Harmonisation Mastères

Atelier n° 2 – Le PC et le réseau

Annexes

A. Quelques notions préliminaires sur les concepts réseau

A.1. Les adresses Ethernet

Ethernet est la technologie prédominante aujourd'hui pour la liaison locale entre équipements. C'est un bus. Chaque équipement sur ce bus est identifié par une adresse dite MAC (*Media Access Control*), appelée en l'occurrence adresse Ethernet, ou aussi adresse physique. Cette adresse est unique, et est configurée par le constructeur de la carte Ethernet. A priori on ne la change pas, et pour communiquer les applications IP utilisent des adresses IP, dont la portée permet d'aller d'une liaison Ethernent à une autre liaison Ethernent en franchissant des routeurs IP.

Exemples : 90:2b:34:36:5a:c5 b0:48:7a:91:60:aa 74:86:7a:71:62:c4

A.2. Les adresses IP

Pour que votre PC puisse communiquer avec les autres machines du réseau ou avec l'Internet il doit posséder une **adresse** qui lui est propre. Le protocole de communication « réseau » utilisé est IP (Internet Protocol), l'adresse affectée à votre PC est donc appelée « **adresse IP** ».

Les adresses IP sont des nombres de 32 bits, donc 4 octets (en IPv4, et 128 bits en IPv6). Pour faciliter la lisibilité de ces adresses pour les utilisateurs elles sont représentées sous la forme de quatre nombres compris entre 0 et 255 (inclus), séparés par le caractère « . » (point).

Exemples : 192.44.75.10 192.168.100.2 172.16.0.4

A.3. Adresse Réseau, adresse machine, netmask

L'adresse affectée à une machine comporte deux parties : la première (à gauche) indique le numéro du réseau (l'adresse du réseau), la seconde (à droite) identifie la machine sur le réseau. Chaque partie comporte un certain nombre de bits. Historiquement ce nombre était fixé par la classe de l'adresse, mais est précisé par le *masque réseau*.

A.3.1. Les classes d'adresses

Il existe 5 classes comme l'indique le tableau suivant :

Nom	*Plage d'adresse Réseau*	*Nombre de machines par réseau*
A	0 à 127	2^{24} - 2
B	128.0 à 191.255	2^{16} - 2
C	192.0.0 à 223.255.255.0	254
D	224.0.0 à 239.255.255	Adresses réservées pour les applications multicast
E	240.0.0 à 255.255.255	Plage inutilisée

Une machine reliées à un réseau IP est munie d'au moins une adresse de classe A, B ou C.

Exemples :

192.44.75.10 : adresse de classe C, sur le réseau 192.44.75.0

172.16.10.5 : adresse de classe B, sur le réseau 172.16.0.0

Notez que les adresses réseaux sont identifiées par leur partie utile (suivant leur classe) suivie par des 0.

On ne donne pas l'adresse machine 255 car elle est réservée pour les messages en diffusion générale (broadcast). Pour la classe A, c'est l'adresse x.255.255.255, pour la classe B x.y.255.255. Pour la classe C il s'agit de x.y.z.255[1].

De même on n'utilise pas l'adresse 0 car elle fut, il y a longtemps, utilisée aussi pour le broadcast et peut-être subsiste-il des machines fonctionnant encore selon ce mode. Ceci explique pourquoi il n'y a par exemple que 254 adresses machines possibles pour un réseau de classe C.

Chaque machine fonctionnant sous IP est aussi munie d'une interface logicielle dite « boucle locale » permettant de réaliser des communications entre applications locales sans envoyer de paquets inutilement sur le réseau. Cette « boucle locale » est munie d'une adresse, toujours la même, à savoir 127.0.0.1 (réseau 127.0.0.0, masque 255.0.0.0, voir ci-après).

A.3.2. Le masque d'adresse ou *netmask*

La répartition des adresses en classe pose un problème de gaspillage d'adresses potentielles qu'il serait trop long d'expliquer ici (vous reverrez ces notions en cours de Réseaux). Les tables de routage dans les routeurs sont aussi affectées par cette classification. Afin de pallier ces problèmes, les membres actifs du développement de l'Internet (regroupés dans l'*Internet Engineering Task Force* ou IETF) ont décidé de briser le carcan des classes et de répartir la partie réseau et la partie machine des adresses de manière variable[2]. Il est alors nécessaire d'associer un indicateur complémentaire aux adresses : le masque.

