U.F.R. Sciences de l'Homme et de la Société
Licence MIASHS

TP 2 sur IP

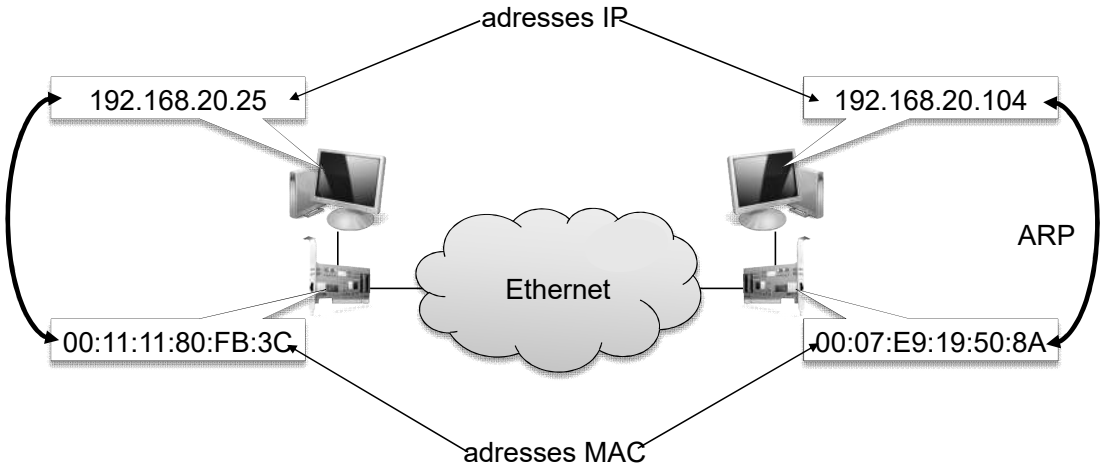
L'objectif de ce second TP est de vous faire comprendre :

- l'adressage IP,
- la fragmentation IP,
- le fonctionnement du TTL IP avec la commande `traceroute`,
- le fonctionnement du protocole ARP,
- le fonctionnement des protocoles de couche transport UDP et TCP à travers l'étude des protocoles applicatifs DNS et SSH

Préambule

Le protocole ARP

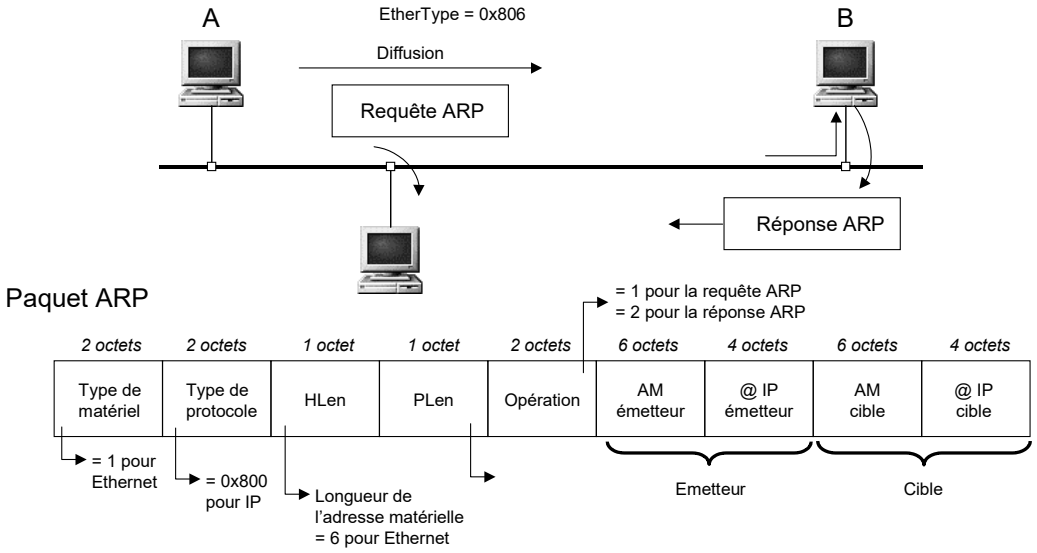
Un mécanisme souple, implémenté sous forme d'un protocole distinct et appelé ARP (*Address Resolution Protocol*) permet de déterminer dynamiquement l'adresse MAC à partir de l'adresse IP d'un hôte.



