JFA 1

CM
Introduction aux services réseaux

Jean-François ANNE
jean-francois.anne@unicaen.fr
http://www.jfanne.fr
IUT de CAEN – Campus 3

2023 - 2024

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

JFA 2

Sommaire

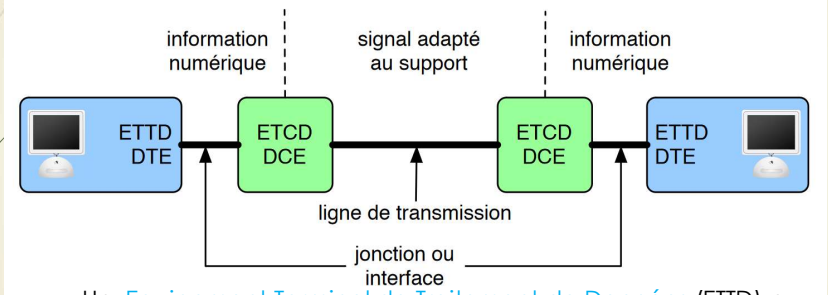
IUT GRAND OUEST NORMANDIE – INFO – R 2.05

JFA 3

Transmission : ETTD et ETCD

R 2.05

- Une transmission de données met en œuvre des calculateurs d'extrémité et des éléments d'adaptation du signal.



- Un Equipement Terminal de Traitement de Données (ETTD) ou Data Terminal Equipment (DTE) contrôle les communications.
- Un Equipement Terminal de Circuit de Données (ETCD) ou Data Circuit Equipment (DCE) réalise l'adaptation du signal entre l'ETTD et le support de transmission.

http://nicolas.baudru.perso.luminy.univ-amu.fr/Ressources/R1_Cours2.pdf

JFA 4

Organisation des échanges

R 2.05

- Les caractéristiques des ETCD sont liées à l'organisation fonctionnelle et physique des échanges. Il faut prendre en compte :
  - le sens de transmission : unidirectionnelle (Simplex), à l'alternat (Half Duplex) ou bidirectionnelle (Full Duplex).
  - le nombre de bits transmis en même temps : transmission parallèle (efficace mais problèmes de diaphonie et de propagation non homogène) ou transmission série (qui est plus adaptée aux longues distances).
  - le type de synchronisation des horloges : une transmission correcte des données nécessite la synchronisation de l'horloge du récepteur sur celle de l'émetteur. Deux possibilités, la transmission synchrone ou asynchrone. Besoin de protocoles spécifiques (SLIP, PPP, HDLC, . . .).
  - le mode de transmission électrique : asymétrique ou symétrique.

JFA 5

Modulation d'un Signal

R 2.05

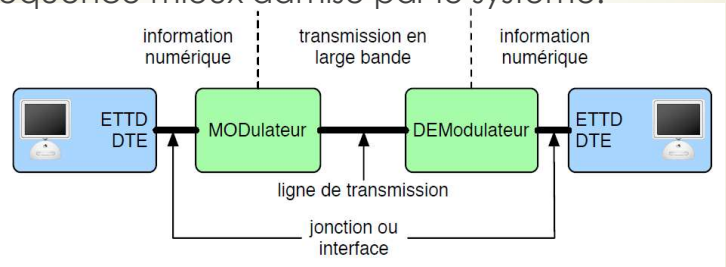
- *Définition :* En télécommunications, le signal transportant une information doit passer par un moyen de transmission entre un émetteur et un récepteur. Le signal est rarement adapté à la transmission directe par le canal de communication choisi, hertzien, filaire, ou optique.
  - La modulation peut être définie comme le processus par lequel le signal est transformé de sa forme originale en une forme adaptée au canal de transmission, par exemple en faisant varier les paramètres d'amplitude et d'argument (phase/fréquence) d'une onde sinusoïdale appelée porteuse, ou en changeant le code du signal en numérique.
  - Le dispositif qui effectue cette modulation, en général électronique, est un **modulateur** (voir modem). L'opération inverse permettant d'extraire le signal de la porteuse est la **démodulation**.

JFA 6

Deux modes d'adaptation du signal

R 2.05

- La transmission en large bande translate le spectre du signal à émettre dans une bande de fréquence mieux admise par le système.



