

Réseaux

Internet

I Un peu d'histoire

La DARPA (Defense Advanced Research Projects Agency) voit le jour en 1958, cette agence gouvernementale américaine a pour but de veiller à la constante suprématie des États unis en matière technologique et scientifique. En 1962 la DARPA soutient le projet du professeur Licklider qui a pour but de mettre en réseau les ordinateurs des universités américaines afin que ces dernières puissent échanger des informations plus rapidement (même à des milliers de kilomètres de distance). En 1968, ARPAnet, 1er réseau informatique à grande échelle de l'histoire voit le jour. Le 29 octobre 1969, le 1er message (le mot "login") est envoyé depuis l'université de Californie à Los Angeles vers l'université de Stanford via le réseau ARPAnet (les 2 universités sont environ distantes de 500 Km). C'est un demi-succès, puisque seules les lettres "l" et "o" arriveront à bon port. En 1972, 23 ordinateurs sont connectés à ARPAnet (on trouve même des ordinateurs en dehors des États unis). En parallèle au projet ARPAnet, d'autres réseaux voient le jour, problème, ils utilisent des protocoles de communication hétéroclite (UUCP, NCP ou encore X.25) et 2 ordinateurs appartenant à 2 réseaux différents sont incapables de communiquer entre eux puisqu'ils n'utilisent les mêmes protocoles. En 1974 Vint Cerf et Bob Khan vont mettre au point le protocole TCP qui sera très rapidement couplé au protocole IP pour donner TCP/IP. TCP/IP, grâce à sa simplicité, va très rapidement s'imposer comme un standard : les différents réseaux (ARPAnet et les autres) vont adopter TCP/IP. Cette adoption va permettre d'interconnecter tous ces réseaux (2 machines appartenant à 2 réseaux différents vont pouvoir communiquer grâce à cette interconnexion). Internet était né (le terme Internet vient de "internetting" qui signifie "Connexion entre plusieurs réseaux"). TCP/IP est donc au cœur d'Internet, voilà pourquoi aujourd'hui, la plupart des machines utilisent TCP/IP.

