Trouver à partir de l'adresse, dans quel réseau se trouve la machine

Idée de base : Pour envoyer un message à une machine d'adresse A

- Soit je m'aperçois que A est dans mon réseau local, et je lui envoie directement
- Soit ce n'est pas le cas, et je trouve quelqu'un (un *routeur*) pour le faire à ma place.

Note : l'adresse MAC ne marche pas.

La pratique

- Chaque machine est dotée d'une adresse A
- Chaque machine possède un couple (A, B)
 - A : adresse de la machine.
 - B : ensemble des adresses situées sur le même réseau.

Quand on parle de machine, il faut plutôt parler d'accès réseau : un routeur aura plusieurs adresses.

1 IPv4

1.1 Principe

IP v4

- Une adresse est codée sur 32 bits (4 octets)
- Exemple : 140.94.16.64

Comment trouver l'ensemble des machines sur le même réseau ?

IP v4 (Adressage avec classes)

Pour une adresse $x.y.z.w$:

classe A $1 \leq x < 128$ (x commence par 0)

Réseau de 2^{24} machines : toutes les machines $x. * . * . *$

classe B $128 \leq x < 192$ (x commence par 10)

Réseau de 2^{16} machines : toutes les machines $x.y. * . *$

classe C $192 \leq x < 224$ (x commence par 110)

Réseau de 2^8 machines : toutes les machines $x.y.z. *$

classe D $224 \leq x < 240$ (x commence par 1110)

multicast (voir plus loin)

classe E $x \geq 240$ Réserve

Le réseau en entier est désigné en remplaçant les * par des 0

Broadcast

- On envoie un message à tout le monde en remplaçant les * par des 255 (ex : 196.168.1.255)
- En général les routeurs ne relaient pas les broadcasts aux autres réseaux
- Plus généralement, l'adresse 255.255.255.255 permet d'envoyer un message à tout le réseau (sans avoir à connaître le réseau)

Problèmes de l'adressage de classe

- Seulement 4 classes possibles
- Pas de hiérarchie. Que ferait un fournisseur d'accès Internet ?

Adressage CIDR (Classless Inter-Domain Routing)

- Un bloc CIDR est donné par une adresse et un *masque*
- Ex : 192.168.1.0/255.255.255.0
- Une interface appartient au réseau si le ET avec le masque est égal à l'adresse
- 192.168.1.58 ?
- 192.168.2.0 ?

Notation CIDR (Classless Inter-Domain Routing)

- Spécifie le nombre de bits à 1 du masque.
- 192.168.1.0/255.255.255.0 = 192.168.1.0/24
- Une machine appartient au réseau si ses 24 premiers bits sont égaux.
- classe A : /8
- classe B : /16
- classe C : /24

Blocs réservés

- 127.0.0.0/8 : Machine locale (ne se voit jamais sur un réseau)

Réseaux privés (ne se voit jamais sur Internet)

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- 169.254.0.0/16

Problématiques

- Comment attribuer les adresses ?
- Comment parler à une machine une fois connue l'adresse ?

1.2 Attribution

Attribution des adresses

- D'abord obtenir un bloc CIDR
- Besoin d'un organisme centralisateur
- ICANN (voir cours d'Outils de l'Internet)

Attribution des adresses (A l'intérieur d'un bloc CIDR)

- Attribution statique.
- Avantages/Inconvénients ?
- Attribution dynamique.
- Autoconfiguration

Attribution dynamique

- La machine demande une adresse pour un temps limité lorsqu'elle rentre sur un réseau
- Peut changer au cours du temps
- BOOTP, DHCP
- DHCP : Protocole niveau application (voir plus tard)

Autoconfiguration

- Obtenir une adresse servant uniquement dans le réseau local
- Bloc 169.254.0.0/16
- Chaque hôte choisit aléatoirement une adresse, et vérifie régulièrement qu'elle n'est pas utilisée (cf. Résolution)
- APIPA (Auto-IP)

1.3 Résolution

Résolution

- Obtenir, à partir de l'adresse IP, l'adresse MAC
- Protocole ARP

ARP (Address Resolution Protocol)

- Chaque machine contient un cache ARP
- Délai d'expiration court (20 min). Pourquoi ?
- Revalidation anticipée

ARP (Paquet (simplifié))

Un paquet ARP contient :