Internet, comme son nom l'indique, est une interconnexion de réseaux. Mais comment savoir que deux adresses internet appartiennent au même réseau ? Il suffit de regarder le masque réseau ! Cette question, les routeurs et même les machines terminales se la posent à chaque instant, chaque fois qu'il y a des paquets à envoyer et que l'on a besoin de savoir quelle direction prendre. Deux adresses internet qui ont une même partie commune appartiennent au même réseau. Le masque réseau indique justement quelle est cette partie commune que l'on doit regarder.

Le masque est un ensemble de 32 bits avec la partie gauche, identifiant la partie réseau, à 1 et la partie droite (machine) à 0. Le masque est indiqué, de manière classique, en notation pointée comme pour les adresses, voyez les exemples suivants.

Pour des adresses standards, qui obéissent à la règle des classes, nous aurions par exemple

192.44.75.10 netmask 255.255.255.0 (une adresse de classe C)

172.16.45.78 netmask 255.255.0.0 (une adresse de classe B)

10.56.78.234 netmask 255.0.0.0 (une adresse de classe A)

On pourrait dire que les netmasks 255.0.0.0, 255.255.0.0 et 255.255.255.0 sont standards, respectivement pour les classes A, B et C.

Il est aussi possible de créer des sous-réseaux à partir d'une adresse réseau. On peut par

1 Il existe quelques autres subtilités sur ce point avec les possibilités de « subnetting » qu'il serait trop long de développer ici.

2 Spécifications dans le document RFC-1519 CIDR : Classless InterDomain Routing

exemple avoir une adresse de classe B comme celle-ci : 172.16.0.0, netmask 255.255.0.0, donc une adresse réseau standard. On peut alors étendre cette adresse réseau su 8 bits, pris dans la partie « adresse machine ». On peut alors avoir les réseaux 172.16.10.0, 172.16.20.0, etc, avec pour netmask 255.255.255.0.

Le netmask peut aussi être indiqué directement par le nombre de bits à 1. Par exemple le netmask 255.255.255.0 peut être indiqué par le nombre 24. On peut ainsi écrire 192.168.100.0/24 pour indiquer une adresse de réseau.

Sous Unix/Linux les deux écritures peuvent coexister dans les commandes en ligne. Cependant les interfaces graphiques de configuration demandent la notation de type 255.255.255.0 (sous Windows également).

A.3.3. Adresse et nom de machine

Vous ne devez pas ignorer l'existence du serveur web de l'école : www.telecom-bretagne.eu. Vous devez vous douter que derrière ce nom se cache une machine. Mais le nom de cette machine www.telecom-bretagne.eu doit bien correspondre à une adresse IP, sans quoi cette machine serait inaccessible par Internet (rien n'est magique, soyez-en certain). Cette adresse (au moins en 2013 il en était ainsi) est 192.108.117.241 (une classe C si le netmask est standard).

Il est plus facile de se souvenir du nom de la machine plutôt que de son adresse IP. Il existe un service, de portée mondiale, appelé DNS (Domain Name Service) qui gère l'association entre les noms et les adresses réelles. Ce service est abrité sur des serveurs gérés par les entreprises (ou dont la gestion est déléguée aux FAI). Les serveurs se connaissent entre eux dans une arborescence mondiale[3].

La commande *nslookup* sous Windows ou *host* sous Unix/Linux permet de consulter le DNS et d'afficher la correspondance entre une adresse et un nom en lui fournissant l'un ou l'autre.

Sous Unix/Linux il existe un mécanisme plus simple : le fichier /etc/hosts (parfois centralisé via le service réseau NIS : Network Information Service). Une machine Unix/Linux peut utiliser conjointement le fichier /etc/host (avec ou sans NIS) et le service DNS.

A.3.4. Attribution des adresses

On ne peut pas attribuer au hasard une adresse IP à une machine. Surtout si on est relié à l'Internet. Le fournisseur d'accès (FAI) doit fournir un préfixe (une adresse réseau) et un netmask à l'entreprise qui désire être raccordée à Internet.