- L'ETCD est un modulateur/démodulateur. Il transforme le signal numérique en un signal sinusoïdal modulé (par fréquence / amplitude / phase) plus résistant que le signal en bande de base. Il permet donc d'atteindre des distances plus importantes. De plus, une transmission en large bande permet le multiplexage spatial.

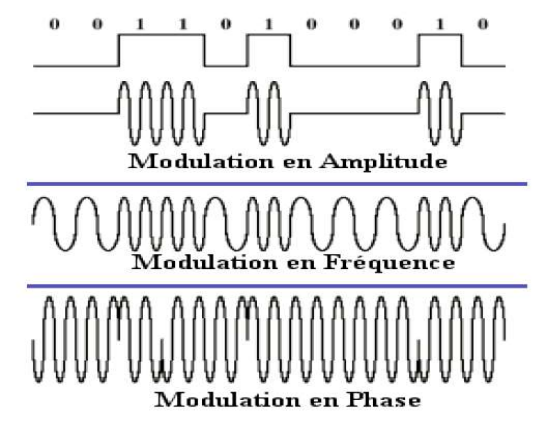
http://nicolas.baudru.perso.luminy.univ-amu.fr/Ressources/R1_Cours2.pdf

JFA 7

Modulations analogiques d'un Signal

R 2.05

- *Différents types de modulations Analogiques:*



Les différentes techniques de modulation peuvent être combinées.

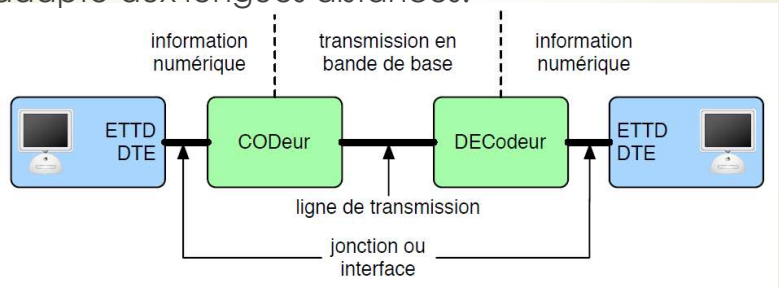
http://nicolas.baudru.perso.luminy.univ-amu.fr/Ressources/R1_Cours2.pdf

JFA 8

Deux modes d'adaptation du signal (bis)

R 2.05

- La transmission en bande de base consiste à modifier légèrement (on dit transcoder) le signal émis par l'ETTD. Ce mode de transmission est peu adapté aux longues distances.



- L'ETCD est un codeur/décodeur. Il a essentiellement pour objet de coder le signal pour supprimer les composantes continues et de maintenir la synchronisation de l'horloge de réception.

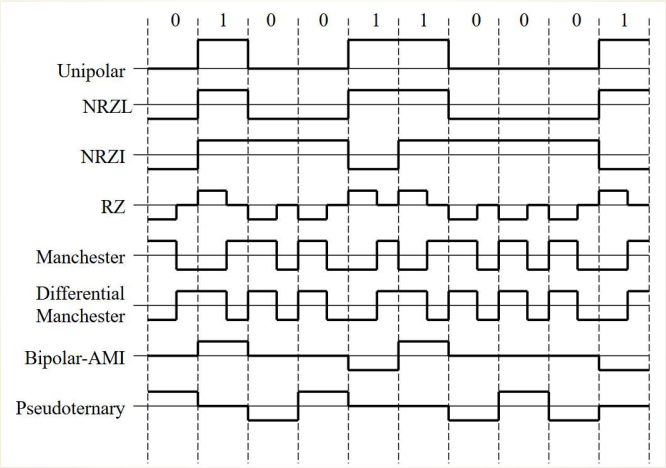
http://nicolas.baudru.perso.luminy.univ-amu.fr/Ressources/R1_Cours2.pdf

JFA 9

Modulation en bande de base d'un Signal

R 2.05

- *Différents types de modulations Numériques :*

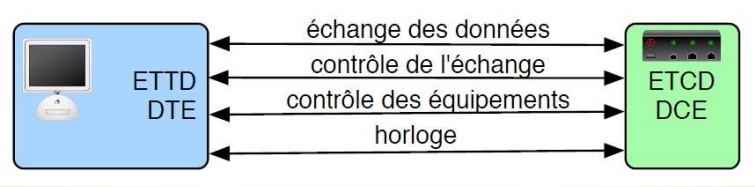


JFA 10

Jonction ETTD/ETCD

R 2.05

- La jonction ETTD/ETCD définit un ensemble de règles (protocole) destinées à assurer la connectivité et le dialogue entre ETTD et ETCD, la synchronisation des horloges, le transfert des données et le contrôle de celui-ci.