Lorsqu'un hôte A souhaite émettre une trame à destination de l'hôte B dont il connaît l'adresse IP, il effectue au préalable une requête ARP en broadcast. Cette requête est de type « quelle est l'adresse MAC correspondant à l'adresse IP *adresseIP* ? Répondez à *monAdresseIP* ».

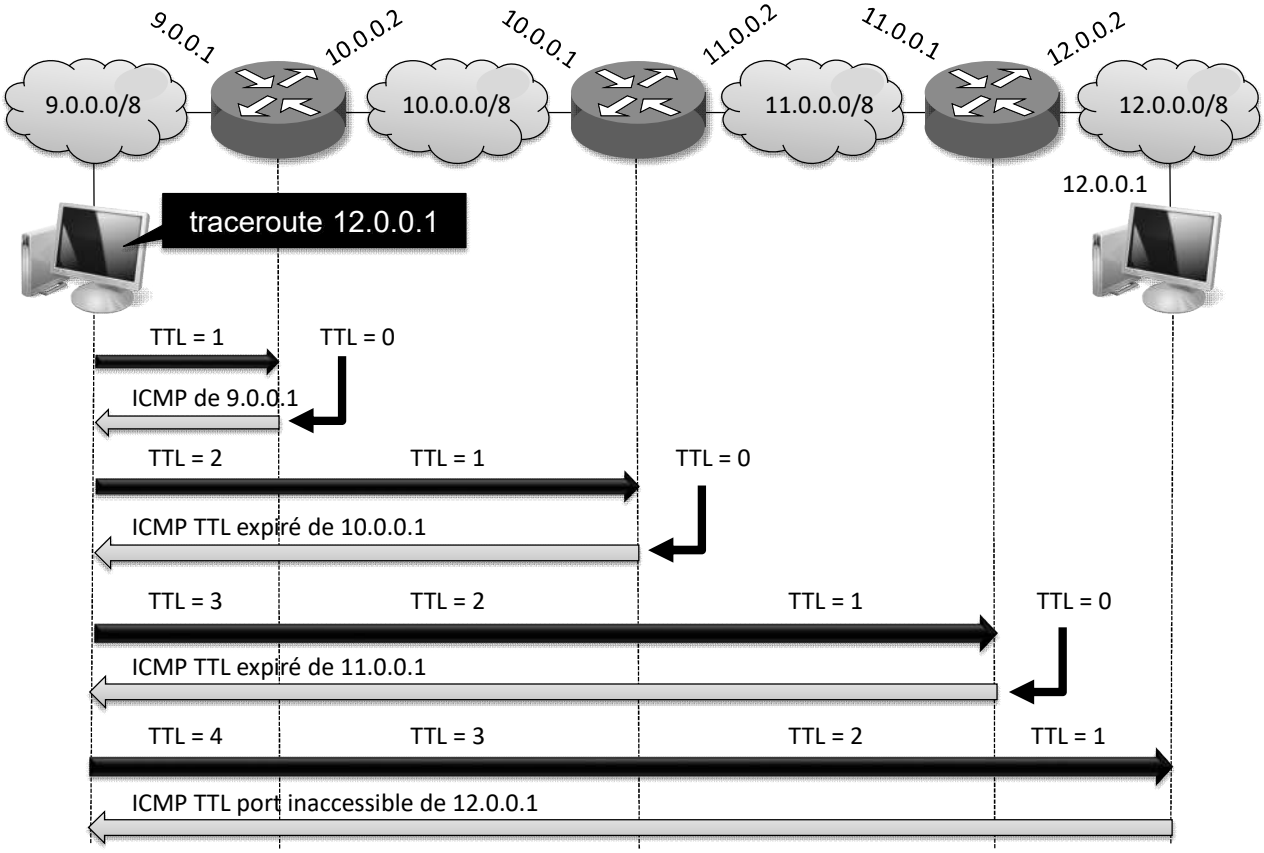
Toutes les hôtes vont recevoir la requête. L'hôte B qui possède cette adresse IP sera le seul à répondre en envoyant à la machine émettrice A une réponse ARP du type « je suis *adresseIP*, mon adresse MAC est *adresseMAC* ».

L'hôte A initialise alors sa table cache ARP (conservée en mémoire) en utilisant la réponse fournie. Les entrées dans cette table expirent après une temporisation donnée. Le cache ARP est consulté par un hôte juste avant l'envoi d'une requête ARP ; si la réponse se trouve dans le cache, la requête n'est pas effectuée.



