ResEI 102 : Présentation des notions de réseau utilisées au ResEI

Association ResEI
<gestion@resel.fr>

Réseau des Élèves de l'ENST Bretagne

4 novembre 2010

Licence

Ces slides sont sous licence GPL (General Public Licence). Ils sont disponibles, avec leur code source sur le site de l'Association ResEl (`http ://resel.fr`).

Ils ont été créés à partir de logiciels libres (LaTeX-beamer).

Plan

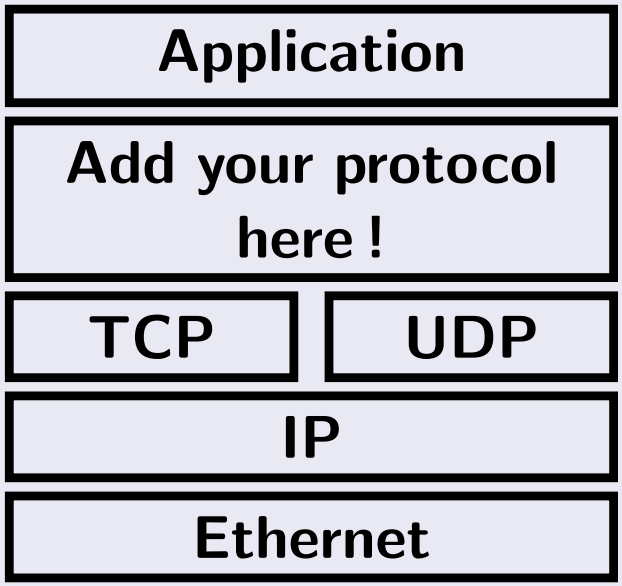
Plan

Ceci n'est pas un cours de RES

- Il faut avoir un minimum suivi en cours (être allé au premier amphi...)
- On ne va pas vous assomer avec trop de théorie :
  - une découverte des protocoles ;
  - présentation rapide de ceux-ci sans entrer dans les détails ;
  - pour ceux qui veulent en savoir plus, beaucoup de documentation sur internet (sites dédiés, RFCs, ...).

Un empilement de couches

De l'application à la transmission physique



votre application

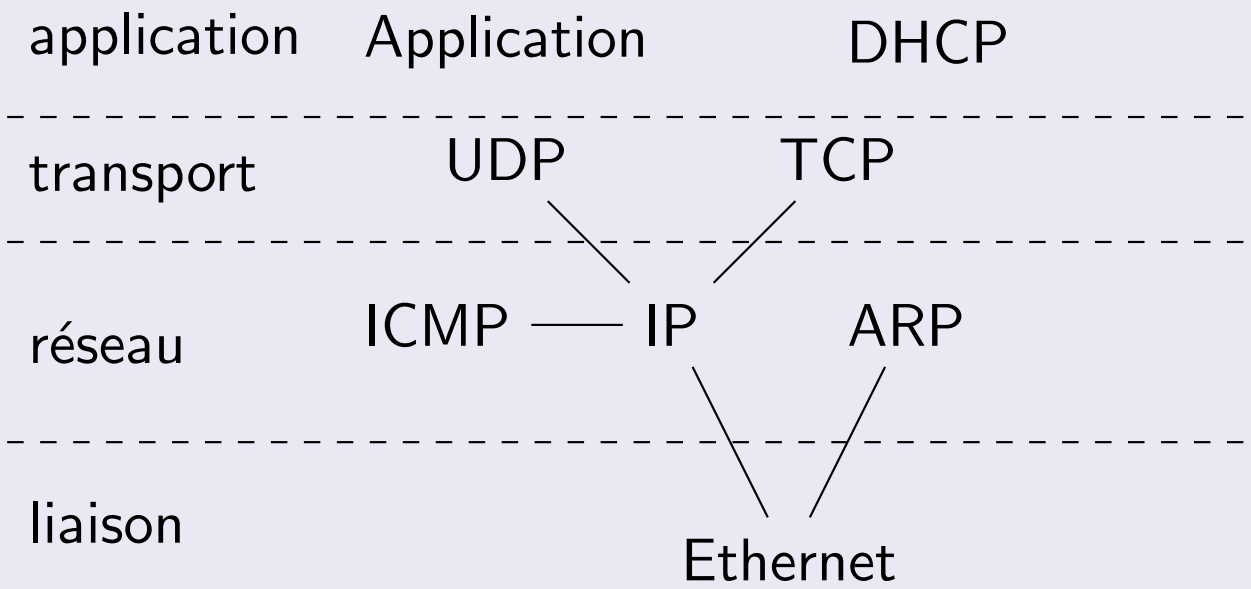
différenciation entre les applications

connexion entre les réseaux locaux

transmission physique et réseaux locaux

Un empilement de couche

Les protocoles utilisés en réseau



Plan

Ethernet

Ethernet

- Définition de la couche physique :
  cable RJ-45, fibre, ...
- Protocole de liaison
- Adressage des interfaces
  MAC = Medium Access Control
  adresse de 6 octets
- Exemple : 00-24-BE-B8-70-B9 souvent écrit 00:24:BE:B8:70:B9

