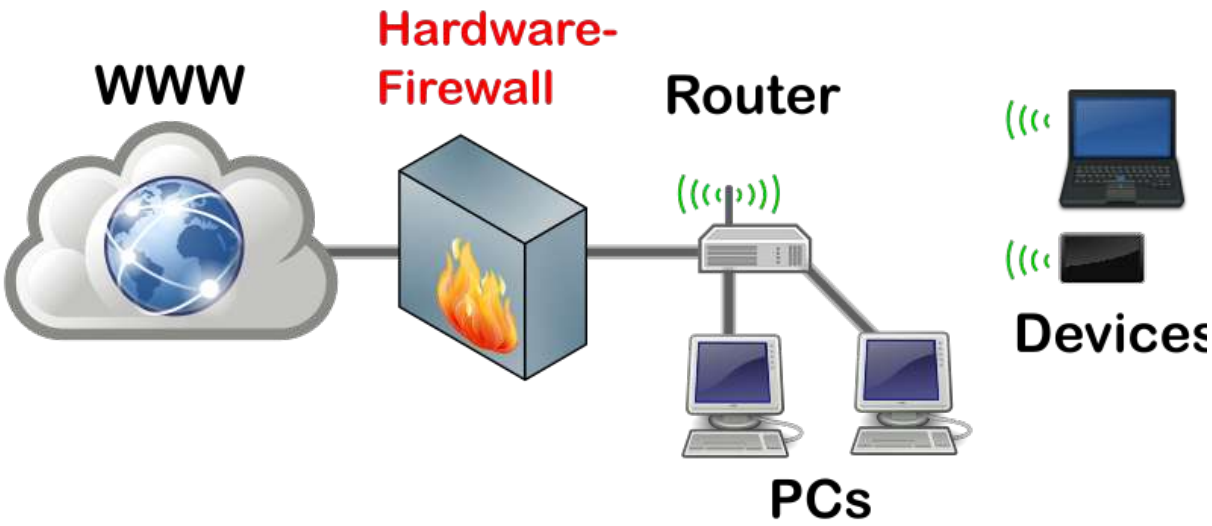
TP de Réseau

Spécialité Électronique et Physique appliquée



Ph Lefebvre – 2021

Séance 1 - Configuration et outils de base des réseaux

Travail préliminaire

Pour configurer l'accès réseau d'une machine, il faut lui associer :

- une adresse IP,
- un netmask,
- une @ IP de passerelle,
- une adresse ip d'un DNS.

Une **adresse IP** est constituée de 4 octets dont la notation classique est « décimale pointée » ; par exemple 10.5.7.8.
Ces 4 octets constituent en fait un mot de 32 bits divisé en 2 parties. La partie haute est l'identifiant du réseau. La partie basse est l'identifiant de la machine dans ce réseau. Où se situe la limite entre la partie haute et basse ? C'est une autre information qui s'appelle le « netmask » ou masque de réseau qui le détermine. Le netmask est également un mot de 32 bits dont tous les bits correspondant à la partie réseau sont à 1, et tous les autres sont à zéro ; par exemple « 255.255.255.0 ». Un netmask peut aussi être noté à la façon CIDR (Class Inter-Domain Routing). Ainsi il serait noté « /24 » puisqu'il y a 24 bits à 1 dans le mot 255.255.255.0.

Dans un réseau local, deux adresses ne peuvent pas être données à des machines. Il s'agit de :

- **L'adresse du réseau,** c'est la première adresse disponible (bits de la partie basse à 0) ;
- **L'adresse de diffusion** (broadcast), c'est la dernière adresse disponible (bits de la partie basse à 1). Elle est utilisée pour envoyer un message à tous les équipements qui sont dans le réseau.

D'autre part, les utilisateurs d'internet connaissent les machines par leur nom, mais pas par leur adresse IP, comme par exemple « www.ensicaen.fr ». C'est une machine s'appelant le DNS (Domain Name System) qui se charge de traduire les noms en adresse IP. Une machine doit donc connaître **l'adresse IP du DNS**.
Enfin, grâce au protocole physique (Ethernet, wifi...) une machine peut dialoguer avec toutes les machines qui sont situées sur le réseau local. Si elle veut atteindre une machine hors du réseau local, elle doit envoyer son message à un routeur (appelé aussi **passerelle**), dont il faut aussi connaître l'adresse IP.

Exemple :

Si l'adresse IP d'une machine est : 10.5.7.8/23

En binaire, son adresse s'écrit :
`00001010 . 00000101 . 00000111 . 00001000`
son netmask s'écrit :
`11111111 . 11111111 . 11111110 . 00000000 == 255.255.254.0`
L'adresse réseau est donc :
`00001010 . 00000101 . 00000110 . 00000000 == 10.5.6.0`
L'adresse de diffusion est donc :
`00001010 . 00000101 . 00000111 . 11111111 == 10.5.7.255`
Le réseau peut donc contenir 2^9-2 = 510 machines. En effet, l'adresse du réseau et l'adresse de broadcast sont des adresses réservées.

Exercice

Si l'adresse IP d'une machine est : 207.119.133.31 /25
a) Donnez le netmask en notation décimale pointée.
b) Donnez l'adresse réseau du sous-réseau dans lequel se trouve la machine.
c) Donnez l'adresse de broadcast du sous-réseau dans lequel se trouve la machine.
d) Combien d'adresses sont disponibles pour l'adressage de machines dans ce réseau ?
e) L'adresse 207.119.133.120 fait-elle partie de ce sous-réseau ?