- Un champ demande/réponse
- L'adresse IP(resp. MAC) de l'émetteur
- L'adresse IP(resp. MAC) du destinataire

ARP est conçu pour fonctionner avec n'importe quel protocole liaison/réseau

- s/IP/réseau/
- s/MAC/liaison/

ARP (Principe (1/2))

Si *A* d'adresse IP 1.6.6.4 et d'adresse MAC 00:de:ad:be:ef:00 veut connaître l'adresse MAC de la machine d'adresse IP 1.6.6.15

- Trame ethernet en broadcast (sur ff:ff:ff:ff:ff:ff)
- ARP en mode demande
- Adresse IP/MAC de l'expéditeur (pourquoi ?)
- Adresse IP du destinataire
- Adresse MAC du destinataire : 00:00:00:00:00:00

ARP (Principe (2/2))

Lorsque *B* veut répondre :

- Trame ethernet vers *A*
- ARP en mode réponse
- Adresse IP/MAC de *A* et de *B*

Attention : seul *B* doit répondre.

ARP (Principe (3/0))

Usages avancés

- Adresse IP de l'expéditeur en 0.0.0.0 : Utilisé dans l'autoconfiguration
- Une interface réseau peut envoyer sa correspondance IP/MAC au réseau pour "prévenir".

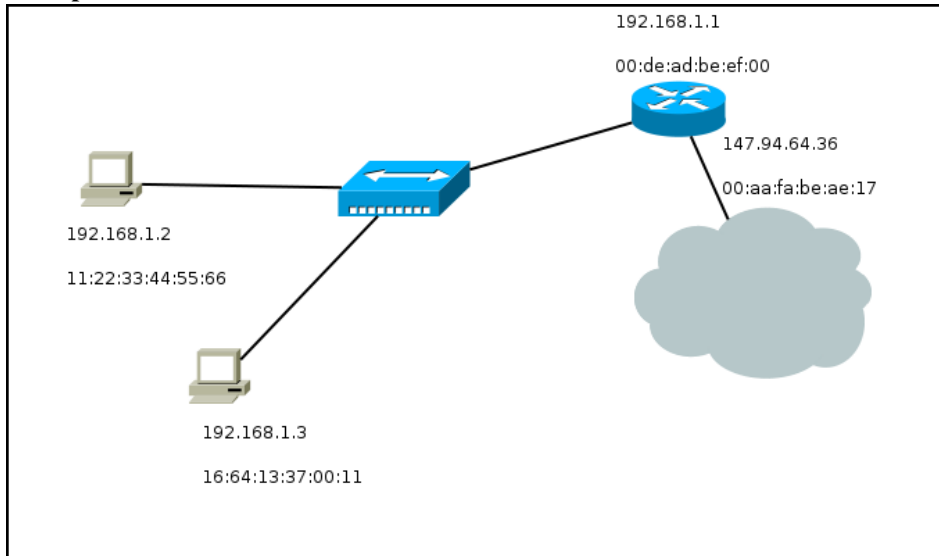
ARP (Principe (4/0))