- La normalisation de ces interfaces émane principalement de l'Electronic Industries Alliance (EIA) et de l'Union internationale des télécommunications (UIT) (V.24, X.21)..

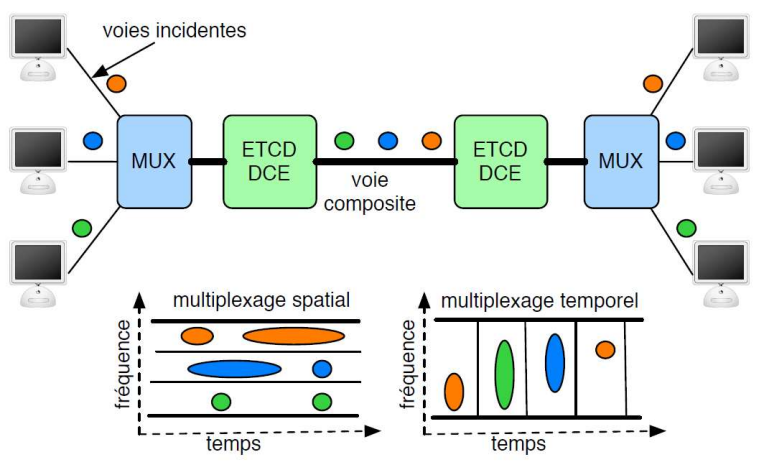
http://nicolas.baudru.perso.luminy.univ-amu.fr/Ressources/R1_Cours2.pdf

JFA 11

Deux techniques de multiplexage

R 2.05

- Le multiplexage spatial et temporel :



http://nicolas.baudru.perso.luminy.univ-amu.fr/Ressources/R1_Cours2.pdf

JFA 12

Configuration Réseau :

R 2.05

- Lorsque vous connectez une machine à un réseau TCP/IP, cette machine, pour fonctionner correctement, doit disposer :
  - ***d'une adresse IP unique dans votre réseau et appartenant au même réseau logique que toutes les autres machines du réseau en question ;***
  - ***un masque de sous-réseau, le même pour tous les hôtes du réseau ;***
  - ***l'adresse de la passerelle qui vous permet de sortir et d'accéder à Internet ;***
  - une adresse de DNS, pour pouvoir résoudre les noms des hôtes, surtout si votre réseau est connecté à Internet.
- Pour les configurer, vous avez trois possibilités :
  - vous utilisez « zeroconf », qui permet à chaque nœud d'un réseau de s'autoattribuer une adresse IP dans le bloc 169.254/16. Tout ce qu'il y a de plus basique, mais ne permet aucune administration du réseau ;
  - vous passez de machine en machine, avec un petit carnet et vous configurez une adresse IP statique à la main, avec le masque et la passerelle ! Et ce qui est davantage gênant, c'est de revenir modifier la configuration à chaque modification du réseau ;
  - vous installez un serveur DHCP sur votre réseau et vous dites à vos clients d'aller chercher toute leur configuration IP sur ce serveur. En gros, il remplacera votre carnet, sera naturellement à jour et vous évitera des déplacements.

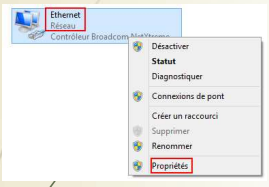
Comme vous le voyez, la troisième solution est la meilleure !