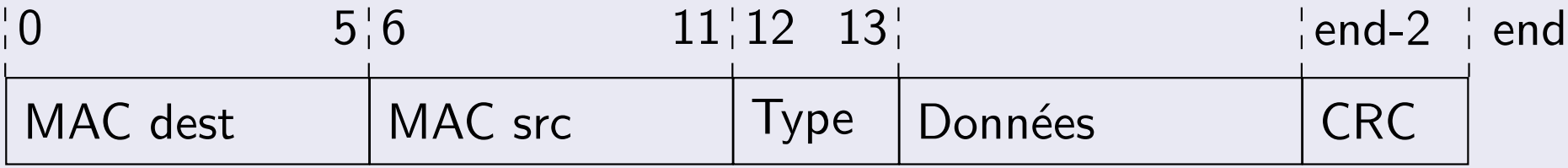
Ethernet

Adresses

- Format : $\underbrace{\text{00-24-BE}}_{\text{Organisationally Unique Identifier (OUI)}}$ - $\underbrace{\text{B8-70-B9}}_{\text{Network Interface Controller (NIC) Specific}}$
- Premier octet :
  - bit 0 :
    0 – unicast
    1 – multicast
  - bit 1 :
    0 – globally unique
    1 – locally administered

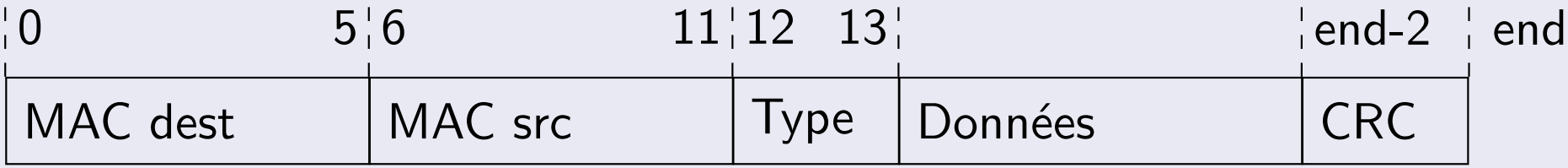
Ethernet

Entête Ethernet



Ethernet

Entête Ethernet



Type

- IPv4 : 0x800
- IPv6 : 0x86DD
- ARP : 0x806
- ...

Pont et commutateur

Pont (bridge)

- Relie deux réseaux
- Recopie les trames d'un réseau vers l'autre et vice-versa
- Écoute le réseau et établit une liste des MAC vue
- Ne recopie la trame que si l'adresse de destination est inconnu ou qu'elle se situe sur le réseau opposé
- Permet la conversion d'un support physique à un autre (exemple : RJ-45 $\rightarrow$ Fibre optique)

Commutateur (switch)

- Architecture similaire à un pont
- De 4 à plus de 48 interfaces réseaux
- Au ResEI, deux switchs par bâtiment (un de 48 et un de 24 ports)

Pont et commutateur

Pont (bridge)

- Relie deux réseaux
- Recopie les trames d'un réseau vers l'autre et vice-versa
- Écoute le réseau et établit une liste des MAC vue
- Ne recopie la trame que si l'adresse de destination est inconnu ou qu'elle se situe sur le réseau opposé
- Permet la conversion d'un support physique à un autre (exemple : RJ-45 $\rightarrow$ Fibre optique)

Commutateur (switch)

- Architecture similaire à un pont
- De 4 à plus de 48 interfaces réseaux
- Au ResEI, deux switchs par bâtiment (un de 48 et un de 24 ports)

Les VLANs

Sécurité de la couche Ethernet

- Problème : tout le monde peut communiquer avec tout le monde
- Pas de protection offerte par le réseau contre les attaques

Utilisation de VLAN

- Séparation en réseaux virtuel (VLAN)
- 1 VLAN = 1 identifiant
- Chaque port est placé dans un VLAN particulier
- Les ports dans des VLAN différents ne peuvent communiquer ensemble
- Ajout d'un champ dans la trame Ethernet

Les VLANs

Sécurité de la couche Ethernet

- Problème : tout le monde peut communiquer avec tout le monde
- Pas de protection offerte par le réseau contre les attaques

Utilisation de VLAN

- Séparation en réseaux virtuel (VLAN)
- 1 VLAN = 1 identifiant
- Chaque port est placé dans un VLAN particulier
- Les ports dans des VLAN différents ne peuvent communiquer ensemble
- Ajout d'un champ dans la trame Ethernet

Les VLANs

Entre les switchs

- trunk : Extension protocole Ethernet pour ajouter les numéros de VLAN dans les trames
- Permet d'avoir plusieurs VLAN sur la même interface
- Sous Linux : création de sous-interfaces virtuelles pour chaque VLAN
- Au ResEI : pas de trunk sur les ports utilisateurs sinon ils pourraient se connecter sur n'importe quel VLAN du trunk