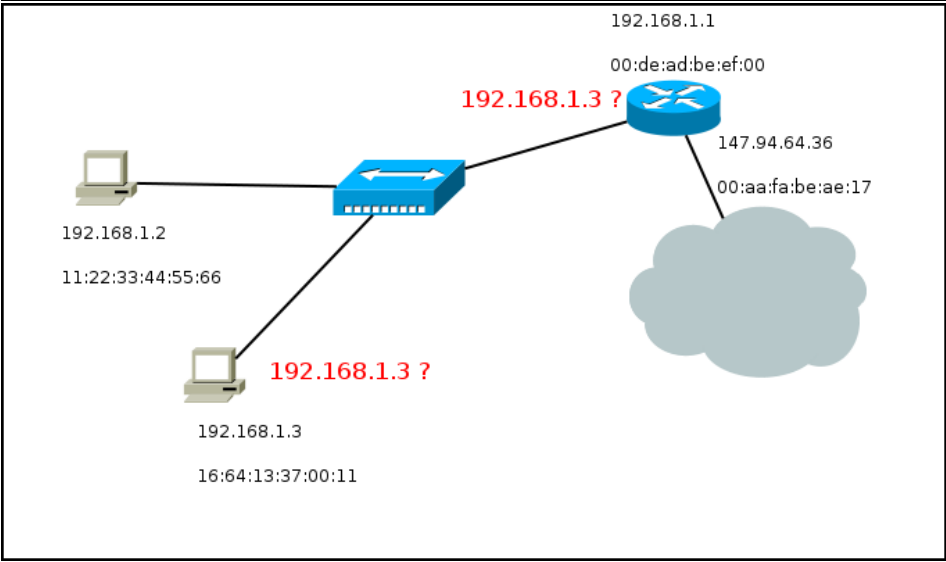
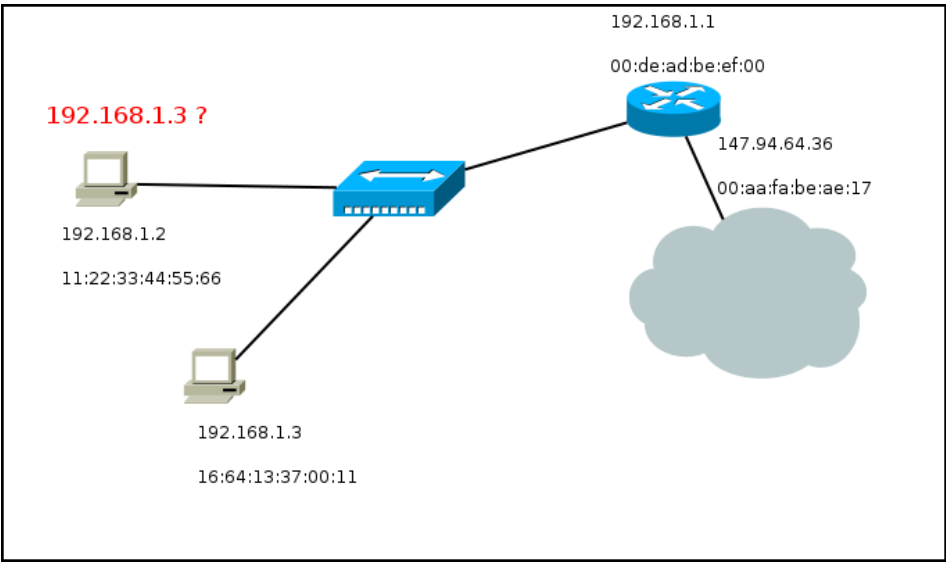
Attention

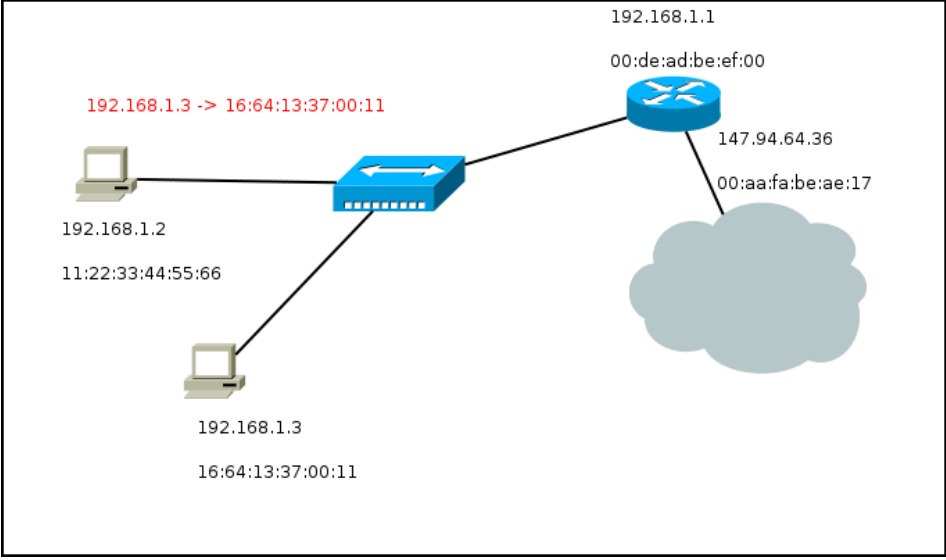
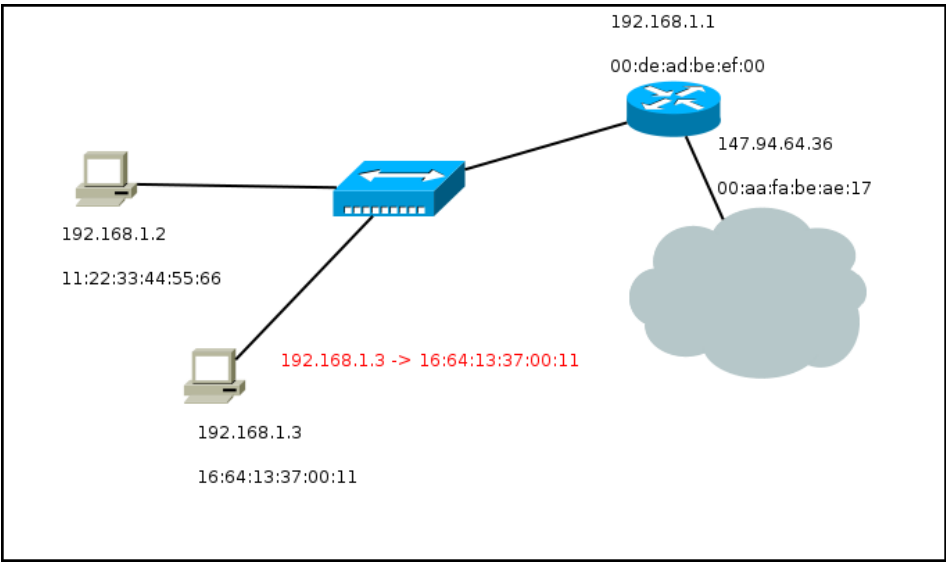
- Toute machine peut répondre théoriquement à une requête ARP.
- Attaques possibles