Configuration réseau sous Linux en ligne de commande

Dans cette partie nous utiliserons les commandes en ligne sous Linux. Ces commandes sont similaires sous windows.

commande « ip » (ou ipconfig sous windows)

C'est la commande de bas niveau permettant de configurer les interfaces réseaux. Elle remplace la commande `/sbin/ifconfig`

Nous ne pouvons pas changer l'adresse IP de la machine faire car il faut les droits de « Super User ou root » pour le faire. Nous utiliserons donc cette commande seulement pour afficher les détails.

Tapez

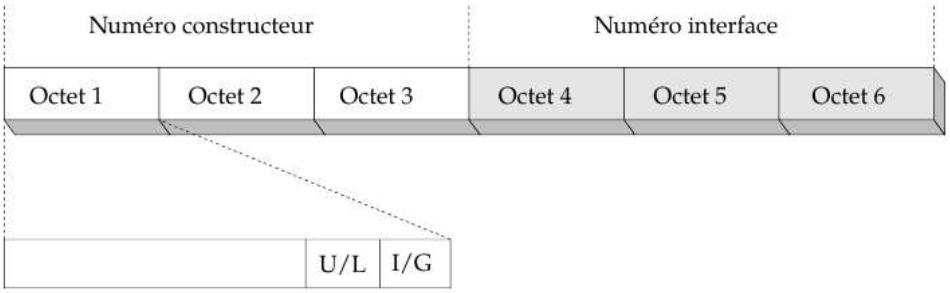
```
ip address
```

La liste des interfaces est alors affichée :
– « lo » correspond à l'interface locale (ou loopback) 127.0.0.1 ;
– « enpXsY » correspond à la carte ethernet. Les valeurs de X et Y dépendent de l'emplacement physique de la carte ethernet (n° du slot sur le bus PCI express...).

L'adresse MAC est l'identifiant de votre carte ethernet. Elle est notée par 6 nombres hexadecimaux séparés par « : » ou par « - ».

1) **Quelle** est l'adresse MAC de votre machine ?

   Pour rappel, voici le format d'une adresse Ethernet :



2) **Donnez** la valeur des champs Individual(0)/Group(1) et Universal(0)/Local(1) de l'adresse MAC. Qu'est-ce que cela signifie ?
3) **Comparez** l'adresse à celles des machines de vos voisins. Y a-t-il un point commun ? Si oui, pourquoi ? **recopiez** les 3 premiers octets des adresses MAC de votre carte ethernet et ou de votre carte WIFI sur le site : https://macvendors.com/ . Quels sont les constructeurs de vos cartes ?
4) **Quelle** est votre adresse IP et son netmask associé ?
5) Pour afficher la table de routage, **entrez** `/sbin/route -n.` La route 0.0.0.0 est la route par défaut. Quelle est l'adresse IP de la passerelle par défaut ? Vérifiez que la passerelle et votre machine sont dans le même réseau local.

Ping

Ping permet de tester l'état d'une liaison entre 2 machines. Cette commande permet, par l'envoi d'un message ICMP, de tester l'état d'une liaison entre deux machines. Cette commande donne en plus les temps d'aller-retour d'un échange. Elle prend en argument le nom d'une machine ou son adresse IP. Par exemple

```
ping 192.168.24.0.1
```

Pour l'arrêter, appuyez sur CTRL-C.
Faites un `ping` sur votre propre adresse IP.
Testez la connexion avec votre passerelle.
L'adresse IP 127.0.0.1 est une adresse avec laquelle une machine peut communiquer avec elle même. Testez cette adresse avec `ping.`

Essayez également de pinger une des machines de Google dont l'adresse est 8.8.8.8. **Quels** sont les temps d'aller-retour pour ces 4 tests ?

ARP

Losqu'une machine veut envoyer un paquet à une autre machine qui est sur le même réseau local, elle doit connaître l'adresse MAC de la carte ethernet destinataire. Pour cela elle utilise le protocole ARP (Address Resolution Protocol) qui permet de faire l'association adresse IP/adresse MAC.
Lancez la commande `arp –n`.

Cette commande permet de visualiser ce que la machine a appris (« cache ARP »).