Au ResEI

- 999 – Utilisateurs
- 995 – Inscription
- 996 – Contamination
- 994 – Administration : zone publique
- 997 – Administration : zone privée

Les VLANs

Entre les switchs

- trunk : Extension protocole Ethernet pour ajouter les numéros de VLAN dans les trames
- Permet d'avoir plusieurs VLAN sur la même interface
- Sous Linux : création de sous-interfaces virtuelles pour chaque VLAN
- Au ResEI : pas de trunk sur les ports utilisateurs sinon ils pourraient se connecter sur n'importe quel VLAN du trunk

Au ResEI

- 999 – Utilisateurs
- 995 – Inscription
- 996 – Contamination
- 994 – Administration : zone publique
- 997 – Administration : zone privée

Atouts et limites de l'Ethernet

Atouts de l'Ethernet

- Permet une connexion entre tout les machines du réseau
- Adressage unique : pas besoin de configuration
- Simple à mettre en œuvre
- Fiable : un paquet erroné est considéré comme perdu

Limites de l'Ethernet

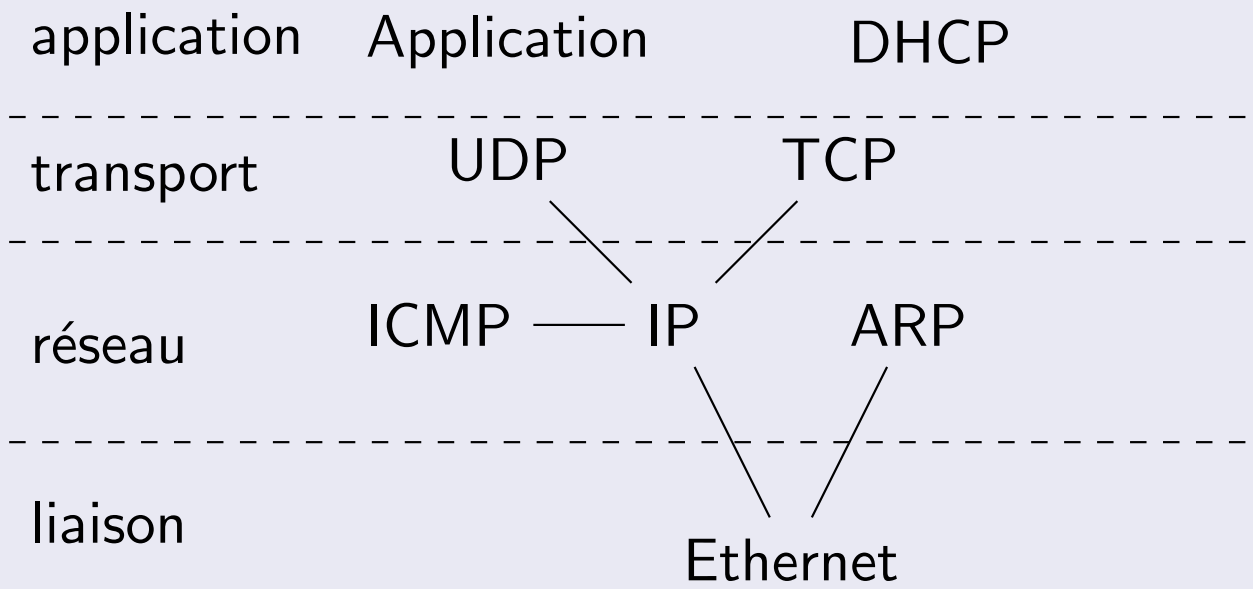
- Pas de contrôle de flux
- Pas de détection des erreurs et de mécanisme de retransmission
- Adressage plat : au niveau mondiale :
  trop de machine pour qu'un switch les connaissent tous
  explosion des algorithmes de routage : plus court chemin

$\Rightarrow$ Ethernet est bien pour un réseau local

Plan

Un empilement de couche

Les protocoles utilisés en réseau



L'Internet Protocol

L'Internet Protocol

- Internet = Inter – Network
- Protocole d'échange entre des réseaux Ethernet
- Réseau hiérarchique pour faciliter le routage

Format des adresses IPv4

- 4 paquets de 8 bits : 192.168.23.1
- Hiérarchie des réseaux : 192.168.23.0/255
- Par exemple au ResEl :
  - 172.22.0.0/16 : Brest
    - 172.22.192.0/19 : Utilisateurs
    - 172.22.224.0/23 : Inscriptions
    - ...
  - 172.23.0.0/16 : Rennes

Format des adresses IPv4

Catégories

- Adresses IP publiques
- Catégories d'adresses spéciales (non-exhaustif) :

Bloc	Usage
10.0.0.0/8	Adresses privés
127.0.0.0/8	Adresses de bouclage (localhost)
169.254.0.0/16	Adresses locales auto-configurées
172.16.0.0/12	Adresses privées
192.88.99.0/24	6to4 anycast
192.168.0.0/16	Adresses privées
224.0.0.0/4	Multicast
255.255.255.255/32	Broadcast

- À quelle catégorie appartient 172.22.215.2 ?
- À quelle catégorie appartient 192.44.76.8 ?