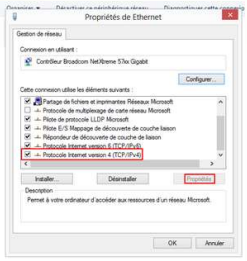
Le client en IP statique sous Windows

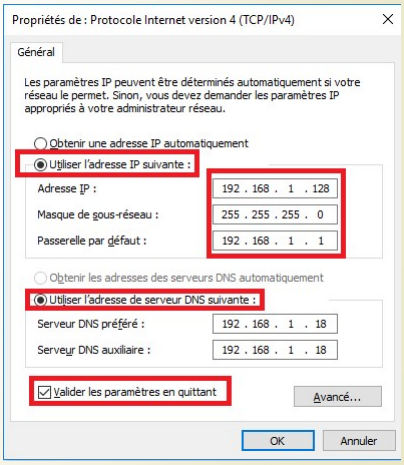
JFA 13

R 2.05

- Sur la machine cliente, on va pouvoir lui préciser une adresse IP statique, dans la configuration de la carte réseau :





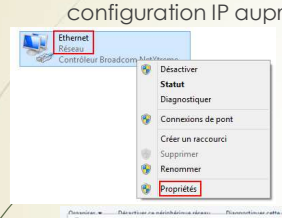


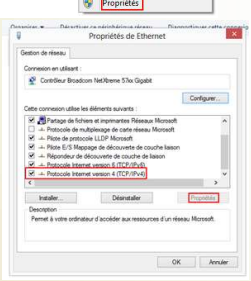
Le client en DHCP sous Windows

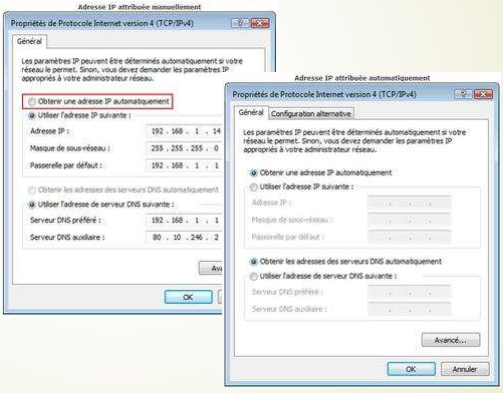
JFA 14

R 2.05

- Sur la machine client, on va pouvoir lui préciser qu'elle doit aller chercher sa configuration IP auprès d'un serveur DHCP, dans la configuration de la carte







JFA 15

Qu'est-ce que le DHCP ?

IUT GRAND OUEST NORMANDIE – iNFO

R 2.05

- Le service DHCP, ou bien le "*Dynamic Host Configuration Protocol*" est un **service TCP/IP,** qu'on installe en général sur une machine serveur mais aussi parfois sur un routeur (box internet, bornes wifi…) , et **qui permet d'automatiser la configuration réseau des équipements d'une infrastructure**.
- Pour simplifier vulgairement le rôle d'un serveur DHCP dans une infra, disons qu'**il évite aux admins de configurer manuellement tous les postes de travail un par un**.
- En fait le service DHCP va **attribuer automatiquement**, *et de façon totalement transparente pour les utilisateurs*, **une configuration réseau complète**, c'est à dire :
  - une adresse IP,
  - un masque,
  - une adresse de passerelle et
  - une adresse de DNS,
- **à tous les postes clients de l'environnement qui lui en feront la demande**. On parle alors d'**attribution "dynamique" d'adresses IP** contrairement à une attribution manuelle dite "**statique**" ou "**fixe**".

https://neptunet.fr/intro-dhcp/

Quels sont les avantages d'avoir un serveur DHCP ?