Pour des machines personnelles, chez soi par exemple, le FAI attribue dynamiquement une adresse lors de la connexion de la machine via un modem téléphonique ou ADSL.

Un réseau local d'entreprise est relié à l'Internet via un routeur d'accès qui possède une interface raccordée au FAI et au moins une interface coté intérieur de l'entreprise. Le gestionnaire du réseau de l'entreprise définit son plan d'adressage et fournit aux utilisateurs l'adresse de leur machine et le netmask associé, ainsi que l'adresse machine du routeur (pour que chaque machine puisse accéder à l'Internet).

Un utilisateur et administrateur de sa machine doit alors configurer son interface réseau pour lui affecter l'adresse et le masque **indiqués par le gestionnaire du réseau**.

En aucun cas l'utilisateur ne doit attribuer une adresse de son cru, il risquerait d'y avoir conflit avec une autre machine. Pour pallier ce genre de problème il existe une méthode d'attribution dynamique et contrôlée car centralisée : la méthode **DHCP** (Dynamic Host Control Protocol) gérée par le gestionnaire du réseau. L'utilisateur/administrateur de sa machine ne précise rien d'autre que

3 Sans gouvernance réelle. Les serveurs doivent simplement utiliser le protocole de communication ad-hoc. Leur gestion n'est pas du tout supervisée par une autorité supérieure.

« Obtenir une adresse automatiquement » (selon le système d'exploitation) et le tour est joué.

A.3.5. Les adresses privées

L'Internet manque d'adresses. Depuis longtemps il n'y a plus d'adresses de classe A et B attribuées. Les adresses disponibles en classe C ont disparues en avril 2011. Une nouvelle version du protocole IP est en attente de déploiement (IP version 6 ou IPv6, la version actuelle de IP étant IPv4). Elle offre des adresses sur 16 octets. Son déploiement effectif tarde... Pour pallier le déficit d'adresses IPv4, l'IETF avait décidé la création de plages d'adresses privées (pouvant être attribuées plusieurs fois à certaines conditions). Ces plages sont les suivantes :

10.0.0.0 à 10.255.255.255, masque à partir de 255.0.0.0, pour la classe A

172.16.0.0 à 172.16.255.255, masque à partir de 255.255.0.0 pour la classe B

192.168.0.0 à 192.168.255.255, masque à partir de 255.255.0.0 pour la classe C

Ces adresses ne peuvent pas être routées dans Internet, elles peuvent l'être à l'intérieur des réseaux privés des entreprises ou des particuliers.

Si malgré tout un réseau privé doit être raccordé à Internet il est nécessaire que le routeur de raccordement soit muni d'une adresse officielle coté Internet et qu'il mette en œuvre la fonction **NAT** (Network Address Translation).

A.4. Les organes du réseau

Les machines des utilisateurs sont reliées à des organes actifs appelés hubs ou commutateurs (on dit encore switches). Ces organes pouvant être à leur tour reliés entre eux pour former une architecture physique plus vaste et couvrir ainsi l'ensemble de l'entreprise.

La technologie employée s'appelle Ethernet. Elle est apparue au tout début des années 80 (concepts définis en 1976). Elle a supplanté toutes ses concurrentes.

