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

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.

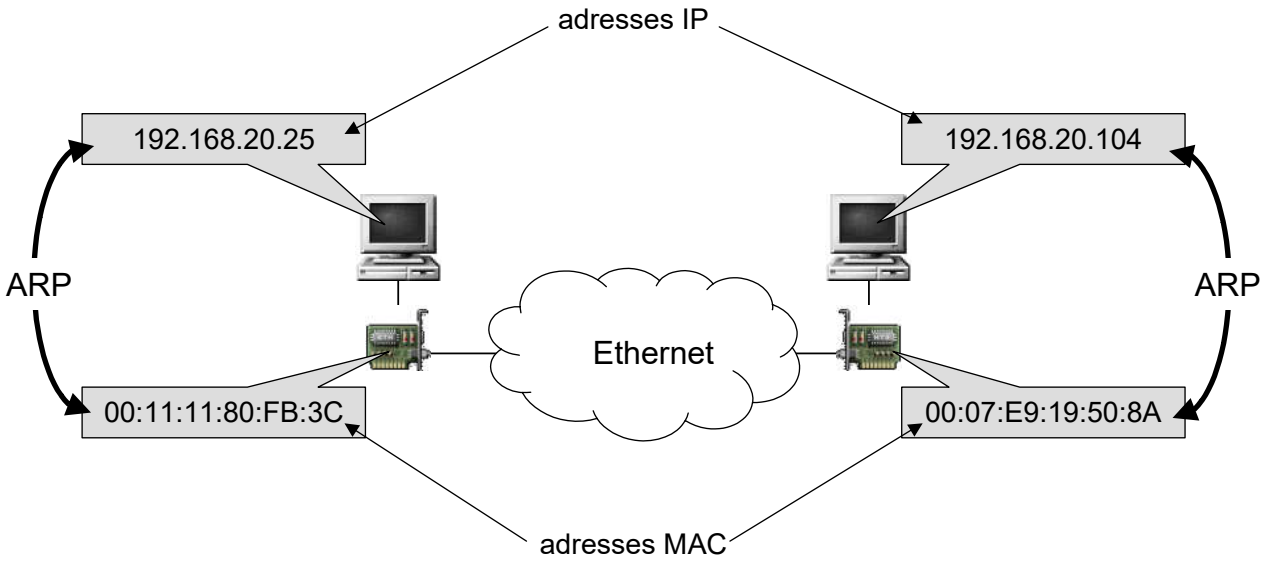
Pour réaliser ce TP, vous utiliserez Marionnet (http://www.marionnet.org). Cet excellent logiciel, conçu par Jean-Vincent Loddo de l'Université Paris 13, est un « laboratoire de réseau virtuel » qui permet d'utiliser un seul ordinateur pour simuler un réseau complet intégrant des hubs virtuels, des switches, 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 : miashs-www.u-ga.fr ⇔ 129.88.230.12).

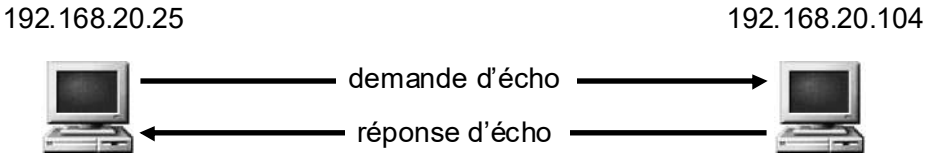
Le protocole ICMP

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.