Utilisation de ICMP : la commande traceroute

Comme la commande `ping`, la commande `traceroute` utilise également des messages ICMP ; elle permet de connaître la route exacte empruntée par les datagrammes. `traceroute` envoie 3 paquets UDP avec un TTL égal à 1 puis recommence en augmentant le TTL de 1 à chaque envoi. A **chaque fois que le TTL arrive à 0**, le routeur renvoie un message **ICMP d'erreur**.

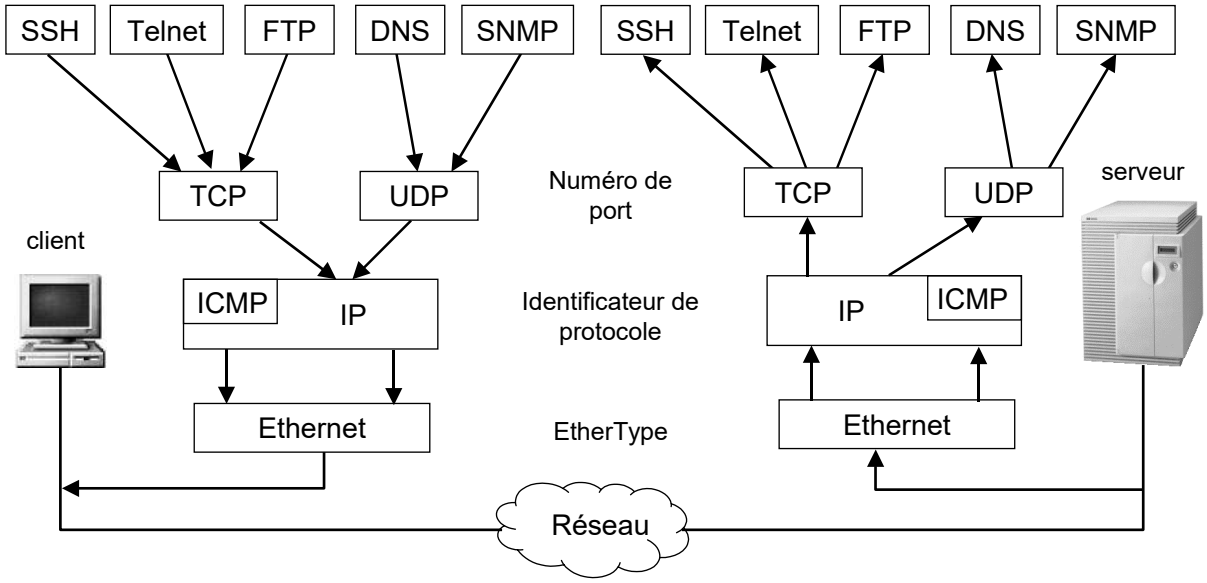


Notion de port

Plusieurs applications peuvent s'exécuter sur une machine cliente ou une machine serveur. Chacune d'entre elles utilise les services de la couche transport UDP ou TCP et est identifiée par un **numéro de port**. Un port est représenté par un entier (sur 16 bits)

- les ports de 0 à 1023 sont les ports **reconnus** ou **réservés.** Ils sont assignés par l'IANA (*Internet Assigned Numbers Authority*) et donnent accès aux services standards : courrier (SMTP port 25), serveur web (HTTP port 80) ...
- les ports > 1024 sont les ports « **utilisateurs** » disponibles pour placer un service applicatif quelconque

Un service est souvent connu par un nom (ftp, http, domain ...). Sur les systèmes Unix, la correspondance entre nom et numéro de port est donnée par le fichier `/etc/services`