JFA 16

IUT GRAND OUEST NORMANDIE – iNFO

R 2.05

- Le 1er avantage, c'est déjà que **les administrateurs informatiques ne vont pas devoir** passer sur l'ensemble des ordinateurs pour leur **attribuer une configuration IP manuellement**. *Et croyez-moi, quand il y en a 25, c'est déjà assez pénible, mais imaginez quand il y en a 1300…*
- Second point, **la gestion de l'adressage IP de l'environnement est** à la fois automatisée, mais aussi et surtout **centralisée**. En effet, nous aurons au moins un (*mais souvent plusieurs*) serveur qui va s'occuper de **configurer l'adressage IP des postes qui en font la demande**. Ce serveur aura une "*liste*" d'adresses à distribuer avec des paramètres complémentaires, des "*options*" comme par exemple la passerelle et le serveur DNS.
- Avantage dans l'avantage, comme la gestion est centralisée, **si demain l'adresse de votre serveur DNS change** (*ou tout autre paramètre*), **vous n'aurez qu'à déclarer la nouvelle adresse IP au service DHCP** qui se chargera de la distribuer aux postes clients à leur redémarrage.
- Autre point, comme il n'y a **pas d'intervention humaine**, il a **diminution du risque de conflit d'adresses IP dans l'infrastructure**. *Je rappelle qu'une adresse IP doit être unique dans un réseau.* Quand le serveur DHCP attribue une adresse à un équipement, **celle-ci lui restera attribuée pour une durée définie**, appelé un **"bail"**. Cette adresse ne pourra donc *pas être attribuée de nouveau tant que la fin du bail n'est pas atteinte*.
- On résume les principaux avantages du DHCP :

Gestion Centralisée | Gain de temps | Diminution des risques

https://neptunet.fr/intro-dhcp/

Comment ça fonctionne le DHCP ?

JFA 17

R 2.05

- Pour qu'un équipement puisse recevoir une configuration réseau, **il doit en faire la demande**. Vous pouvez tout à fait avoir un équipement sur lequel vous configurer vous-même l'adressage IP, comme sur un serveur par exemple ou encore un routeur. *Par défaut, tous les postes de travail sont en attente d'une configuration automatique*. Lorsque l'on connecte un ordinateur à un réseau, **celui-ci va chercher un serveur DHCP pour lui transmettre les informations dont il a besoin pour communiquer avec le reste du réseau.**
- Si on effectue une capture des trames sur un réseau lorsqu'un poste de travail souhaite obtenir une configuration réseau automatiquement, on devrait voir apparaître ceci :

No.	Source	Destination	Protocol	Length	Info
1	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Trans…
2	10.45.0.1	255.255.255.255	DHCP	342	DHCP Offer - Trans…
3	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Trans…
4	10.45.0.1	255.255.255.255	DHCP	342	DHCP ACK - Trans…

https://neptunet.fr/intro-dhcp/

Décryptons ces trames ensemble :

JFA 18

No.	Source	Destination	Protocol	Length	Info
1	0.0.0.0	255.255.255.255	DHCP	343	DHCP Discover - Trans…
2	10.45.0.1	255.255.255.255	DHCP	342	DHCP Offer - Trans…
3	0.0.0.0	255.255.255.255	DHCP	369	DHCP Request - Trans…
4	10.45.0.1	255.255.255.255	DHCP	342	DHCP ACK - Trans…

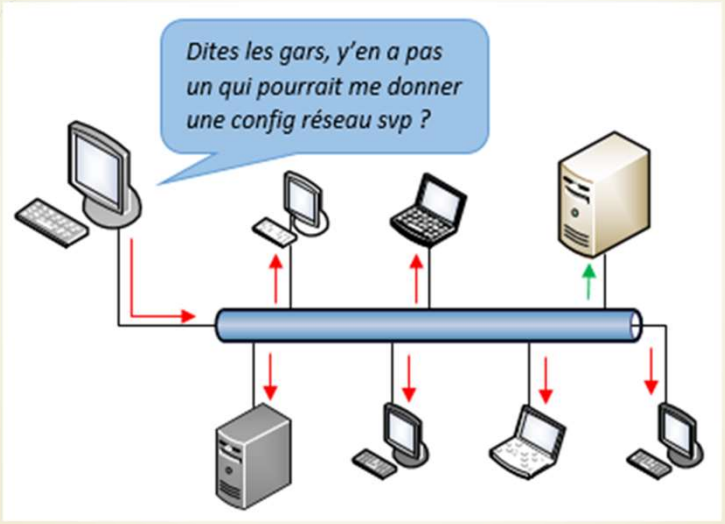
- Dans la 1ère ligne, on voit **une demande émanant de la source 0.0.0.0** qui représente en fait notre **poste de travail**, qui **envoie un message à destination de 255.255.255.255**. On dit alors que l'ordinateur, **le "client"**, diffuse en "***broadcast***" un message sur l'ensemble du réseau. Un broadcast ça signifie **envoyer une requête à destination** de l'adresse 255.255.255.255, soit, **à tout le monde sur le réseau où l'on se trouve**…
- Info + : L'adresse de broadcast 255.255.255.255 est générale pour le cas d'un poste cherchant un DHCP étant donné qu'il n'appartient pas encore à un réseau. Des broadcasts peuvent être émis pour d'autres usages par un poste appartenant par exemple au réseau 192.168.10.0/24. Dans ce cas, le broadcast sera émis à l'attention de l'adresse 192.168.10.255 et va donc cibler toutes les adresses du réseau 192.168.10.0/24.
- En fait dans ce broadcast, on trouvera une **requête appelée "*DHCP DISCOVER*"**. Cette requête va contenir un paquet, un "***datagramme***", contenant entres autres, l'adresse physique de la carte réseau de la machine, *l'adresse MAC*, et sera émise **à destination du port 67**, c'est à dire le **port d'écoute utilisés par les serveurs DHCP** pour ce protocole. **Le but de ce datagramme est de découvrir sur le réseau où se situe le client, un serveur DHCP**.

