

# 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.

Pour réaliser ce TP, vous utiliserez Marionnet (<http://www.marionnet.org>). Cet excellent logiciel, conçu par Jean-Vincent Loddo de l'Université Paris 13, est un « laboratoire de réseau virtuel » qui permet d'utiliser un seul ordinateur pour simuler un réseau complet intégrant des hubs virtuels, des switches, des routeurs, des câbles et de nombreux ordinateurs.

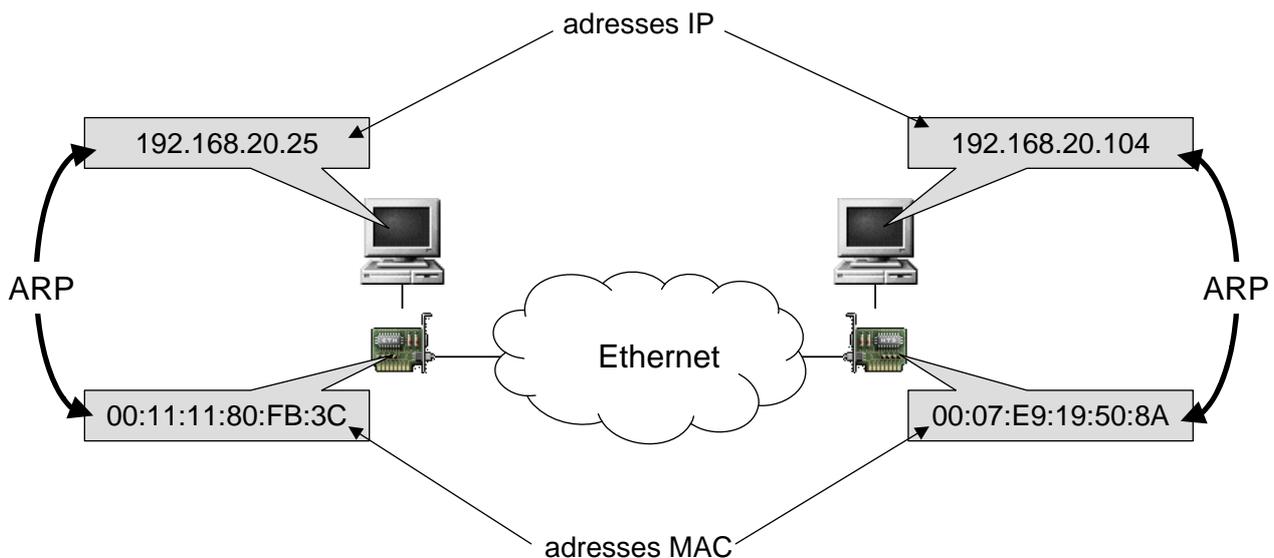
# Préambule

## 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.

Un protocole, le protocole ARP ou *Address Resolution Protocol*, permet de faire la correspondance entre les deux adresses (son fonctionnement sera détaillé dans les prochaines séances).



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

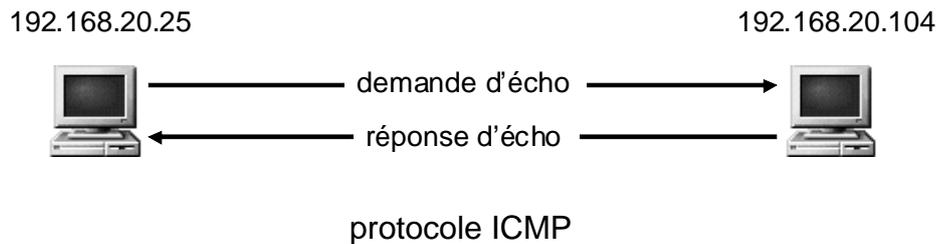
Le protocole ICMP (*Internet Control Message Protocol*) permet de gérer des problèmes au niveau de la couche IP. Il fournit des messages de contrôle pour indiquer les erreurs pendant la transmission du datagramme IP.

