

# TP sur IP

L'objectif de ce premier TP est de vous montrer comment les données circulent dans un réseau, comment elles sont représentées, empilées/dépilées par la pile TCP/IP. Accessoirement vous verrez comment configurer une interface réseau sous Linux.

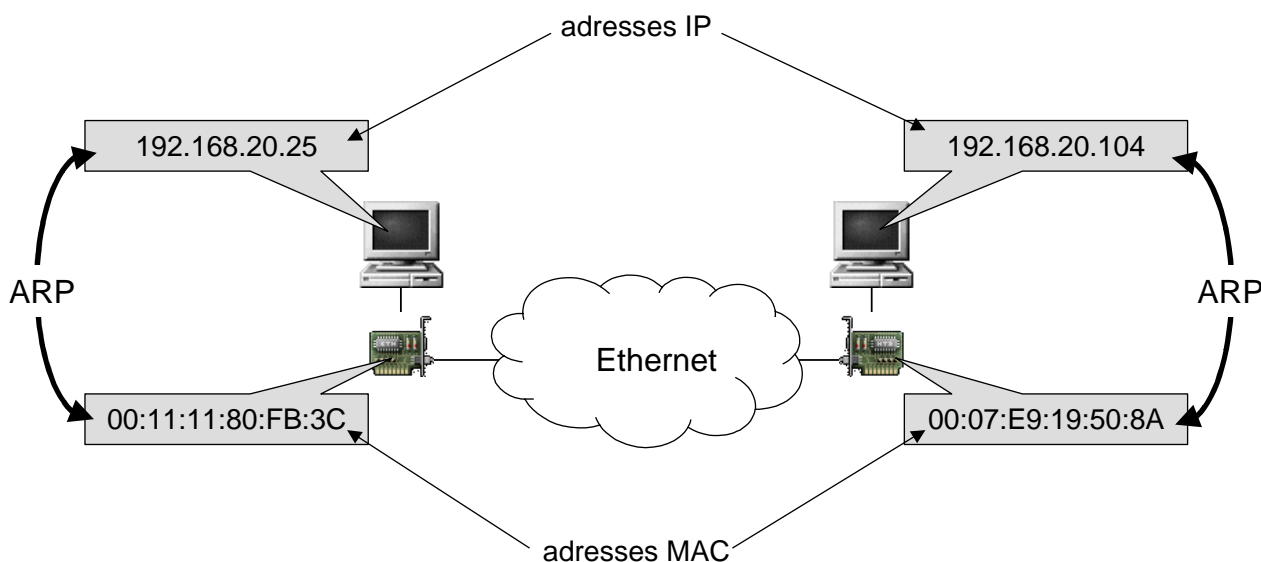
# Préambule

## Adresses MAC, adresses IP, système DNS

- En TCP/IP, chaque machine du réseau est identifiée par une adresse codée sur 32 bits (4 octets en notation décimale pointée), son **adresse IP**  
Exemple : 192.168.20.25
- Chaque carte réseau dispose d'une adresse codée sur 48 bits (6 octets en notation hexadécimale), son **adresse MAC**.  
Exemple : 00:11:11:80:FB:3C

Les machines utilisent leurs adresses IP pour communiquer entre elles, mais au niveau du réseau physique sous-jacent (Ethernet dans notre cas), c'est l'adresse MAC qui est utilisée dans les trames échangées.

Le protocole ARP ou *Address Resolution Protocol*, permet de faire la correspondance entre les deux adresses (son fonctionnement fait l'objet de ce premier TP).