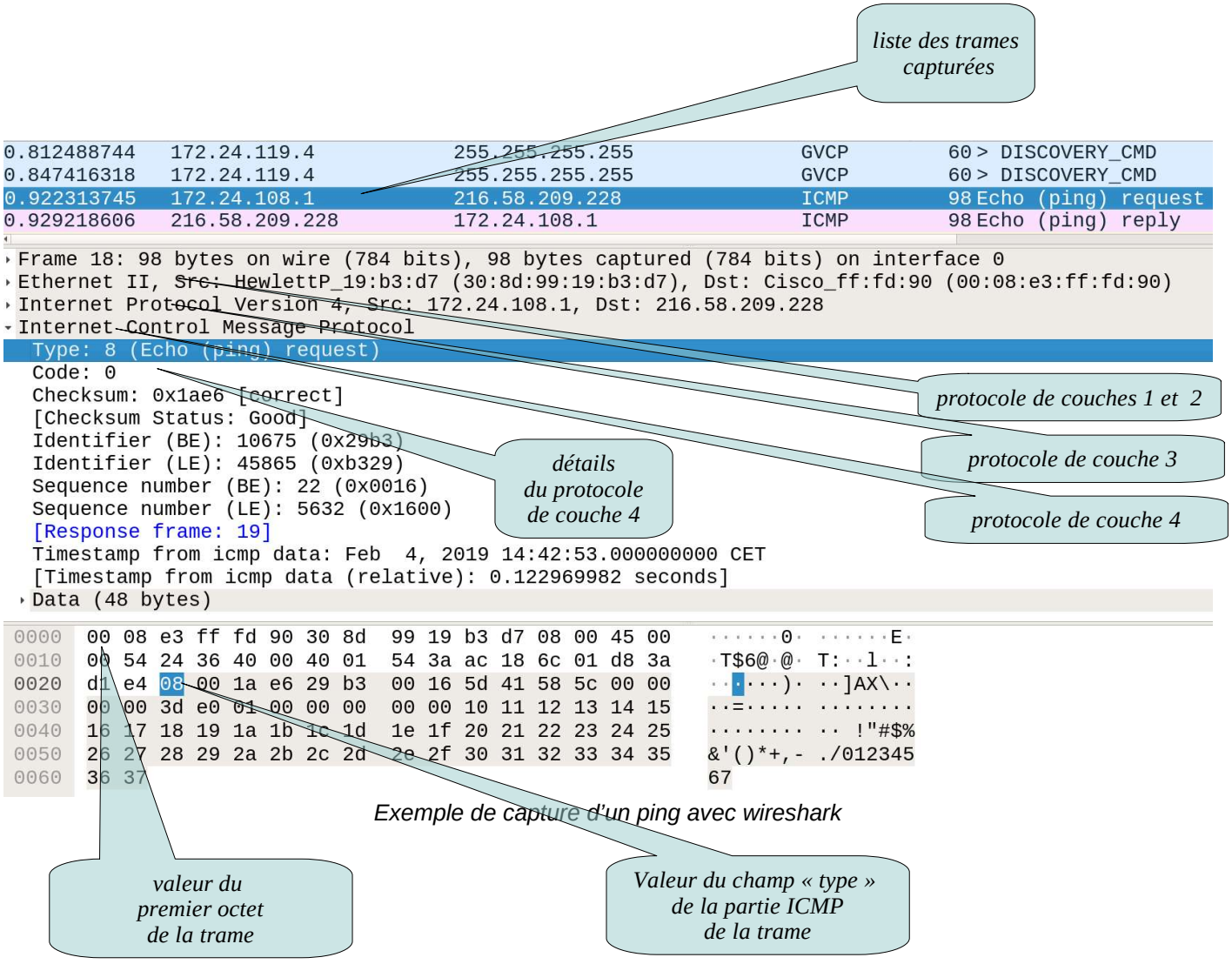
1) **Quelles** adresses IP se trouvent dans votre cache ARP. Quel est l'adresse MAC de votre passerelle ? Quel est le fabricant de la carte réseau ?
2) **Pourquoi** le cache ARP est-il vidé par le système d'exploitation avec le temps ?

Analyse de trames ARP

Wireshark

Cet utilitaire permet d'écouter une interface réseau et d'afficher les trames capturées. Lancez « `wireshark` ».
Pour capturer une trame, cliquer sur Capture puis Interfaces.
Choisir l'interface sur laquelle vous voulez écouter puis « start ».
Pour arrêter la capture cliquez sur l'icône représentée par un carré rouge.
La fenêtre est divisée en trois parties.

- La première partie présente un résumé des trames capturées.
- La deuxième partie de la fenêtre reprend la trame sélectionnée et la détaille.
- La troisième et dernière partie est une vision de la trame en codage hexadécimal.



Exemple de capture d'un ping avec wireshark

remarques : Vous pouvez filtrer les trames affichées en tapant dans le champ « filter », de wireshark, des motifs de recherche. Exemple de motifs :

arp	*filtre les trames contenant le protocole ARP*
icmp	*filtre les trames contenant le protocole ICMP*

ip.addr==10.0.0.1 filtre les trames dont l'adresse IP source OU destination est 10.0.0.1
ip.src==10.0.0.1 filtre les trames dont l'adresse IP source est 10.0.0.1
Attention à remettre à zéro le filtre lors d'une nouvelle capture.

Dans une fenêtre de commande lancez un ping sur une machine qui n'est pas listée dans le cache ARP de votre machine. Arrêtez le, puis relancez ce ping.

1) **Combien** de trames sont utiles à votre machine pour faire la correspondance adresse MAC / adresse IP ?
2) **Combien** de trames sont utiles à votre machine pour tester la communication avec une autre machine par ping
3) Quelle est l'adresse destination d'une trame ARP request ?
4) Décrivez le mécanisme ARP et celui de ping.

Dans une fenêtre de commande lancez un `ping` sur une adresse « bidon » qui pourrait être dans votre réseau local. Par exemple, si l'adresse de votre passerelle est **192.168.1**.1 faites un ping sur 192.168.1.57.
Capturez la trame ARP request ainsi générée.

Format de trame Ethernet II

Préambule	**Adresse destination**	**Adresse source**	**Type de protocole**	**Données**	**Bourrage**	**CRC**
8 octets	6 octets	6 octets	2 octets	1 à 1500 oct	Seult. si données < 46 o.	4 o.