Format des adresses IPv4

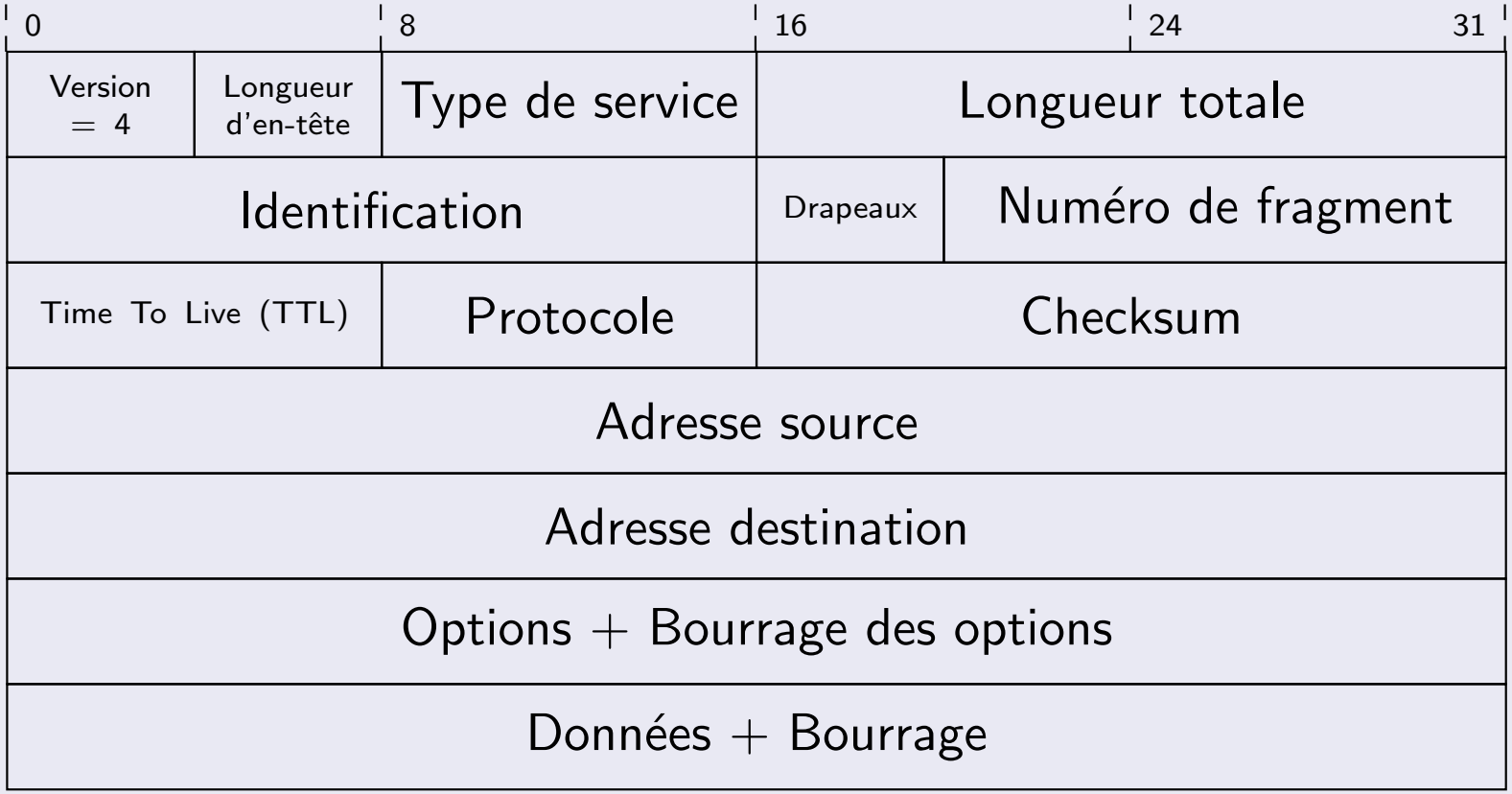
En binaire

- 172.22.215.2 → 10101100 00010110 11010111 00000010
- 19 premiers bits fixés : masque de sous-réseau
  255.255.255.224 → 11111111 11111111 11100000 00000000
- Retrouvez l'adresse réseau à partir d'une adresse de machine :
  10101100000101101101011100000010
  & 11111111111111111110000000000000
  10101100000101101100000000000000

  10101100 00010110 11000000 00000000 → 172.22.192.0

Les paquets IP

Entête IPv4



Le routage

Les routeurs

- Reçoit des paquets et les transmet sur la bonne interface
- Utilise une table de routage
- Table de routage d'une machine Linux :

```
Kernel IP routing table
Destination     Gateway         Genmask         Iface
172.22.192.0    *               255.255.224.0   eth0
default         grandours.cop.m 0.0.0.0         eth0
```