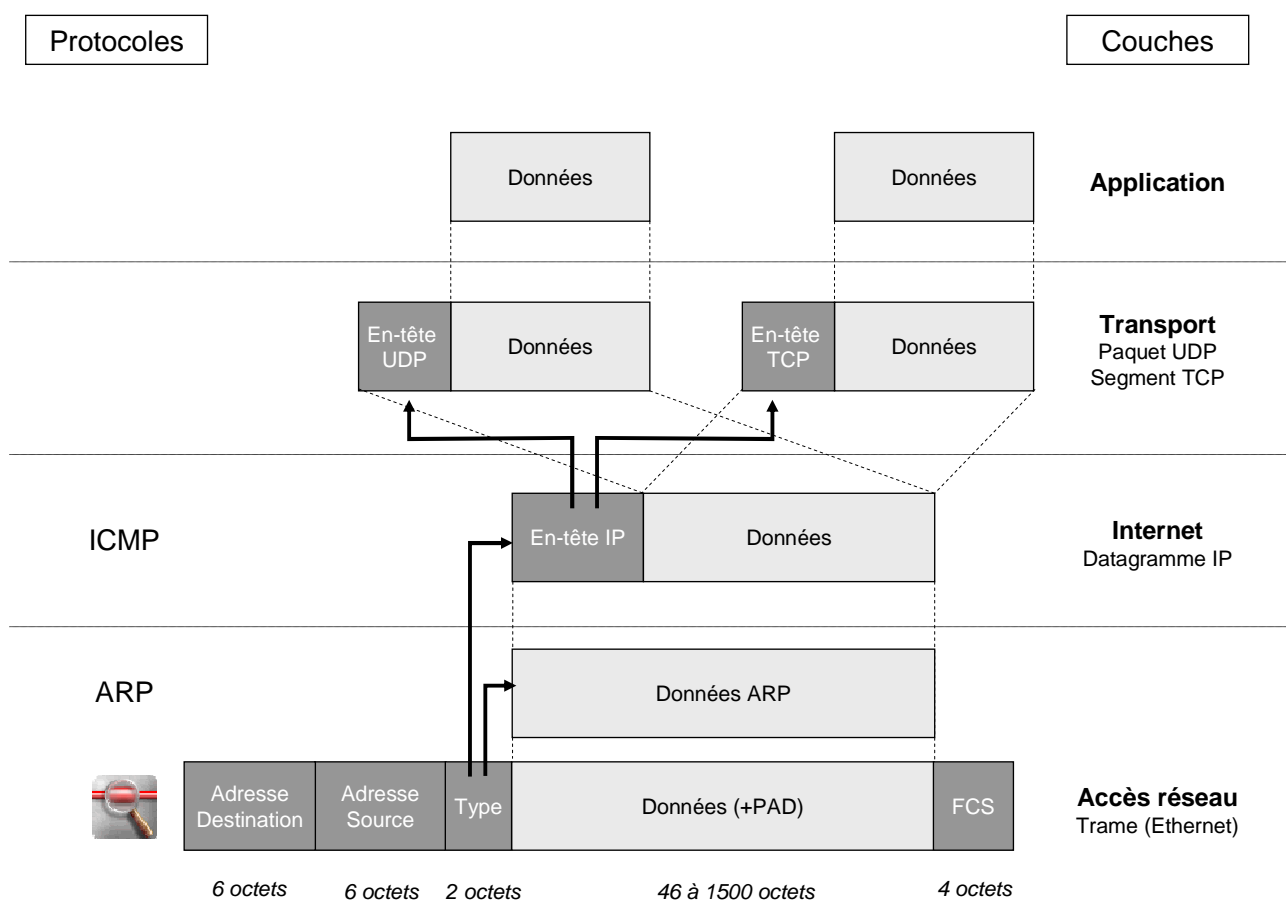
Chaque machine possède donc une adresse IP qui lui est propre. Cependant, il est plus commode pour les utilisateurs de travailler avec des noms symboliques plutôt qu'avec des adresses numériques. Un mécanisme présent dans TCP/IP, le **système DNS** (*Domain Name System*), permet d'associer des noms en langage courant aux adresses IP (exemple : prevert.upmf-grenoble.fr  $\Leftrightarrow$  195.221.42.159).

## Le protocole ICMP

Le protocole ICMP (*Internet Control Message Protocol*) permet de gérer des problèmes au niveau de la couche IP. Il fournit des messages de contrôle pour indiquer les erreurs pendant la transmission du datagramme IP.

Il existe 18 types de messages ICMP. Les deux types de messages employés par la commande ping sont :

- Le type 8 (echo request) est émis vers la machine distante.
- Le type 0 (echo reply) est émis par la machine distante en réponse.



