

Nom :

Prénom :

TP SIN

ETUDE D'UN RESEAU INFORMATIQUE

Support : Réseau informatique

Pré requis (l'élève doit savoir):

- Savoir utiliser un ordinateur

Programme

Objectif terminale :

L'élève doit être capable de réaliser le montage d'un réseau et de le paramétrer

Matériels :

- Logiciel wireshark, Cisco Packet Tracer

1. Questions

- A quoi peut servir un réseau informatique

- Expliquer son principe de fonctionnement

Nom :

Prénom :

2. Manipulation (indiquer la commande réseau qui vous a permis d'obtenir le résultat)

- Donner l'adresse IP de votre ordinateur et le masque de sous réseau

- Donner la classe du réseau local (A, B, C, D) et expliquer votre réponse

- Donner l'adresse mac

Nom :

Prénom :

- Donner l'adresse IP d'au moins deux ordinateurs branchés sur le réseau

a. Etude protocole Arp

- Depuis votre terminal avec l'invite de command (cmd), vider le cash de la table arp : arp -d
- Dans un terminal, affichez la table ARP (capturer la table et la coller sur le TP)

Exemple :

```
C:\Windows\system32>arp -a

Interface : 192.168.1.17 --- 0xc
Adresse Internet      Adresse physique      Type
192.168.1.1          34-8a-ae-21-75-d2    dynamique
192.168.1.10         f0-82-61-36-83-92    dynamique
192.168.1.15         24-0a-64-80-47-69    dynamique
192.168.1.255        ff-ff-ff-ff-ff-ff    statique
224.0.0.2            01-00-5e-00-00-02    statique
224.0.0.22          01-00-5e-00-00-16    statique
224.0.0.251         01-00-5e-00-00-fb    statique
224.0.0.252         01-00-5e-00-00-fc    statique
224.0.0.253         01-00-5e-00-00-fd    statique
239.255.255.250     01-00-5e-7f-ff-fa    statique
255.255.255.255     ff-ff-ff-ff-ff-ff    statique
```

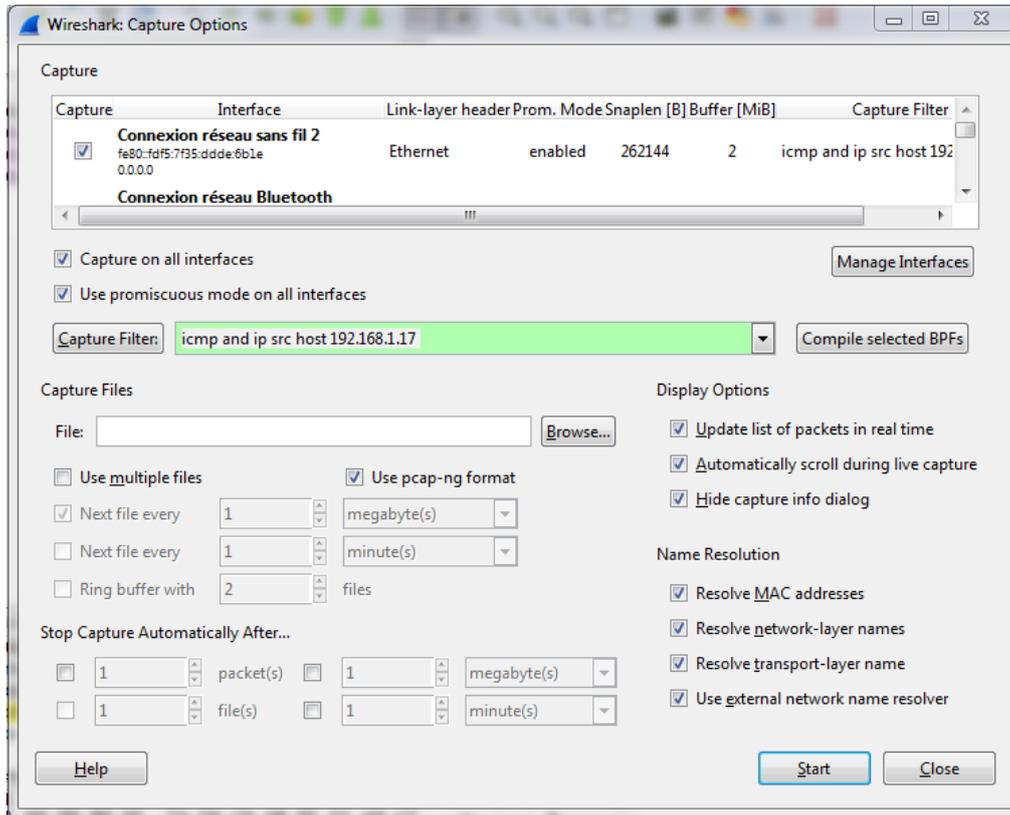
- Pinguer sur une machine du réseau qui n'est pas encore dans la table ARP.
- Afficher la nouvelle table ARP, que constatez-vous ?