La commande `ping` utilise principalement deux types de messages du protocole ICMP pour informer l'utilisateur sur les conditions de transmissions :

- La machine distante est-elle active ou inactive.
- Le temps de propagation en boucle (*round-trip delay*) lors de la communication avec la machine distante.
- Les pertes de paquets pendant la communication.

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

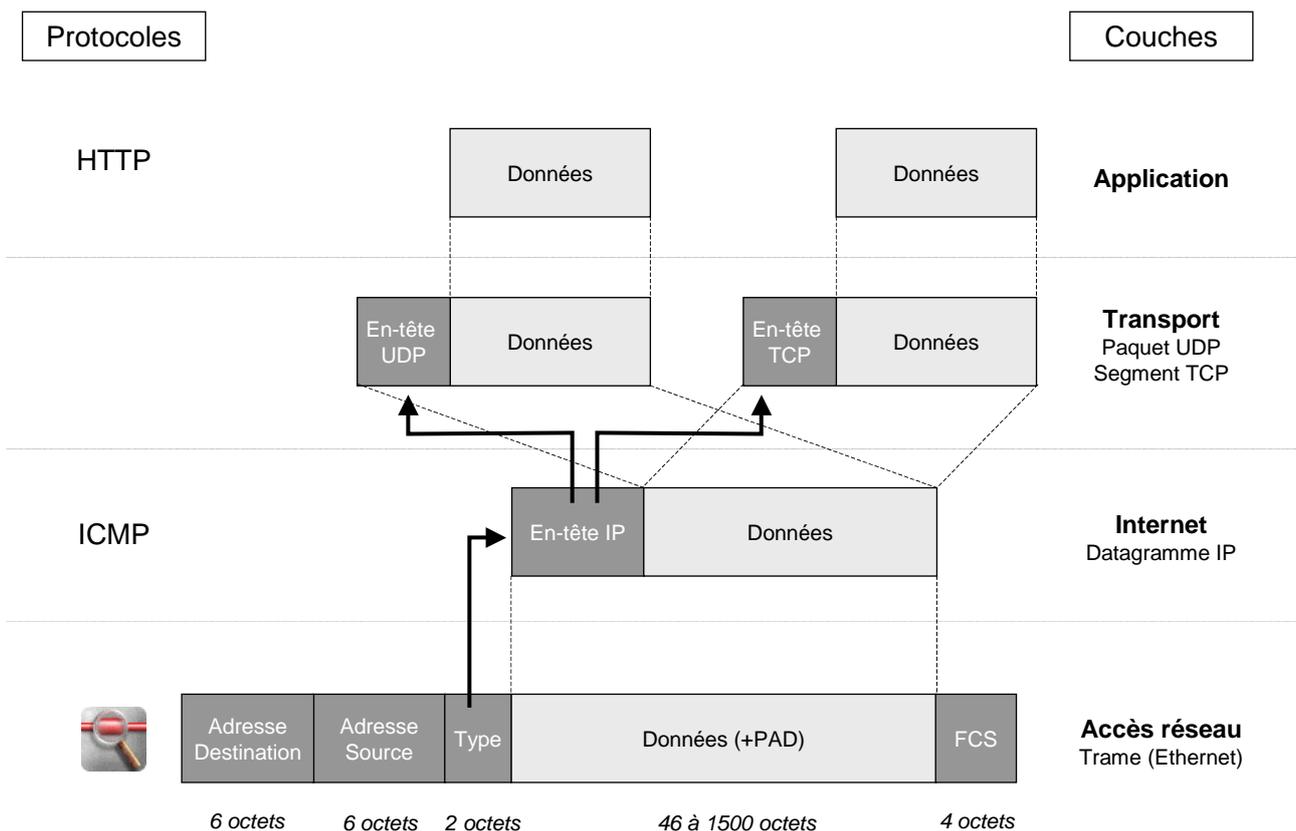
- Le type 8 (*echo request*) est émis vers la machine distante.
- Le type 0 (*echo reply*) est émis par la machine distante en réponse.