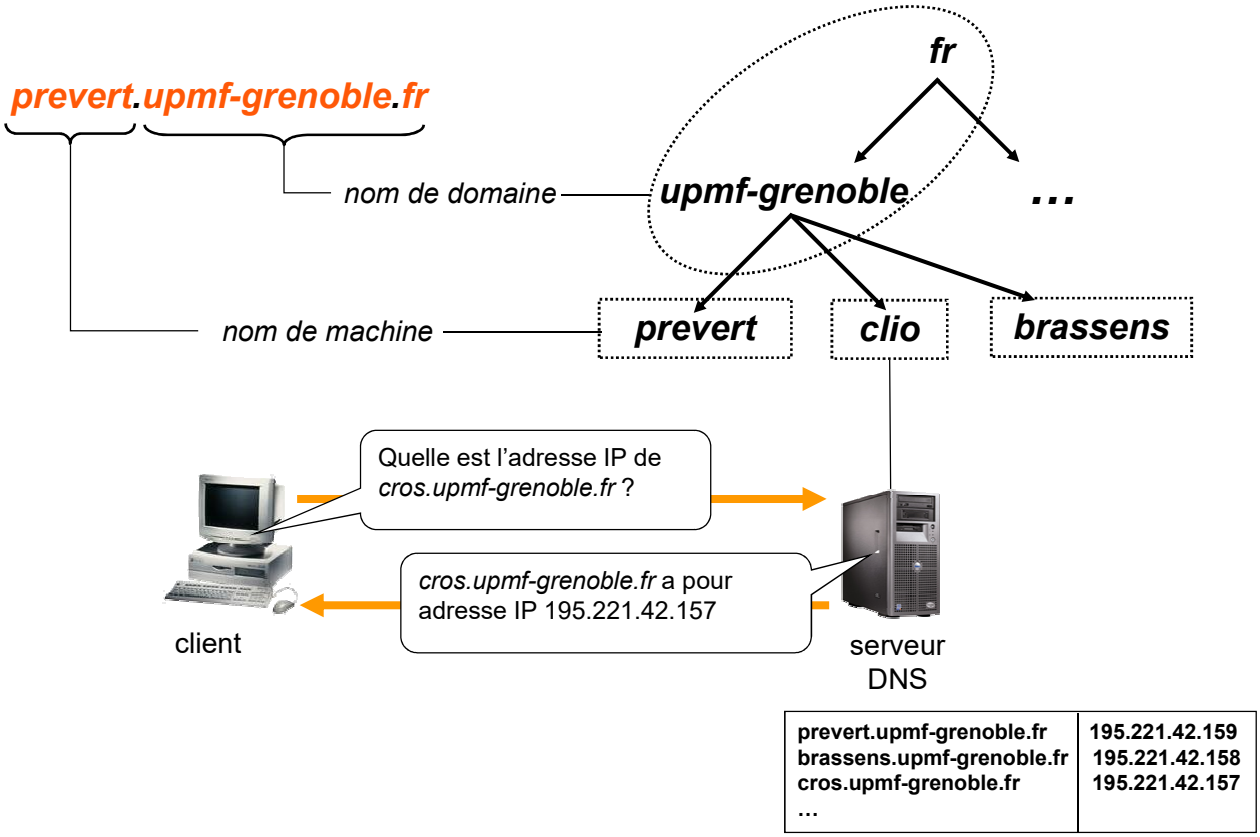


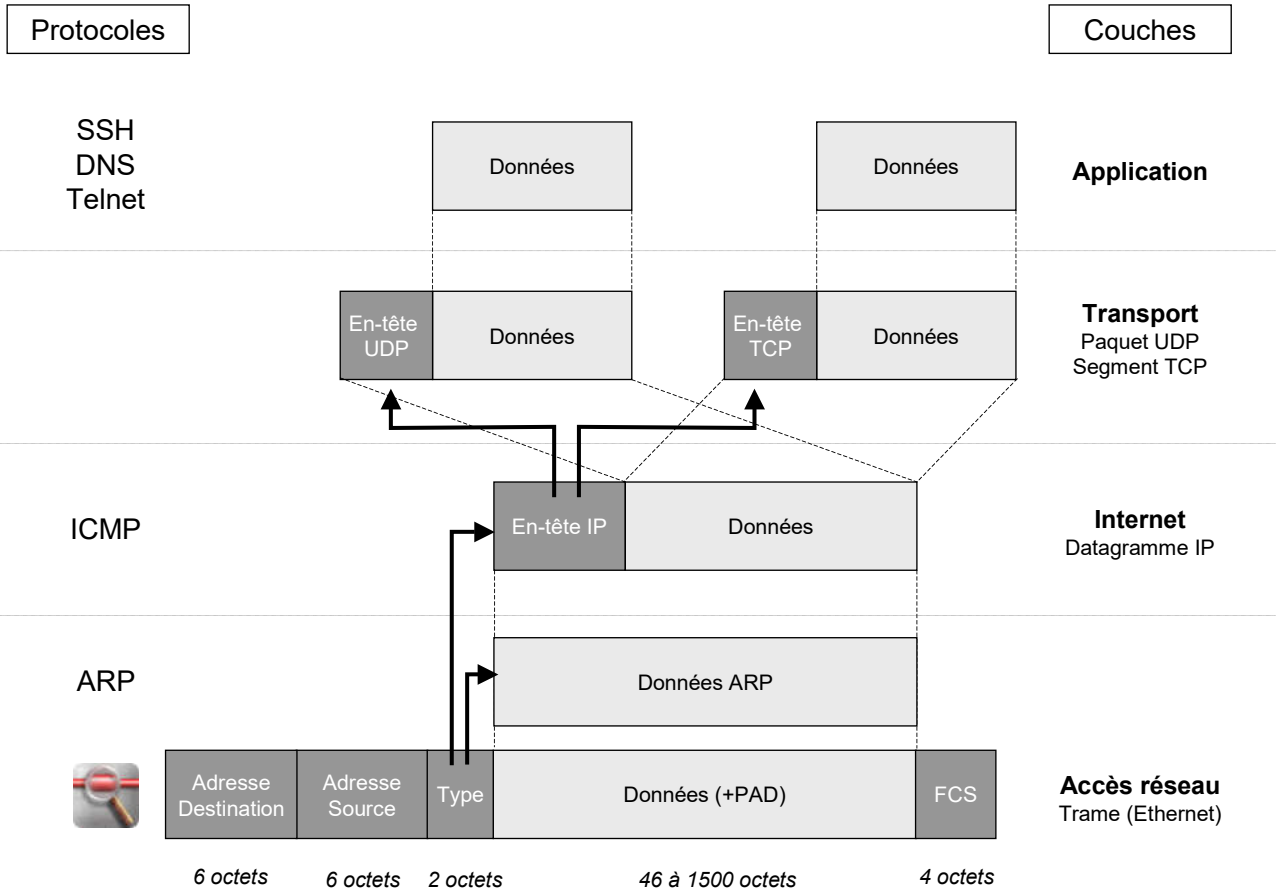
Le système DNS

Le système DNS (*Domain Name System*) permet d'associer des noms symboliques à des adresses numériques. Comme les adresses IP, les noms symboliques sont **structurées** et **hiérarchiques**

- une partie désigne le **nom de la machine** (*hostname*)
- l'autre partie désigne le **nom de domaine** (*domain name*) auquel la machine appartient.