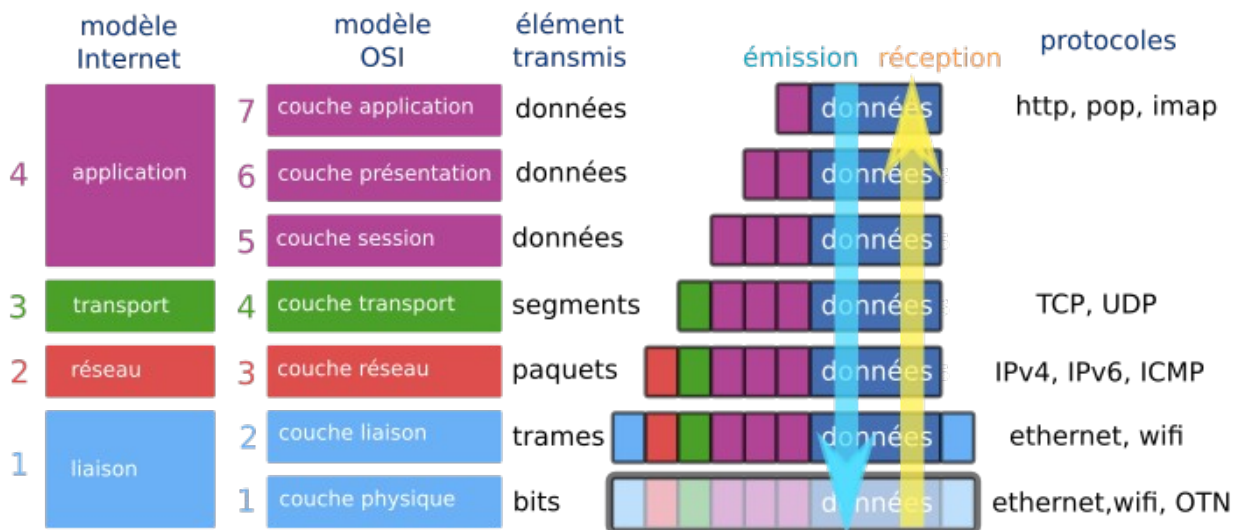
II Modèles théoriques

Les bits transmis d'un ordinateur à un autre contiennent, en plus des données *utiles* (le mot « bonjour » dans un e-mail), une multitude de données (tout aussi utiles) qui vont aider à l'acheminement de ces bits au bon endroit, puis au bon ordinateur, puis au bon logiciel. Les différents protocoles qui régissent cette transmission sont regroupés dans ce qui est appelé un **modèle**.

Deux modèles synthétisent ces protocoles :

- le **modèle Internet** (ou modèle **TCP/IP**, 1974), organisé en **4** couche : liaison, réseau, transport, application.
- le **modèle OSI** (Open Systems Interconnection, 1984), organisé en **7** couches : physique, liaison, réseau, transport, session, présentation, application.

Ces deux modèles coïncident suivant le schéma ci-dessus. Ce sont des modèles théoriques et d'une certaine rigidité. Leur utilisation dans la pratique est parfois plus floue, avec des protocoles à cheval sur plusieurs couches.



Dans la suite du cours on fera référence au modèle Internet (TCP/IP).

On retient pour TCP/IP un modèle à quatre couches :

Couche	Modèle TCP/IP	protocole
4	Application	HTPP(S) FTP DNS SMTP POP IMAP...
3	Transport	TCP UDP
2	Internet	IP
1 – Accès réseau	1b – liaison	
	1 – Physique	Ethernet, Wi-Fi

III Éléments physiques d'un réseau

Un réseau est constitué de machines (ordinateurs, téléphones, réfrigérateurs connectés, voitures connectés, consoles de jeu, etc.) reliés entre eux, physiquement via une paire torsadée avec des prises RJ45, ou par Wifi, ou encore 4G, Bluetooth, etc.

Définition – adresse physique, adresse MAC

Chaque carte réseau est associée à un identifiant unique appelé **adresse MAC** ou **adresse physique**.

Si une machine a à la fois une carte réseau par câble RJ45 et une carte Wifi, alors elle aura deux adresses MAC.

Cette adresse est codée sur 48 bits, présentés sous la forme de 6 octets en hexadécimal séparée par des « : »

Exemple : fc : aa : 14 : 75 : 45 : a5

Les trois premiers octets correspondent au code du fabricant. Un site comme <https://www.macvendorlookup.com/> vous permet de retrouver le fabricant d'une adresse MAC quelconque.

Exercice 1

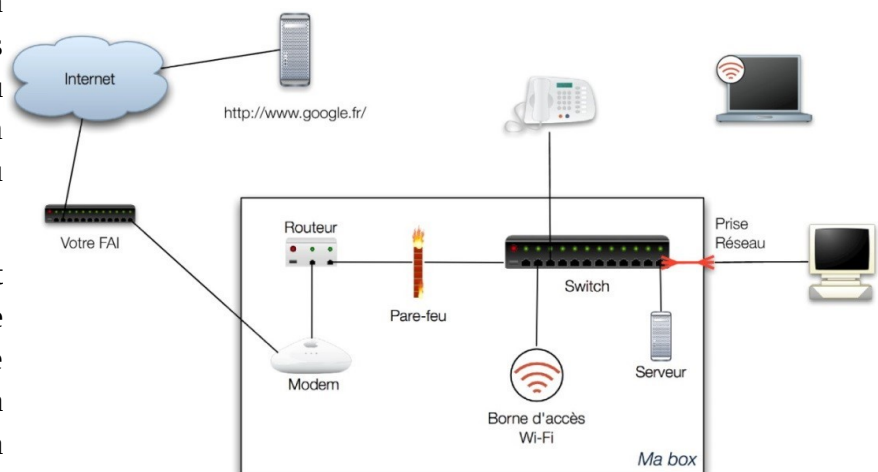
- Ouvrez une console de commande.
- Déterminez la ou les adresse(s) MAC de votre ordinateur à l'aide des commandes :
 - **Linux** : `ip link`, l'adresse MAC est celle qui figure après `link/ether` ou `link/ieee802.11`.
 - **MacOs** : `ifconfig` l'adresse MAC est celle qui figure après `ether`
 - **Windows** : `ipconfig -all`, l'adresse MAC est l'adresse physique.
- Trouver le vendeur associé à votre ou vos carte(s) réseau(x).

