



LES BASES DES RESEAUX TCP/IP

L'INSTITUT DES RESSOURCES INDUSTRIELLES

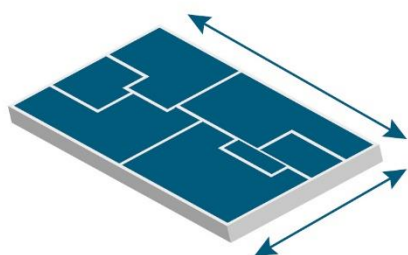
2 STRUCTURES
JURIDIQUES



AFPI LYON

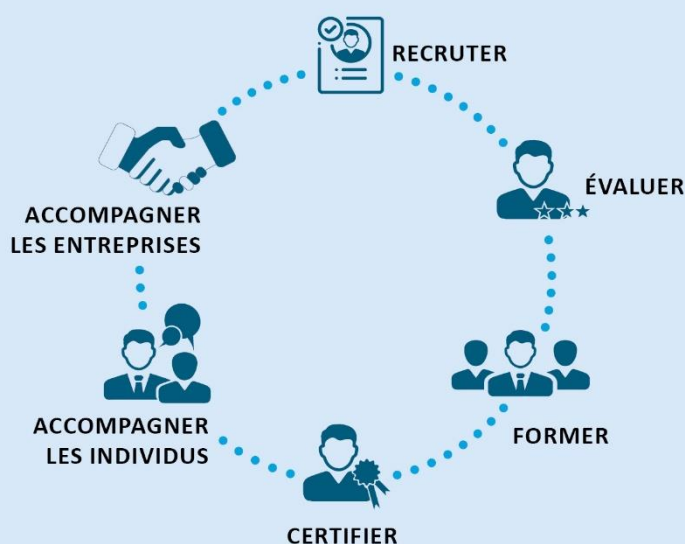


CFAI LYON



30'000 M²
DE MOYENS ET D'ÉQUIPEMENTS

6 SOLUTIONS



180

SPÉCIALISTES

FORMATEURS
INGÉNIEURS
CONSULTANTS
COLLABORATEURS



11

DOMAINES
D'EXPERTISE



MAINTENANCE
INDUSTRIELLE



ELECTROTECHNIQUE
ELECTRONIQUE
AUTOMATISMES



CHAUDRONNERIE
TUYAUTERIE
SOUDAGE



MECANIQUE
PRODUCTIQUE



RÉSEAUX
NUMÉRIQUES



GENIE
ENERGETIQUE



ORGANISATION
ET PERFORMANCE
INDUSTRIELLE



MANAGEMENT
RESSOURCES
HUMAINES



QUALITE- HYGIENE
SECURITE
ENVIRONNEMENT



PILOTAGE
D'EQUIPEMENTS
INDUSTRIELS



ROBOTIQUE
MECATRONIQUE

NOTES PERSONNELLES

Modèles OSI et TCP-IP

La communication en réseau fonctionne sur le même principe que celui évoqué dans l'analogie.

Afin de rendre les logiciels indépendants du matériel, l'ensemble du processus de communication est découpé en couches, chacune :

- ☐ assurant une fonction précise,
- ☐ utilisant un protocole de communication parfaitement codifié.

Entre deux appareils reliés, les couches doivent être les mêmes et pouvoir communiquer en utilisant le même protocole.

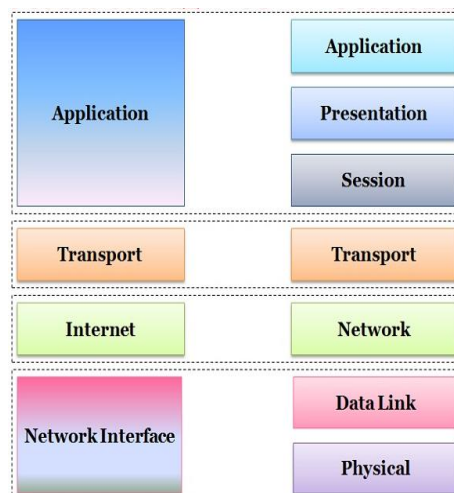


© Thierry Schanen - 2013

© Thierry Schanen - 2013

TCP/IP

OSI



Un peu de littérature...

Le modèle OSI définit 7 couches au lieu de 4 pour le modèle TCP/IP (les couches physique et liaison de données étant réunifiées en une couche identifiée comme couche physique).

Internet utilise le modèle TCP/IP, le modèle OSI étant un modèle théorique.

Pourquoi a-t-on recours à des notions de couches pour décrire ou implémenter les communications entre machines ?

- Interopérabilité
- Evolutivité (services)

Présentation du protocole TCP/IP

On appelle protocole TCP/IP l'ensemble des règles qui permet à des machines (modem, ordinateur, routeur,) de communiquer entre elles sur un réseau informatique. Ces règles (RFC Requests For Comments) sont définies par des organismes internationaux, comme IETF, IEEE... et tous les constructeurs doivent les respecter pour que leurs matériels soient interopérables.

Certains protocoles sont spécialisés dans le transfert des fichiers (FTP par exemple), d'autres dans la consultation de pages web (http) ou pour gérer l'état des transmissions et des erreurs (ICMP).

Sur Internet, l'ensemble des protocoles utilisés porte le nom de suite TCP/IP, elle contient entre-autres les protocoles suivants : http, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, IMAP...

Principe de fonctionnement de TCP/IP

TCP/IP est à la fois une architecture réseau, mais aussi l'acronyme de 2 protocoles réseau liés :

- [TCP \(Transmission Control Protocol\)](#) : protocole de transport
- [IP \(Internet Protocol\)](#) : protocole réseau (adressage)

L'architecture réseau TCP/IP se décompose en 4 couches dans laquelle les protocoles TCP et IP jouent un rôle important.

Couche 4 : Application

C'est ici que l'on trouve les protocoles de communication entre les clients et les serveurs. ([HTTP](#), [FTP](#), [POP](#) et [SMTP](#))

Couche 3 : Transport

On retrouve ici les protocoles de transport des données. Les plus utilisés sont : [Protocole TCP](#) - [Protocole UDP](#)

Couche 2 : Réseau

Dans cette couche on trouve principalement deux protocoles. Le [protocole IP](#) qui permet le routage des informations entre réseaux (Utilisation de l'[adresse IP](#)) et le [protocole ICMP](#) qui permet le contrôle d'erreur et de signalisation.

Couche 1 : Accès réseau

C'est la couche de plus bas niveau sur le réseau. Cette couche contient des protocoles qui gèrent l'acheminement des informations entre émetteur et destinataire. On retrouve dans cette couche [les adresses MAC](#) ainsi que le [protocole Ethernet](#) et le protocole [WiFi \(802.11\)](#)

TCP UDP Quelle différence ?

- **TCP protocole orienté connexion** : opère un contrôle des transmissions. La machine réceptrice envoie un accusé de réception pour chaque donnée reçue avec une vérification de son intégrité. La machine émettrice a la garantie de la validité des données qu'elle envoie, c'est l'équivalent postal de la lettre recommandée avec accusé de réception.
- **UDP protocole non orienté connexion** : la machine émettrice envoie des données sans prévenir la machine réceptrice, et cette dernière ne communique pas à l'émettrice la réception ou la validité des données éventuellement reçues.

En résumé

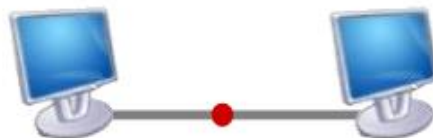
- TCP est plus fiable que UDP car le protocole garantit que les paquets sont bien arrivés ;

- TCP est plus courant que UDP, ce qui lui permet donc de fonctionner dans la plupart des situations, y compris à travers des firewalls, qui laissent par défaut un certain nombre de ports TCP ouverts (80, 443.etc...).
- UDP est plus rapide que TCP, puisque le protocole ne nécessite pas d'aller-retour pour vérifier la bonne livraison des paquets. Ce protocole est privilégié quand un flux peut supporter une dégradation temporaire du service (téléphonie sur IP, Vidéo streaming).

Les **protocoles orientés connexion** : opérant un contrôle de transmission des données pendant une communication établie entre deux machines. La machine réceptrice envoie des accusés de réception lors de la communication.



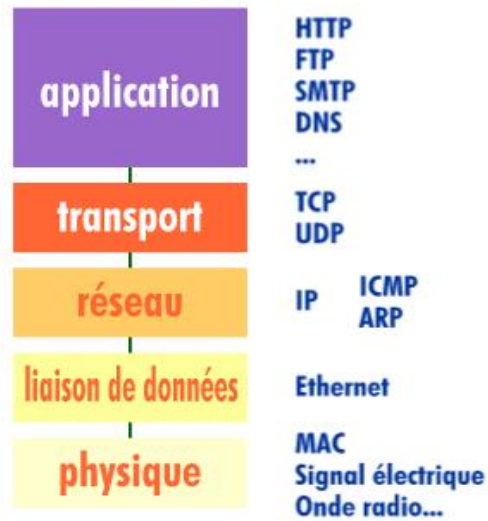
Les **protocoles non orientés connexion** : mode de communication dans lequel la machine émettrice envoie des données sans prévenir la machine réceptrice et la machine réceptrice reçoit les données sans envoyer d'avis de réception à la première.



Protocoles

Sur Internet, les protocoles utilisés font partie d'une **suite de protocoles**, c'est-à-dire un ensemble de protocoles reliés entre-eux.