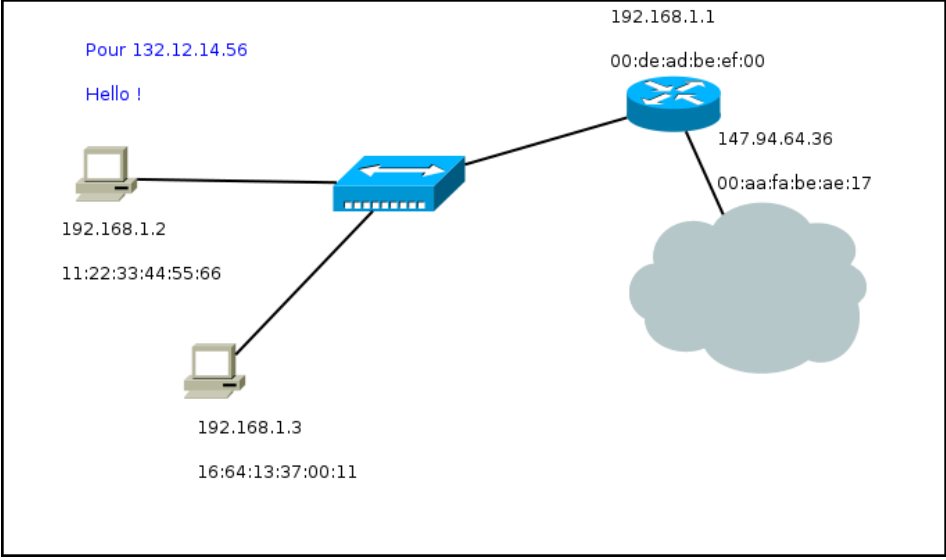
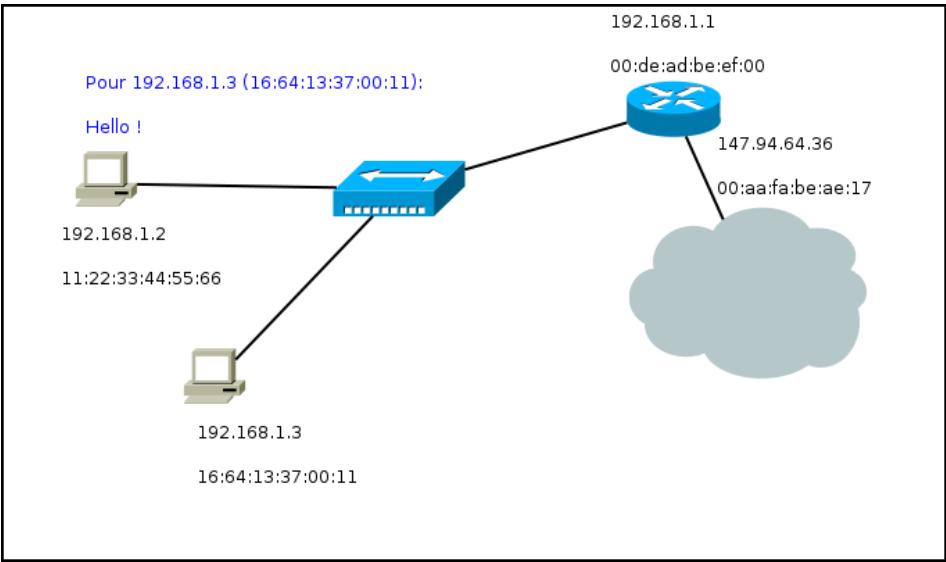
1.4 Conclusion