# Paramètres réseau

- La commande `ethtool` permet de visualiser ou de changer les paramètres d'une carte Ethernet. Dans les systèmes Linux, les interfaces réseau sont nommées de la façon suivante : le type de l'interface plus un numéro 0, 1, 2,... Ainsi, l'interface `eth0` est la première interface de type Ethernet.
- La commande `ifconfig` permet de visualiser ou changer les paramètres TCP/IP d'une interface réseau.



Changer les paramètres de la carte Ethernet ou de l'interface réseau requiert des privilèges administrateur

- 1) Donnez les propriétés et capacités de la carte Ethernet `eth0` de votre machine à l'aide de la commande `ethtool`
  - quel est le type de réseau Ethernet utilisé ?
  - quelle est la vitesse de transmission ?
  - quel est le mode de transmission ?
- 2) Trouvez à l'aide de la commande : **`ifconfig`**
  - l'adresse Ethernet de votre carte réseau,
  - l'adresse IP de votre machine,
  - l'adresse du réseau,
  - l'adresse de broadcast du réseau,
  - le masque du réseau,
  - la classe du réseau
  - la *Maximum Transfer Unit*
- 3) A l'aide de la commande `ifconfig`, attribuez à votre machine une nouvelle adresse IP. Vous utiliserez comme adresse `192.168.x.y` avec *x* correspondant au numéro de la salle et *y* au dernier nombre qui apparaît dans le nom de votre machine. Par exemple, la machine `bshm-120-2` aura comme adresse IP `192.168.120.2`, `bshm-121-5` aura comme adresse `192.168.121.5`.

La syntaxe de la commande est la suivante :

```
ifconfig eth0 adresse_ip netmask 255.255.255.0 up
```

- 4) Affichez à nouveau la configuration des paramètres réseau avec la commande `ifconfig`. Que constatez-vous ?
- 5) Avant de poursuivre le TP, remettez les paramètres TCP/IP par défaut en tapant la commande :  
`service network restart`

# ARP

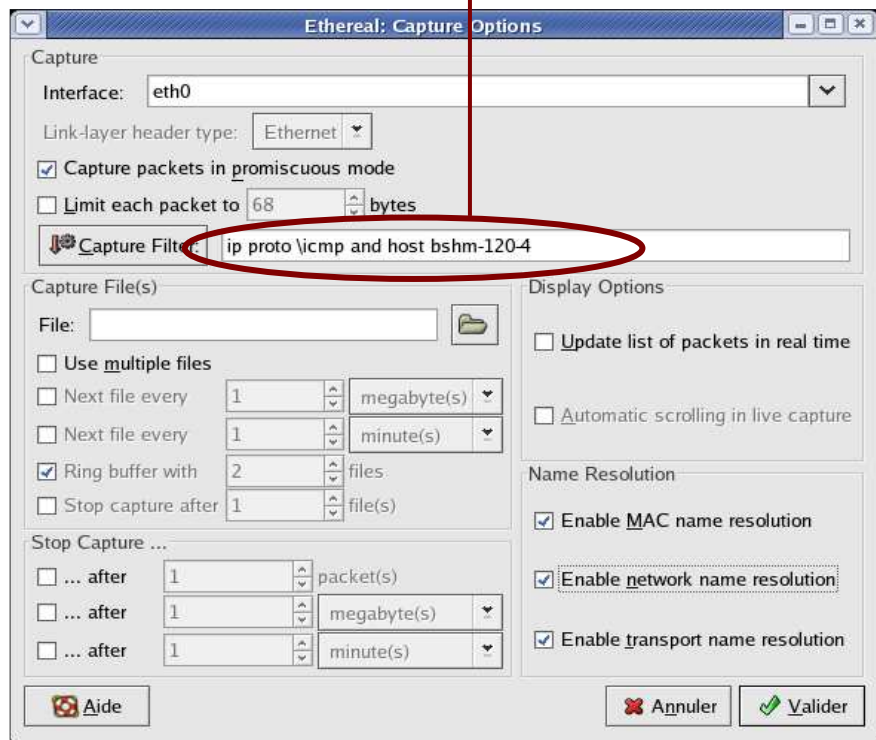
## (*Address Resolution Protocol*)

- Affichez le contenu de la table ARP avec la commande : `arp`
- Pour obtenir de l'aide sur `arp`
  - `arp -h`
  - `man arp`
- Affichez le contenu de la table `arp` avec les adresses IP au lieu des noms de machines
- Lancez la commande `ping brassens.upmf-grenoble.fr`
  - Appuyez sur Ctrl+C pour arrêter
- Affichez à nouveau le contenu de la table ARP. Que constate-t-on ?
- Quelle est l'adresse Ethernet de *brassens* ?
- Lancez la commande `ping ntp.imag.fr`
- Affichez à nouveau le contenu de la table ARP. Que constate-t-on ?