Les machines sont reliées à un **switch** (commutateur, dont le rôle est détaillé plus bas). On est dans un réseau **LAN** (Local Area Network).

Remarque pour les joueurs : quand vous jouez en **VLAN** (Virtual Local Area Network), vous isolez une partie du switch pour créer un réseau local de jeu.

Les switches sont reliés à un routeur, qui interprète les adresses **IP** (cf. paragraphe du même nom) à l'aide d'un serveur **DNS** (cf. paragraphe du même nom).

Le **routeur**, dont le rôle est détaillé plus bas, communique avec les autres réseaux par le biais d'un modem, dans un réseau **WAN** (Wide Area Network).

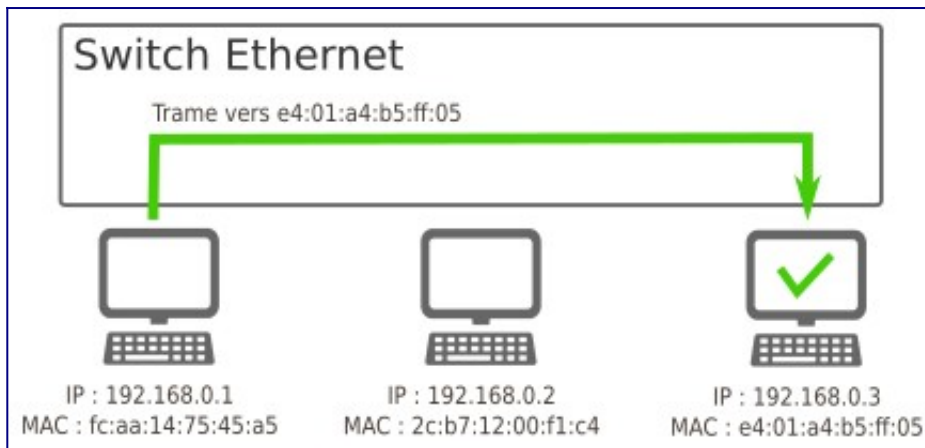


Ci-contre le schéma d'une box domestique.

Le **pare-feu** permet de filtrer les données entre une zone où la confiance est nulle (Internet), et une zone où la confiance est plus importante (le réseau local).