Table de routage de Grand Ours

```
grandours>show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 172.16.29.1 to network 0.0.0.0

C    192.168.29.0/24 is directly connected, Vlan990
R    192.44.75.0/24 [120/1] via 172.16.29.1, 00:00:31, Vlan999
     192.44.76.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.44.76.0/24 [1/0] via 172.16.19.1
S       192.44.76.8/32 [1/0] via 172.16.29.1
S       192.44.76.108/32 [1/0] via 172.16.29.1
C    172.16.0.0/16 is directly connected, Vlan999
     172.23.0.0/16 is variably subnetted, 5 subnets, 3 masks
S       172.23.192.0/19 [1/0] via 172.16.29.1
S       172.23.42.0/23 [1/0] via 172.16.29.1
S       172.23.2.0/23 [1/0] via 172.16.29.1
S       172.23.0.0/23 [1/0] via 172.16.29.1
S       172.23.99.0/24 [1/0] via 172.16.29.1
```

Table de routage de Grand Ours

```
      172.22.0.0/16 is variably subnetted, 8 subnets, 4 masks
R        172.22.150.35/32 [120/1] via 172.16.29.1, 00:00:31, Vlan999
C        172.22.224.0/23 is directly connected, Vlan999
C        172.22.230.0/24 is directly connected, Vlan999
C        172.22.228.0/23 is directly connected, Vlan999
C        172.22.192.0/19 is directly connected, Vlan999
C        172.22.42.0/23 is directly connected, Vlan994
C        172.22.2.0/23 is directly connected, Vlan997
C        172.22.92.0/24 is directly connected, Vlan992
      192.108.115.0/24 is variably subnetted, 2 subnets, 2 masks
S        192.108.115.12/32 [1/0] via 172.16.29.1
S        192.108.115.0/24 [1/0] via 172.16.19.1
      193.50.97.0/25 is subnetted, 1 subnets
R        193.50.97.128 [120/1] via 172.16.29.1, 00:00:31, Vlan999
      10.0.0.0/16 is subnetted, 3 subnets
S        10.29.0.0 [1/0] via 172.16.19.1
S        10.35.0.0 [1/0] via 172.16.29.1
S        10.66.0.0 [1/0] via 172.16.19.1
S     192.168.0.0/24 [1/0] via 172.16.29.1
S     192.108.118.0/24 [1/0] via 172.16.19.1
S     192.108.117.0/24 [1/0] via 172.16.19.1
S     192.108.116.0/24 [1/0] via 172.16.19.1
S*    0.0.0.0/0 [1/0] via 172.16.29.1
S     192.168.0.0/16 [1/0] via 172.16.19.1
```

Traceroute

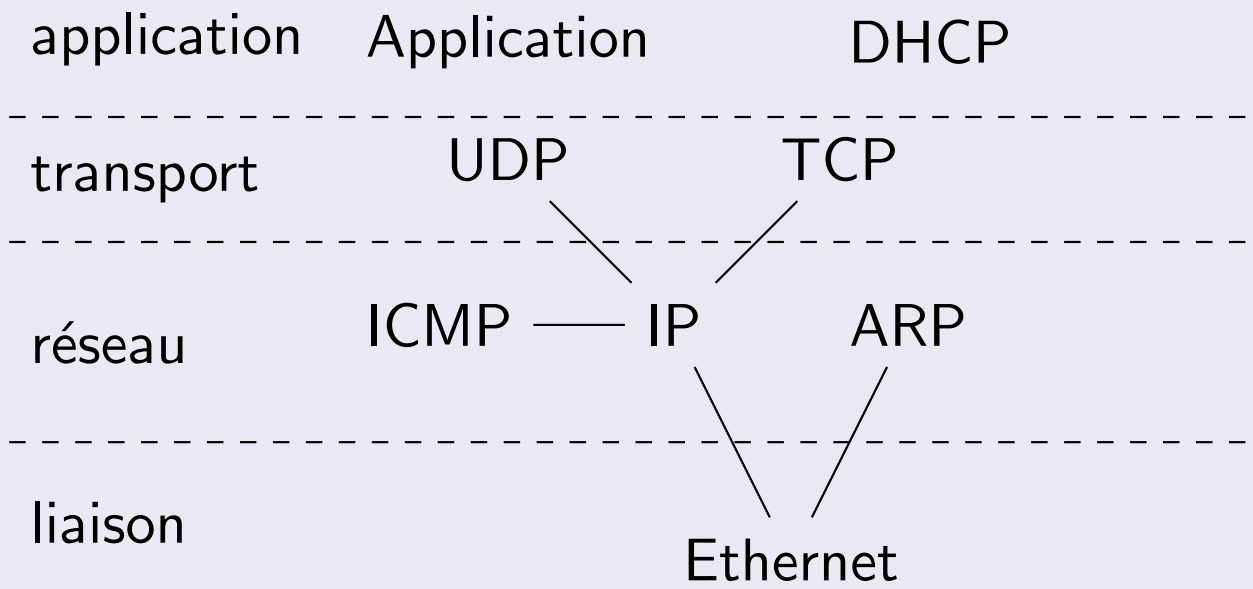
```
traceroute [(172.22.215.2:33456) -> (66.211.214.131:33457)], protocol icmp, algo hopbyhop, d
 1  grandours.cop.maisel.enst-bretagne.fr (172.22.199.1)  0.582 ms   0.630 ms   0.862 ms
 2  serveur.old.maisel.enst-bretagne.fr (172.16.29.1)  0.410 ms   0.424 ms   0.431 ms
 3  galaxie-76.enst-bretagne.fr (192.44.76.1)  0.923 ms   0.781 ms   0.711 ms
 4  gw-out.enst-bretagne.fr (192.108.117.65)  0.716 ms   0.989 ms   0.746 ms
 5  vl807-te1-5-brest1-rtr-021.noc.renater.fr (193.51.188.10)  1.436 ms   1.184 ms   1.171 m
 6  te1-3-lannion-rtr-021.noc.renater.fr (193.51.179.130)  63.165 ms !T2   60.969 ms !T2
62.698 ms !T2
    MPLS Label 27 TTL=1
 7  te1-3-stbrieuc-rtr-021.noc.renater.fr (193.51.179.126)  16.769 ms !T3   16.659 ms !T3
16.831 ms !T3
    MPLS Label 169 TTL=1
 8  te2-1-rennes-rtr-021.noc.renater.fr (193.51.179.122)  16.765 ms !T4   16.879 ms !T4
16.683 ms !T4
    MPLS Label 138 TTL=1
 9  te4-1-caen-rtr-021.noc.renater.fr (193.51.189.54)  16.781 ms !T5   16.674 ms !T5   16.882
    MPLS Label 408 TTL=1
10  te4-1-rouen-rtr-021.noc.renater.fr (193.51.189.46)  17.016 ms !T6   16.722 ms !T6   16.69
    MPLS Label 130 TTL=1
```