Cette suite de protocole s'appelle **TCP-IP**.



Quelques protocoles...

Un peu de mathématiques

Numérotation hexadécimale

Équivalents décimaux et binaires des caractères hexadécimaux 0 à F

Décimal	Binaire	Hexadécimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Adressage physique des stations

L'adressage physique permet l'identification fiable de chaque poste connecté à un réseau mais pose des difficultés pour localiser l'appareil car la distribution des adresses MAC est anarchique.



Aucune méthode fiable et systématique ne permet de retrouver une adresse MAC donnée à l'intérieur d'un vaste réseau.

Il convient de mettre en place un système d'identification permettant de localiser un poste avec efficacité. C'est le rôle de l'**adressage logique IP**.

Adressage physique des stations

L'information à transmettre est mise en forme, les trames sont constituées en respectant les protocoles définis, les bits circulent dans les fils ou par les ondes... Et nous venons de voir que chaque trame doit contenir l'**adresse du destinataire** afin d'être convenablement acheminée...

Mais comment trouver le destinataire ?

Chaque appareil connecté au réseau est identifié par un code ou une **adresse unique**. Cet **identifiant unique** est déterminé à la fabrication de la carte réseau.

Sur un réseau de type Ethernet, cet identifiant s'appelle l'**adresse MAC** (Media Access Control). Il est affecté par le fabricant de la carte réseau et se présente sous forme d'une suite de 6 octets.

Exemple d'adresse physique (notée en hexadécimal) :



Adresse IP

Cette adresse logique est nommée adresse **IP** (Internet Protocol). Actuellement, la majorité des systèmes utilisent encore une ancienne version : **IP v4**. Une nouvelle version est en cours de déploiement : **IP v6**.

Une adresse IP v4 est un nombre codé sur 32 bits présenté sous forme d'un groupement de 4 octets :

a.b.c.d

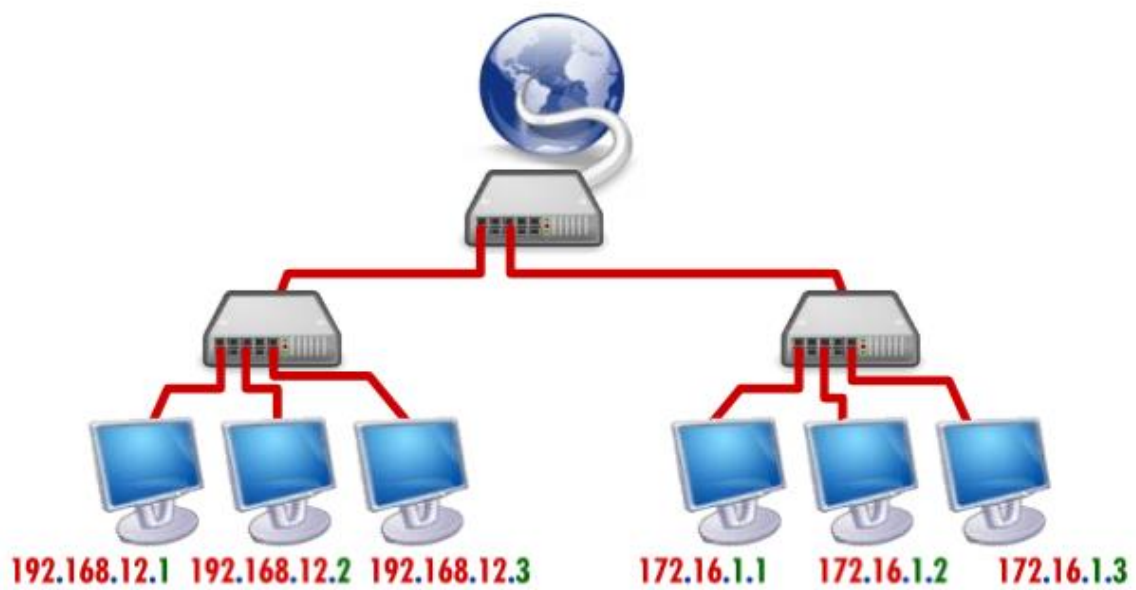
Chaque lettre représente un octet (un nombre entre 0 et 255 ou \$00 et \$FF).



Dans un même réseau, il ne peut y avoir deux postes ayant la même adresse IP.

Décodage d'une adresse IP - exemple

Deux petits réseaux sont connectés à Internet. Chacun a son propre net-ID.



Adresses IP réservées

Deux appareils connectés à un même réseau ne peuvent avoir la même adresse IP. Si un réseau est connecté à Internet, l'attribution des adresses IP des machines reliées à l'extérieur ne peut pas se faire sans prendre en compte toutes les adresses déjà occupées par des postes reliés à Internet.

Il est possible d'obtenir auprès de l'**ICANN** une adresse libre fixe.

Tous les autres ordinateurs du réseau ayant cependant besoin d'une adresse IP, il a été défini une série d'adresses IP à utiliser dans les réseaux locaux qui n'interféreront pas avec les adresses réservées au WEB.

Adresses disponibles pour les réseaux privés :

! Aucune autre adresse ne doit être utilisée dès lors que l'appareil est connecté à Internet.

Classe A

- ☐ net-ID : **10**
- ☐ host-ID de 0.0.1 à 255.255.254

Classe B

- ☐ net-ID : **172.16 à 172.31**
- ☐ host-ID de 0.1 à 255.254

Classe C

- ☐ net-ID : **192.168.0 à 192.168.255**
- ☐ host-ID de 1 à 254

Les plages des adresses privées

Classe	Début de la plage	Fin de la plage	Nombre de réseaux
A	10.0.0.0	10.255.255.254	1
B	172.16.0.0	172.31.255.254	16
C	192.168.0.0	192.168.255.0	255

Les adresses privées constituent la substantifique moelle des réseaux locaux d'entreprises et domestiques et c'est à l'une ou l'autre de ces plages d'adresses que vous aurez affaire dans vos tâches de configuration d'équipements, ou que vous aurez à faire dans vos tâches d'administration. Ces adresses ont la portée d'un réseau local et ne devraient pas circuler sur le réseau Internet.

Masque de sous réseau

Lors du **roulage des données** (leur acheminement vers le bon ordinateur à travers les ramifications du réseau), il est nécessaire d'identifier le net-ID à l'intérieur de l'adresse IP.

A cet effet, on applique un **masque de sous réseau** qui se présente comme une adresse IP. Il comprend, dans sa notation binaire, des 0 au niveau des bits de l'host-ID et des 1 au niveau de ceux du net-ID.

Par application d'un **ET logique** entre l'adresse IP et le masque, on obtient le net-ID :

Exemple :

adresse IP : 10.208.123.12 (il s'agit d'une adresse de classe A)

soit en binaire : 00001010 11010000.01111011.00001100

masque : 11111111.00000000.00000000.00000000

résultat après masquage en ET : 00001010.00000000.00000000.00000000

Classe A

☐ masque : 255.0.0.0

Classe B

☐ masque : 255.255.0.0

Classe C

☐ masque : 255.255.255.0

Ainsi, on retrouvera toujours les mêmes valeurs pour les octets d'un masque, qui sont les suivantes :

00000000	> 0
10000000	> 128
11000000	> 192
11100000	> 224
11110000	> 240
11111000	> 248
11111100	> 252
11111110	> 254
11111111	> 255

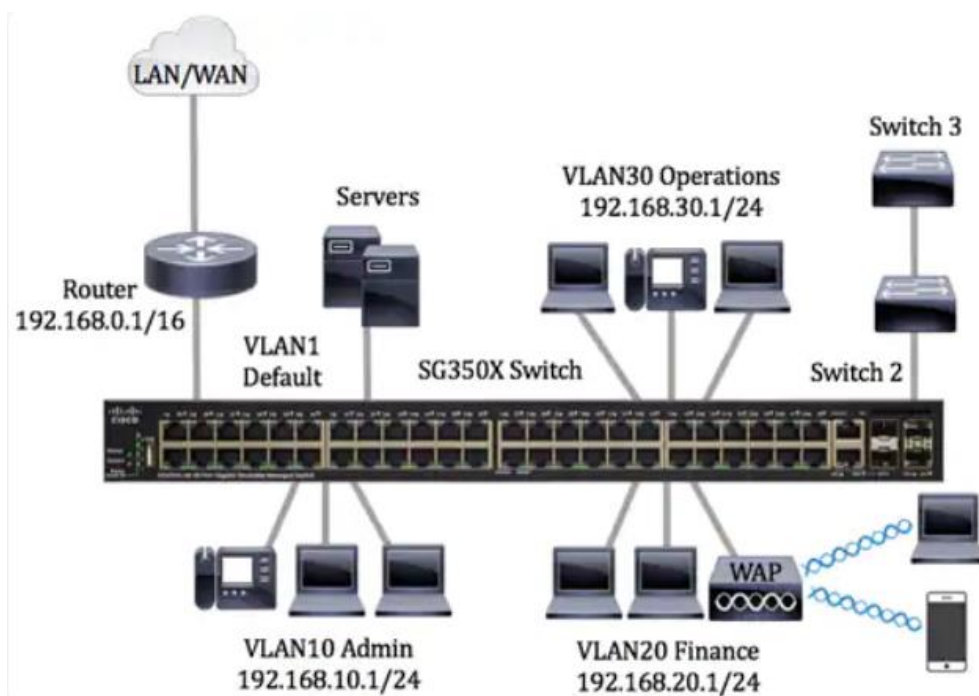
Ecriture CIDR

Le masque 255.255.255.0 contient 24 bits à 1 on le notera /24

Au lieu d'écrire 192.168.0.1/255.255.255.0, on écrira 192.168.0.1/24. /24 se nomme le préfixe

On écrira donc /20 au lieu de 255.255.240.0

VLAN ...What's up ?