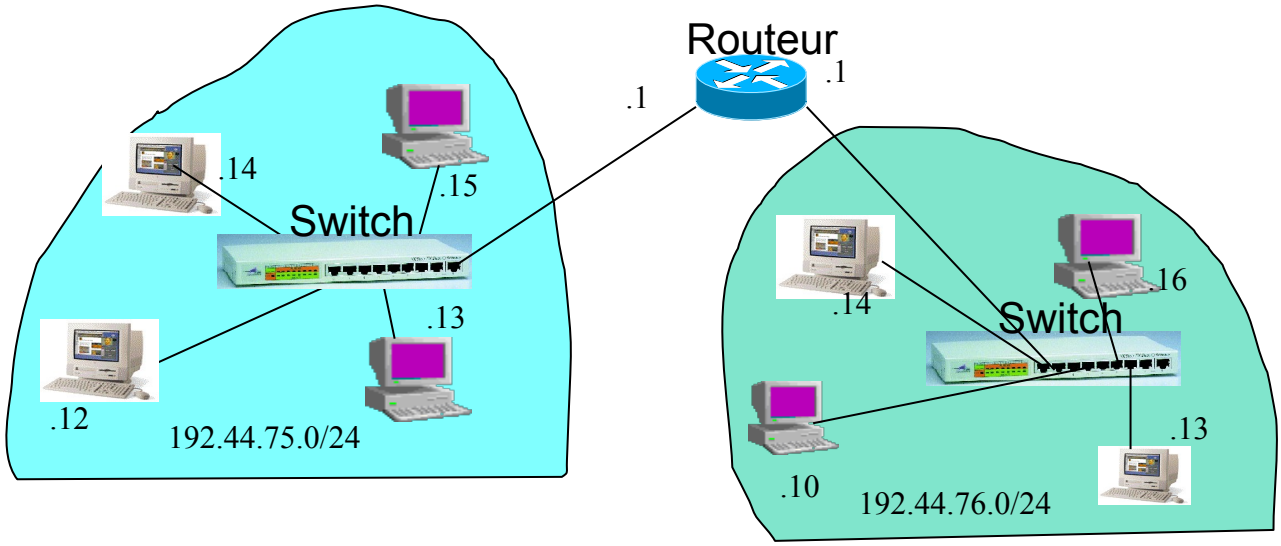
Un réseau ainsi constitué va être muni d'un adressage IP constitué d'un seul préfixe, par exemple 192.168.100.0, netmask 255.255.255.0.

Pour des raisons diverses l'entreprise crée généralement plusieurs réseaux séparés par des moyens physiques ou logiciels. Chacun de ces réseaux est muni d'un préfixe différent. Il ne peut pas y avoir de communication entre eux directement. Pour que les communications soient possibles entre ces réseaux il est nécessaires qu'ils soient chacun raccordés à un organe appelé « routeur ».

La figure suivante présente une vue simplifiée d'une partie du réseau de l'école.

Questions :

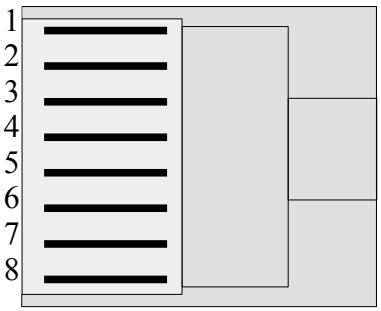
Indiquez les adresses complètes de chacune des machines ainsi que de chaque interface du routeur sous la forme `A.B.C.D – netmask x.x.x.x` ou x vaut 255 ou 0.



A.5. Le câblage

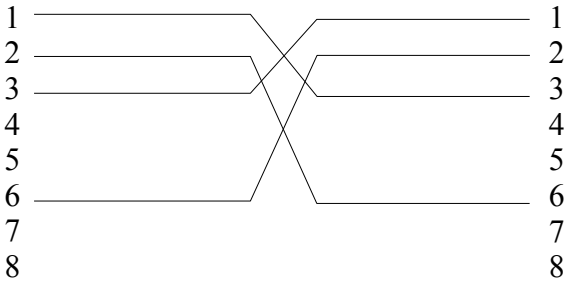
Les câbles sont généralement en cuivre. Ils ont une longueur inférieure à 100m et le débit supporté est typiquement de 100Mb/s (historiquement du 10Mb/s, et maintenant du 1Gb/s).

Le schéma suivant fournit des indications sur le type de prise utilisé ainsi que sur le brochage



1	T+	Blanc orange
2	T-	Orange
3	R+	Blanc Vert
4		
5		
6	R-	Vert
7		
8		

Il est possible de relier des machines directement entre elles, sans l'intermédiaire de hub ou de switch. Il faut alors utiliser un câble dit « croisé », on comprendra pourquoi en regardant le schéma suivant :



B. Notions de métrologie réseau

...et les limites du recours à un estimateur...

Pour qualifier une liaison réseau, il convient d'évaluer un certain nombre de choses : capacité du lien, bande passante disponible, latence, gigue, taux de pertes, etc. Ces mots ne vous sont pas inconnus, mais concrètement, comment on fait pour savoir ?