Traceroute

```
11  te0-0-0-1-paris1-rtr-001.noc.renater.fr (193.51.189.49)  17.563 ms !T7   17.058 ms !T7
17.289 ms !T7
    MPLS Label 16401 TTL=255
12  te0-3-1-0-lyon1-rtr-001.noc.renater.fr (193.51.189.126)  17.500 ms   17.248 ms   17.236 m
13  xe-8-0-0.edge5.Paris1.Level3.net (212.73.207.173)  96.025 ms   95.993 ms   96.898 ms
14  ae-34-52.ebr2.Paris1.Level3.net (4.69.139.225)  96.227 ms   96.189 ms   96.130 ms
15  ae-47-47.ebr1.Frankfurt1.Level3.net (4.69.143.141)  106.159 ms   105.767 ms   105.385 ms
16  ae-81-81.csw3.Frankfurt1.Level3.net (4.69.140.10)  113.334 ms   161.281 ms   111.731 ms
17  ae-82-82.ebr2.Frankfurt1.Level3.net (4.69.140.25)  106.770 ms   106.756 ms   106.562 ms
18  ae-41-41.ebr2.Washington1.Level3.net (4.69.137.50)  106.990 ms   106.833 ms   106.622 ms
19  ae-72-72.csw2.Washington1.Level3.net (4.69.134.150)  112.615 ms   116.777 ms   106.913 m
20  ae-71-71.ebr1.Washington1.Level3.net (4.69.134.133)  107.090 ms   107.171 ms   107.630 m
21  ae-5-5.car1.Pittsburgh3.Level3.net (4.69.135.241)  112.523 ms   113.242 ms   113.261 ms
22  ae-11-11.car2.Pittsburgh3.Level3.net (4.69.135.246)  251.504 ms   201.958 ms   152.441 m
23  VELOCITYNET.car2.Pittsburgh3.Level3.net (4.49.110.66)  120.077 ms   120.124 ms   120.167
24  cust02-ge-0-0.eri.velocity.net (66.211.250.2)  121.259 ms   120.932 ms   120.730 ms
25  gudrun.archlinux.org (66.211.214.131)  120.003 ms   204.690 ms   155.079 ms
```