b. Etude protocole ICMP

- Dans Capture/Option, remplissez les champs :
- Interface
- Capture Filter (icmp and ip src host (adresse ip ordinateur source))
- Enable network name resolution
- Démarrez la capture

Nom :

Prénom :



- Dans une fenêtre de terminal, lancez la commande ping www.google.fr pendant quelques secondes.
- Cliquez sur Stop
- Analysez les trames :
 - Quelle est l'adresse MAC de l'interface réseau du serveur google?
 - Quelle est la taille d'un paquet en octets?
 - Quelles sont les adresses IP source et destination?

```
⊕ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 3
⊕ Ethernet II, Src: Azurewav_a7:97:88 (1c:4b:d6:a7:97:88), Dst: Sagemcom_21:75:d2 (34:8a:ae:21:75:d2)
⊕ Internet Protocol Version 4, Src: 192.168.1.17 (192.168.1.17), Dst: 173.194.78.94 (173.194.78.94)
  Version: 4
  Header Length: 20 bytes
  ⊕ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 60
  Identification: 0x02d1 (721)
  ⊕ Flags: 0x00
  Fragment offset: 0
  Time to live: 128
  Protocol: ICMP (1)
  ⊕ Header checksum: 0x7a16 [validation disabled]
  Source: pc5.home (192.168.1.17)
  Destination: google.com (173.194.78.94)
0000  34 8a ae 21 75 d2 1c 4b d6 a7 97 88 08 00 45 00  4...u..K .....E.
0010  00 3c 02 d1 00 00 80 01 7a 16 c0 a8 01 11 ad c2  .<.....Z.L.....
0020  4e 5e 08 00 4d 52 00 01 00 09 61 62 63 64 65 66  NA..MR...abcdef
0030  67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76  ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67 68 69                    wabcdefg hi
```

- Calculer chaque adresse en hexadécimal (détailler les calculs) et la comparer à la valeur affichée sur wireshark

Exemple :

192.168.1.17 => c0 a8 01 11

Nom :

Prénom :

Remarque :

Selon votre capture, il peut être utile d'appliquer un filtre qui ne va afficher que certains paquets.

Donc pour mettre en place un filtrage (par exemple pour n'afficher que les paquets dont l'adresse source est 192.168.200.21) il faut saisir le filtre dans la **section Filter** puis cliquer sur le bouton **Apply**:

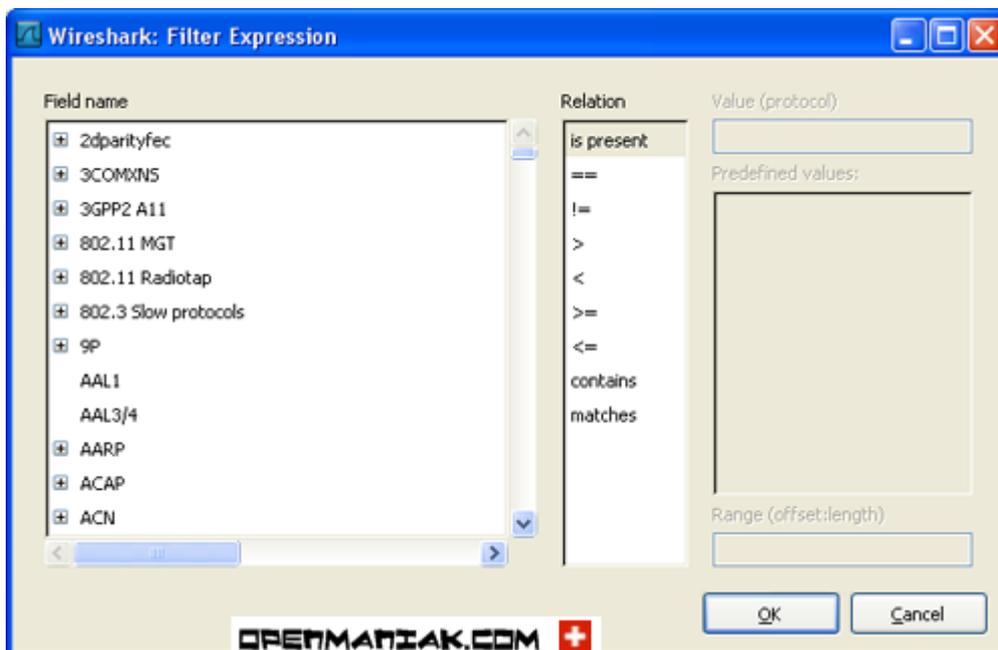
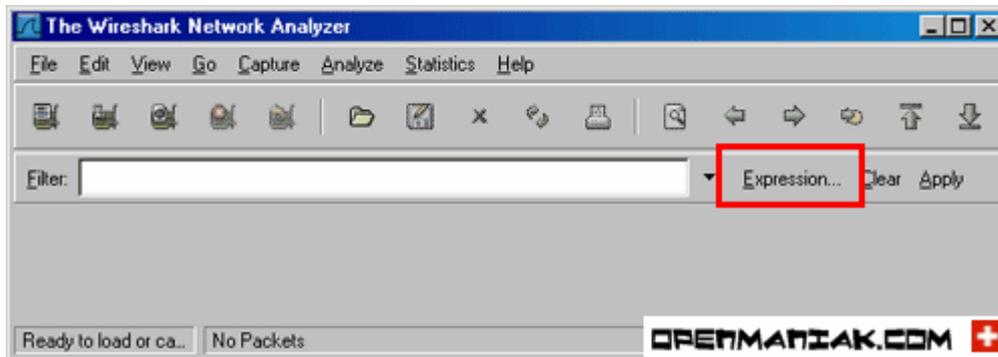


Si le fond de la zone de saisie du filtre n'est pas vert, c'est qu'il y a une erreur de syntaxe.

Dans le cas d'un trafic ftp vous pouvez aussi dans le champ Filter saisir ftp puis cliquez sur Apply.

Un grand nombre de protocoles compris entre les couches deux et sept du modèle OSI est disponible. Ils peuvent être consultés quand vous cliquez sur le bouton "Expression ..." dans la fenêtre principal de Wireshark.

Quelques exemples de protocole sont: IP, TCP, DNS, SSH.



Exemple de syntaxe de filtre :

ip.addr == 10.1.1.1

Affiche les paquets avec une adresse source ou destination de 10.1.1.1.

Nom :

Prénom :

ip.src != 10.1.2.3 or ip.dst != 10.4.5.6

Affiche les paquets avec une adresse IP source différente de 10.1.2.3 ou avec une adresse IP destination différente de 10.4.5.6.

Tcp.port==25

Affiche les paquets dont le port TCP source ou destination est égal à 25.