Types : 0806 (ARP) / 0800 (IP)
Attention : la plupart des drivers de carte Ethernet ne fournissent pas la valeur du préambule ni le FCS. Wireshark ne peut donc pas les afficher.

Format d'une trame ARP :

bit 0 à 7	bit 8 à 15	bit 16 à 23	bit 24 à 31
Typed'adresse physique : MAC = 0001		Type d'adresse réseau: IP = 0800	
long. @ physique	long. @ réseau	Code : demande (0001) / réponse (0002)	
adresse physique de l'émetteur ...			
... du paquet		Adresse réseau de l'émetteur du ...	
... paquet		Adresse physique du ...	
... récepteur du paquet			
adresse réseau du récepteur du paquet			

En analysant la capture d'une trame « echo request » **déterminez** où se trouvent les adresses MAC destination et source et les adresses IP sources et destination.
5) Se trouvent-elles toujours au même endroit (par rapport au début de trame) ?
6) **Donnez** le code et le type ICMP associés à une requête ping et celui associé à une réponse ping.

Notions de routage

Grâce au protocole Ethernet ou WIFI, votre machine peut dialoguer avec toutes les autres machines de votre réseau local. Si elle veut atteindre une machine hors de ce réseau, elle doit envoyer son message à une passerelle (nommée « gateway » en anglais). La passerelle se chargera de router ce message vers la machine destinataire ou vers un autre routeur intermédiaire mieux à même de router ce message.

Connectez votre téléphone portable en wifi. Relevez l'adresse IP de votre téléphone portable en allant dans « paramètre→ à propos du téléphone→ état »

Avec wireshark **relevez** les 2 adresses MAC source/destination MAC et les 2 adresses IP source/destination lors d'un ping entre votre PC et :

1. votre téléphone
2. l'adresse 8.8.8.8

2) A quelle machine votre PC envoi-t-il localement ses paquets pour atteindre votre téléphone ?
3) A quelle machine votre PC envoi-t-il localement ses paquets pour atteindre 8.8.8.8 ?

traceroute / tracepath (tracert sous window's)

Lorsqu'un paquet passe à travers un routeur le champ TTL de l'entête IP est décrémenté de 1. Si le TTL atteint la valeur 0 alors le routeur détruit le paquet et renvoie une trame « Time to live exceeded » à l'émetteur initial du paquet.
L'option **-t** de la commande ping permet de fixer la valeur du TTL au départ du paquet.

4) **Entrez** les commandes suivantes, capturez-les avec wireshark et **expliquez** :

```
ping -t 1 www.google.com
ping -t 2 www.google.com
ping -t 3 www.google.com
```

5) A l'aide de wireshark donnez le type des trames « Time to live exceeded » ?

Les commandes traceroute ou tracepath permettent de connaître le nombre de routeurs séparant deux machines en exploitant la valeur du TTL.
`traceroute 193.49.200.1` liste les routeurs vous séparant du routeur d'adresse `193.49.200.1.`
La commande **mtr** est plus moderne et effectue le même travail.

Lancez `mtr www.google.com` et analysez le fonctionnement de mtr du point de vue du TTL.

avec un navigateur, consultez le site https://www.mon-ip.co/localiser-ip (service de Baptiste Lemonnier, IUT de Caen) ou au site « www.whatismyip.com ».

6) Avec quelle adresse IP êtes-vous « vus » depuis l'extérieur ?

7) Entrez la commande « `mtr 129.78.5.8` » . Cette adresse est celle d'une machine se trouvant en Australie. Qu'en **déduire** sur le nombre de routeurs permettant de « traverser le monde » ? Est-on sûr que ce nombre ne variera pas au cours d'une journée ?

Ouvrez la carte du réseau Renater sur www.renater.fr , cliquez sur « Réseau », puis « Infrastructure en Métropole ». Par quel chemin passent les données pour atteindre « www.ensicaen.fr » et « www.univ-bordeaux.fr » ?

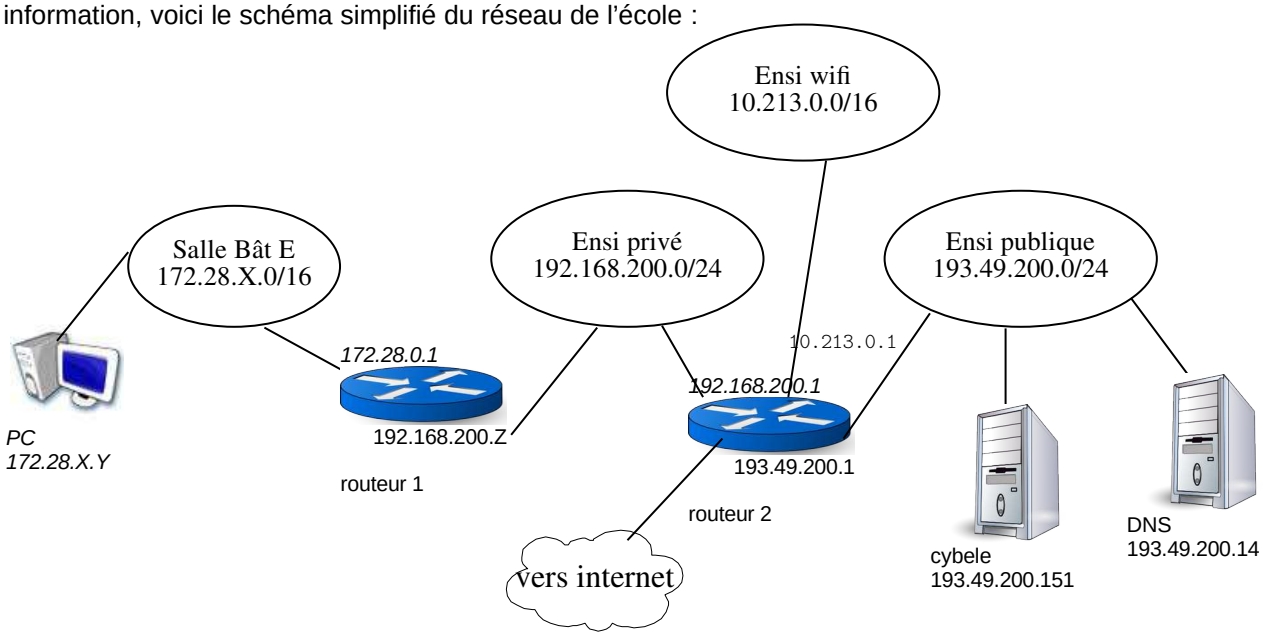
Consultez « http://submarine-cable-map-2015.telegeography.com/ » pour vous faire une idée des interconnexions mondiales.