Un empilement de couche

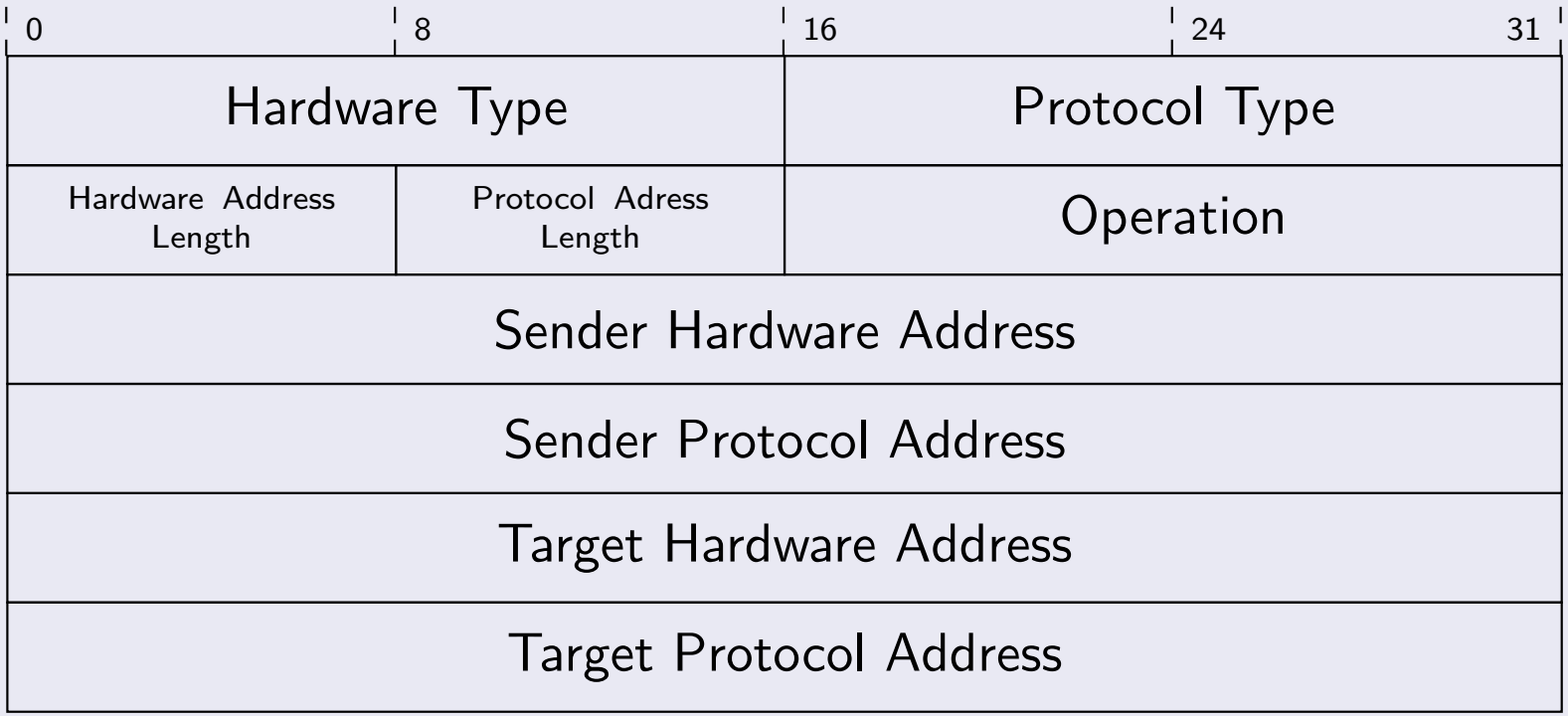
Les protocoles utilisés en réseau



Les requêtes ARP

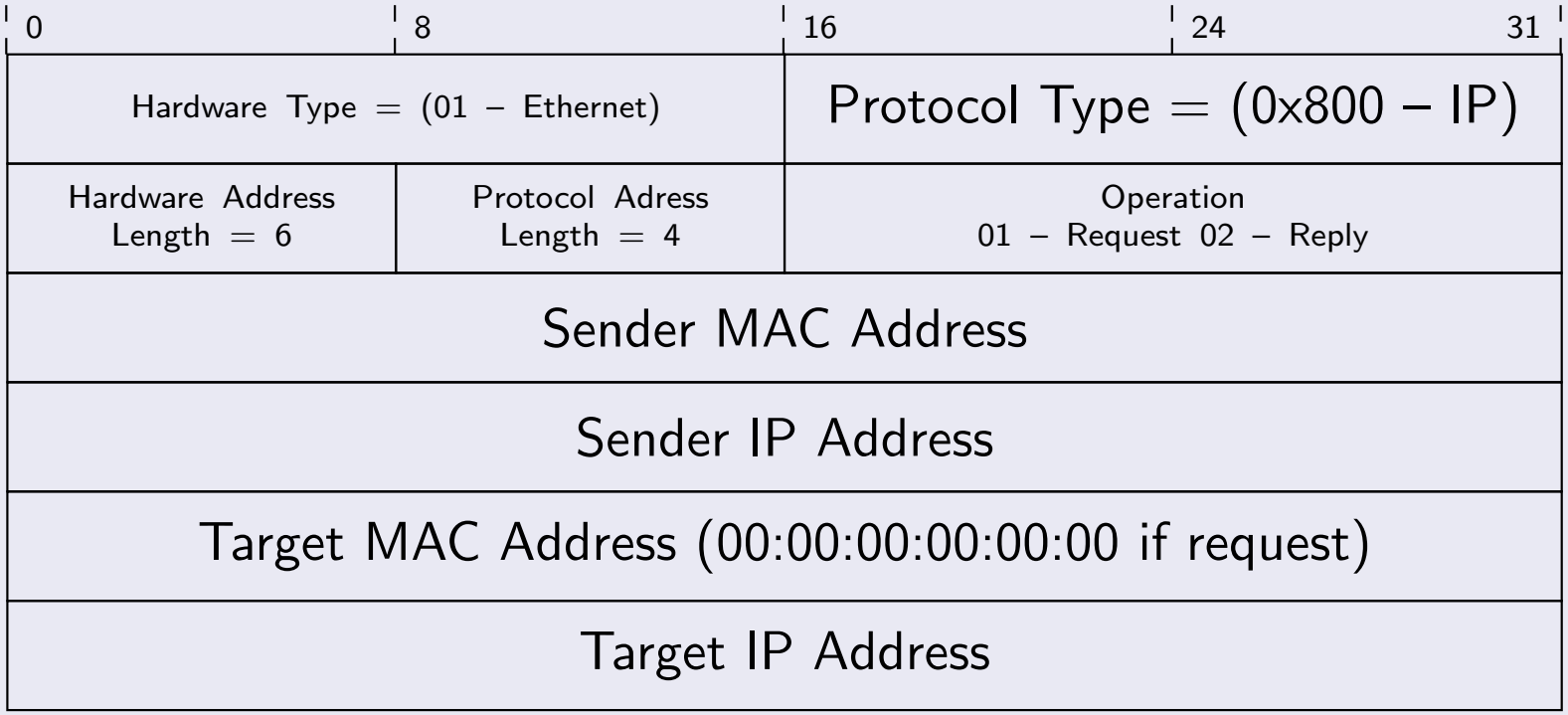
But d'ARP

- ARP : Address Resolution Protocol
- Protocole générique trouver une adresse matériel
- Utilisation : Résolution IP $\longrightarrow$ MAC



Les requêtes ARP

Requête ARP en IPv4



Transmission d'un paquet IP

Description du réseau

- Sous-réseau 172.22.192.0/19
- Machine A (@a, 172.22.215.2)
- Machine B (@b, 172.22.203.127)
- Routeur C grandours (@c, 172.22.199.1)

Transmission de A vers B

- A et B sont dans le même sous-réseau

Transmission de A vers B

- A et B sont dans le même sous-réseau
- A émet une requête ARP who-has 172.22.203.172

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.203.172

Transmission de A vers B

- A et B sont dans le même sous-réseau
- A émet une requête ARP who-has 172.22.203.172

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.203.172

- B répond (@b, 172.22.203.172)

dest mac	src mac	proto	op	target mac	target IP
@a	@b	ARP	reply	@b	172.22.203.172

Transmission de A vers B

- A et B sont dans le même sous-réseau
- A émet une requête ARP who-has 172.22.203.172

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.203.172

- B répond (@b, 172.22.203.172)

dest mac	src mac	proto	op	target mac	target IP
@a	@b	ARP	reply	@b	172.22.203.172

- A envoie le paquet IP à l'adresse @b

dest mac	src mac	proto	ip src	ip dest
@b	@a	IP	172.22.215.2	172.22.203.172

Transmission de A vers google.fr

- A et C ne sont pas dans le même sous-réseau

Transmission de A vers google.fr

- A et C ne sont pas dans le même sous-réseau
- le paquet doit être routé par C d'après la table de routage

Transmission de A vers google.fr

- A et C ne sont pas dans le même sous-réseau