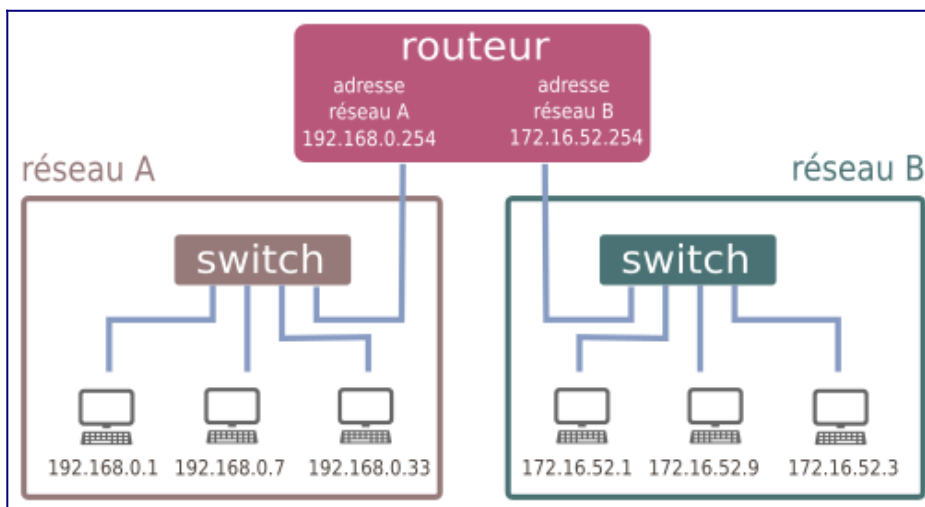
Le switch

Au sein d'un **switch Ethernet**, une analyse est effectuée sur la trame qui est à distribuer. Lors d'un branchement d'un nouvel ordinateur sur le switch, celui-ci récupère son adresse MAC, ce qui lui permet de **trier** les messages et de ne les distribuer qu'au bon destinataire.



Le routeur

Pour que les machines de deux réseaux différents puissent être connectées, on va utiliser un dispositif équipé de **deux cartes réseaux**, situé à cheval entre les deux sous-réseaux. Cet équipement de réseau est appelé **routeur** ou **passerelle**. La nécessité d'un routeur sera expliquée plus loin dans le cours.



IV Les adresses IP – masque de sous-réseau

Le protocole IP (Internet Protocol) est chargé d'acheminer au mieux les paquets de données d'une machine à une autre. Il permet d'identifier des machines grâce à leur adresse IP.

Les adresses IP sont de deux types :

- IPv4, constituée de quatre nombres entre 0 et 255, séparés par des points. Il y a en théorie 4 294 967 296 adresses possibles. Ces adresses sont en cours « d'épuisement », c'est-à-dire qu'il n'y en a plus assez par rapport aux besoins du monde actuel.

- IPv6, constitué de huit nombres entre 0 et 65 535, écrits en hexadécimal. Il y a $1,3 \times 10^{38}$ adresses IPv6 possibles. Ce protocole semble permettre de fournir un nombre quasi inépuisable d'adresses IP.

Dans la suite de ce cours nous ne parlerons que d'adresse IPv4.

Exercice 2

- Recherchez l'adresse IPv4 attribuée à votre machine.
Sous linux entrez la commande `ip address` pour chaque carte l'adresse IPv4 est après `inet` et l'IPv6 après `inet6`.
Sous macOs ou windows, il faut utiliser respectivement `ifconfig` et `ipconfig -all`, comme dans le premier exercice.
- Notez cette adresse.
- Comparer cette adresse IP avec celles de camarades de votre classe.
- Dans un navigateur accédez à la page <http://www.mon-ip.com/>
- Notez l'adresse IP que vous donne ce site.

Quelques explications

- L'adresse de votre machine est une adresse IP locale. C'est-à-dire qu'elle correspond à l'adresse sur votre réseau local. C'est pour cela que plusieurs personnes peuvent avoir la même adresse IP locale : elles sont sur des réseaux locaux différents. Très souvent, sur les réseaux locaux domestiques, les adresses sont de la forme `192.168.0.X` où X est un nombre entre 1 et 254, les adresses se terminant par 0 et 255 ayant un rôle particulier.
- L'adresse IP visible d'Internet est en fait l'adresse IP du routeur. C'est une adresse dite publique.

Sur un réseau local, à chaque adresse MAC d'une carte réseau connectée est associée une adresse IP locale à ce réseau. Cela permet d'utiliser de nombreuses fois les mêmes adresses IP et ainsi d'économiser le nombre d'adresses IP publiques. Malgré l'augmentation du nombre d'objets connectés, le déploiement d'IPv6 rend moins nécessaire ce type de pratique. Néanmoins, être connecté à un réseau local permet d'être en zone plus sûre grâce au routeur et au firewall que directement sur Internet. Un routeur permet la communication entre machines connectées à des réseaux distincts. La méthode pour le faire dépasse le cadre de ce cours.