Dans chaque domaine, un serveur de noms ou serveur DNS est chargé de répondre aux requêtes des clients (les clients internes comme les clients externes au domaine).

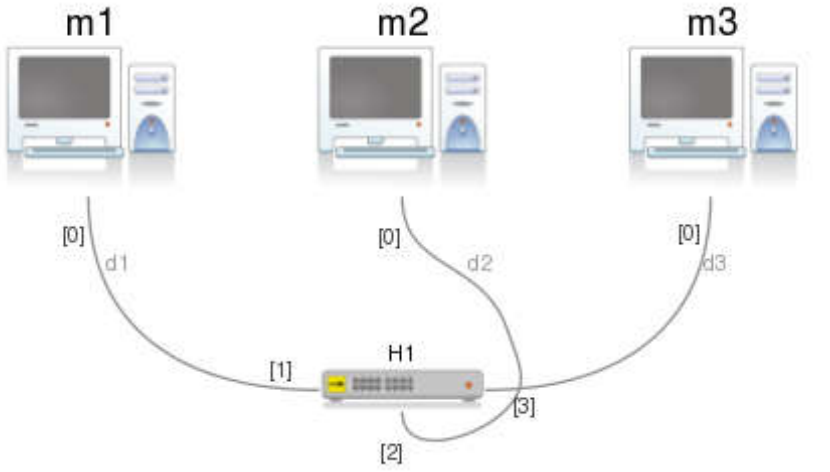

prevert.upmf-grenoble.fr
nom de domaine
nom de machine
fr
upmf-grenoble
...
prevert
clio
brassens
Quelle est l'adresse IP de cros.upmf-grenoble.fr ?
cros.upmf-grenoble.fr a pour adresse IP 195.221.42.157
client
serveur DNS
prevert.upmf-grenoble.fr 195.221.42.159
brassens.upmf-grenoble.fr 195.221.42.158
cros.upmf-grenoble.fr 195.221.42.157
...