## Le protocole HTTP

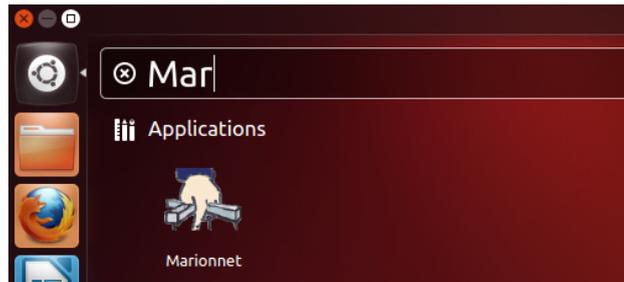
Le protocole HTTP (*HyperText Transfer Protocol*) est le protocole le plus utilisé sur Internet depuis 1990. Il permet un transfert de fichiers (essentiellement au format HTML) localisés grâce à une chaîne de caractères appelée URL entre un navigateur (le client) et un serveur Web.

- Le navigateur effectue une **requête HTTP** (par exemple obtenir la page référencée par l'adresse `http://www.mon-site.com/page.html`)
- Le serveur traite la requête puis envoie une **réponse HTTP** (par exemple le code HTML du fichier `page.html`)

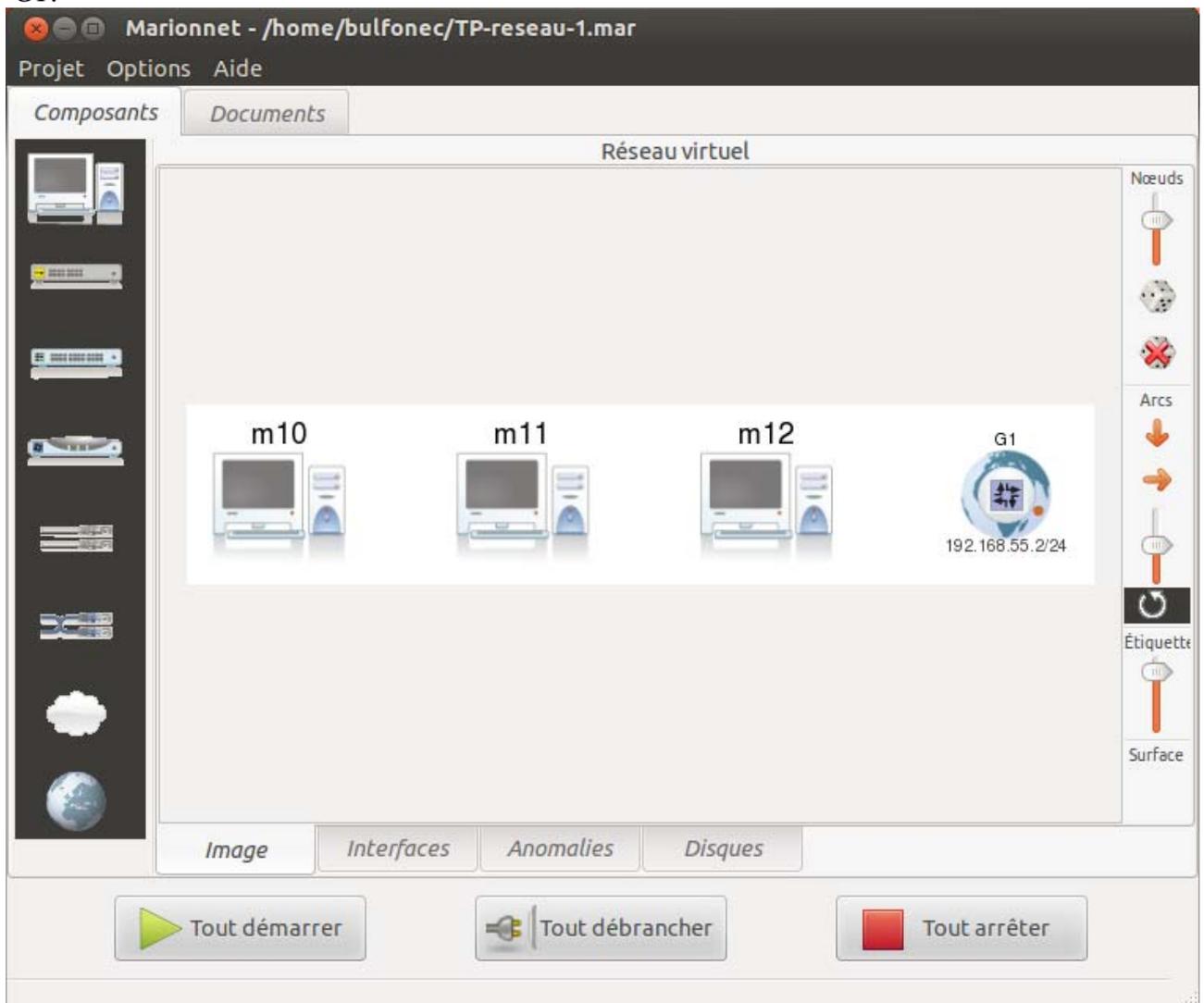


# Câblage et configuration du réseau

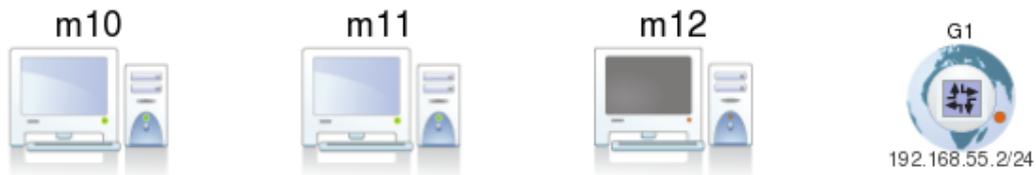