https://neptunet.fr/intro-dhcp/

JFA 19

DHCP DISCOVER :

R 2.05



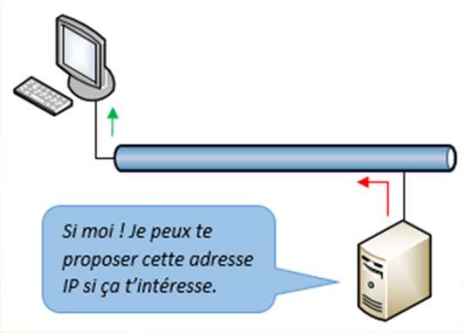
https://neptunet.fr/intro-dhcp/

JFA 20

DHCP OFFER :

R 2.05

Le (ou les) **serveur(s) DHCP se trouvant sur le réseau et qui va recevoir** le datagramme va alors répondre à son tour par une **requête "*DHCP OFFER*" sur le port 68** cette fois-ci qui est le **port d'écoute utilisé par le protocole DHCP pour les clients**. Il va en fait **proposer au client, une potentielle configuration IP**.



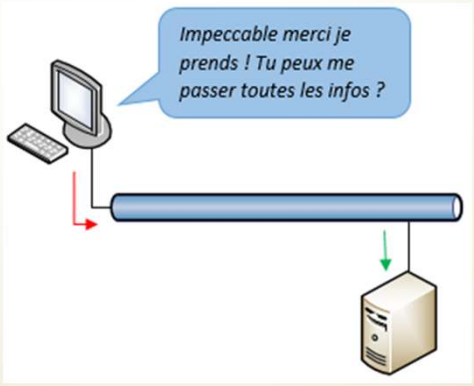
https://neptunet.fr/intro-dhcp/

DCHP REQUEST :

JFA 21

R 2.05

Le client va alors **retenir la 1ère offre qu'il recevra d'un serveur DHCP** et va de nouveau diffuser un datagramme avec la **requête "*DCHP REQUEST*"**. Dans ce datagramme, on trouvera l'adresse IP du serveur DHCP qui a répondu à la demande du client et également l'adresse IP qui lui a été proposée. En fait, **cette nouvelle requête sert à demander au serveur DHCP de lui assigner l'adresse offerte et de lui transmettre les éventuelles autres options nécessaires**. S'il y a plusieurs serveurs DHCP dans l'environnement qui ont eux aussi fait une offre, *ce datagramme va également leur signaler que leur offre n'a pas été retenue.*



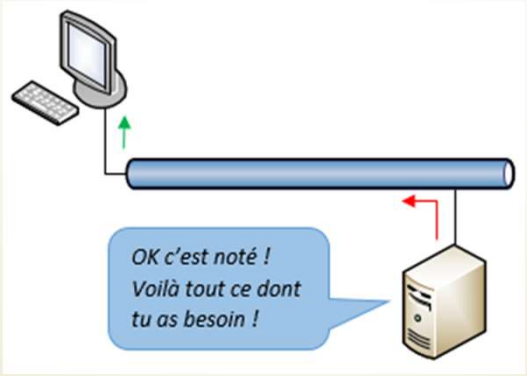
https://neptunet.fr/intro-dhcp/

DHCP ACK :