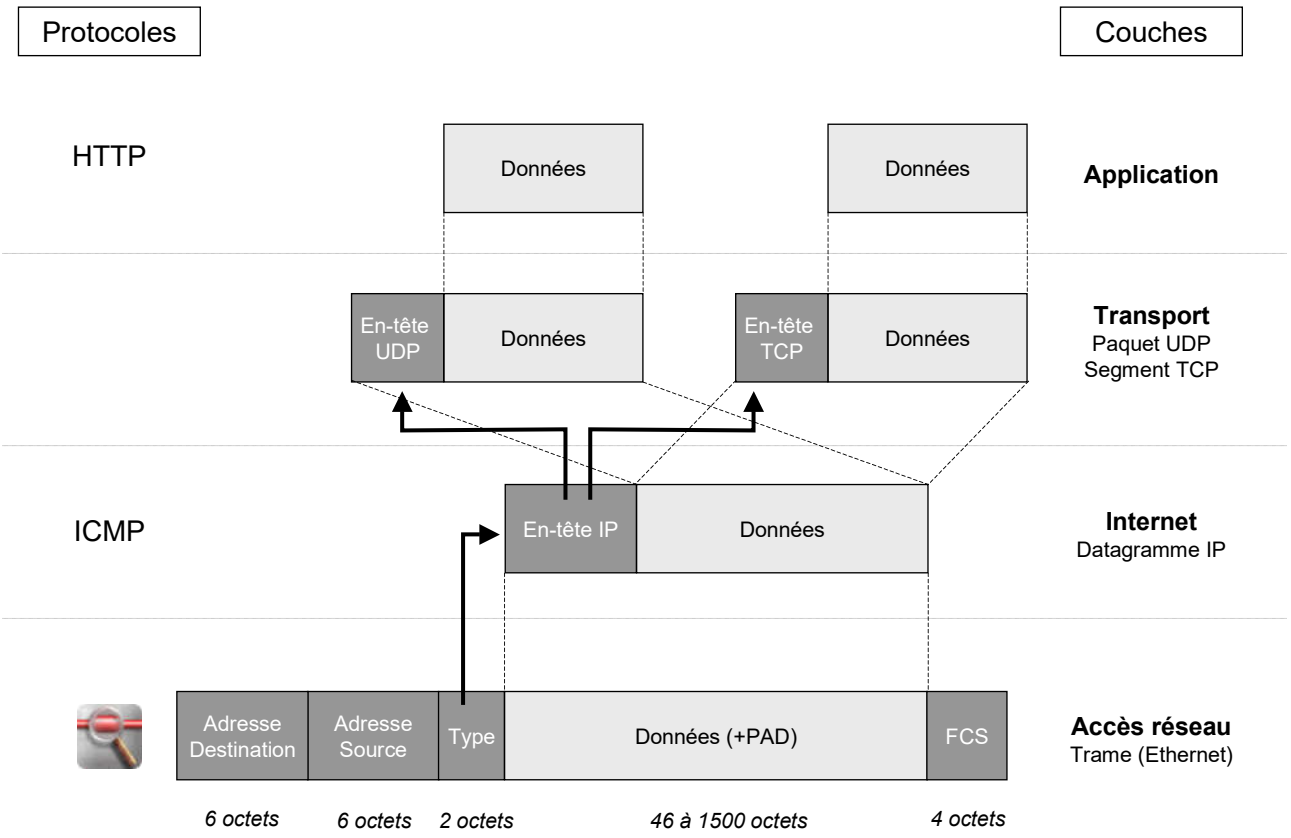


protocole ICMP

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`)