● Les techniques de *mesure passive* consistent à regarder ce qu'il advient pour les paquets circulant déjà dans le réseau et générés les applications en cours. L'avantage est que l'on ne perturbe pas le réseau que l'on mesure. L'inconvénient est que l'on ne sait pas trop si les paramètres que l'on observe sont ceux inhérents au lien réseau ou bien aux applications en cours...

● Les techniques de *mesure active* consistent au contraire à regarder ce qu'il se passe pour des paquets que l'on injecte exprès dans le réseau. L'avantage est que l'on identifie mieux le phénomène que l'on observe (puisqu'on l'a provoqué exprès), mais que du coup cela perturbe le lien réseau que l'on veut observer...

L'outil *ping* fait de la mesure active (chronomètre le temps d'aller-retour sur un paquet qu'il a envoyé). Cependant les paquets sont peu nombreux, et par défaut de petite taille. C'est un compromis acceptable. C'est aujourd'hui l'outil de prédilection pour évaluer la latence, la gigue, le taux de pertes.

Pour évaluer la bande passante, la stratégie la plus simple consiste à télécharger un gros fichier et à chronométrer. On est indéniablement dans de la mesure active, et qui plus est un peu perturbante pour le réseau observé. Mais c'est efficace. Cependant, cela ne mesure que la bande passante *restante*. Si l'on veut mesurer la *capacité totale* du lien, il faut s'assurer que l'on est tout seul sur le réseau au moment de la mesure.

● Une autre façon de faire consiste à avoir recours à un *estimateur*. On cherche à faire le même compromis que pour ping : injecter des paquets, certes, mais en petit nombre pour ne pas perturber le réseau, et de regarder ce qu'il advient de ces paquets sonde pour en déduire une estimation du débit.

▪ Une première stratégie consiste à regarder le délai sur des paquets de taille variable. (On peut citer par exemple les outils `bing`, `pchar`, etc.)[4] L'idée est la suivante : considérons la fonction $f(t)$ qui représente la quantité de données transmises sur le lien au cours du temps. En première approximation, f est une droite. Le débit du lien est simplement la pente $d=f'$. La latence l sur le lien est définie par $f(l)=0$. Comme avec ping, on mesure le temps d'aller-retour sur quelques paquets seulement, mais de taille différente. Le débit du lien est donc simplement le différentiel sur deux mesures, a priori. Et s'il y a d'autres applications réseau en parallèle, cela n'a pas d'impact tant que nos paquets sonde peuvent passer. Bien entendu, cela ne donne qu'une estimation, reste à savoir dans quels cas elle est pertinente.