VLAN : Virtual Local Area Network

Qu'est-ce qu'un Vlan ? En quoi contribue-t-il à la sécurité et la flexibilité d'un réseau local ?

Protocole ARP

Le protocole **ARP** de la couche réseau permet de connaître l'adresse physique d'une carte réseau correspondant à une adresse IP connue.

ARP interroge toutes les machines du réseau. S'il obtient une réponse, il met à jour une table de correspondance entre les adresses logiques et les adresses physiques.

ARP = Address Resolution Protocol (Protocole de résolution d'adresse)

Lorsqu'une machine doit communiquer avec une autre, elle le fait à partir de l'adresse IP (seule adresse connue par les couches supérieures).

Si l'adresse IP demandée n'est pas encore connue par l'émetteur, le protocole ARP émet une requête sur le réseau.

Les machines du réseau vont comparer l'adresse IP cherchée avec la leur.

Celle qui se reconnaît va répondre à ARP.



ARP est un protocole indispensable au fonctionnement des réseaux locaux, mais il présente une faille de sécurité aisément exploitable par un intrus pour détourner les communications vers une station et pire si cette attaque porte sur la passerelle ou sur le serveur DNS.

Mais pourquoi doit-on avoir 2 adresses MAC + IP pour une seule interface (machine) ?

Connaitre les adresses IP et MAC de mon ordinateur

Lancer, sous Windows, la fenêtre de la ligne de commande, également connue sous Shell ou fenêtre DOS. Une fois le prompt affiché, saisir la commande suivante :

Ipconfig /all *meilleurs rendu que ipconfig*

Scruter le résultat affiché pour retrouver vos interfaces de connexion au réseau (cartes Ethernet et Wifi)

```
Carte réseau sans fil Wi-Fi :
    Suffixe DNS propre à la connexion. . . : lan
    Description. . . . . : Qualcomm Atheros AR956x Wireless Net
work Adapter
    Adresse physique . . . . . : 40-E2-30-FF-11-61
    DHCP activé. . . . . : Oui
    Configuration automatique activée. . . : Oui
    Adresse IPv6 de liaison locale. . . . . : fe80::fc20:f4ad:70d5:ea75%4<préféré>

    Adresse IPv4. . . . . : 192.168.1.50<préféré>
    Masque de sous-réseau. . . . . : 255.255.255.0
    Bail obtenu. . . . . : jeudi 31 octobre 2019 19:30:47
    Bail expirant. . . . . : lundi 4 novembre 2019 22:46:59
    Passerelle par défaut. . . . . : 192.168.1.254
    Serveur DHCP . . . . . : 192.168.1.254
    IAID DHCPv6 . . . . . : 88138288
    DUID de client DHCPv6. . . . . : 00-01-00-01-1C-B2-AD-3E-1C-B7-2C-15-D7
-BB
    Serveurs DNS. . . . . : 192.168.1.254
    NetBIOS sur Tcpip. . . . . : Activé
```

Exemple de résultat d'ipconfig sur un PC relié à un réseau par WiFi

Décortiquons ensemble quelques points remarquables du résultat de ipconfig, à vos plumes :

- DHCP
- Deux BAUX
- Passerelle par défaut
- **Serveurs DNS** (s'il y en a qu'un seul, c'est la passerelle par défaut qui joue ce rôle...en règle générale).

```

Interface : 192.168.1.50 --- 0x4
  Adresse Internet  Adresse physique  Type
192.168.1.6        b8-78-26-93-58-0d  dynamique
192.168.1.8        c0-c9-76-cb-74-ab  dynamique
192.168.1.30       9c-80-df-e8-5e-09  dynamique
192.168.1.35       fc-18-3c-9f-8e-96  dynamique
192.168.1.45       d0-05-2a-c2-ba-98  dynamique
192.168.1.65       6c-19-c0-b4-07-c4  dynamique
192.168.1.75       b8-27-eb-fa-00-fe  dynamique
192.168.1.92       b8-27-eb-af-55-ab  dynamique
192.168.1.97       9c-8c-6e-64-0a-34  dynamique
192.168.1.254      d0-6e-de-c1-40-8c  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
224.0.1.187        01-00-5e-00-01-bb  statique
239.255.255.250    01-00-5e-7f-ff-fa  statique
255.255.255.255    ff-ff-ff-ff-ff-ff  statique

Interface : 169.254.18.35 --- 0x14
  Adresse Internet  Adresse physique  Type
169.254.255.255    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
224.0.0.252        01-00-5e-00-00-fc  statique
224.0.1.187        01-00-5e-00-01-bb  statique
255.255.255.255    ff-ff-ff-ff-ff-ff  statique

Interface : 169.254.125.161 --- 0x15
  Adresse Internet  Adresse physique  Type

```

Exemple de résultat de arp -a

Sur la figure ci-dessus, on voit les table ARP de différentes interfaces, pour ne consulter que la table ARP d'une seule interface, par exemple l'interface 192.168.1.56 on procède ainsi : **arp -a -N 192.168.1.56**

```

C:\Users\ [redacted] >arp -a -N 192.168.1.50

Interface : 192.168.1.50 --- 0x4
Adresse Internet      Adresse physique      Type
192.168.1.6           b8-78-26-93-58-0d    dynamique
192.168.1.8           c0-c9-76-cb-74-ab    dynamique
192.168.1.30          9c-80-df-e8-5e-09    dynamique
192.168.1.45          d0-05-2a-c2-ba-98    dynamique
192.168.1.92          b8-27-eb-af-55-ab    dynamique
192.168.1.97          9c-8c-6e-64-0a-34    dynamique
192.168.1.254         d0-6e-de-c1-40-8c    dynamique
192.168.1.255         ff-ff-ff-ff-ff-ff    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
224.0.1.187           01-00-5e-00-01-bb    statique
239.255.255.250       01-00-5e-7f-ff-fa    statique
255.255.255.255       ff-ff-ff-ff-ff-ff    statique
C:\Users\ [redacted]

```

Configurer manuellement une adresse IP sous MS Windows



Afficher l'état et la gestion du réseau

Modifier les paramètres de la carte

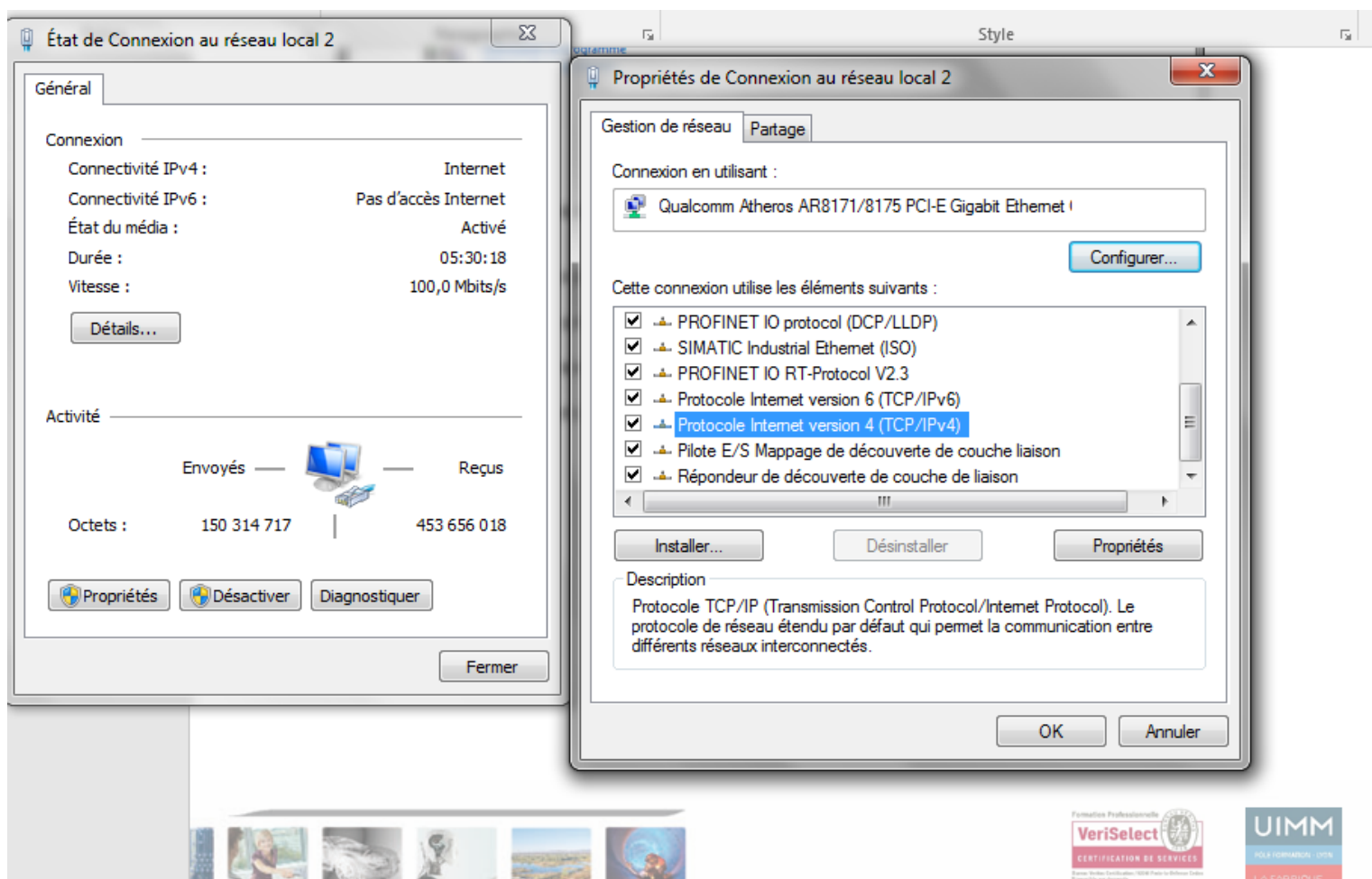
Double-Cliquer sur « connexion au réseau local 2 (afpm.fr)

Puis sur « propriétés » dans la fenêtre qui s'ouvre.