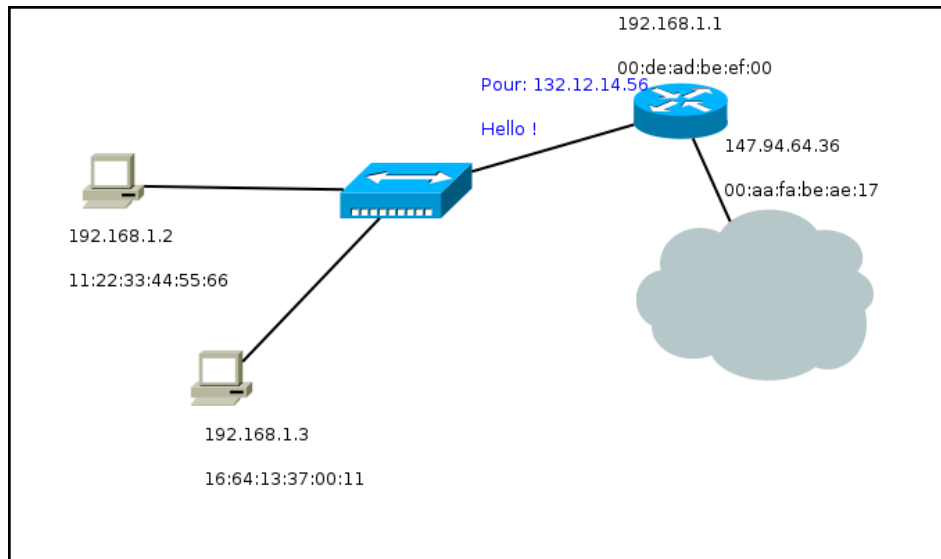
Exemple











2 IPv6

IPv6 (En bref)

- Adresses sur 16 octets (128 bits)
- Exemple : `aa00:fe80:dead:0213:a9ff:fea4:1919:ba0d`
- On utilise la notation `::` pour spécifier un groupe de 0.
- Exemple : `aa00::1213`
- `aa00::baba::ff00` n'est PAS valide
- Masque de 64 bits (4 paires) au maximum

IPv6 (Blocs réservés)

- `::1/128` : Machine locale (ne se voit jamais sur un réseau)

Réseaux privés (ne se voit jamais sur Internet)

- `fe80::/10` (plus exactement `fe80::/64`)
- Utilisé dans l'autoconfiguration (64 bits → on peut y coder l'adresse MAC)
- Toute interface IPv6 doit avoir au minimum une telle adresse

Également `fc00::/7`

IPv6 (Broadcast)

- Aucun moyen de faire un broadcast, mais des adresses de multicast (broadcast spécifique)
- `ff02::1` Tous les hôtes du réseau local
- `ff05::1:3` Tous les serveurs DHCP du réseau local

IPv6 (Services)

- ARP → NDP (Neighbor Discovery Protocol)
- NDP contient aussi bien ARP que ICMP (ping, etc)

3 Plus loin

Problème

- Mon FAI ne me donne qu'une adresse IPv4
- Comment brancher plusieurs machines derrière ?

NAT (Network address translation)

- Un réseau privé relié par un routeur à Internet
- Le routeur transforme les adresses privées pour faire croire que les messages viennent de lui
- Problème ?

NAT (Network address translation)

- Impossible à mettre en place uniquement au niveau IP.
- Utilise des propriétés des protocoles TCP/UDP.