Protocoles
Couches
SSH
DNS
Telnet
ICMP
ARP
Données
En-tête UDP
En-tête TCP
En-tête IP
Données ARP
Adresse Destination
Adresse Source
Type
Données (+PAD)
FCS
Application
Transport
Paquet UDP
Segment TCP
Internet
Datagramme IP
Accès réseau
Trame (Ethernet)
6 octets
6 octets
2 octets
46 à 1500 octets
4 octets

Configuration réseau

1) Démarrez la machine virtuelle, ouvrez la session et lancez Marionnet

   Créez un nouveau projet en allant dans le menu Projet > Nouveau, et donnez-lui un nom. Installez 3 machines nommées *m1*, *m2* et *m3* et reliez-les entre elles à l'aide de câbles droits et d'un *hub*.



   A l'aide de la commande `ifconfig` attribuez les adresses IP 192.168.169.1, 192.168.169.2 et 192.168.169.3, chacune de masque 255.255.255.0, respectivement à *m1*, *m2* et *m3*

   La syntaxe de la commande est la suivante :
   `ifconfig eth0` *`adresse_ip`* **`netmask`** *`masque_reseau`* **`up`**

2) Sur *m1*, vérifiez que vous pouvez bien atteindre les adresses IP de *m2* et *m3* à l'aide de la commande `ping`.

3) Sous Unix il est possible d'utiliser des noms de machines symboliques à la place des numéros IP sans passer par un serveur de noms (DNS), mais en modifiant simplement un fichier nommé `/etc/hosts`, dont les lignes sont de la forme :

   ```
   <IP> <NOM> <NOM>
   ```

   Par exemple :

   ```
   127.0.0.1 localhost
   10.10.10.1 self this me
   74.125.43.106 www.google.fr moteur
   ```

   Ces lignes se lisent de la droite vers la gauche : tous les noms symboliques (séparés par des blancs) seront traduits dans le numéro IP spécifié tout à gauche.

4) Modifiez donc ce fichier avec un éditeur de texte (par exemple avec la commande `nano /etc/hosts`) **sur les 3 machines** de façon à pouvoir par la suite exprimer toute adresse de façon symbolique depuis n'importe quel poste du réseau. **Remarque** : après ce travail, effectué sur 3 machines, vous pourrez facilement constater les limites de cette approche pour des réseaux plus grands et donc l'intérêt des serveurs de noms.

5) Testez la résolution de noms, que vous avez mis en oeuvre sur votre réseau, par des `ping` « singuliers » (pas en boucle, un seul aller-retour, voir le sens de l'option `-c` dans le manuel de `ping`) :

```
m1# ping -c 1 m2
m1# ping -c 1 m3

m2# ping -c 1 m1
m2# ping -c 1 m3

m3# ping -c 1 m1
m3# ping -c 1 m2
```

Analyse de la fragmentation IP

La commande `ping` permet d'envoyer des requêtes *echo ICMP* d'une taille (en octets) paramétrable (avec l'option `-s` *`taille_en_octets`*). Pour chacun des points suivants, vous constaterez avec `wireshark` lancé sur la machine *m3*, la fragmentation des paquets survenue.

1) Provoquez une fragmentation avec des paquets de taille supérieure à la MTU qui, par défaut, est fixée à 1500 octets en faisant un `ping` depuis *m1* sur *m2*.

2) Provoquez une fragmentation avec des paquets de taille 1200 et une MTU que vous fixerez (par la commande `ifconfig eth0 mtu 1000`) à la valeur 1000 sur toutes les machines

3) Provoquez la fragmentation d'un seul message *echo ICMP* en 10 fragments

Analyse de la commande *traceroute*

1) Recopiez sur votre bureau le projet nommé `traceroute.mar` qui est téléchargeable depuis le lien « ressource » sur la page Web depuis laquelle vous avez récupéré le sujet.

2) Démarrez l'ensemble des composants du réseau.

3) Déterminez l'adresse IP de *m11*, puis sur *m10* lancez le logiciel d'analyse de trames avec la commande :
   `wireshark &`

4) Démarrez la capture des trames, puis sur *m10* tapez la commande :
   `traceroute -n` *`adresse_IP_m11`*

5) Arrêtez la capture dès la fin de l'exécution de la commande en tapant CTRL-E ou en cliquant sur la 4ème icone de la barre d'outils en partant de la gauche.