# Analyse du trafic ICMP (Internet Control Message Protocol)

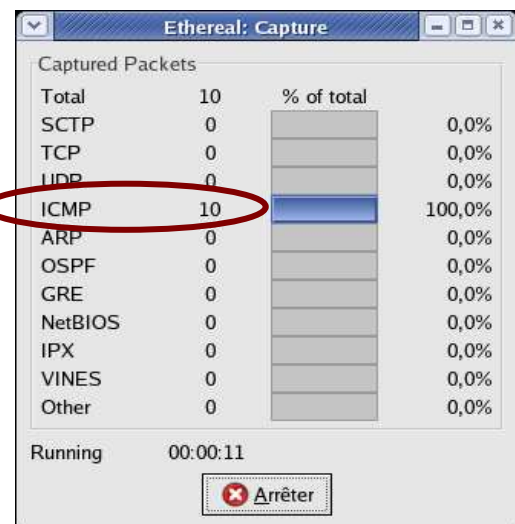
- 1) Dans ethereal, capturez (menu Capture->Start) les trames ICMP en partance ou à destination de votre machine générées par la commande ping
  - Utilisez comme filtre de capture :  
`ip proto \icmp and host nom_machine`
  - Exemple pour la machine `bshm-120-4`, le filtre sera :  
`ip proto \icmp and host bshm-120-4`

N'oubliez pas de préfixer le nom du protocole par le caractère « \ » et de remplacer `bshm-120-4` par le nom exacte de votre machine



- 2) Une fois la capture démarrée, **dans une autre fenêtre shell** exécutez la commande `ping brassens.upmf-grenoble.fr`
- 3) Arrêtez la capture au bout de 10 trames ICMP minimum

Nombre de trames ICMP capturées



L'interface du logiciel ethereal regroupe plusieurs zones.

- La zone (1) contient la liste des paquets capturés disponibles avec un affichage synthétique du contenu de chaque paquet
- La zone (2) contient le décodage exact du paquet actuellement sélectionné dans la liste. Ce décodage permet de visualiser les champs des entêtes des protocoles ainsi que l'imbrication des différentes couches de protocoles connus.
- La zone (3) contient le paquet (le début s'il est trop gros) affiché en hexadécimal et en ASCII.
- La zone (4) permet de spécifier les critères d'affichage des paquets capturés (par exemple parmi tous les paquets capturés, afficher uniquement les paquets ARP). Attention : **la syntaxe du filtre d'affichage est différente de celle du filtre de capture.**

4) Pour les trames 1 à 4 :

- Analysez le contenu de la trame Ethernet
- Analysez les données IP
- Analyser les données ICMP

The screenshot shows the Ethereal interface with the following content:

**Zone 1: Packet List**

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	bsh-m-120-4.upmf-grenoble.fr	cros.upmf-grenoble.fr	ICMP	Echo (ping) request
2	0.000510	cros.upmf-grenoble.fr	bsh-m-120-4.upmf-grenoble.fr	ICMP	Echo (ping) reply
3	1.000439	bsh-m-120-4.upmf-grenoble.fr	cros.upmf-grenoble.fr	ICMP	Echo (ping) request
4	1.000855	cros.upmf-grenoble.fr	bsh-m-120-4.upmf-grenoble.fr	ICMP	Echo (ping) reply
5	2.000289	bsh-m-120-4.upmf-grenoble.fr	cros.upmf-grenoble.fr	ICMP	Echo (ping) request
6	2.000671	cros.upmf-grenoble.fr	bsh-m-120-4.upmf-grenoble.fr	ICMP	Echo (ping) reply
7	3.000137	bsh-m-120-4.upmf-grenoble.fr	cros.upmf-grenoble.fr	ICMP	Echo (ping) request
8	3.000545	cros.upmf-grenoble.fr	bsh-m-120-4.upmf-grenoble.fr	ICMP	Echo (ping) reply
9	3.999984	bsh-m-120-4.upmf-grenoble.fr	cros.upmf-grenoble.fr	ICMP	Echo (ping) request
10	4.000322	cros.upmf-grenoble.fr	bsh-m-120-4.upmf-grenoble.fr	ICMP	Echo (ping) reply