Aller chercher la ligne suivante « **Protocole Internet version 4 (TCP/IP V4)** », le sélectionner puis :

Cliquer sur propriétés

Procéder aux affectations manuelles d'adresses IP, DNS...etc...(Des informations que l'on peut trouver grâce à la commande *ipconfig /all*)



Ports TCP/IP

On dit d'une machine qu'elle est un serveur, dès lors qu'elle fournit un service.

Le client est simplement un programme qui se connecte à un service pour l'utiliser.

Un navigateur web Mozilla FireFox, IE, MS Edge, Chrome, Opera ...sont des clients web permettant de se connecter à un serveur.

C'est bien une **connexion client/serveur** qui est établie entre le navigateur et un serveur web distant ou local.

C'est quoi un port ?



Non ce n'est pas ça ! Là il s'agit de ports de switch (commutateur ou multiplexeur logique)

Un port TCP/IP est une adresse ! C'est même l'adresse d'une application sur une machine. Un nombre entier sur 16 bits (de 0 à 65535) servant à identifier une application parmi tant d'autres sur une même machine. C'est bien donc « l'adresse » ou l'identifiant d'une application s'exécutant sur une machine et ayant une connexion « réseau » avec une autre.

Un serveur écoute sur un port dédié, et un client utilise son propre port pour recevoir les données du serveur. Le couple adresse IP + Port se nomme **Socket**.

Plusieurs programmes **TCP/IP** peuvent être exécutés simultanément sur le même ordinateur, chacun de ces programmes travaille avec un protocole, toutefois l'ordinateur doit pouvoir distinguer les différentes sources et destination des données.

- Les ports **0 à 1023** sont les « **ports reconnus** » ou réservés «**Well Known Ports**». Ils sont, de manière générale, réservés à des applications standardisées.
- Les ports **1024 à 49151** sont appelés « **ports enregistrés** » (« **Registered Ports** »).
- Les ports **49152 à 65535** sont les « **ports dynamiques et/ou privés** » «**Dynamic and/or Private Ports**».

Voici certains des ports reconnus les plus couramment utilisés :

Port	Service ou Application
21	FTP
23	Telnet
25	SMTP
53	Domain Name System
63	Whois
70	Gopher
79	Finger
80	HTTP
110	POP3

SSH → **22** HTTPS → **443**

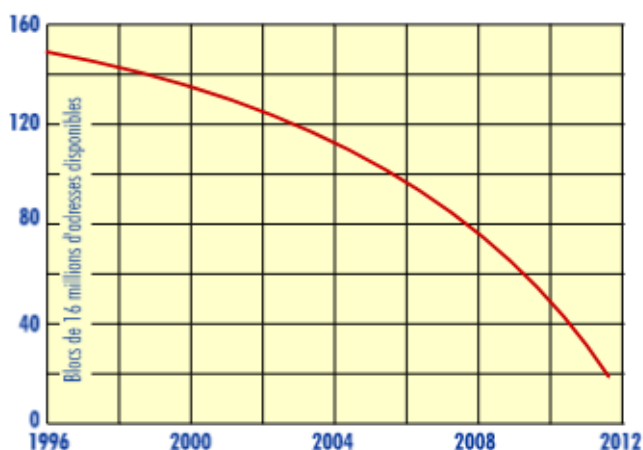
Mais où sont les numéros de port pour TCP ? UDP ?

Si vous réitérez une question de cet acabit, je demanderai à ce que vous soyez réinscrit pour une nouvelle session de formation.

IPv6

Le nombre d'adresses IP disponibles avec le protocole actuel IPv4 (environ 4 milliards) ne suffit plus pour répondre à la demande croissante d'adresses fixes (téléphonie par IP, réseaux embarqués dans l'automobile, Internet dans les pays en voie de développement...)

L'épuisement des adresses publiques est inévitable (la technique d'attribution par classes ainsi que des pans entiers d'adresses bloquées limitent d'autant la réserve d'adresses).



En avril 2011, les derniers blocs libres ont commencé à être assignés et les prévisionnistes estiment l'épuisement complet pour le début de l'année 2015.

C'est la raison principale du développement d'un nouveau protocole Internet. :

IPv6

IPv6

La nouvelle norme **IPv6** (publiée dès 1995) est encore en cours de développement et de déploiement.

A terme, cette nouvelle norme doit remplacer l'actuelle norme IPv4 mais des contraintes matérielles et économiques en freinent le déploiement.

Outre l'augmentation du nombre d'adresses, la norme IPv6 améliore le routage des données en simplifiant les entêtes des paquets manipulés et offre des mécanismes de configuration et de renumérotation automatique.

L'adressage se fera sur 8 doubles octets, soit 2^{128} adresses possibles.

aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa.aaaa

La notation hexadécimale pointée utilisée avec IPv4 est abandonnée au profit d'une notation hexadécimale avec séparation des doubles octets par ":"

2011:10B5:0000:46E7:0000:0000:AA28:2A26

Les groupes consécutifs de 16 bits nuls peuvent être omis en conservant les séparateurs :

2011:10B5::46E7::AA28:2A26

La commande netsat

netstat est un outil utile pour vérifier les connexions réseau et Internet.

Options de la commande Netstat

Commutateur	Description
-a	Affiche toutes les connexions et les ports en écoute
-n	Affiche les adresses et les numéros de ports au format numérique

Les connexions TCP et UDP ainsi que leurs adresses IP et port peuvent être obtenues en entrant la commande :

netstat -an

Description des différents statuts de connexion

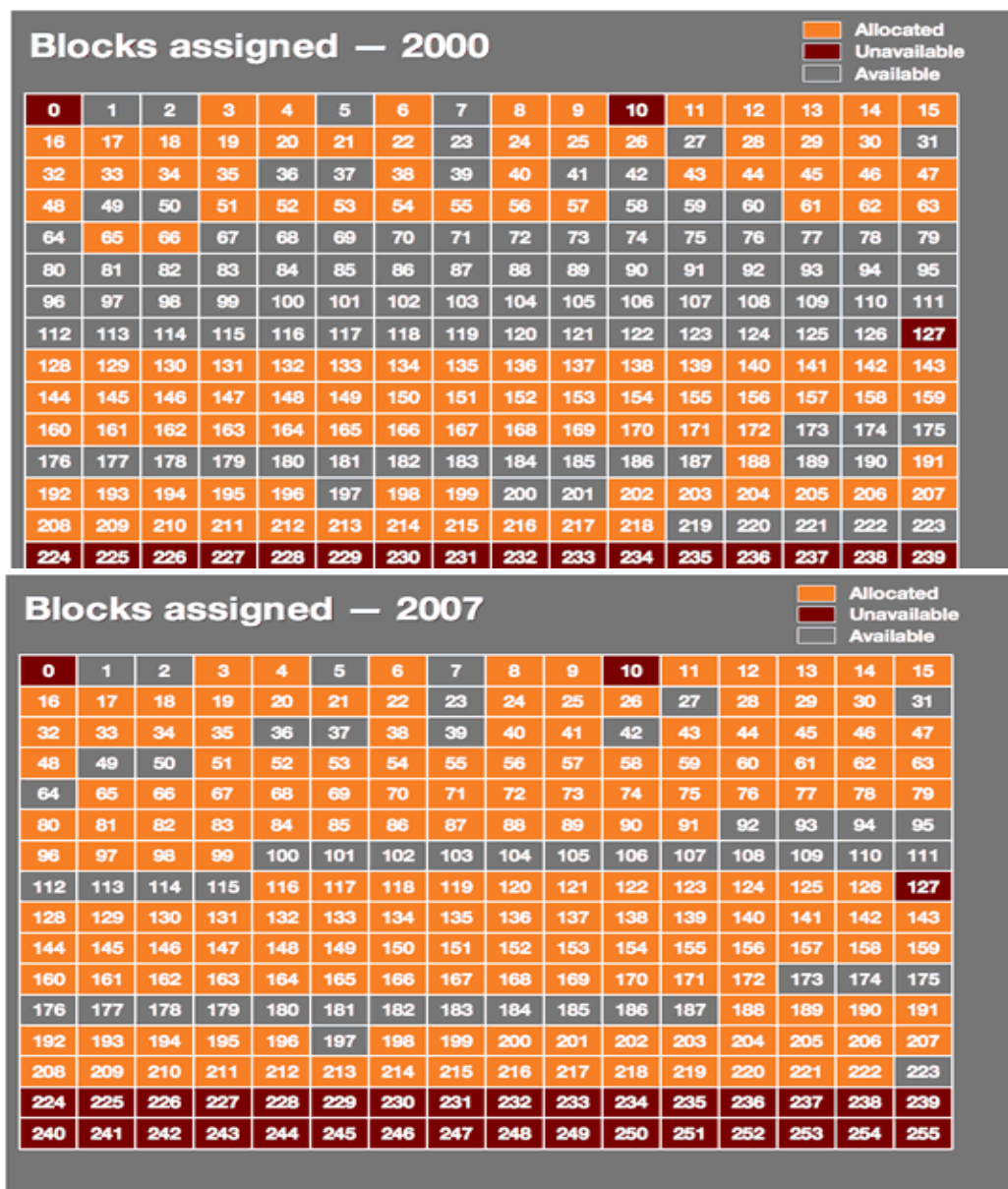
État	Description
CLOSED	Indique que le serveur a reçu un signal ACK envoyé par le client et que la connexion est fermée.
CLOSE_WAIT	Indique que le serveur a reçu le premier signal FIN envoyé par le client et que la connexion est en train d'être fermée.
ESTABLISHED	Indique que le serveur a reçu le signal SYN envoyé par le client et que la session est établie.
FIN_WAIT_1	Indique que la connexion est toujours active mais n'est pas utilisée actuellement.
FIN_WAIT_2	Indique que le client vient juste de recevoir l'accusé de réception du premier signal FIN envoyé par le serveur.
LAST_ACK	Indique que le serveur est en train d'envoyer son propre signal FIN.
LISTENING	Indique que le serveur est prêt à accepter une connexion.
SYN_RECEIVED	Indique que le serveur vient de recevoir un signal SYN envoyé par le client.
SYN_SEND	Indique que la connexion est ouverte et active.
TIME_WAIT	Indique que le client reconnaît la connexion comme encore activé mais non utilisée actuellement.