- 1) Copier sur votre bureau le projet nommé TP-reseau-1.mar qui se trouve dans /media/commun/LiMass/TPReseaux.
- 2) Lancer Marionnet : cliquez sur le bouton du haut du panel de gauche, et saisissez les premières lettres du mot « Marionnet ». Cliquez sur l'icône correspondante.



Allez dans le menu Projet > Ouvrir, puis sélectionnez le projet que vous venez de copier. Vous devriez vous retrouver avec 3 machines nommées *m10*, *m11* et *m12* et un équipement nommé *G1*.



- 3) Démarrez les hôtes *m10*, *m11*, et connectez-vous sur chacun d'entre eux en tant que « root », mot de passe « root ».

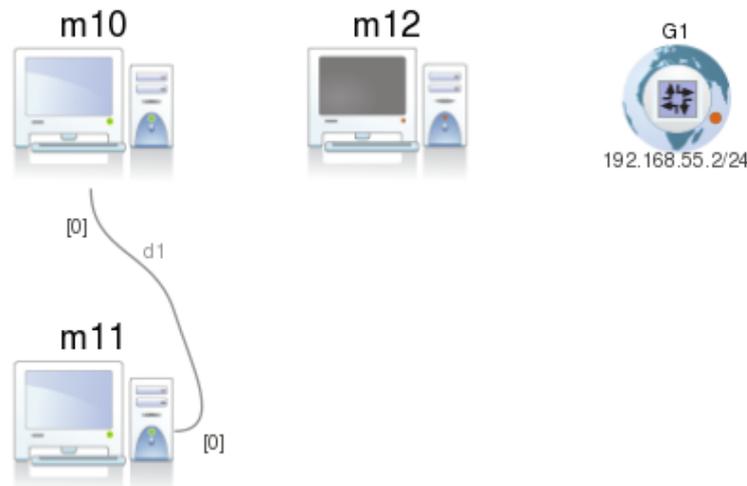


- 4) A l'aide de la commande `ifconfig` sur chacun des deux hôtes, trouvez et notez :
- l'adresse Ethernet de la carte réseau,
  - l'adresse IP