Exercice 3

- Taper dans une console la commande `arp -a`. Elle affiche la table de correspondance entre adresse IPv4 et les adresses MAC de votre réseau local.
- Si vous trouvez dans cette liste une IP de type dynamique, c'est certainement une des machines de votre réseau local domestique. Vérifier en allant chercher son IP comme vu précédemment.
- Vérifiez que vous pouvez communiquer avec cette machine en tapant la commande `ping adresseIP`. Si la communication est possible, vous devez obtenir quelque chose ressemblant à :

```
C:\Users>ping 192.168.0.18
Envoi d'une requête 'Ping' 192.168.0.18 avec 32 octets de données :
Réponse de 192.168.0.18 : octets=32 temps=48 ms TTL=64
Réponse de 192.168.0.18 : octets=32 temps=4 ms TTL=64
Réponse de 192.168.0.18 : octets=32 temps=63 ms TTL=64
Réponse de 192.168.0.18 : octets=32 temps=67 ms TTL=64

Statistiques Ping pour 192.168.0.18:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 4ms, Maximum = 67ms, Moyenne = 45ms
```

Sinon, la communication n'est pas possible et vous obtenez quelque chose ressemblant à :

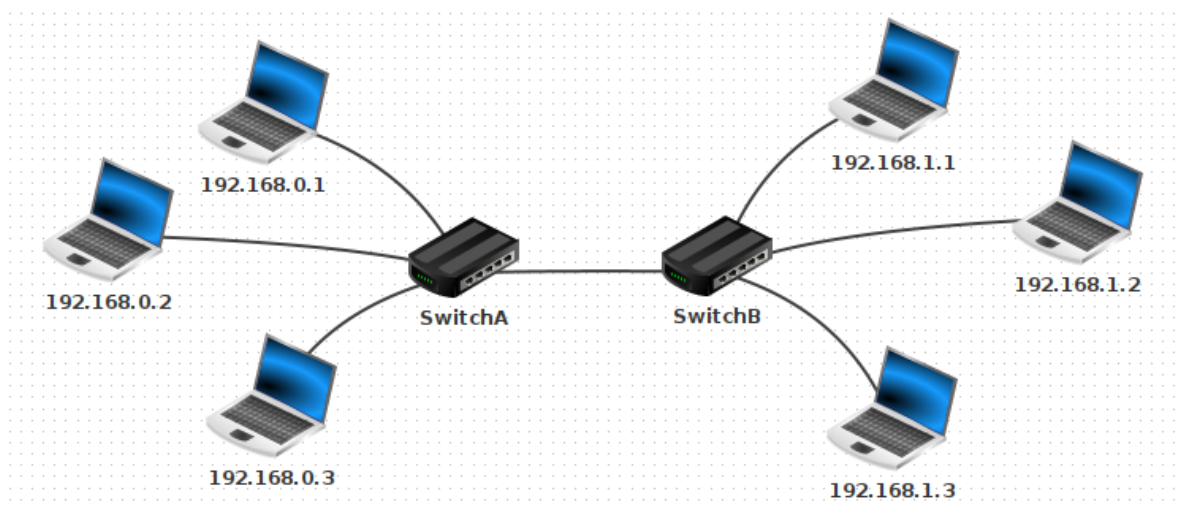
```
C:\Users>ping 192.168.1.18

Envoi d'une requête 'Ping' 192.168.1.18 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.1.18:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Est-il possible de joindre deux machines sur des réseaux locaux distincts à l'aide d'un câble ?

Observons la configuration suivante :



Il y a deux réseaux locaux respectivement reliés entre eux par le SwitchA et le SwitchB. Les deux switches sont reliés par un câble.

Que se passe-t-il si depuis la machine d'adresse IP 192.168.0.1, on tape la commande ping 192.168.1.1. ?

Réponse : Délai d'attente de la demande dépassé.

On en déduit que relier, deux réseaux physiquement entre eux ne suffit pas.

Modifions temporairement l'IP de la machine dont l'IP est 192.168.1.1 par l'IP 192.168.0.18

Que se passe-t-il si depuis la machine d'adresse IP 192.168.0.1, on tape la commande ping 192.168.0.18. ?

Réponse : Réponse de 192.168.0.18 : octets=32 temps=67 ms TTL=64

Les machines communiquent. Elles appartiennent donc maintenant au même sous-réseau. On en déduit que la notion de sous-réseau n'est pas *topologique* (« il suffit de relier les ordinateurs entre eux ») mais obéit à des règles numériques.

En effet, on ne peut parler d'adresse IP sans parler de **masque de sous-réseau**.

Dans cet exemple le masque de sous-réseau était 255.255.255.0.