- le paquet doit être routé par C d'après la table de routage
- A émet une requête ARP who-has 172.22.199.1

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.199.1

Transmission de A vers google.fr

- A et C ne sont pas dans le même sous-réseau
- le paquet doit être routé par C d'après la table de routage
- A émet une requête ARP who-has 172.22.199.1

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.199.1

- C répond (@c, 172.22.199.1)

dest mac	src mac	proto	op	target mac	target IP
@a	@c	ARP	reply	@c	172.22.199.1

Transmission de A vers google.fr

- A et C ne sont pas dans le même sous-réseau
- le paquet doit être routé par C d'après la table de routage
- A émet une requête ARP who-has 172.22.199.1

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.199.1

- C répond (@c, 172.22.199.1)

dest mac	src mac	proto	op	target mac	target IP
@a	@c	ARP	reply	@c	172.22.199.1

- A envoie le paquet IP à l'adresse @c qui le retransmet en utilisant sa table de routage

dest mac	src mac	proto	ip src	ip dest
@c	@a	IP	172.22.215.2	66.249.92.104

Transmission de A vers google.fr

- A et C ne sont pas dans le même sous-réseau
- le paquet doit être routé par C d'après la table de routage
- A émet une requête ARP who-has 172.22.199.1

dest mac	src mac	proto	op	target mac	target IP
broadcast	@a	ARP	request	0	172.22.199.1

- C répond (@c, 172.22.199.1)

dest mac	src mac	proto	op	target mac	target IP
@a	@c	ARP	reply	@c	172.22.199.1

- A envoie le paquet IP à l'adresse @c qui le retransmet en utilisant sa table de routage

dest mac	src mac	proto	ip src	ip dest
@c	@a	IP	172.22.215.2	66.249.92.104

- et C va renvoyer le paquet à D par exemple et ainsi de suite jusqu'à destination finale

dest mac	src mac	proto	ip src	ip dest
@d	@c	IP	172.22.215.2	66.249.92.104