Exemple d'exécution de netstat -an

```
TCP    127.0.0.1:14031    127.0.0.1:52001    ESTABLISHED
TCP    127.0.0.1:14032    127.0.0.1:52001    ESTABLISHED
TCP    127.0.0.1:14033    127.0.0.1:52001    ESTABLISHED
TCP    127.0.0.1:14034    127.0.0.1:52001    ESTABLISHED
TCP    127.0.0.1:21320    0.0.0.0:0          LISTENING
TCP    127.0.0.1:21321    0.0.0.0:0          LISTENING
TCP    127.0.0.1:21322    0.0.0.0:0          LISTENING
TCP    127.0.0.1:21323    0.0.0.0:0          LISTENING
TCP    127.0.0.1:21327    0.0.0.0:0          LISTENING
TCP    127.0.0.1:23165    127.0.0.1:23166    ESTABLISHED
TCP    127.0.0.1:23166    127.0.0.1:23165    ESTABLISHED
TCP    127.0.0.1:27015    0.0.0.0:0          LISTENING
TCP    127.0.0.1:27015    127.0.0.1:1121     ESTABLISHED
TCP    127.0.0.1:52001    0.0.0.0:0          LISTENING
TCP    127.0.0.1:52001    127.0.0.1:14031    ESTABLISHED
TCP    127.0.0.1:52001    127.0.0.1:14032    ESTABLISHED
TCP    127.0.0.1:52001    127.0.0.1:14033    ESTABLISHED
TCP    127.0.0.1:52001    127.0.0.1:14034    ESTABLISHED
TCP    169.254.18.35:139  0.0.0.0:0          LISTENING
TCP    169.254.125.161:139 0.0.0.0:0          LISTENING
TCP    192.168.1.50:139   0.0.0.0:0          LISTENING
TCP    192.168.1.50:32871 52.36.210.126:443   ESTABLISHED
TCP    192.168.1.50:32899 52.142.84.61:443    ESTABLISHED
TCP    192.168.1.50:34832 92.42.73.150:80     CLOSE_WAIT
TCP    192.168.56.1:139   0.0.0.0:0          LISTENING
TCP    [::]:135           [::]:0             LISTENING
TCP    [::]:1445          [::]:0             LISTENING
```

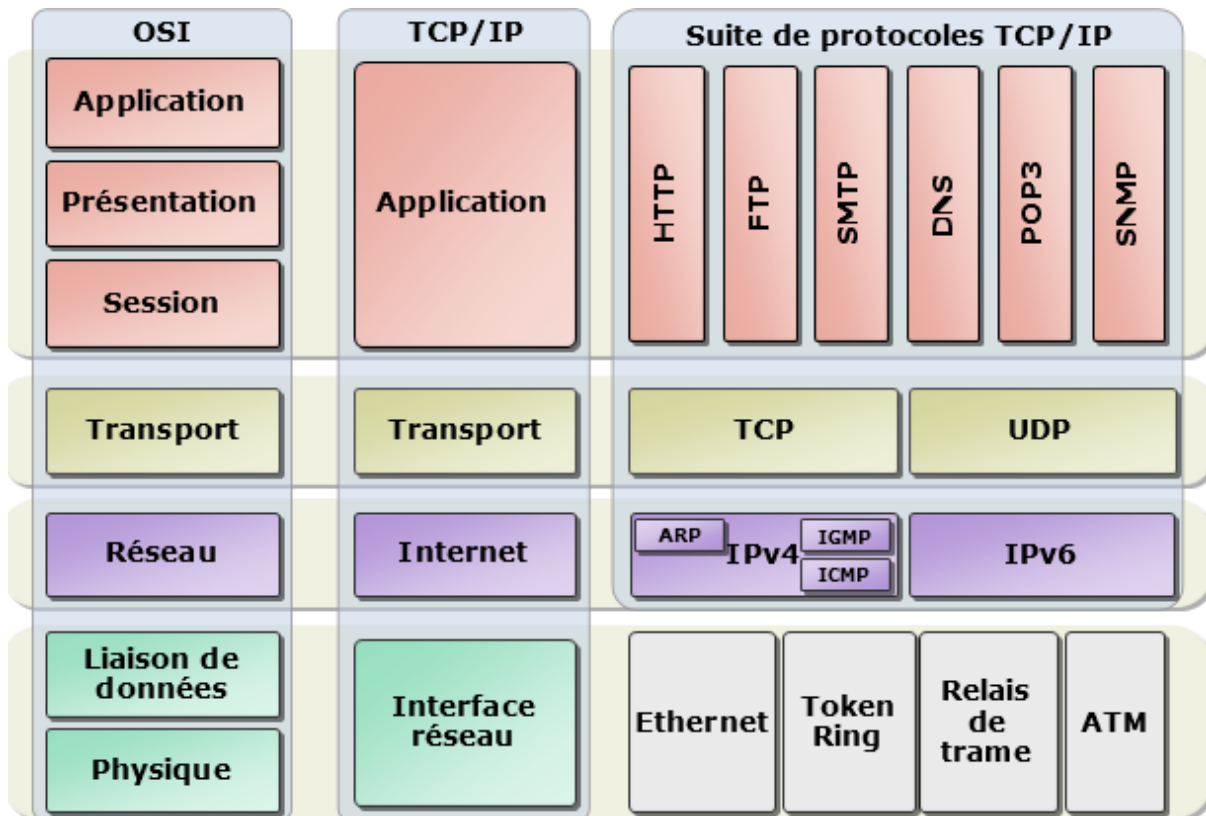
IP Angry : un outil de scan du réseau local parmi tant d'autres

Le NAT et Port Forwarding



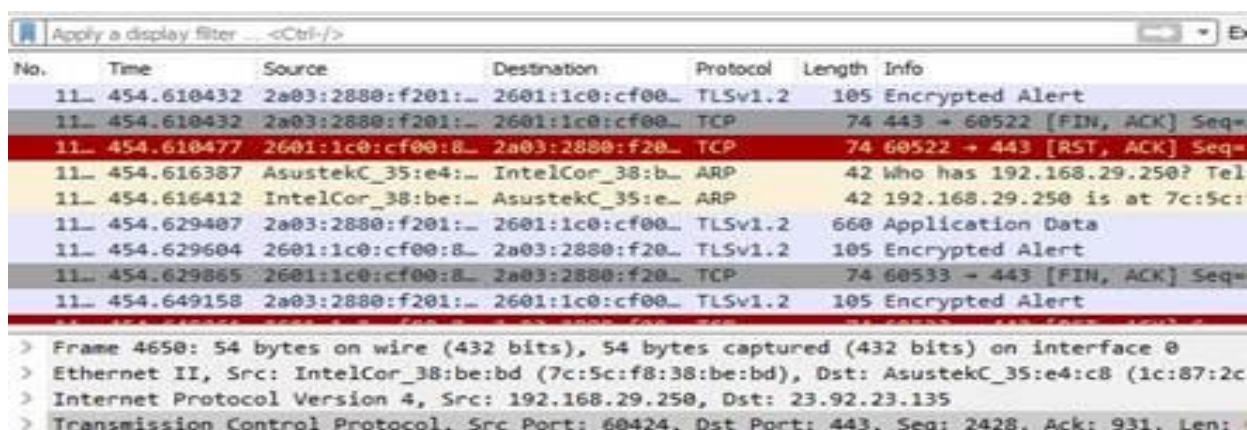
Utilisation des blocs d'adresses IP en 2007

Comment Utiliser Wireshark Pour Capturer, Filtrer Et Inspecter Les Paquets?



Wireshark, un outil d'analyse du réseau anciennement connu sous le nom d'Ethereal, capture les paquets en temps réel et les affiche dans un format lisible par un humain.