Revenons à la configuration initiale, mais modifions le masque de sous-réseau en le mettant à 255.255.0.0.

Que se passe-t-il si depuis la machine d'adresse IP 192.168.0.1, on tape la commande `ping 192.168.1.1` ?

Réponse : Réponse de 192.168.1.1 : octets=32 temps=67 ms TTL=64
Les machines communiquent. Elles sont donc sur le même sous-réseau.

On voit donc l'importance du masque de sous-réseau.

Lorsqu'une machine A veut envoyer un message à une machine B, elle doit déterminer si cette machine :

- appartient au même sous-réseau : auquel cas le message est envoyé directement via un ou plusieurs switches.
- n'appartient pas au même sous-réseau : auquel cas le message doit d'abord transiter par un routeur.

Exercice 4

Chercher le masque de sous-réseau de votre machine.

Le masque de sous-réseau permet de scinder l'adresse IP en deux parties :

- L'adresse du réseau ;
- L'adresse de l'hôte.

Par exemple, si l'adresse IP 192.168.0.18 associée au masque de sous-réseau 255.255.255.0, on peut la décomposer ainsi : $\underbrace{192.168.0}_{\text{adresse du réseau}} \underbrace{.18}_{\text{adresse de l'hôte}}$.

Nous verrons plus bas comment le faire avec d'autres masques de sous-réseau et que cela veut dire que dans ce réseau les adresses des machines iront de 192.168.0.1 à 192.168.0.254.

Il y a deux adresses spéciales :

- La première adresse, ici 192.168.0.0, d'une plage est l'adresse du réseau proprement dit, elle ne peut pas être utilisée par une machine.
- La dernière adresse, ici 192.168.0.255 est l'adresse de « broadcast », elle permet d'envoyer un message à toutes les machines du réseau.

Méthode pour déterminer si deux machines appartiennent à un même sous-réseau.

Nous allons avoir besoin de l'opérateur booléen ET, appelé aussi de conjonction, que l'on va noter & dont la table de vérité est ci-contre.

a	b	a ET b
0	0	0
0	1	0
1	0	0
1	1	1

Exemple

Prenons l'adresse 192.168.1.18 et le masque de sous-réseau 255.255.255.0

192.168.1.18 s'écrit en binaire :
 11000000.10101000.00000001.00010010
 255.255.255.0 s'écrit en binaire :
 11111111.11111111.11111111.00000000

Pour obtenir l'adresse du réseau il suffit de faire la conjonction entre les deux :

```

    11000000 . 10101000 . 00000001 . 00010010
&
    11111111 . 11111111 . 11111111 . 00000000
=
    11000000 . 10101000 . 00000001 . 00000000
  
```

Soit en base 10 : 192.168.1.0

L'adresse de la machine est obtenue en utilisant le complément à 1 du masque de sous-réseau.
 On obtient :