Certains sites appelés « looking glass » proposent d'exécuter des commandes `traceroute` à partir de leur site. Le site http://lg.aarnet.edu.au/cgi-bin/lg est le looking glass du réseau Education et Recherche australien. A partir de ce site, effectuez une commande `tcptrace` (équivalent de traceroute -T) sur l'adresse 192.93.212.87, qui est une machine de l'école. Combien de routeurs sont traversés ?

8) Nous verrons en cours la notion de système autonome. Grossièrement, un système autonome est une entité (typiquement un FAI) qui gère un pool d'adresses publiques et gère les connexions entre ces adresses et les

autres systèmes autonomes. En utilisant le résultat de la question précédente et le site https://stat.ripe.net/widget/prefix-overview , indiquez le numéro et le nom des systèmes autonomes traversés par les paquets générés par le `tcptrace` de la question précédente.

Pour information, voici le schéma simplifié du réseau de l'école :



La résolution de noms

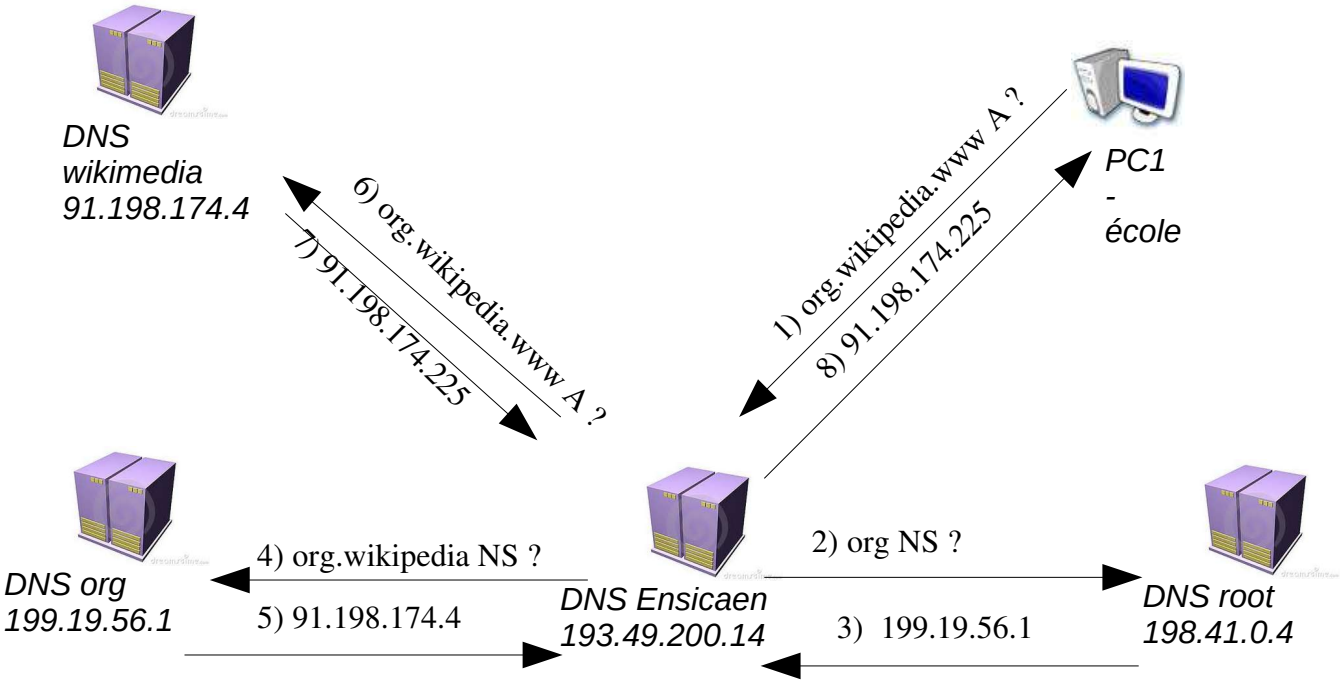
Lorsqu'une application veut envoyer un message à une autre elle utilise en général le nom de domaine. Par exemple la machine cybele de l'école possède le nom suivant : *cybele.ecole.ensicaen.fr*. Cependant, le protocole IP n'utilise pas les noms de machines pour qu'un paquet arrive à la bonne destination, mais les adresses IP, par exemple 193.49.200.151.
La machine doit donc pouvoir faire la correspondance entre les noms et les adresses IP.
Plusieurs techniques existent :