Wireshark inclut des filtres, un codage couleur et d'autres fonctionnalités qui vous permettent de creuser profondément dans le trafic réseau et d'inspecter les paquets individuels.



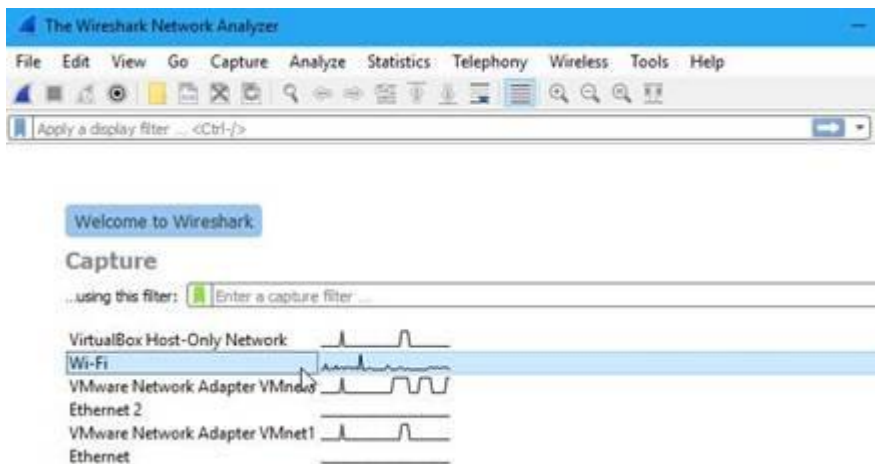
UTILISER Wireshark

Wireshark est en téléchargement libre sur son site officiel. Il suffit de taper son nom dans votre navigateur préféré pour y accéder.

Avertissement Beaucoup d'organisations n'autorisent pas Wireshark et les outils similaires sur leurs réseaux. N'utilisez pas cet outil au travail sans autorisation.

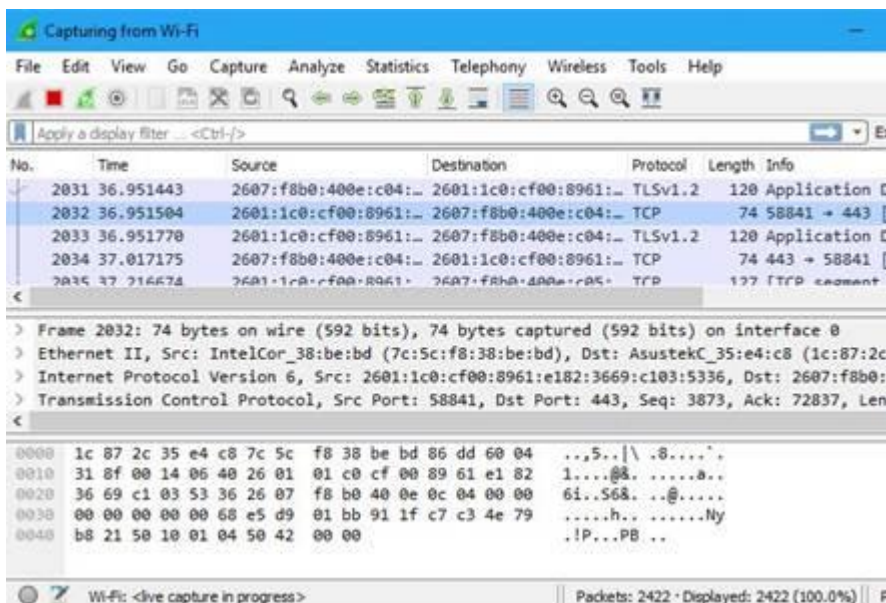
Capter Les Paquets

Après avoir téléchargé et installé Wireshark, vous pouvez le lancer et double-cliquer sur le nom de l'interface réseau (*network interface*) sous **Capture** pour commencer à capturer les paquets sur cette interface. Par exemple, si vous souhaitez capturer du trafic sur votre réseau sans fil, cliquez sur votre interface sans fil (*Wi-Fi*).

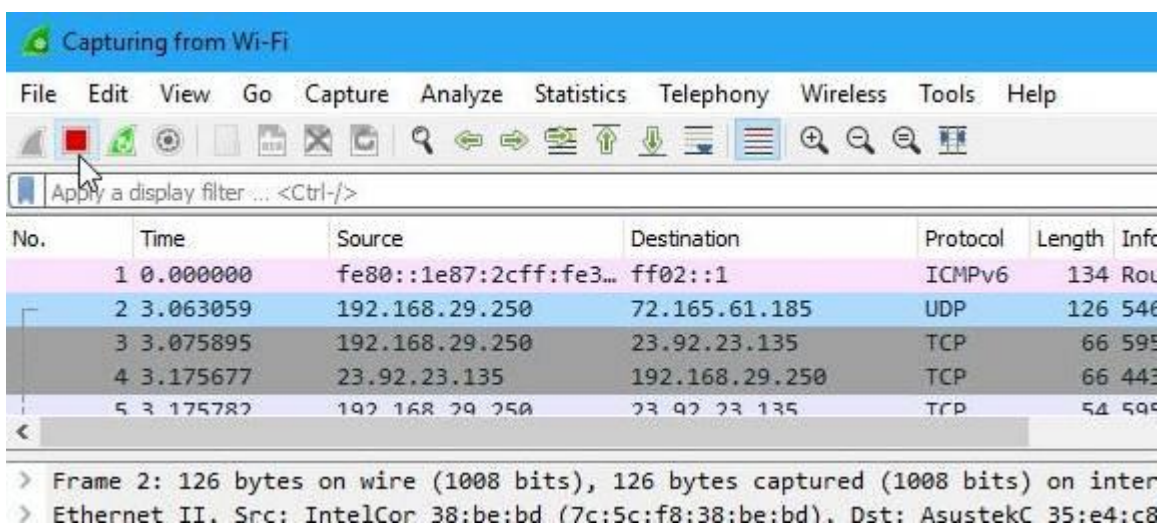


Dès que vous cliquez sur le nom de l'interface, les paquets commencent à apparaître en temps réel. Wireshark capture chaque paquet envoyé vers ou depuis le système hôte.

Si le mode Promiscuous est activé (*promiscuous mode*) —il est activé par défaut— tous les autres paquets du réseau sont également affichés et non pas uniquement les paquets destinés à votre carte réseau. Pour vérifier si le mode promiscuous (*promiscuous mode*) est activé, cliquez sur **Capture > Options** et vérifiez que la case à cocher « Activer le mode promiscuous sur toutes les interfaces » (*Enable promiscuous mode on all interfaces*) est activée au bas de cette fenêtre.



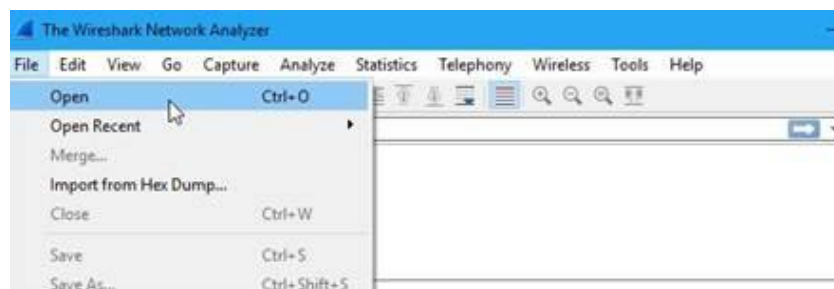
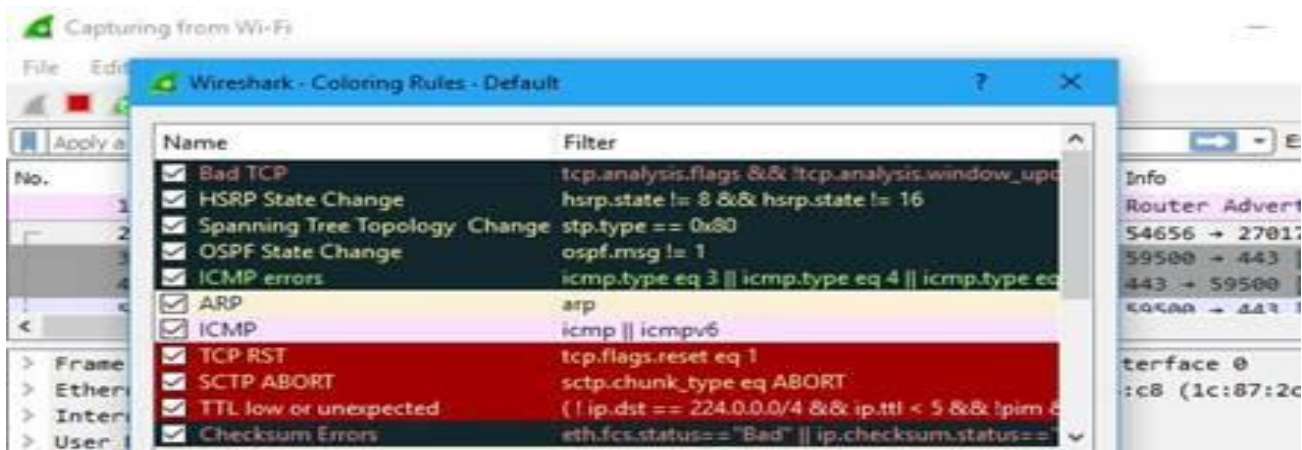
Cliquez sur le bouton rouge « *Stop* » près du coin supérieur gauche de la fenêtre lorsque vous souhaitez arrêter la capture du trafic.