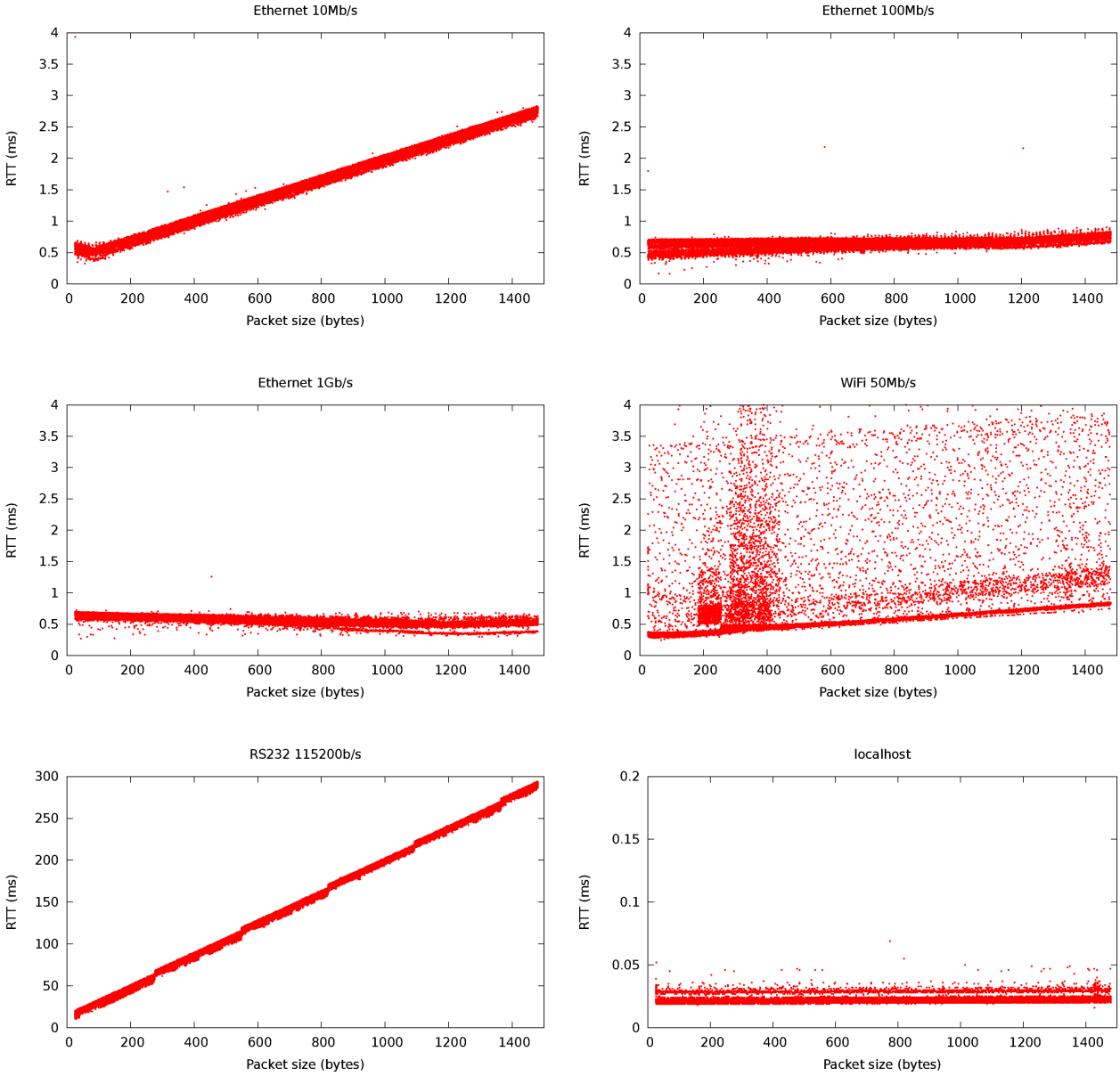
Les figures suivantes représentent des mesures de ping sur des liaisons de nature différentes entre deux PC, et en fonction de la taille des paquets (compter 24h pour obtenir une courbe à peu près propre). En abscisse la taille des paquets variant de 18 à 1472 octets (tiens, pourquoi ces valeurs ?). En ordonnée le temps en ms (attention à l'échelle d'une courbe à l'autre). Notez tout de même qu'une mesure de ping est un temps aller-retour pour une taille donnée. C'est donc le double du temps de transfert, et la fonction f précédente n'est pas le temps de transfert par quantité de données, mais la quantité de données transférées par unité de temps. Un ping est très facile à obtenir concrètement, mais ce n'est pas la courbe $f(t)$ précédente ; c'est plutôt $ping(data)=2*f^{-1}(data)$. Plus la courbe est « horizontale » plus le débit est élevé. Plus la courbe est « haute », plus la latence est

4 Outils de métrologie ; http://www.caida.org/tools/taxonomy/perftaxonomy.xml http://www.icir.org/models/tools.html
Quelques études scientifiques comparatives : http://www.caida.org/research/performance/bandwidth/

importante. Plus le trait est « épais », plus la gigue est importante (dispersion autour d'une valeur nominale).

Ces figures donnent la caractérisation de liens Ethernet 10Mb/s, 100Mb/s, 1Gb/s. On a aussi la caractérisation d'une liaison WiFi 54Mb/s. Vous constaterez que la courbe est assez similaire à celle de la liaison Ethernet 100Mb/s, mais que la dispersion des mesures autour de la courbe nominale est très importante. Il y a beaucoup plus de gigue en radio qu'en filaire, même à débit comparable. Pour confirmer cette hypothèse, on a également mesuré une liaison de type RS232 à 115200b/s qui a un débit très faible, mais avec une dispersion moindre comparativement. Finalement, voyant une telle dispersion en WiFi, on peut se demander s'il est bien judicieux de modéliser la fonction de transfert par une simple droite.

À titre de comparaison on a aussi caractérisé la liaison `localhost`, c'est-à-dire l'interface virtuelle locale d'un PC. Cela permet d'estimer en quelque sorte l'overhead de la couche réseau du système d'exploitation.



