Introduction aux réseaux IP

TD

Ph Lefebvre

1. Configuration réseau

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

Ifconfig (ou ipconfig sous windows)

C'est la commande de bas niveau permettant de configurer les interfaces réseaux. Nous ne pouvons pas le faire car il faut les droits de « Super User ou root » pour le faire. Nous utiliserons donc cette commande seulement pour afficher les détails.

Entrez `/sbin/ifconfig`
La liste des interfaces est alors affichée :
- *lo* correspond à l'interface locale (ou loopback) 127.0.0.1
- *eth0 correspond* à la première carte ethernet trouvée.

L'adresse MAC est l'identifiant de votre carte ethernet. C'est un numéro unique au niveau mondial C'est une adresse de la couche physique. Elle est notée par 6 nombres hexadécimaux séparés par « : » ou par « - ».

1) Quelle est l'adresse MAC de votre machine ?
2) Comparez à celles de vos voisins. Quels sont les points communs ?
3) Quel est votre adresse IP et son netmask associé ?
4) 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 ?

ping

Ping permet de tester l'état d'une liaison entre 2 machines. Cette commande donne en plus les temps d'aller-retour d'un échange. Elle prend en argument le nom d'une machine ou une adresse IP. Appuyez sur CTRL-C pour l'arrêter.
Testez un ping sur votre propre adresse IP.
Testez la connexion avec votre voisin.
L'adresse IP 127.0.0.1 est une adresse avec laquelle une machine peut communiquer avec elle même, **testez** un ping sur cette adresse.

5) Quels sont les temps d'aller-retour pour ces 3 tests ?

ARP

Losqu'une machine veut envoyer un paquet à une autre machine (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) pour faire l'association adresse IP/adresse MAC.
Faites `arp -a`.
Cette commande permet de visualiser le cache ARP qui contient les couples (@IP/@MAC) que la machine a appris.
Faites une série de ping sur les machines autour de vous et constatez que le cache ARP augmente.

6) Pourquoi le cache ARP se vide-t-il avec le temps ?

Analyse de trames

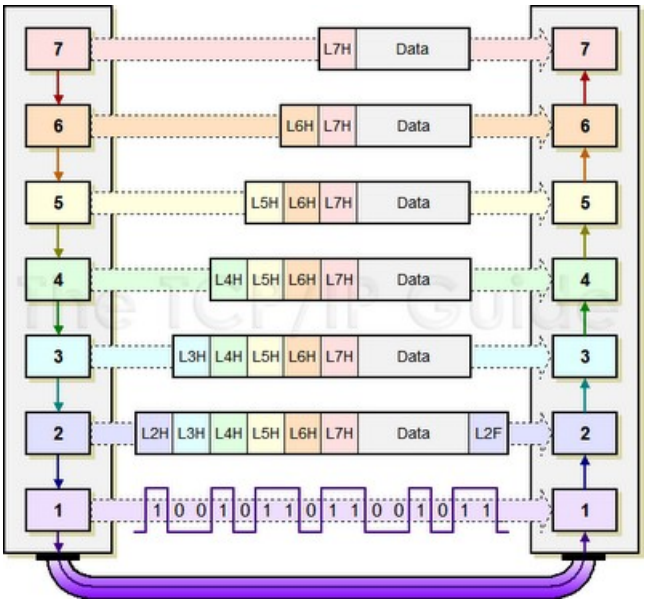
Pour échanger de l'information, il faut établir des règles de codage, de vitesse, de tour de parole. Ces règles s'appellent des protocoles. Internet, Ethernet, ARP, HTTP… sont des protocoles.

Les problématiques que gèrent les protocoles ne se situent pas sur le même plan : supervision du réseau, intégrité des données échangées… On les classe donc par niveau. C'est le modèle OSI (Open System Interconnection) en couches :