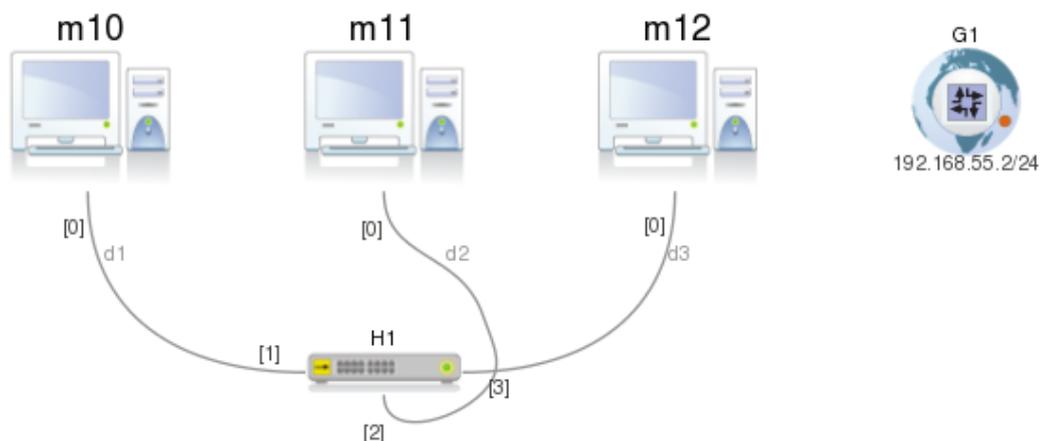


Respectez la syntaxe de la commande : `ifconfig` ≠ `if config`

- 5) Reliez les hôtes *m10* et *m11* à l'aide d'un **câble droit**. Depuis *m10*, testez la connectivité réseau en tapant la commande `ping adresse_IP_m11` (faites CTRL-C pour arrêter la commande). Que constatez-vous ?

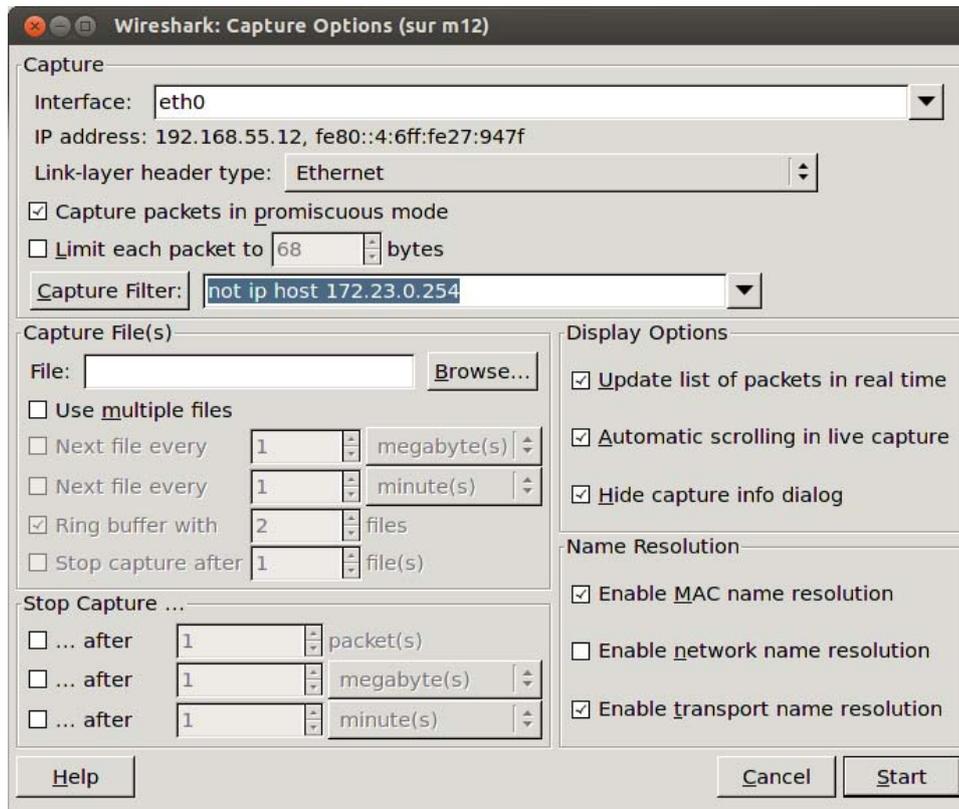


- 6) Remplacez le câble droit par un **câble croisé**, et refaites le test de connectivité. Que constatez-vous à présent ?
- 7) Supprimez le câble croisé entre *m10* et *m11*, et ajoutez un **concentrateur** (hub) *H1*. Reliez par des câbles droits les 3 hôtes à *H1*.