**Zone 2: Packet Details (Frame 1)**

```

Frame 1 (98 bytes on wire, 98 bytes captured)
Ethernet II, Src: 00:0f:1f:d8:9b:0d, Dst: 00:60:b0:57:43:bc
Internet Protocol, Src Addr: bsh-m-120-4.upmf-grenoble.fr (195.221.42.99), Dst Addr: cros.upmf-grenoble.fr (195.221.42.157)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 84
  Identification: 0x0000 (0)
  Flags: 0x04
  Fragment offset: 0
  Time to live: 64
  Protocol: ICMP (0x01)
  Header checksum: 0x5dee (correct)
  Source: bsh-m-120-4.upmf-grenoble.fr (195.221.42.99)
  Destination: cros.upmf-grenoble.fr (195.221.42.157)
Internet Control Message Protocol
  
```

**Zone 3: Hex Dump**

```

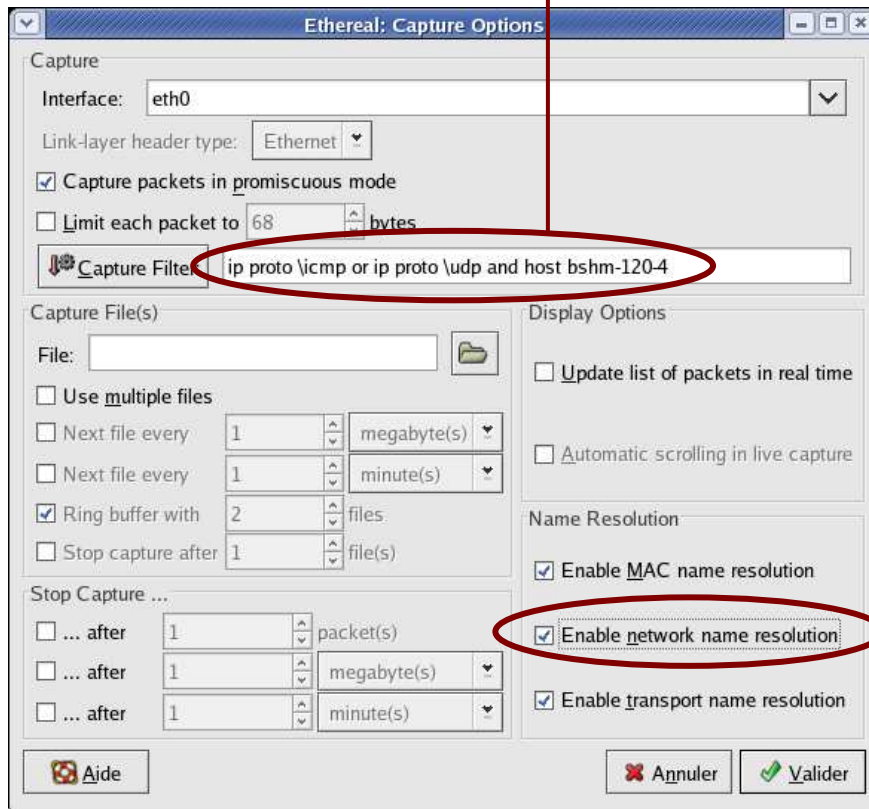
0000  00 60 b0 57 43 bc 00 0f 1f d8 9b 0d 08 00 45 00  .`.WC... ..E.
0010  00 54 00 00 40 00 40 01 5d ee c3 dd 2a 63 c3 dd  .T..@.@ ]...*c..
0020  2a 9d 08 00 2c 8c 16 12 00 00 9e 74 08 42 16 a8  *....,... ..t.B..
0030  0d 00 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15  .....!""#$%
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  &'()*+,- ./012345
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  67
0060  36 37
  
```

**Zone 4: Filter Bar**

Filter: [ ] Expression... Effacer Appliquer Protocol (ip.pr P: 10 D: 10 M

# Analyse de la commande *traceroute*

- 1) Dans *ethereal*, capturez (menu Capture->Start) les paquets ICMP et UDP en partance ou à destination de votre machine
  - Utilisez comme filtre de capture :  
`ip proto \icmp or ip proto \udp and host nom_machine`
  - Exemple pour la machine *bshm-120-4*



Cochez cette case pour afficher dans les trames capturées les noms des machines au lieu des adresses IP.