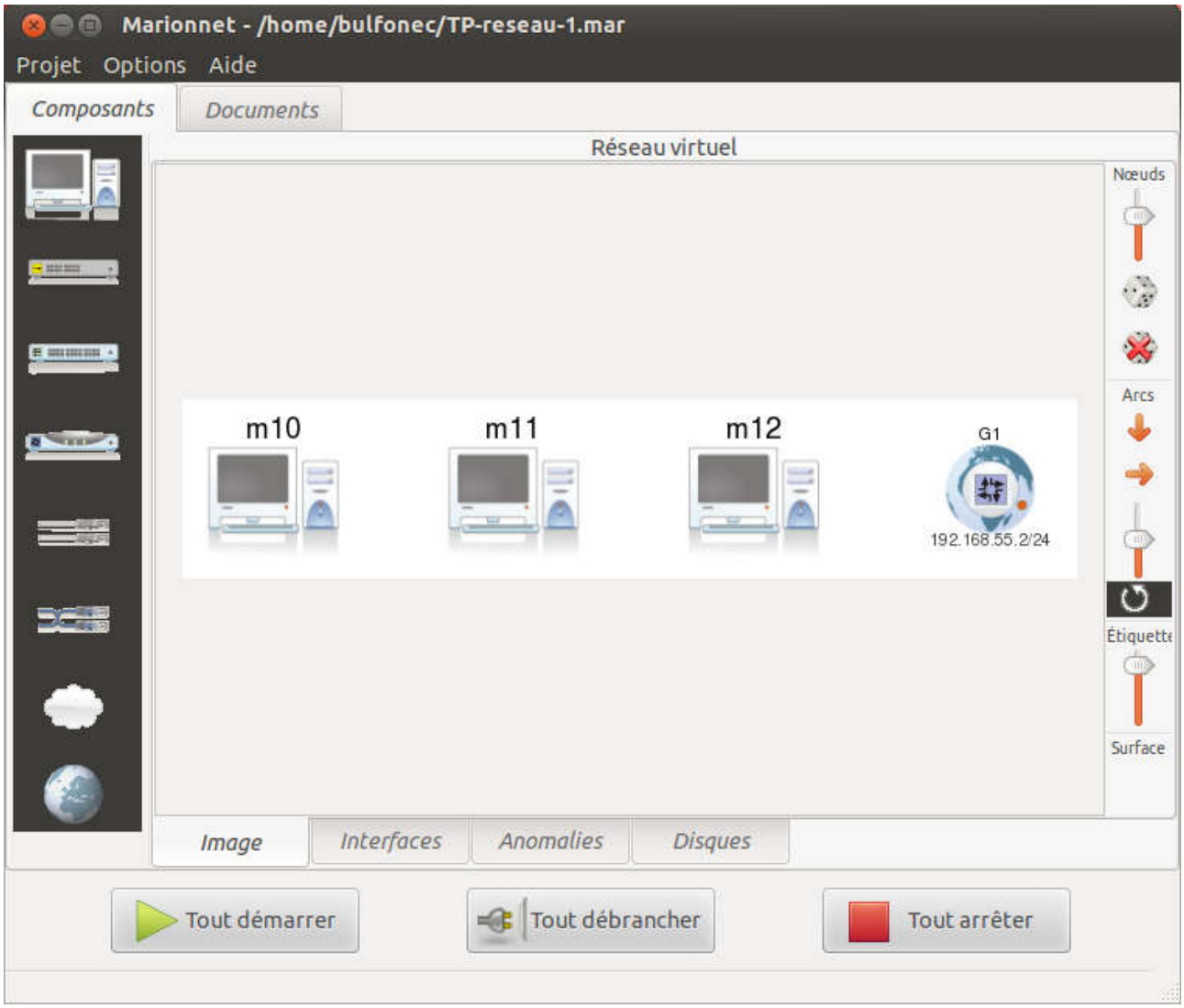
Câblage et configuration du réseau

1) Démarrez la machine virtuelle et ouvrez la session

2) Lancez le navigateur et téléchargez le projet Marionnet `capture1.mar` depuis la page Web où vous avez trouvé le présent sujet.

3) Lancer Marionnet en cliquant sur l'icône présente sur le bureau.

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



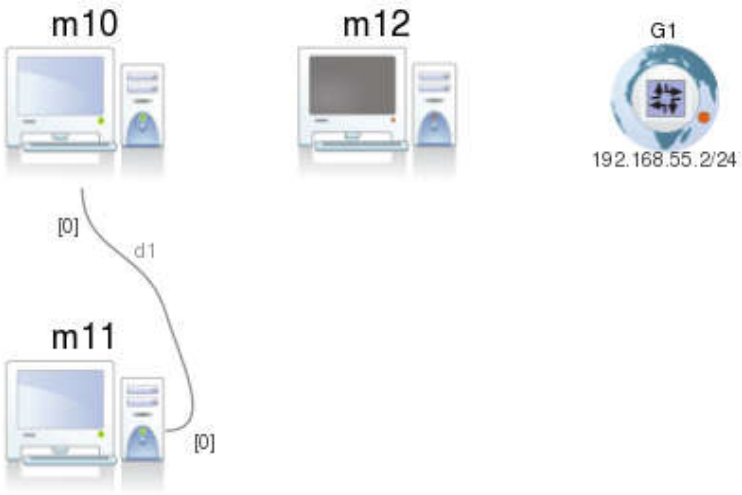
4) Démarrez les hôtes *m10*, *m11*, et connectez-vous sur chacun d'entre eux en tant que « root », mot de passe « root »

Lorsque vous saisissez le mot de passe, les caractères ne s'affichent pas, c'est normal ! Faites attention à ne pas vous tromper !