Tcp.dstport==25

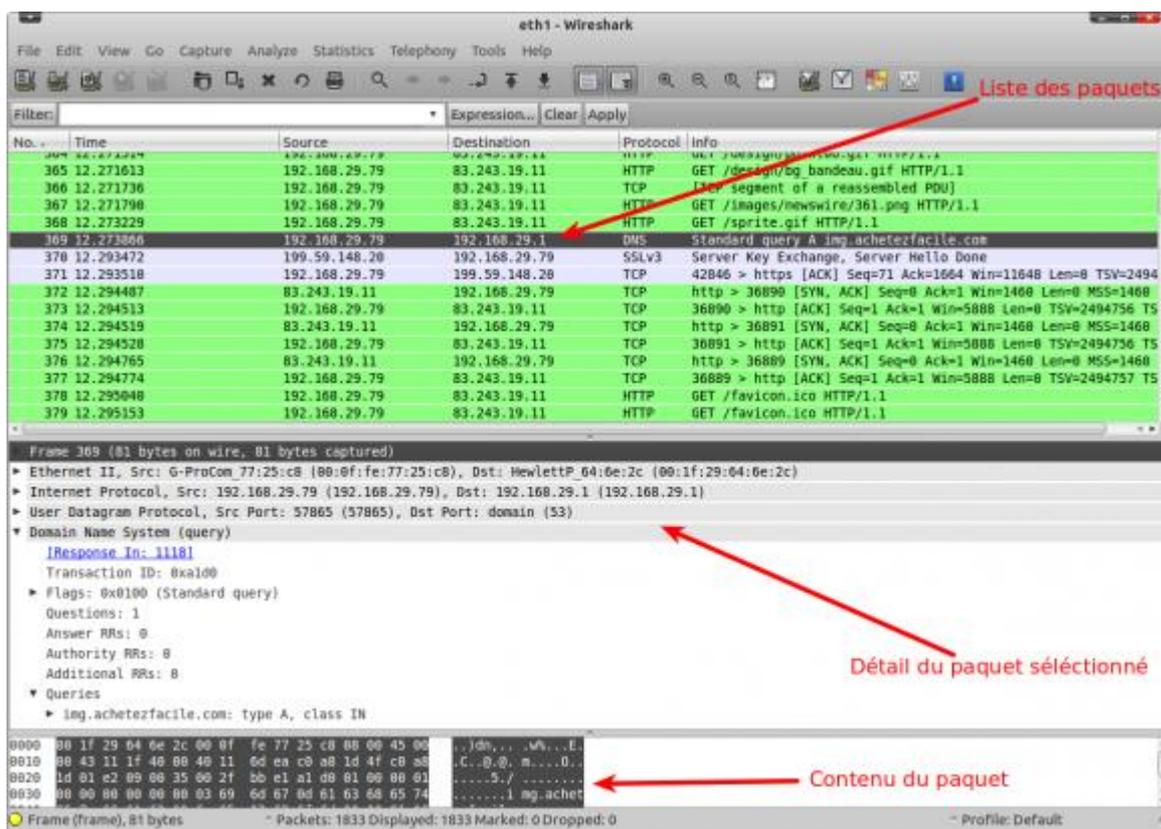
Affiche Les paquets avec un port TCP de destination 25.

Comment analyser la capture réseau ?

On commence par charger la capture par le menu File > Open (/tmp/capture.pcap). Une fois le fichier chargé, on peut voir que la fenêtre de Wireshark est, par défaut, divisée en 3 sections:

- la première affiche une liste des paquets IP capturés
- la seconde donne le détail du paquet IP sélectionné dans la première section
- la troisième affiche le contenu (en hexadécimal) du paquet IP sélectionné dans la première section

Le volet de milieu affiche les détails de ce paquet. Les protocoles et les champs de protocole du paquet sélectionné sont indiqués. Ils s'affichent sous la forme d'une arborescence que vous pouvez développer ou réduire.