Codes de couleurs

Vous verrez probablement les paquets mis en évidence dans une variété de couleurs différentes. **Wireshark** utilise des couleurs pour vous aider à identifier les types de trafic en un coup d'œil. Par défaut, violet clair est le trafic TCP, bleu clair est le trafic UDP et noir identifie les paquets avec des erreurs, par exemple, ils pourraient avoir été livrés dans le désordre.

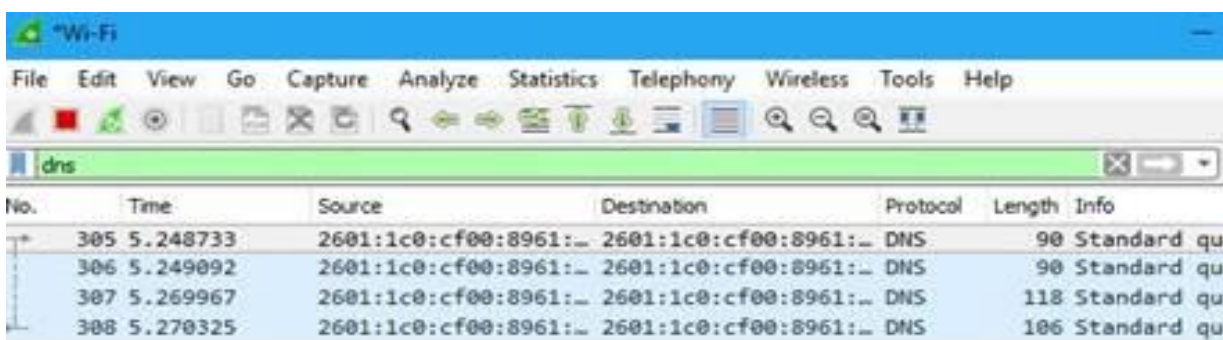
Pour voir exactement ce que signifient les codes de couleur, cliquez sur Affichage (ou vue) → Règles de coloration (**View > Coloring Rules**). Ces règles sont modifiables.



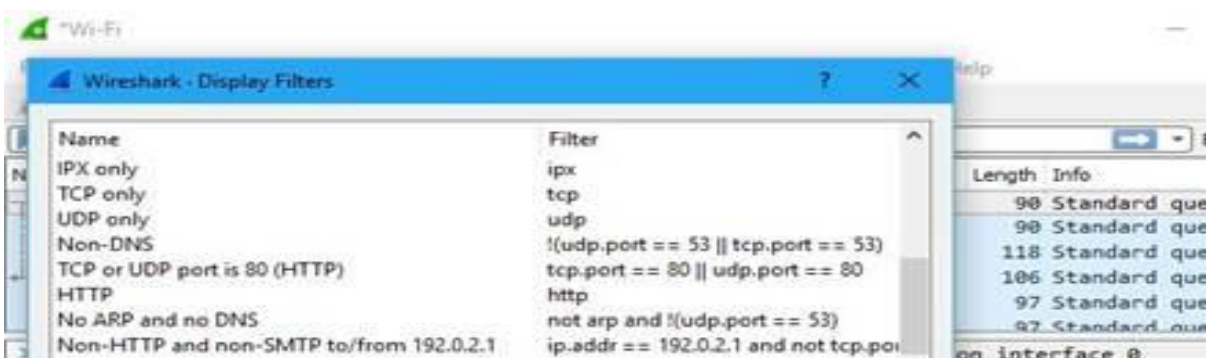
Filtrage des paquets

La manière la plus simple d'appliquer un filtre consiste à le saisir dans la zone de filtre en haut de la fenêtre et à cliquer sur Appliquer **Apply** (ou sur Entrée).

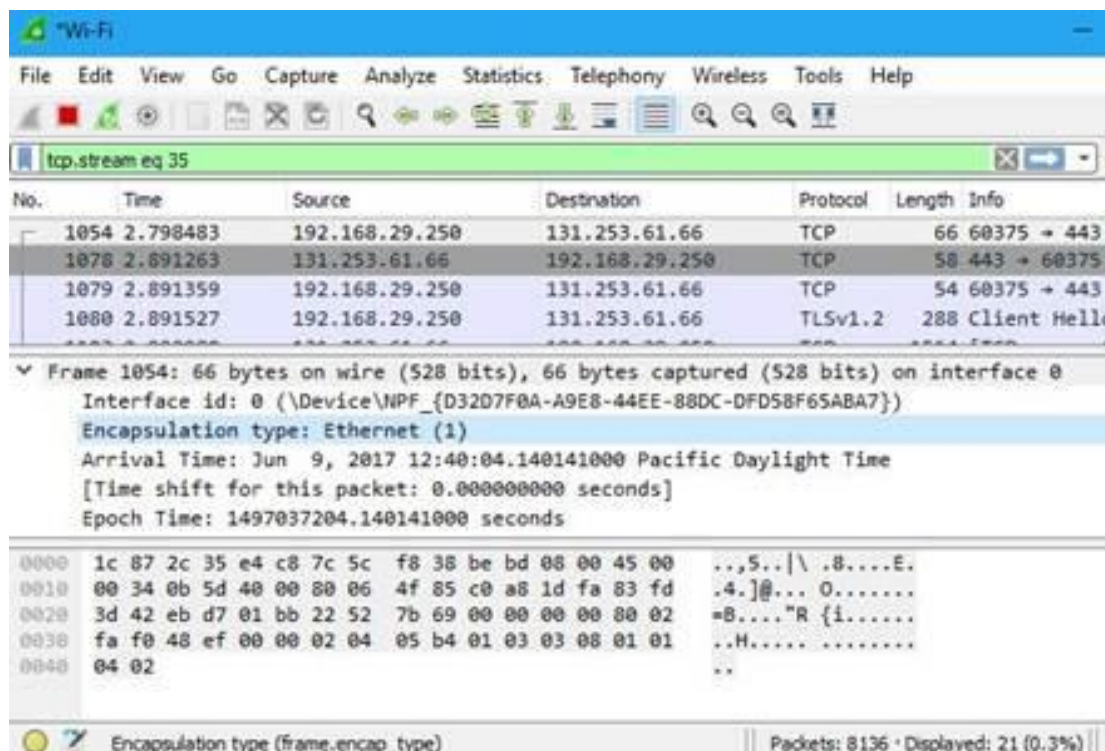
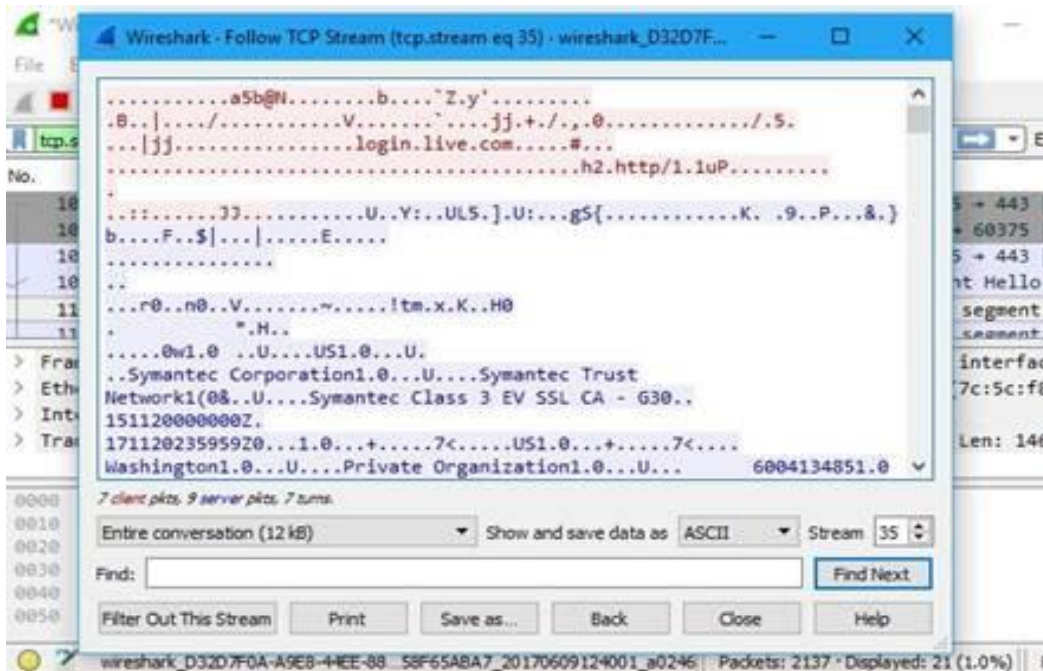
Par exemple, taper « **dns** » et on verra uniquement les paquets DNS.



On pourrait également cliquer sur Analyser > Afficher les filtres (**Analyze > Display Filters**) pour choisir un filtre parmi les filtres par défaut inclus dans Wireshark.



Une autre particularité intéressante à explorer est de cliquer avec le bouton droit sur un paquet et de sélectionner Suivre> Flux TCP (*Follow > TCP Stream*).