5) 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

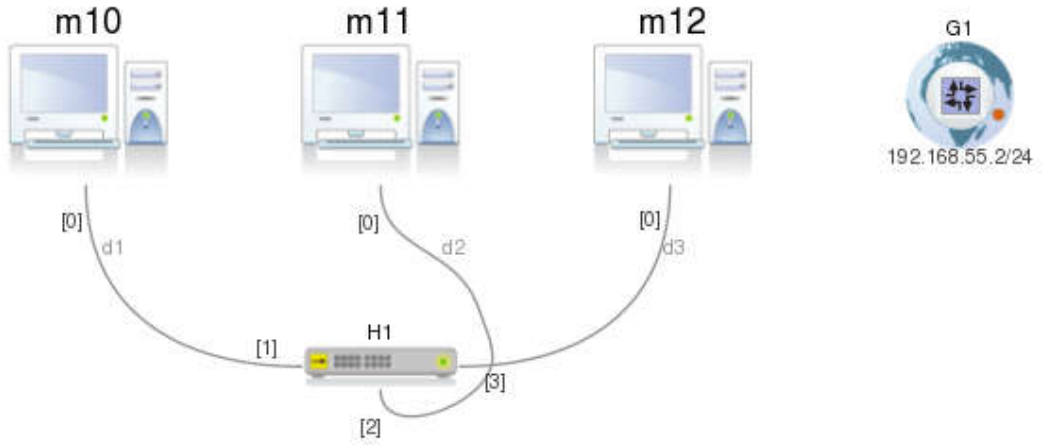
Respectez la syntaxe de la commande : `ifconfig` ≠ `if config`

6) 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 ?



7) Remplacez le câble droit par un **câble croisé**, et refaites le test de connectivité. Que constatez-vous à présent ?

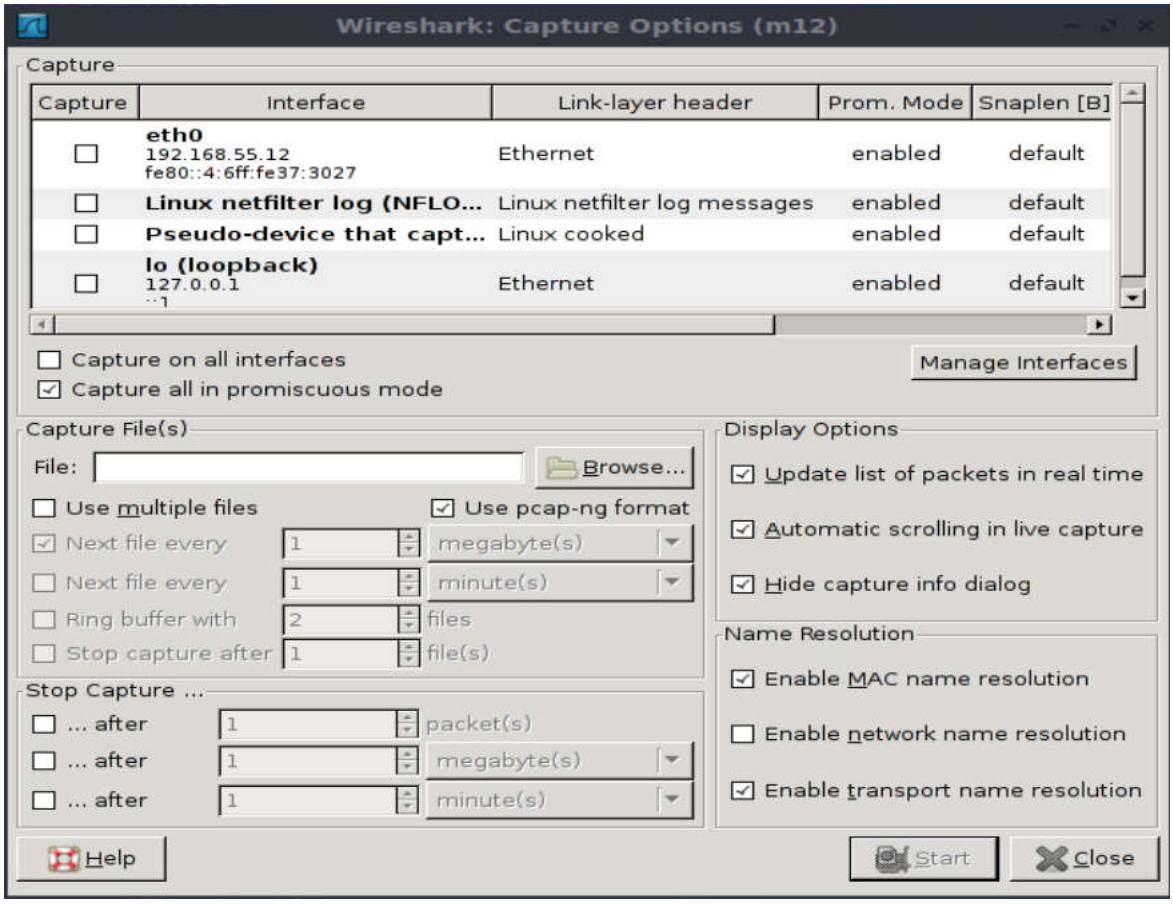
8) Supprimez le câble croisé entre *m10* et *m11*, et ajoutez un **concentrateur** (hub) *H1*. Reliez par des câbles droits les 3 hôtes à *H1*.