Mais revenons à notre hypothèse de départ pour notre estimateur : le phénomène à observer peut être approximé par une droite. Mais est-ce vraiment le cas ? Pour s'en assurer, on a tenté une régression linéaire simple sur les nuages de point précédents. Le tableau ci-après donne les paramètres ainsi calculés.

	100Mb	10Mb	1Gb	WiFi	RS232	localhost
Pente	0,0001091097	0,0016065393	-0,000119068	0,0001195564	0,1888760777	1,002896421E-006
Ordonnée	0,5685228356	0,3910439754	0,6567719657	0,8118460001	10,3418502878	0,0218204204
R^2	0,3128210787	0,9961655507	0,6374526684	0,0003175807	0,999275246	0,0759206327

Observons plus particulièrement le coefficient de détermination R^2. (Rappel : plus ce coefficient est proche de 1, plus le nuage de points se rapproche de la droite approximée ; une valeur faible indique au contraire que les points sont très dispersés autour de la droite sensée les modéliser.) Comme on l'avait deviné précédemment, R^2 est particulièrement mauvais pour un lien WiFi. Mais ce qui peut être plus fâcheu est qu'il n'est pas si bon que ça pour les liens 100Mb et 1Gb : le débit est tel que le temps mesuré est trop court et se trouve finalement noyé dans la gigue.

En conclusion, cet estimateur qui reste une bonne idée pour les liaisons bas débit est malheureusement peu représentatif pour les liens haut débit que l'on connaît aujourd'hui... Il faudra chercher une autre idée...

▪ Une seconde stratégie consiste à regarder le temps inter-paquets, lorsque l'on envoie des paires de paquets ou des trains de paquets. (On peut citer par exemple les outils `pathload`, `pathrate`, `SProbe`, `scriptroute`, etc.) L'idée est la suivante : en première approximation, le temps qui sépare deux paquets successifs de taille identique est déterminé par la taille d'un paquet et du débit du lien, auquel s'ajoute le silence entre trames imposé par la technologie du lien, plus l'impact des files d'attentes et des stratégies d'accès au média de la couche liaison. Bref, le délai inter-paquet est caractéristique du lien. C'est un peu plus compliqué que cela car on constate que sur des trains de paquets, le temps inter-paquets augmente progressivement puis se stabilise. Toujours est-il que ce temps inter-paquets est quelque chose d'intéressant à regarder. Avec l'aide d'une étude statistique, on arrive à en déduire une estimation du débit [1-5].

Ces estimateurs basés sur la dispersion temporelle inter-paquets sont plus complexes que les précédents basés simplement sur le RTT. Par contre ils offrent une meilleure stabilité. Un bémol tout de même : s'ils ne sont tout de même pas aussi invasifs qu'une mesure directe (télécharger un gros fichier et chronométrer), le train de paquets à envoyer peut être non négligeable (p.ex. Comptez environ 10Mb pour l'outil pathload).

[1] M. Jain and C. Dovrolis, *Pathload: A measurement tool for end-to-end available bandwidth*, PAM 2002. http://www.cc.gatech.edu/~dovrolis/Papers/pam02.ps

[2] M. Jain and C. Dovrolis, *End-to-End Available Bandwidth: Measurement methodology, Dynamics, and Relation with TCP Throughput*, ACM SIGCOMM 2002. http://www.cc.gatech.edu/~dovrolis/Papers/sigcomm02.ps.gz

[3] C. Dovrolis, P. Ramanathan, D.Mo*ore, What do packet dispersion techniques me*asure?, IEEE Infocom 2001, http://www.cc.gatech.edu/~dovrolis/Papers/infocom01.ps

[4] C. Dovrolis, P. Ramanathan, and D. Moore, *Packet Dispersion Techniques and Capacity Estimation*, IEEE/ACM Transactions on Networking 2004. http://www.cc.gatech.edu/~dovrolis/Papers/ton_dispersion.ps

[5] N. Spring, D. Wetherall, and T. Anderson, Scriptroute: *A facility for distributed Internet measurement*, North American Network Operator's Group 202 (NANOG 26). http://www.cs.umd.edu/~nspring/talks/nanog-scriptroute.ps