```

    11000000 . 10101000 . 00000001 . 00010010
&
    00000000 . 00000000 . 00000000 . 11111111
=
    00000000 . 00000000 . 00000000 . 00010010
  
```

Soit en base 10 : 0.0.0.18

L'adresse du réseau est donc 192.168.1.0 et celui de la machine de ce réseau 0.0.0.18.

Remarque : Les bits à 1 du masque de sous-réseau indiquent la place des bits du réseau et ceux à 0 indiquent la place des bits de la machine liée à ce réseau (on dit aussi de l'hôte).

Exercice 5

Considérons trois machines A, B, C d'adresse IP respectives 192 . 168 . 129 . 10,
 192 . 168 . 135 . 200 et 192 . 168 . 145 . 1, configurées avec un masque de sous-réseau égal à
 255 . 255 . 248 . 0.

Peuvent-elles communiquer entre elles ?

Vous pouvez vous aider du convertisseur entre binaire et base 10 :

<https://integer.exposed>

Pour bien commencer :

129 & 248 s'écrit en binaire 10000001 & 11111000 qui vaut 10000000, soit 128 en décimal.

Méthode déterminer le nombre de machines maximal sur un sous-réseau

Le nombre maximum de machine est déterminé par le masque de sous-réseau.

Si le masque de sous-réseau contient n 1, le nombre maximal de machines connectées, on dit aussi le nombre d'hôtes est :

$$2^{32-n} - 2$$

En effet, il y a $32-n$ bits à 0 dans le masque sous-réseau ce qui fait 2^{32-n} adresses possibles auxquelles il faut soustraire l'adresse du réseau et l'adresse de « broadcast » dite aussi adresse de diffusion.

Exemple

Déterminons l'adresse du réseau, l'adresse de « broadcast » et le nombre d'hôtes du réseau. Dans le cas où une adresse IP est 192.168.1.80 et son masque de sous-réseau est 255.255.255.192 .

255.255.255.192 s'écrit en binaire : 11111111.11111111.11111111.11000000

192.168.1.80 s'écrit en binaire : 11000000.10101000.00000001.1010000.

11000000.10101000.00000001.01010000

& 11111111.11111111.11111111.11000000

= 11000000.10101000.00000001.01000000

Soit 192.168.1.64.

L'adresse du réseau est donc 192.168.1.64

Déterminons l'adresse de « broadcast ». Pour cela il faut faire un OU entre l'adresse du réseau et le complément à 1 du masque de sous-réseau.

La table du vérité du OU est rappelée ci-contre.

On obtient :

11000000.10101000.00000001.01000000

OU 00000000.00000000.00000000.00111111

= 11000000.10101000.00000001.01111111

Soit 192.168.1.127.

L'adresse de « broadcast » est donc 192.168.1.127.

Le nombre d'hôte est : $2^{32-26} - 2 = 2^6 - 2 = 62$.

Ce sous-réseau permet d'avoir au maximum 62 hôtes.

a	b	a OU b
0	0	0
0	1	1
1	0	1
1	1	1

Exercice 6

Déterminer l'adresse du réseau, l'adresse de « broadcast » et le nombre d'hôtes d'un réseau dont une adresse IP est 192.168.1.133 et dont le masque de sous-réseau est 255.255.255.224.

Notation CIDR

Une forme plus courte pour les adresses IP est connue sous le nom de notation CIDR (Classless Inter-Domain Routing). Elle donne l'adresse IP suivie par une barre oblique et le nombre de bits consécutifs égaux à 1 dans la notation binaire du masque de sous-réseau, les autres bits valant 0. Ainsi, le masque 255.255.192.0 admettant 18 bits égaux à 1, l'adresse IP 172.16.133.20 s'écrit plus simplement 172.16.133.20/18.

C'est cette notation que vous aviez rencontré lorsque vous avez utilisé la commande ip address.

V Le protocole DNS