9) 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`.

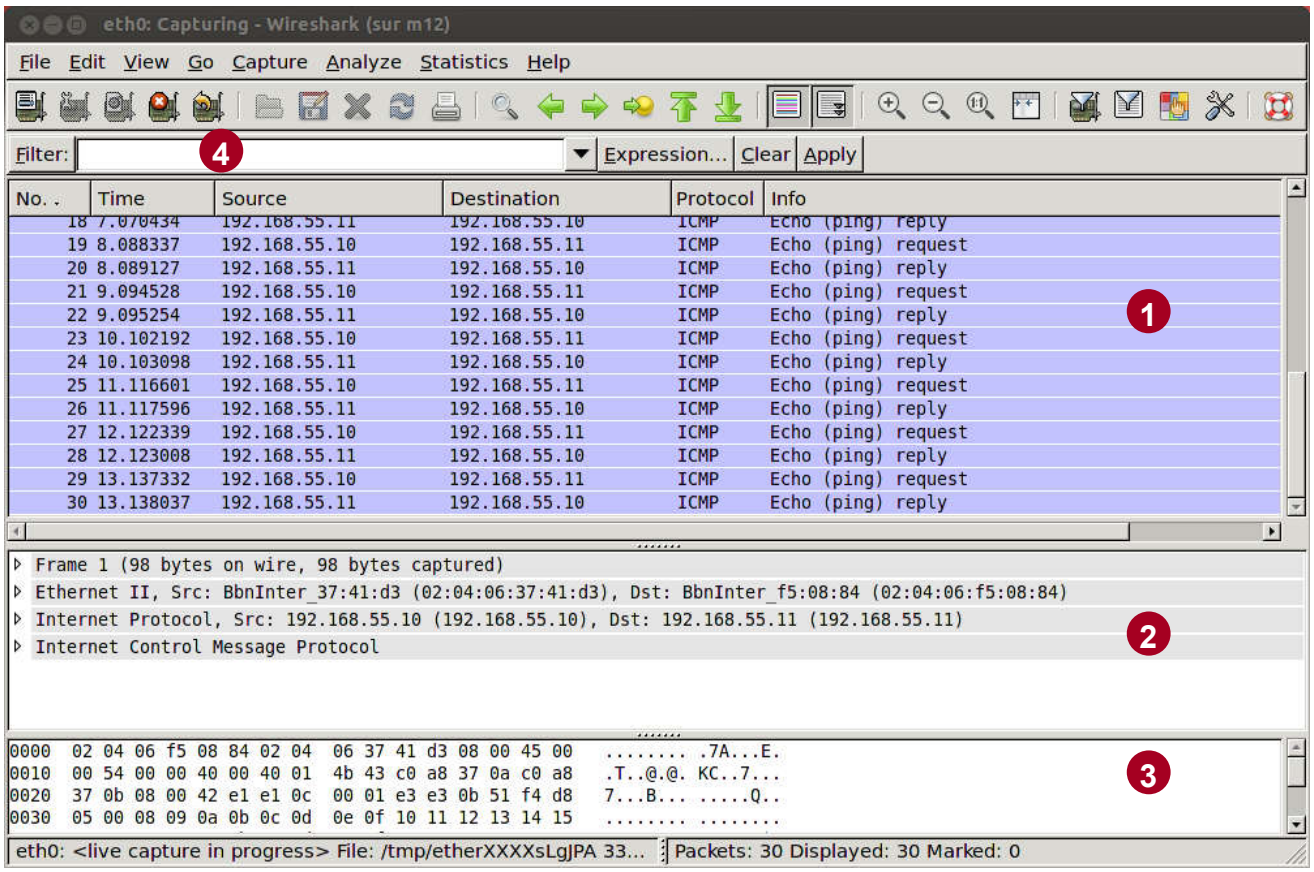
Introduction à la capture de trames

1) 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 :



   - Sélectionnez l'interface *eth0* et démarrez la capture en cliquant sur le bouton « Start »

2) 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 4e 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'imbriquation 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



3) 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`**

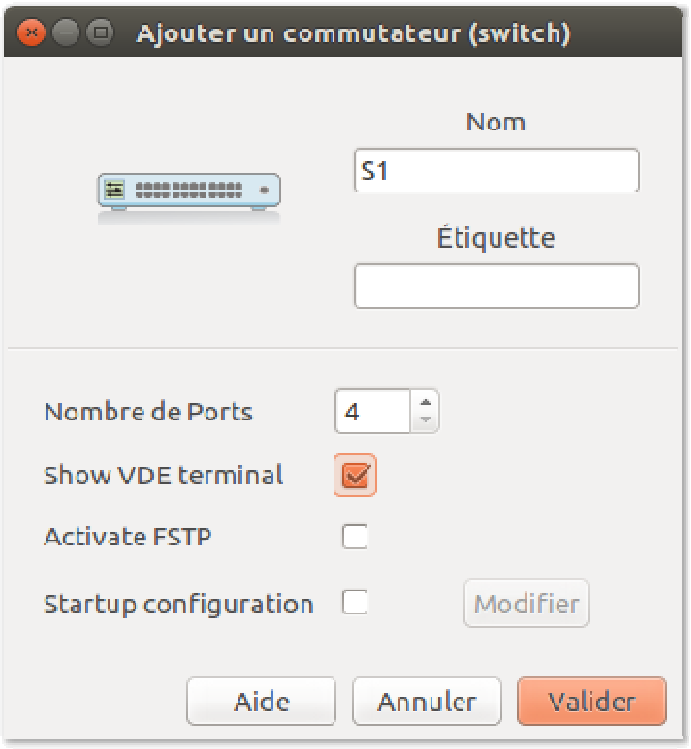
4) Relancez une nouvelle capture, puis depuis *m10* faites un `ping` à destination de l'ancienne adresse de *m11*. Que constatez-vous ? Redémarrez la machine *m11* avant de continuer.

5) Reliez le concentrateur *H1* à la passerelle *G1*.

6) Lancez une nouvelle capture. Sur *m10*, ouvrez le navigateur avec la commande `epiphany`, puis tapez l'URL : *www.gnu.org*
   - 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 »

Utilisation des VLANs

Le composant **commutateur** (switch) de Marionnet permet de simuler la fonctionnalité VLAN de niveau 1 (en pilotant le logiciel sous-jacent `vde_switch` du projet *virtualsquare*). Pour pouvoir configurer les VLANs, il faut passer par le terminal de configuration qui s'affiche au démarrage du composant lorsque la case « Show VDE terminal » est cochée.