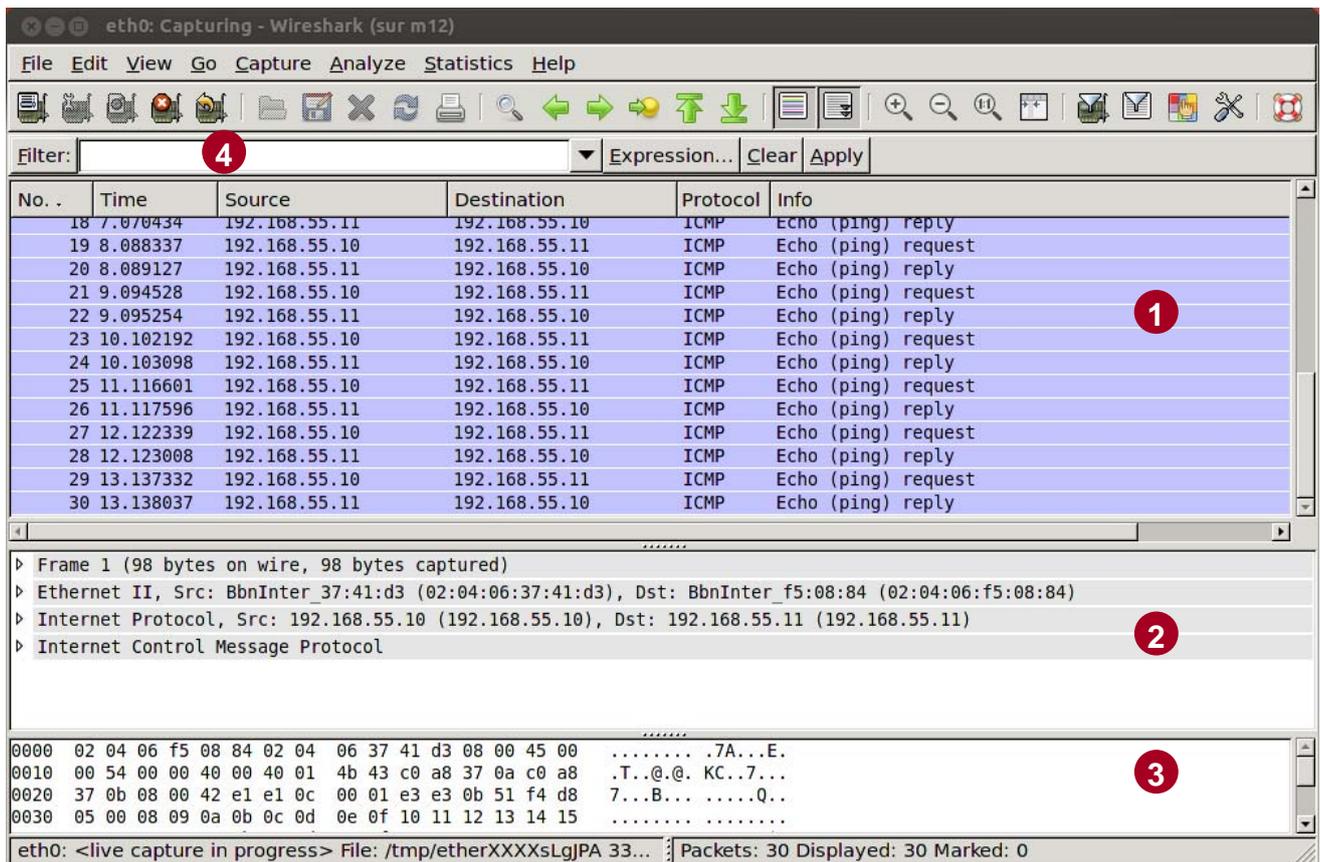


- 8) Démarrez *m12* (connectez-vous en tant que « root ») et notez son adresse IP) et *H1* et testez la connectivité réseau entre *m10*, *m11* et *m12* à l'aide de la commande `ping`.