- 2) Dans une autre fenêtre shell, lancez la commande `traceroute www.lip6.fr`
- 3) Arrêtez la capture dès la fin de l'exécution de la commande
- 4) Expliquez le fonctionnement de la commande `traceroute` en analysant les trames capturées



Après la capture, pour n'avoir dans *ethereal* que les trames UDP et ICMP générées par la commande `traceroute`, vous pouvez appliquer un filtre d'affichage. Indiquez dans la zone (4) en bas à gauche (cf schéma page précédente) :

```
udp.srcport > 30000 and udp.dstport > 30000
```



# Analyse de l'exécution de *traceroute*

- Exemple de l'exécution de traceroute depuis la machine *arsenic.icp.inpg.fr* vers *prevert.upmf-grenoble.fr* :
  - traceroute envoie 3 paquets UDP avec un Time To Live (TTL) égal à 1, puis à 2, à 3, ... jusqu'à atteindre la destination
  - un message d'erreur ICMP est généré à chaque fois que le TTL arrive à 0

(Untitled) - Ethereal

File Edit View Go Capture Analyze Statistics Help

No. -	Time	Source	Destination	Protocol	Info
5	0.017100	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33435
6	0.017628	rt-vlan1.icp.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
9	0.019282	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33436
10	0.019755	rt-vlan1.icp.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
11	0.019941	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33437
12	0.020506	rt-vlan1.icp.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
13	0.021376	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33438
14	0.022000	cisco-icp.icp.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
17	0.023645	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33439
18	0.024254	cisco-icp.icp.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
19	0.028871	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33440
20	0.029499	cisco-icp.icp.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
21	0.029899	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33441
22	0.030371	C6-viallet.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
25	0.037124	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33442
26	0.037495	C6-viallet.inpg.fr	arsenic.icp.inpg.fr	ICMP	Time-to-live exceeded
27	0.037843	arsenic.icp.inpg.fr	prevert.upmf-grenoble.fr	UDP	Source port: 32785 Destination port: 33443

▶ Frame 5 (52 bytes on wire, 52 bytes captured)

▶ Ethernet II, Src: 00:07:e9:19:a0:3e, Dst: 00:0a:b7:a3:4a:00

▼ Internet Protocol, Src Addr: arsenic.icp.inpg.fr (195.83.80.28), Dst Addr: prevert.upmf-grenoble.fr (195.221.42.159)

- Version: 4
- Header length: 20 bytes
- ▶ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
- Total Length: 38
- Identification: 0x6d9f (28063)
- ▶ Flags: 0x00
- Fragment offset: 0
- Time to live: 1
- Protocol: UDP (0x11)

```
0000  00 0a b7 a3 4a 00 00 07 e9 19 a0 3e 08 00 45 00  ....J... >...E.
0010  00 26 6d 9f 00 00 01 11 4a 3c c3 53 50 1c c3 dd  .&m..... J<.SP...
0020  2a 9f 80 11 82 9b 00 12 0c ea 01 01 63 66 24 42  *..... .cf$B
0030  58 9d 0d 00                                     X...
```

Filter: udp.srcport > 30000 and udp.dstport > 30000

File: (Untitled) 3722 bytes 0 P: 37 D: 25 M: 0

# Analyse du protocole ARP

- Analysez une séquence de résolution d'adresse avec ARP
  - 1) Utilisez comme filtre de capture : `ether proto \arp`
  - 2) Afficher la table ARP
  - 3) « pingez » une machine de votre réseau qui n'est pas encore dans votre table ARP
  - 4) Arrêtez la capture et analysez les deux trames échangées