No	nom	Rôle	exemple de protocole
7	Application	Applications s'appuyant sur le réseau : transfert de fichiers, émulation de terminal, messagerie, partage de fichiers, web…	telnet, HTTP, mail, NFS, FTP
6	Présentation	Conversion des données numériques propres au réseau dans leur version finale ou abstraite compréhensible par le programme. Cette couche est souvent associée à un langage possédant des règles lexicales (les mots), syntaxiques (la grammaire) et sémantique (le sens).	XDR, ASN1 UTF-8 MPEG, JPEG
5	Session	Gestion d'une session : ouverture, mots de passe, reprise en cas d'erreur, fermeture.	Netbios cookies
4	Transport	Multiplexage/démultiplexage des paquets, segmentation, contrôle de flux, correction des erreurs. Service de bout en bout.	~TCP
3	Réseau	Assure le routage, l'adressage.	~IP
2	Liaison	Délimitation d'une trame, contrôle et correction d'erreurs, contrôle de flux, règle d'accès au médium. Service point à point.	HDLC, ethernet wifi
1	Physique	Conversion des signaux électriques en bits. Définition des caractéristiques électriques et mécaniques du support de transmission.	RS232 ethernet

Ensuite, les données sont regroupées en paquet. Chaque protocole ne voit pas le format du paquet de la même manière. Un protocole de transfert de fichiers s'intéresse aux fichiers. Mais l'envoie d'un fichier peut nécessiter de découper le fichiers en plusieurs paquets.
Les protocoles de haut niveau ont besoin des protocoles de bas niveau. Par exemple pour envoyer un fichier, il faut le coder, le découper en trame, puis l'acheminer vers de relais en relais et transformer les bits en signaux électriques.

A l'intérieur du paquet on retrouvera donc des informations de chaque protocole (ou presque).
Les données du protocole supérieure sont encapsulées dans le protocole du niveau d'en dessous.



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 cercle rouge et une croix blanche.
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.

Analyse ARP

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.

7) **Combien** de trames sont utiles à votre machine pour tester la communication avec une autre machine par ping ?
8) **Combien** de trames sont utiles à votre machine pour faire la correspondance adresse MAC / adresse IP ?
9) Décrivez le mécanisme ARP et celui de ping.

Par une série de ping sur des machines dont les adresses MAC ne sont pas dans le cache ARP, capturez une trame ARP-request et une trame ARP-reply et analysez les avec les formats de trames ci-dessous.

10) Donnez la valeur de tous les champs.

Format de trame Ethernet

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)

Format d'une trame ARP :

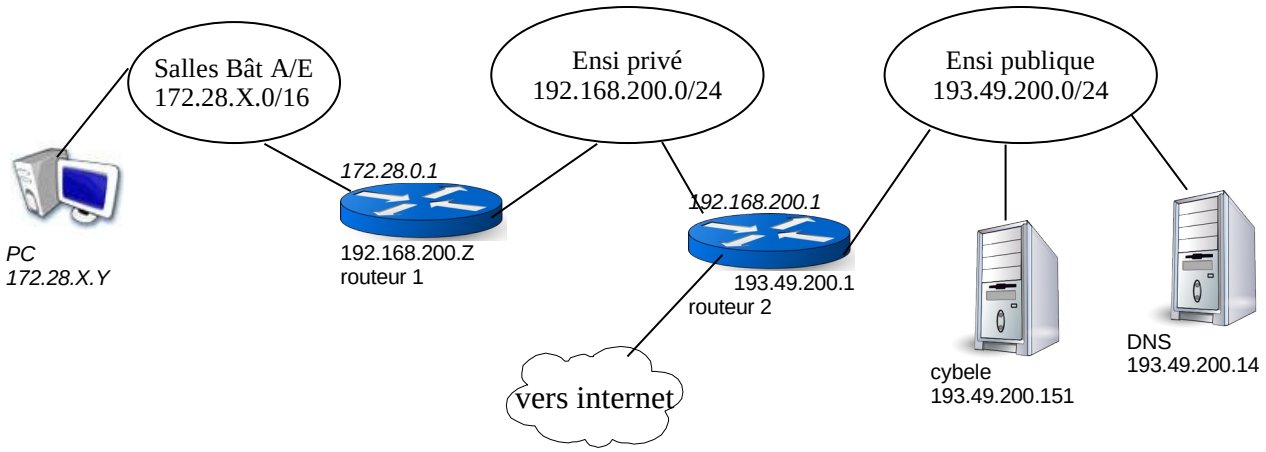
bit 0 à 7	bit 8 à 15	bit 16 à 23	bit 24 à 31
Typed'adresse physique : MAC = 0001		Type d'adresse réseau: IP = 0800	
long. @ physique	long. @ réseau	Code : demande (0001) / réponse (0002)	
adresse physique de l'émetteur ...			
... du paquet		Adresse réseau de l'émetteur du ...	
... paquet		Adresse physique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

11) Se trouvent-elles toujours au même endroit ?