- fichier local faisant la correspondance. Ce fichier se trouve souvent dans « etc/hosts »
- Netbios Name Server : service offert sur un réseau local par les machines Windows
- Domain Name server : Le système hiérarchique le plus utilisé.
- Multicast DNS : utilisé par Avahi/zeroconf sur les machines Linux

Interrogation d'un DNS (Domain name System)

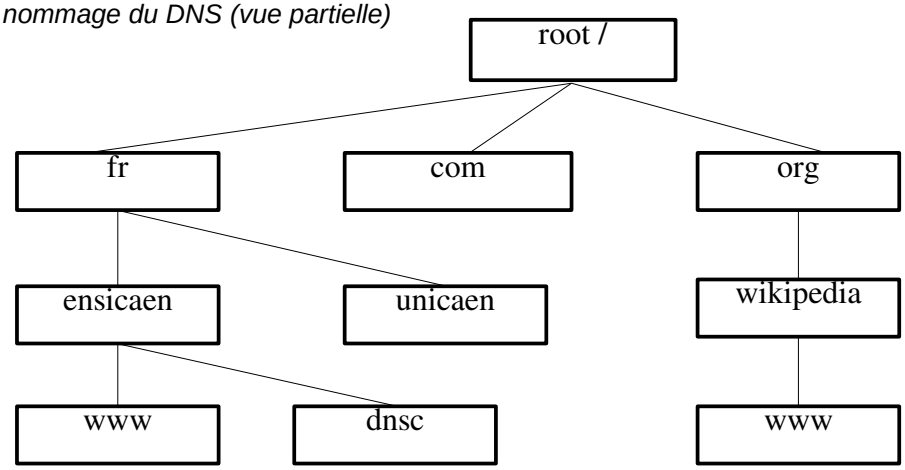
Un serveur DNS est une machine qui répond à des requêtes de noms de domaines. Ainsi chaque domaine ou sous-domaine est géré par une machine qui fait autorité. C'est elle qui connaît toutes les adresses IP de toutes les machines du domaine. Cette machine est capable aussi d'aller interroger le bon serveur DNS quand elle ne connaît pas la réponse. Souvent, elle stocke en cache la réponse et devient capable de donner la réponse la prochaine fois. Cette réponse sera dite « non authoritative ». Les serveurs DNS permettent aussi de fournir l'adresse IP du serveur de mail (serveur SMTP) d'un domaine.

Exemple d'interrogation DNS : Un serveur de l'école demande l'adresse IP de www.wikipedia.org.



Il y a une phase récursive : le PC demande au serveur DNS de l'ENSICAEN de prendre en charge sa requête et récupère la réponse à la fin. Le DNS de l'ENSICAEN, lui, résout la requête de manière itérative : interrogation d'un serveur racine, puis du serveur gérant « org », puis du serveur gérant « org.wikipedia ».

Arbre de nommage du DNS (vue partielle)



Configuration
Tapez « `nmcli dev show` » pour connaître l'adresse IP du serveur DNS utilisé par votre machine.

nslookup

Cette commande permet d'interroger le serveur de nom (DNS) et de connaître l'adresse IP d'une machine dont vous connaissez le nom ou l'inverse.
Tapez `nslookup` puis entrez le nom ou l'adresse IP à rechercher. **Quels** sont les adresses IP de « www.ensicaen.fr » et de « www.dailymotion.fr » ?

23) Quel est le non « canonique » de www.ensicaen.fr (cherhcez le nom correspondant à l'@ IP).

Pour connaître l'adresse IP d'un serveur de courrier électronique correspondant à un domaine tapez :
`nslookup -type=MX`
puis tapez le nom de domaine à rechercher.

24) **Quel** est le serveur de courrier de ensicaen.fr ?
25) Avec wireshark, donnez les noms des **protocoles de couche 3 et 4** utilisés par nslookup ?
26) Quel est l'adresse IP du serveur DNS qui a répondu à vos requêtes ?

Séance 2 – Les services applicatifs simples.

Travail préparatoire – À rendre au début de la séance.