Le protocole DNS (Domain Name System) ce que l'on peut traduire par « système de noms de domaine » permet de relier les adresses IP aux adresses URL (Universal Resource Locator). En français, URL se traduit par adresse symbolique ou adresse universelle. Les URL sont les adresses du type soussite.sitemachin.org.

Ce protocole fait appel à des ordinateurs spécialisés, les serveurs DNS.

Un serveur DNS ne connaît qu'une petite partie des adresses. Lorsque l'on tape une URL dans la barre du navigateur, la première étape réalisée est cette conversion, qui se fait en plusieurs étapes.

Par exemple, lorsque l'on tape www.wikipedia.fr :

Le serveur DNS (situé dans la box chez vous) ne reconnaît pas cette adresse. Il va donc transmettre sa demande au serveur DNS spécialisé dans le Top Level Domain (TLD) « .fr ». Votre box connaît les IP de tous les serveurs de TLD (.com, .eu, .fr, ...).

Le serveur DNS de « .fr » ne connaît pas www.wikipedia.fr, mais il connaît « wikipedia.fr ». Il va donc demander au serveur DNS « wikipedia.fr » l'adresse.

Le serveur DNS « wikipedia.fr » connaît l'IP de www.wikipedia.fr, il renvoie cette adresse au serveur « .fr », qui la renvoie à la box, qui la renvoie à l'ordinateur.

Une URL est décodée donc décodée en partant du TLD (.fr, .com, .net, .io, ...) puis en remontant jusqu'à l'adresse que vous avez demandée.

Rentrer une IP ou rentrer une adresse symbolique dans le champ de saisie d'un navigateur revient au même. Par contre, pour créer un réseau local, il est nécessaire de connaître les IP de chaque machine, car elles n'ont pas d'adresse symbolique.

Exercice 7

Recherchez l'IP du site google.fr.

- Dans une fenêtre de console exécuter la commande `ping google.fr` (remarquez qu'il n'y a pas le www). Elle envoie des paquets de données pour tester si un site est joignable. L'IP du site est donnée en première ligne. Ctrl +C pour interrompre sous Linux. La commande `ping` est un incontournable des réseaux.
- Entrez cette adresse dans un navigateur et vérifiez que vous arrivez bien sur la page d'accueil du moteur de recherche google.fr.
- Exécutez maintenant la commande `nslookup google.fr` sous Windows ou `dig google.fr` si vous êtes sous Linux. Notez l'adresse IP obtenue.
- Exécutez la commande `nslookup adresseIp` où *adresseIp* est l'IP de l'étape précédente si vous êtes sous Windows ou `host adresseIp` si vous êtes sous Linux.
- Faites de même avec le site Wikipedia.org
- Faites quelques tests avec d'autres sites, vous verrez que cela ne fonctionne pas toujours. En effet, les « très petits » comme les « très gros » sites ont un système d'IP bien plus compliqué que ce que vous apprendrez dans ce cours.
- Avec vos camarades, cherchez plusieurs fois l'IP de google.com. Que constatez-vous ? A votre avis, pourquoi a-t-on ce phénomène ?

Sources :

- https://github.com/glassus/nsi/blob/master/Premiere/Theme04_Architecture_materielle/04_Protocoles_de_communication.md
- http://www.maths-info-lycee.fr/pdfs/nsi_7_web_cours.pdf
- http://www.maths-info-lycee.fr/pdfs/nsi_6_internet.pdf
- https://pixees.fr/informatiquelycee/n_site/nsi_prem_tcpip.html

Pour aller plus loin :

- <https://fr.wikipedia.org/wiki/Sous-r%C3%A9seau>
- <https://cric.grenoble.cnrs.fr/Administrateurs/Outils/CalculMasque/>
- https://en.wikipedia.org/wiki/Reserved_IP_addresses
- https://fr.wikipedia.org/wiki/Domain_Name_System