2. Notions de routage

Voici une vision simplifiée du réseau de l'école.



12) Avec *wireshark* **relevez** les adresses source/destination MAC et IP d'un échange *ping* entre votre machine et celle de votre voisin.
13) Faites de même lors d'un échange de trames *ping* entre *cybele* et votre machine.
14) Connectez-vous à cybele en utilisant « ssh » (*ssh login@cybele.ecole.ensicaen.fr)* et le login habituel de l'école. En utilisant `ifconfig`, **déterminez** l'adresse MAC de *cybele*. **Expliquez**. Pourquoi l'adresse MAC destination capturée par wireshark n'est pas celle de *cybele* ?
15) Donnez une adresse MAC du routeur 2 ?
16) Combien peut-on adresser de machines sur le réseau du bâtiment E ?

traceroute / tracepath (tracert sous window's)

Cette commande permet de connaître le nombre de routeurs séparant deux machines. Par exemple :
`tracepath 193.49.200.1` liste les routeurs vous séparant du routeur d'adresse `193.49.200.1.`
Pour des raisons de sécurité, cette commande ne fonctionne pas à l'Ensi. Nous allons cependant analyser son fonctionnement et utiliser la commande ping pour retrouver les informations que cette commande aurait pu nous donner.

17) Lancez cette commande et **analysez** à l'aide de wireshark le champ TTL de chaque trame IP envoyée. **Expliquez** alors le fonctionnement de *tracepath.*
18) **Quel protocole** de couche 4 est utilisé par tracepath ?
Ce protocole étant filtré nous allons utiliser le protocole ICMP. **Entrez** les commandes suivantes et **expliquez** :

```
ping -t 1 193.49.200.16
ping -t 2 193.49.200.16
ping -t 3 193.49.200.16
```

19) A l'aide de wireshark donnez le type des trames « Time to live exceeded » ?
20) Connectez vous au site « www.whatismyip.com ». Avec quelle adresse IP êtes-vous « vus » depuis l'extérieur ?
21) Que fait la commande mtr -n sydney.edu.au **Analysez** avec wireshark.

22) 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 » ?
23) Consultez « http://submarine-cable-map-2015.telegeography.com/ » pour vous faire une idée des interconnexions mondiales.

3. La résolution de noms

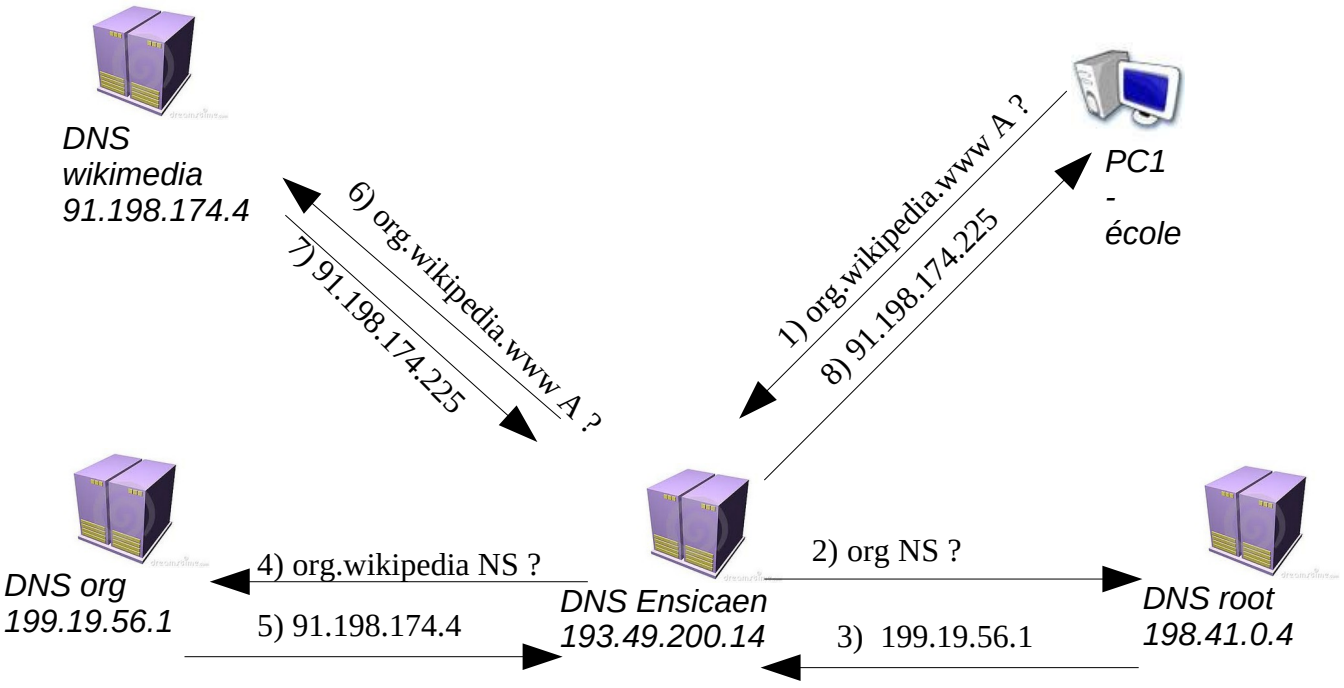
Lorsqu'une application veut envoyer un message à une autre elle utilise en général le nom de domaine. Par exemple la machine cybele de l'école possède le nom suivant : *cybele.ecole.ensicaen.fr*. Cependant, le protocole IP n'utilise pas les noms de machines pour qu'un paquet arrive à la bonne destination, 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)