- 9) Sur *m12*, lancez l'analyseur de protocoles réseau en tapant la commande `wireshark`
- Choisissez le menu Capture/Options
  - Une fenêtre vous permettant de définir les paramètres de la capture apparaît à l'écran :



- Démarrez la capture en cliquant sur le bouton « Start »
- 10) Depuis l'hôte *m10*, faites un ping sur *m11*. Vous devriez voir s'afficher dans la fenêtre de Wireshark les trames capturées. Arrêtez le ping sur *m10* puis la capture en cliquant sur la 4<sup>e</sup> icône en partant de la gauche dans la barre d'outils. Parcourez les trames que vous avez capturées et explorez leurs différents champs décodés.
- L'interface du logiciel Wireshark est découpée en 3 parties.
- La partie supérieure ❶ contient la liste des paquets capturés disponibles avec un affichage synthétique du contenu de chaque paquet
  - La partie centrale ❷ 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 partie inférieure ❸ contient le paquet (le début s'il est trop gros) affiché en hexadécimal et en ASCII.
  - La zone de saisie ❹ permet de définir un filtre d'affichage des paquets capturés



- 11) Remplacez le concentrateur *H1* par un **commutateur** (switch) *S1* et refaites le câblage de *S1* vers *m10*, *m11* et *m12*.
- 12) Relancez une nouvelle capture, puis refaites un ping vers *m11* depuis *m10*. Que constatez-vous ?
- 13) A l'aide de la commande `ifconfig`, attribuez à l'hôte *m11* l'adresse IP 192.168.55.111. La syntaxe de la commande est la suivante :  
`ifconfig eth0 adresse_ip netmask 255.255.255.0 up`
- 14) Relancez une nouvelle capture, puis depuis *m10* faites un ping à destination de l'ancienne adresse de *m11*. Que constatez-vous ?
- 15) Sur l'hôte *m10*, configurez l'accès vers les réseaux extérieurs à travers la passerelle *G1* avec la commande :  
`route add default gw 192.168.55.2`
- 16) Remplacez le commutateur *S1* par un concentrateur *H1*, et reliez-le à *m10*, *m11*, *m12* et *G1*. Démarrez *H1* et *G1*.
- 17) Lancez une nouvelle capture. Sur *m10*, ouvrez le navigateur avec la commande `firefox`, puis tapez l'URL : `http://www.upmf-grenoble.fr`
  - Arrêtez la capture une fois la page affichée dans le navigateur
  - Analysez le contenu des trames capturées
  - Décodez l'ensemble du dialogue HTTP entre votre navigateur et le serveur Web, en cliquant sur la première trame capturée, puis en sélectionnant le menu « Analyze » puis l'item « Follow TCP Stream »

Follow TCP Stream

Stream Content

```
GET / HTTP/1.1
Host: www.upmf-grenoble.fr
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.9.2.8) Gecko/20100723 Ubuntu/10.04 (lucid) Firefox/3.6.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
Connection: keep-alive

HTTP/1.1 302 D.plac. Temporairement
Date: Mon, 14 Feb 2011 09:26:24 GMT
Server: Apache/2.2.3 (Unix) PHP/5.2.6 mod_jk/1.2.26
Set-Cookie: JSESSIONID=21A41E92722ED10738CC8B8A17BB8A3; Path=/
Location: http://www.upmf-grenoble.fr/55458523/0/fiche__pagelibre/&RF=U2
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=ISO-8859-1

GET /55458523/0/fiche__pagelibre/&RF=U2 HTTP/1.1
Host: www.upmf-grenoble.fr
User-Agent: Mozilla/5.0 (X11; U; Linux i686; fr; rv:1.9.2.8) Gecko/20100723 Ubuntu/10.04 (lucid) Firefox/3.6.8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Rechercher Enregistrer sous Imprimer Entière conversation (72665 bytes)  ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Aide Filter Out This Stream Fermer