6) Expliquez le fonctionnement de la commande `traceroute` en analysant les trames capturées. Pourquoi y-a-t'il deux types de messages ICMP ?

7) Ouvrez un terminal de commande hors de Marionnet sur votre machine hôte et faites un traceroute vers la machine www.atr.jp. Observez le chemin emprunté par les paquets IP. Essayez avec d'autres sites répartis dans le monde.

8) Arrêtez tous les composants du projet précédent puis ouvrez le projet nommé `capture1.mar` (que vous pouvez télécharger depuis la même page Web).

9) Démarrez l'ensemble des composants du réseau.

ARP
(*Address Resolution Protocol*)

1) Connectez-vous sur les différentes machines et relevez l'adresse IP de chacune d'elles

2) Sur la machine *m10*, affichez le contenu de la table ARP avec la commande : `arp -n`
   Pour obtenir de l'aide sur arp
   - `arp -h`
   - `man arp`

3) Lancez la commande `ping` *`adresse_IP_m11`*
   Appuyez sur Ctrl+C pour arrêter

4) Affichez à nouveau le contenu de la table ARP. Que constate-t-on ? Quelle est l'adresse Ethernet de *m11* ?

5) Affichez maintenant le contenu de la table avec les adresses IP au lieu des noms de machines.

6) En utilisant la commande `ifconfig`, vérifiez sur *m11* l'exactitude de l'association (IP,MAC) relevée sur la table ARP de *m10*.

7) Faites un `ping` sur l'adresse IP 172.23.0.254
   Appuyez sur Ctrl+C pour arrêter

8) Affichez à nouveau le contenu de la table ARP. Que constatez-vous ?

Analyse du protocole ARP

Analysez une séquence de résolution d'adresse avec ARP

1) Sur *m12*, lancez le logiciel `wireshark`

2) Sur *m10*, affichez la table ARP

3) Faites un « ping » singulier (`ping -c 1`) sur une machine de votre réseau qui n'est pas encore dans votre table ARP

4) Arrêtez la capture et analysez les trames échangées. Vous devez constater la présence de 4 trames, deux ARP et deux ICMP :
   - quel est la valeur du champ `type` à l'intérieur des trames Ethernet contenant la requête et la réponse ARP ?
   - quel est, en revanche, la valeur du champ `type` à l'intérieur des trames Ethernet contenant la requête echo ICMP et la réponse echo ICMP ?
   - par le biais de `wireshark`, combien de niveaux d'encapsulation observez-vous pour chaque ligne (trame) ? Est-il différent selon le protocole (ARP vs ICMP) encapsulé ?

Analyse d'UDP à travers le protocole
DNS (*Domain Name System*)

- Le service DNS permet d'utiliser des noms symboliques pour accéder aux hôtes au lieu de leurs adresses IP.
- Il s'agit d'une sorte d'annuaire fonctionnant sur le principe requête/réponse et s'appuyant sur le protocole de transport UDP.
- Le serveur écoute les requêtes des clients sur le port 53.

1) Sur *m12*, capturez les paquets UDP correspondant à une requête/réponse DNS en utilisant le **filtre de capture** : `ip proto \udp and port domain`

2) Une fois la capture démarrée, sur *m10* executez la commande :
   `host miashs-www.u-ga.fr`

3) Etudiez les différents champs de l'entête UDP

4) Etudiez les requête et réponse DNS encapsulées :
   - quelle est l'adresse IP de *miashs-www.u-ga.fr* ?
   - qui a répondu ?

Analyse de TCP à travers le protocole SSH (*Secure SHell*)

- SSH permet de se connecter d'une manière sécurisée (chiffrement des communications) sur une machine distante.
- Il utilise TCP comme protocole de transport.
- Le serveur écoute sur le port 22.

Analysez les segments TCP échangés dans un dialogue SSH lorsque vous vous connectez sur un serveur distant.

1) Utilisez comme filtre de capture : `ip proto \tcp and port ssh`

2) Lancez la capture et exécuter sur *m10* la commande :
   `ssh login@nom_hote`
   Avec *login* votre identifiant et *nom_hote*, le nom de la machine hôte que vous utilisez.

3) Arrêtez la capture

4) Décodez le dialogue SSH en cliquant sur la première trame capturée, puis en sélectionnant le menu « Analyze » puis l'item « Follow TCP Stream ». Que constatez-vous ?