Contenu du paquet :

La première colonne indique, avec 4 chiffres hexadécimaux, le rang du premier octet de la ligne courante dans la trame ;
La seconde affiche la valeur hexadécimale de 16 octets capturés à chaque ligne (un octet est représenté par deux caractères hexadécimaux) ;
La dernière représente à chaque ligne les caractères ASCII correspondants aux 16 octets de la seconde colonne (la correspondance n'est significative que lorsque du texte "imprimable" se trouve encodé dans ces octets).

Nom : Prénom :

c. Réalisation d'un réseau informatique

Simulation :

- Installer le logiciel Cisco Packet Tracer

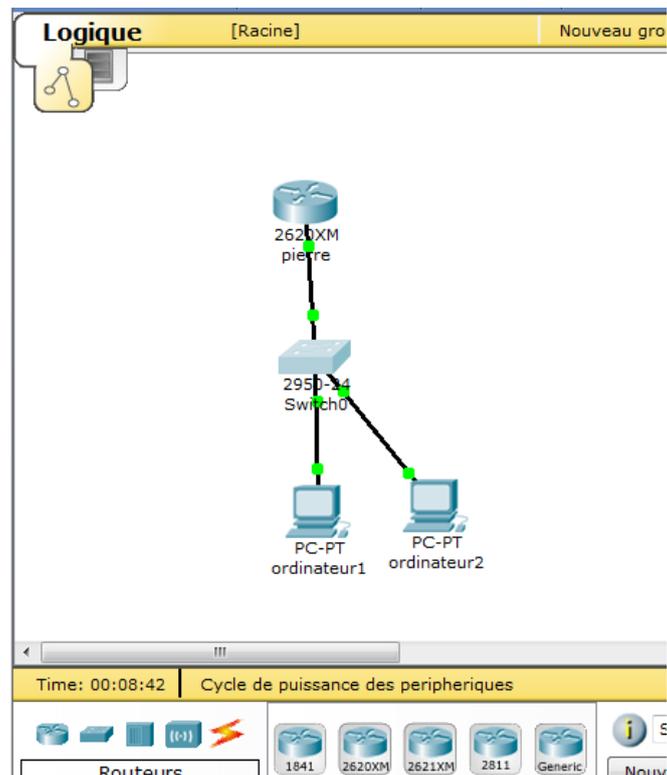
Nom	Modifié le	Type	Taille
blank.pkt	09/09/2012 15:09	Cisco Packet Trac...	1 Ko
Cisco Packet Tracer 6.2 for Windows Stud...	25/08/2015 13:56	Application	150 207 Ko
french.ptl	09/09/2012 15:16	Fichier PTL	977 Ko
notice francaise.txt	09/09/2012 15:17	Document texte	1 Ko
Packet Tracer 4.11.pdf	09/09/2012 14:53	Adobe Acrobat D...	4 570 Ko

- Modifier la langue voir notice

Nom	Modifié le	Type	Taille
blank.pkt	09/09/2012 15:09	Cisco Packet Trac...	1 Ko
Cisco Packet Tracer 6.2 for Windows Stud...	25/08/2015 13:56	Application	150 207 Ko
french.ptl	09/09/2012 15:16	Fichier PTL	977 Ko
notice francaise.txt	09/09/2012 15:17	Document texte	1 Ko
Packet Tracer 4.11.pdf	09/09/2012 14:53	Adobe Acrobat D...	4 570 Ko

- En suivant les instructions sur la vidéo (<http://www.sti2dsinhyrome.fr/video%20cisco%20packet%20tracer.html>), réaliser le réseau suivant et le tester

Rentrer les mêmes caractéristiques que le réseau de la salle, adresse ip de votre ordinateur et d'un autre ordinateur de la salle.



Nom :

Prénom :

- Appeler professeur

- Refaire le montage en rajoutant un point d'accès wifi et un nouvel ordinateur connecté en wifi.
Configurer le avec une sécurité WPA2 (clé : votre nom suivi de votre date de naissance, suivi nom lycée,
Ex : dupont18101999hyrome)