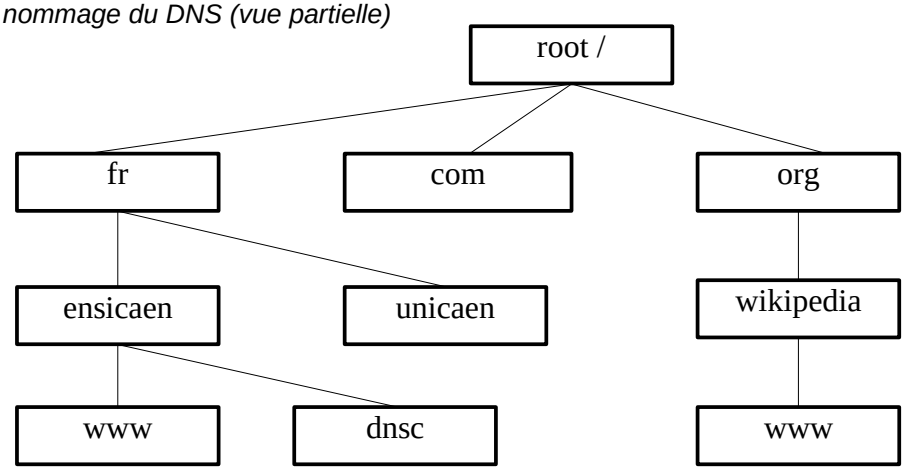
Un serveur DNS est une machine qui répond à des requêtes de noms de domaines. Ainsi chaque domaine ou sous-domaine est géré par une machine qui fait autorité. C'est elle qui connaît toutes les adresses IP de toutes les machines du domaine. Cette machine est capable aussi d'aller interroger le bon serveur 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)



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) À quelle machine correspond l'adresse wwwensicaen.ecole.ensicaen.fr ? Qu'en **conclure** ?

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 ?

Une machine peut aussi faire la correspondance « @IP / nom de domaine » par le fichier hosts se situant dans C:\WINDOWS\system32\drivers\etc . Attention, dans ce cas, le nom n'est défini que pour votre machine, et ne sera partagé avec personne d'autre...
Rajouter le nom de la machine de votre voisin.
Tester l'ajout avec « ping nom »

4. Exercice

Pour configurer l'accès réseau d'une machine, il faut d'abord lui associer une **adresse IP**. 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 local. 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). Dans notre exemple, il sera ainsi noté « /24 » puisqu'il y a 24 bits à 1 dans le mot 255.255.255.0.
L'adresse du réseau est la première adresse disponible (bits de la partie basse à 0).
L'adresse de diffusion (broadcast) est la dernière adresse disponible (bits de la partie basse à 1).
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 :

Soit le réseau d'adresse 10.6.8.0/22.

1) La machine 10.6.10.37 fait elle partie de ce réseau ?
2) Donnez le netmask en notation décimale pointée
3) Donnez l'adresse de diffusion sur ce réseau.
4) Combien de machines peuvent-être adressées sur ce réseau ?