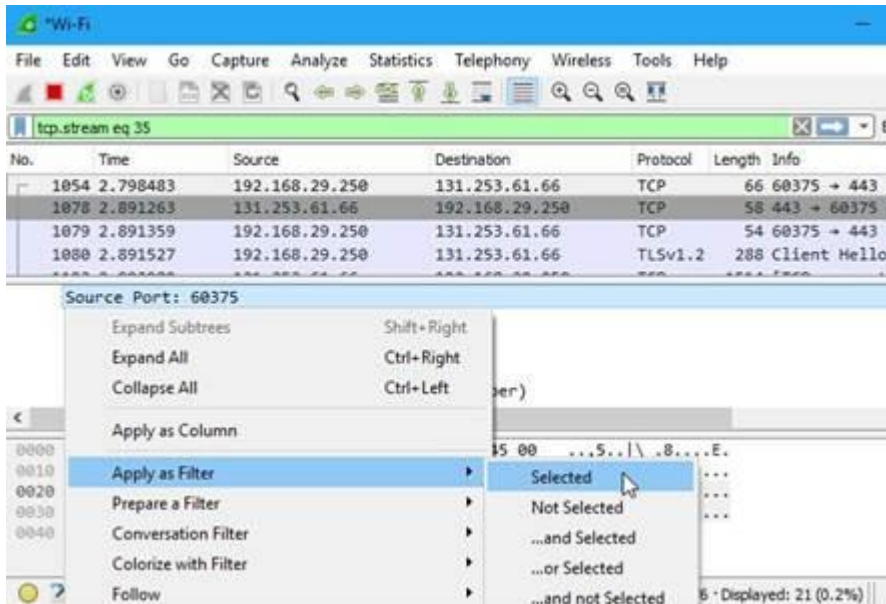
Quand bien même il capture beaucoup de trames réseaux par unité de temps, Wireshark en rate plein d'autres surtout si aucun filtre n'est appliqué. Comment font donc les switches, qui eux doivent aiguiller toutes les trames sans en perdre une ?

Même avec un Intel i9 64Go de RAM, difficile d'imaginer un OS avec une aussi-faible latence !

Inspection des paquets

Cliquez sur un paquet pour le sélectionner et vous pouvez creuser pour voir ses détails.

Vous pouvez également créer des filtres à partir d'ici – cliquez avec le bouton droit sur l'un des détails et utilisez le sous-menu Appliquer (*Apply*) en tant que filtre pour créer un filtre basé sur celui-ci.



Wireshark est un outil extrêmement puissant. Les professionnels l'utilisent pour déboguer les implémentations de protocoles réseaux, examiner les problèmes de sécurité et inspecter les composants internes d'un protocole réseau donné.

Exemple de filtres récurrents

ftp || tcp - Paquets dont le type est : FTP, TCP.

ip.addr == 10.20.144.150 - Paquets dont l'adresse IP source ou destination est 10.20.144.150

ip.src == 10.20.144.150 - Paquets dont l'adresse IP source 10.20.144.150

ip.dst == 10.20.144.151 - Paquets dont l'adresse IP source 10.20.144.151

tcp.port == 35974 - Paquets dont le port source ou destination est 35974.

tcp.srcport == 21 - Paquets dont le port source est 21 (port FTP).

tcp.dstport == 21 - Paquets dont le port destination est 21.

Opérateurs de comparaison :

==	Est égal à
!=	N'est pas égal à
>	Plus grand que
<	Plus petit que
>=	Plus grand ou égal que
<=	Plus petit ou égal que

Opérateurs logiques :

	Ou
&&	Et
^^	Ou exclusif
!	Négation

Exemple de filtres plus complexes :

`ip.dst == 10.20.144.151 && (tcp.dstport == 35974 || tcp.dstport == 21)`

Recherche les paquets à destination de 10.20.144.151 sur les ports TCP 35974 ou 21

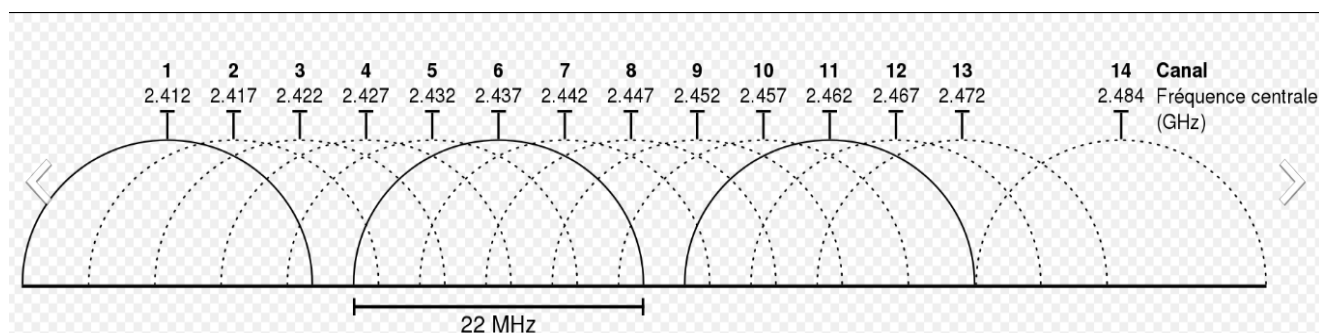
Wireshark ne fait pas de miracle, il est possible de l'aveugler moyennant l'envoi de trames Ethernet qu'il ne saurait déchiffrer comme des trames Ethernet IEEE802.3.

Notions de communications sans Fil WiFi

- Année 1999 : la genèse du WiFi à 2Mbit/s !!! (Les modems 56K étaient encore courants, même les PC ne pouvaient franchir le seuil des 115 200 Bauds en liaison série).
- Septembre 1999 deux standards WiFi s'affrontent : WiFi a (54 Mbit/s) vs Apple WiFi b (11 Mbit/s)
- Marketing efficace de Apple pour promouvoir le 'b' grâce à son iBook => Apple gagne la bataille de la portée grâce à l'usage de l'ISM.
- 2000/2001 WiFi g compatible avec le 'b' (2.4GHz) mais supportant le débit du 'a' (54Mbit/s), il sonne le glas du b tout en étant compatible avec lui avec un débit plus limité, mais surtout il marque la mise à mort du 'a' !
- Arrivée du n à 150 Mbit/s à 2.4GHz et 5GHz, compatible avec b, g et a ! Mais ne ressuscite pas le 'a' car ce dernier est limité à 2 Mbits/s et ne supporte pas les techniques de modulation OFDM ou MIMO.

Aujourd'hui les équipements WiFi ac compatible 2.4GHz et 5GHz annoncent des débits théoriques de 300 Mbit/s avec une portée de près de 100m (Outdoor).

Les routeurs et Point d'Accès WiFi récents n'autorisent plus le mode de sécurité WEP, seul le WPA et mieux le WPA2 sont autorisés et pour cause l'usage du WEP ne se justifie plus, même avec un codage sur 256 bits.



Les Box (Orange, SFR, Bbox, Free..) et les équipements WiFi (b, g, n) en général, offrent la possibilité de choisir un canal. Que signifient ces canaux WiFi, et en quoi peuvent-ils m'être utiles ?

Ils sont espacés de 5MHz, ont une bande passante de +/-11 dB et s'étalent sur 11 canaux dans la majorité des pays (jusqu'à 14 au Japon).

Le WiFi et la santé

2.4GHz ou 5GHz quelle différence ? Que choisir ?

Intérêts du 5 GHz par rapports au 2.4 GHz (interférences, interaction rayonnement matière biologique, portée des liaisons, débit).

NB : les fours micro-onde opèrent sur 2.45GHz et atteignent plusieurs centaines de Watts.

L'OFDM et le MIMO (WiFi n et ac) sont des techniques implémentées par défaut dans la bande des 5GHz, limitant les effets de chevauchement des canaux et permettant d'accroître les débits.


Les téléphones portables sont en fait des récepteur/émetteur radios qui échangent des données via des ondes avec les antennes-relais installées à travers le territoire. Ces ondes ont une fréquence qui varie en fonction de la technologie utilisée :

- **900 ou 1800 MHz pour le réseau GSM (c'est-à-dire la 2G) ;**
- **2100 MHz pour le réseau UMTS (c'est-à-dire la 3G) ;**
- **800 MHz ou 2,6 GHz pour le réseau LTE (c'est-à-dire la 4G)**

Les puissances d'émission autorisées s'en déduisent :

- **2 W pour le réseau GSM 900 MHz ;**
- **1 W pour le réseau GSM 1800 MHz ;**
- **0,125 W pour le réseau UMTS 2100 MHz ;**

Evolution des communications sans fil



Les différentes générations

Génération	Exemple	Signal	Informations
1G	Radiocom 2000	Analogique	voix
2G	GSM	Numérique 900, 1800 Mhz	voix et courts messages textuels (SMS)
2,5 G	GPRS	Numérique	données
3G	UMTS	Numérique 800, 2100 Mhz	données
4G	LTE	Numérique 800, 1800 et 2600 Mhz	voix et données IP

Si les premiers réseaux mobiles ont permis de transporter la parole, ils ont rapidement évolué pour transporter des données. Les opérateurs ont alors interconnecté leur réseau voix GSM à commutation de circuits à leur réseau de données.

Mais ce sont les réseaux de troisième génération 3G, comme l'UMTS, qui vont offrir de nouveaux services comme l'accès à Internet, la lecture de vidéos, la TV en ligne, ou encore la visiophonie.

Enfin, le réseau de 4^{ème} génération 4G, le LTE (Long Terme Evolution) diffère des générations précédentes du fait qu'il est "tout IP" et présente une architecture nouvelle.

Les opérateurs le déploient depuis 2010 environ, d'abord pour les données et accès Internet. Ce réseau haut débit permet des connexions théoriques jusqu'à 100 Mb/s.

5G → le GiGa bits/s voire plus ?