Dans le terminal du commutateur la commande `help` permet d'avoir un aperçu rapide des possibilités de configuration du commutateur :

```
VDE switch V.2.2.1
(C) Virtual Square Team (coord. R. Davoli) 2005,2006,2007 - GPLv2
vde$ help
0000 DATA END WITH '.'
COMMAND PATH        SYNTAX          HELP
————————————————————————————————————————
ds                  ============    DATA SOCKET MENU
ds/showinfo                         show ds info
help                [arg]           Help (limited to arg when specified)
logout                              logout from this mgmt terminal
shutdown                            shutdown of the switch
showinfo                            show switch version and info
load                path            load a configuration script
debug               ============    DEBUG MENU
...
...
fstp/print          [N]             print fst data for the defined vlan
port                ============    PORT STATUS MENU
port/showinfo                       show port info
port/setnumports    N               set the number of ports
```

```
port/sethub         0/1             1=HUB 0=switch
port/setvlan        N VLAN          set port VLAN (untagged)
port/create         N               create the port N (inactive|notallocatable)
port/remove         N               remove the port N
port/allocatable    N 0/1           Is the port allocatable as unnamed? 1=Y 0=N
port/epclose        N ID            remove the endpoint port N/id ID
port/resetcounter   [N]             reset the port (N) counters
port/print          [N]             print the port/endpoint table
port/allprint       [N]             print the port/endpoint table (including
inactive port)
vlan                ============    VLAN MANAGEMENT MENU
vlan/create         N               create the VLAN with tag N
vlan/remove         N               remove the VLAN with tag N
vlan/addport        N PORT          add port to the vlan N (tagged)
vlan/delport        N PORT          delete port to the vlan N (tagged)
vlan/print          [N]             print the list of defined vlan
vlan/allprint       [N]             print the list of defined vlan (including
inactive port)
.
1000 Success
vde$
```

La commande `vlan/create` permet de créer un VLAN en lui affectant l'étiquette numérique (tag) N. La commande `port/setvlan` permet d'associer un port au VLAN identifié par son étiquette.

1) Remplacez le concentrateur *H1* par un **commutateur** *S1* et refaites le câblage de *S1* vers *m10*, *m11* et *m12*. N'oubliez pas de cocher la case « Show VDE terminal » au moment de l'ajout du composant. Notez les ports sur lesquel chaque machine est connectée.

2) Lancez une nouvelle capture avec Wireshark sur *m12*, puis depuis *m10* faites un `ping` à destination de *m11*. Que constatez-vous ? Pourquoi ?

3) Sur *m11* et *m12*, mettez-vous à l'écoute des requêtes ICMP à l'aide de la commande en ligne `tcpdump` (`man tcpdump` pour plus de détails).
   `tcpdump -e icmp`

4) Testez que le switch joue bien son rôle de « segmentation » en ne redistribuant les trames **unicast qu'aux machines concernées**, en faisant depuis *m10* d'abord un `ping` vers *m11*, puis vers *m12*.

5) Testez à présent que les trames en **broadcast sont transmises à toutes les machines**. Vous utiliserez la commande `netcat` (`man netcat` pour plus de détails) pour générer une requête en broadcast vers le port de notre choix 8888. Pour cela, sur *m11* et *m12* mettez-vous à l'écoute des requêtes sur le port en question (utilisez CTRL-C pour sortir de la commande) :
   `tcpdump -e port 8888`

6) Sur *m10*, générez une requête en broadcast avec la commande :
   `echo "bonjour" | netcat -ub 192.168.55.255 8888`
   Vérifiez que la trame est reçue à la fois sur *m11* et sur *m12*.

7) Utilisez les VLANs pour créer des domaines de broadcast différents. Dans le terminal du switch, créez les VLANs 100 et 200 à l'aide de la commande `vlan/create`
   `vlan/create 100`
   `vlan/create 200`
   puis à l'aide la commande `port/setvlan` affectez les ports sur lesquels sont connectés les machines *m10* et *m11* au VLAN 100, et le port sur lequel est connecté *m12* au VLAN 200. Vérifiez l'affectation des ports avec la commande `vlan/print`

8) Sur *m10* re-générez la requête en broadcast (CTRL-C pour sortir) et vérifiez qu'elle n'est à présent reçue que sur *m11*.

9) Affectez le port de la machine *m10* au VLAN 200, puis refaites le test. Vérifiez que la requête n'est reçue que sur *m12* à présent.