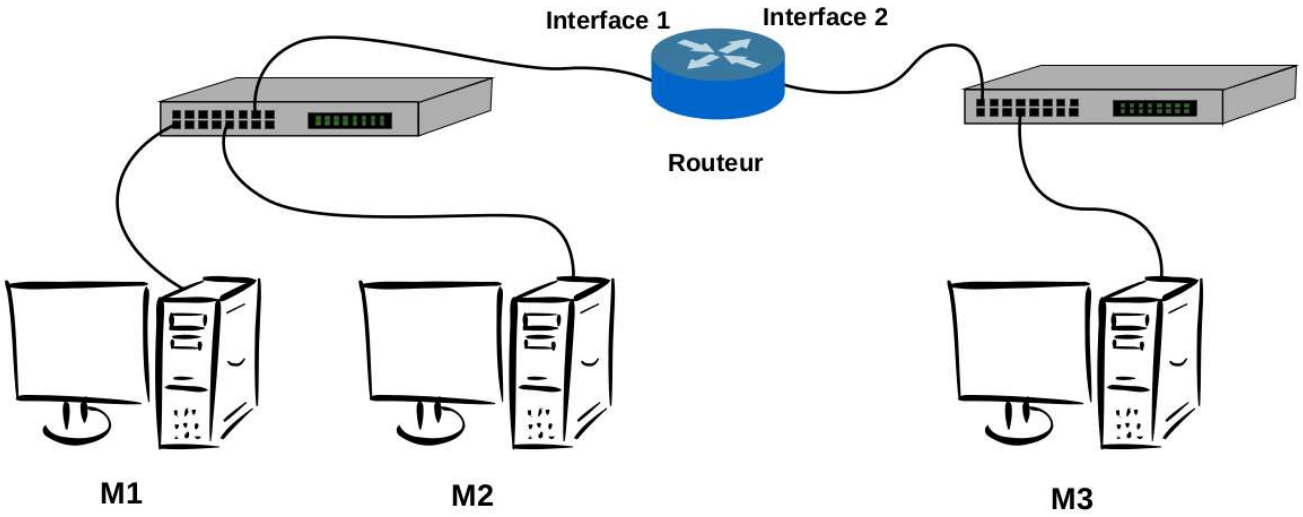
Ex1

Soit le réseau d'adresse 172.16.0.0/12 (pour info, c'est l'un des 3 réseaux privés)

1) découpez ce réseau en 2 réseaux /14 et un /13.

Ex2

Voici un schéma de réseau composé de 3 PC, 2 switches et 1 routeur.



M1 et M2 sont sur le réseau 192.168.13.0/24.
M3 est sur le réseau 10.0.0.0/16.
Les adresses MAC des machines sont les suivantes :
M1 : 00AA00 0000AA
M2 : 00BB00 0000BB
M3 : 00CC00 0000CC
Interface 1 du routeur : 001100 000011
Interface 2 du routeur : 002200 000022

1) **Donnez** des adresses IP au routeur et aux 3 machines.
2) **Quelle** est l'adresses IP de la passerelle par défaut de M2 ?
3) **Quelle** est l'adresses IP de la passerelle par défaut de M3 ?

4) On s'intéresse aux trames échangées entre la machine M1 et M3. La machine M1 envoie 10 octets de données en UDP sur le port n° 9 de la machine M3. La machine M1 utilise le port 2000. Le TTL est initialisé à 127 par M1. On rappelle que la taille de l'entête IP est de 20 octets et que l'entête UDP fait 8 octets. Sachant que la trame est capturée par Wireshark lancé sur M1, **donnez** la valeur des champs suivants dans cette trame : **adresse MAC source, adresse MAC destination, protocole transporté par ethernet, adresse IP source, adresse IP destination, protocole transporté par IP, longueur totale IP, TTL, port source, port destination.**
5) La trame est maintenant capturée par Wireshark lancé sur M3, **donnez** la valeur des champs précédemment listés.
6) Quels sont les protocoles dans la trame ?
7) **Précisez** à quelle couche appartient chacun de ces champs.

Manipulation (une partie des réponses aux questions seront à rendre)

Telnet / netcat

Telnet permet de se connecter à distance sur une autre machine en mode texte. C'est un logiciel très simple. Il est utilisé par exemple pour configurer du matériel à distance.

Lorsque vous lancez telnet celui-ci effectue les actions suivantes :

1. Connexion à la machine distante par des trames TCP de type SYN**.**
2. Envoie les caractères entrés au clavier et affiche les caractères reçus.
3. Déconnexion par des trames TCP de type FIN.

Depuis les machines libre service de l'Ensicaen il n'est pas possible de se connecter à un serveur de telnet. Nous allons donc analyser en local le fonctionnement de telnet en le faisant communiquer avec la commande **netcat.** Cette dernière ressemble à telnet en plus complet. Elle permet notamment d'attendre une connexion en mode serveur.

Lancez wireshark.
Demandez à votre voisin de taper dans une fenêtre : `nc -l 3000` *attention, c'est la lette « l » et no le chiffre 1*
Connectez-vous en tapant : `telnet @IP_du_voisin 3000`
Le premier paramètre de la commande telnet est l'adresse IP d serveur et le deuxième le numéro de port de l'application sur le serveur.

1. Quelles trames viennent d'être échangées (protocoles dans les trames) ?
2. Quels ports source/destination sont utilisés ?
3. Tapez « ABCDE » suivi de la touche <Entrée>. Quelles trames viennent d'être échangées ? (protocoles, longueur des données transportées par TCP...)
4. Tapez en même temps les touches <ctrl><atl Gr><] > suivi de la touche <entrée>.
   Tapez « QUIT ».
   Quelles trames viennent d'être échangées ?

Nous allons utiliser telnet pour découvrir quelques protocoles applicatifs. En effet certains protocoles, qui utilisent IP/TCP, codent les données en mode texte. Puisque telnet affiche tout ce qu'il reçoit (sauf la partie Ethernet/IP/TCP) nous observerons tout le protocole. Nous pourrons même interagir avec lui si nous envoyons les bonnes chaînes de caractères. Pour cela, nous devrons modifier le numéro de port TCP auquel telnet cherche à se connecter.

1) Consulter le fichier «/etc/services » de votre machine. Quels services sont associés aux ports 21, 23, 25, 80, et 443 ?
2) **Essayez** `telnet www.ecole.ensicaen.fr.` Que se passe-t-il ?
3) **Essayez** `telnet proxy.ensicaen.fr 80` puis tapez « `GET / HTTP/1.0` » suivi de 2 fois entrée.

   Vous venez d'envoyer une requête HTTP au serveur web de l'école comme le ferait un navigateur. Puisque la syntaxe de cette requête est correcte, le serveur vous renvoie une réponse HTTP transportant du HTML. HTTP veut dire Hyper Text Transfer Protocol. C'est le protocole qui permet de dialoguer avec un serveur web. Il est organisé de la façon suivante :

entête
saut de ligne : '\r\n'
corps

   Le corps du message contient soit des options pour la requête, soit la réponse du serveur. Il peut être codé en HTML, mais aussi transporter des images, de la video...
   L'entête contient divers champs comme le type de la requête. Pour une réponse, il décrit sa longueur, son format...

Afin de permettre à plusieurs noms de site d'être hébergés sur la même machine, HTTP 1.1 impose que les requêtes soient formées avec le champs Host. Par exemple :

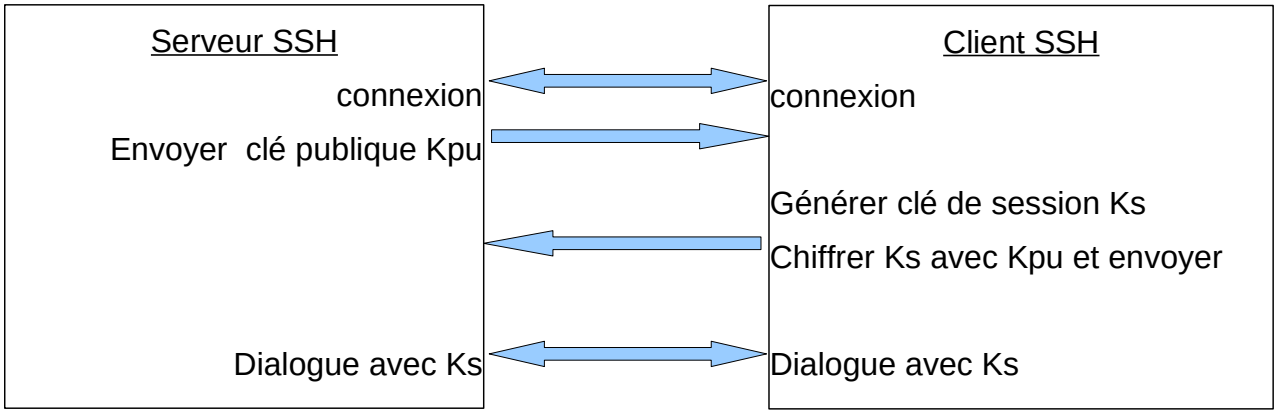
```
GET /index.html HTTP/1.1
Host: foad.ensicaen.fr
```

4) **Essayez** `telnet proxy.ensicaen.fr 3128` puis tapez « `GET / HTTP/1.0` » suivi de 2 fois entrée.
5) **Comment** s'appellent les champs HTTP qui décrivent le type de réponse et la longueur dans l'entête ?

6) **Essayez** `telnet proxy.ensicaen.fr 3128,` puis vous taperez `GET http://www.google.fr/ HTTP/1.1` suivi de 2 fois entrée. Cette fois, l'application qui tourne sur le port 3128 de la machine *proxy.ensicaen.fr* est un proxy. Son rôle est de relayer les requêtes HTTP. Pourquoi votre machine doit-elle se connecter à un proxy pour pouvoir dialoguer avec google ?

SSH

SSH est un service de chiffrement des données. Il est basé sur le principe suivant. Il existe des algorithmes de chiffrement dit asymétrique qui nécessitent 2 clés : 1 pour coder les données et une autre pour les décoder. Si la clé de codage est suffisamment grande (par exemple 2048 bits) il est difficile de trouver la clé de décodage à partir de cette première clé. Seul celui qui a généré la première clé connaît la clé de décodage. La clé de codage est appelée clé publique et peut être distribuée à quiconque.
Cependant, le codage avec une telle clé est très coûteux en temps processeur. SSH utilise en fait cette clé pour échanger une clé de session pour un algorithme de chiffrement symétrique, moins coûteux, qui sera utilisé pour le temps du dialogue.



11) Connectez-vous à *cybele* avec ssh. Avec wireshark retrouvez les phases d'échange de clés. Puis déterminez combien de trames sont générées pour l'envoi d'un caractère.
12) Combien d'octets sont nécessaires pour coder l'envoi d'un caractère avec ssh ?
13) Est-ce la même clé de codage pour coder un caractère à l'aller et au retour ?
14) Est-ce la même clé de codage pour 2 envois successifs ?

Exploration des ports ouverts : nmap

Exécutez `nmap 127.0.0.1` puis `nmap` avec l'adresse IP de votre voisin.

10) A quoi sert cette commande (faites *man nmap*) . Analysez son fonctionnement avec wireshark.

Netstat

15) Dans une autre fenêtre **tapez** « `netstat -antp` ». A quoi **sert** cette commande (faites *man netstat*) ?