JFA 22

R 2.05

Et pour terminer, le serveur DHCP choisi, **envoie un dernier datagramme servant d'accusé de réception appelé "*DHCP ACK*"**. Cette **dernière requête assigne au client son adresse IP et lui transmet toutes les informations** dont il aura besoin comme par exemple, **le masque de sous-réseau, la durée du bail de cette adresse**, et les options éventuelles (Passerelle, DNS, NTP, routeur…).



https://neptunet.fr/intro-dhcp/

JFA 23

Le Service DHCP : Le bail

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

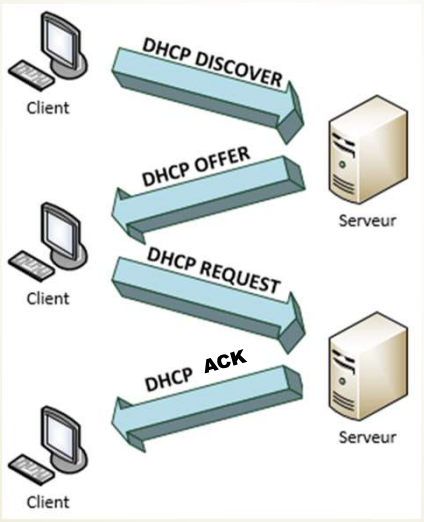
- Le bail est le temps pendant lequel l'adresse IP est réservée à la machine,
- Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration comme :
  - l'adresse d'un ou de plusieurs DNS (résolution de noms) ;
  - l'adresse de la passerelle par défaut (pour sortir du réseau IP où le DHCP vous a installé) ;
  - l'adresse du serveur DHCP (nous allons voir pourquoi).
- il existe en effet une grande quantité d'options qui peuvent être aussi transmises.
- Lorsque le bail arrive à environ la moitié de son temps de vie, le client va essayer de renouveler ce bail, cette fois-ci en s'adressant directement au serveur qui le lui a attribué. Il n'y aura alors qu'un DHCP REQUEST et un DHCP ACK.
- Si, au bout des 7/8e de la durée de vie du bail en cours, ce dernier n'a pu être renouvelé, le client essayera d'obtenir un nouveau bail auprès d'un DHCP quelconque qui voudra bien lui répondre. Il pourra alors se faire que le client change d'adresse IP en cours de session. Normalement, cette situation ne devrait pas se produire, sauf en cas de panne du DHCP.

JFA 24

Synthèse :

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

On récapitule le fonctionnement du DHCP, ou plutôt **les échanges entre le client et le serveur** :



https://neptunet.fr/intro-dhcp/

JFA 25

Le Service DHCP

R 2.05

Le dialogue est décrit de la manière suivante :

- Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau,
- Il envoie donc une trame « DHCP DISCOVER », destinée à trouver un serveur DHCP. Cette trame est un « broadcast », donc envoyé à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi son « Adresse MAC». Le système devra fonctionner uniquement avec les adresses MAC lors du premier dialogue.
- Le serveur DHCP du réseau qui va recevoir cette trame va se sentir concernés et répondre par un « DHCP OFFER ». Cette trame contient une proposition de bail et l' « Adresse MAC » du client, avec également l'adresse IP du serveur. Si plusieurs serveurs DHCP répondent, le client normalement accepte la première réponse venue. Le « DHCP OFFER » sera un broadcast,
- Le client répond alors par un DHCP REQUEST à tous les serveurs (donc toujours en « Broadcast ») pour indiquer quelle offre il accepte ;
- Le serveur DHCP concerné répond définitivement par un DHCP ACK qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

JFA 26

Que se passe-t-il si aucun serveur DHCP ne me répond ? :

R 2.05

Dans ce cas, vous aurez une **adresse attribuée automatiquement dans le réseau 169.254.0.0/16**. Ce réseau est spécifique et est connu sous le nom de ***réseau APIPA*** ("***Automatic Private Internet Protocol***"). APIPA c'est un **processus qui permet à un système de s'attribuer lui même une adresse IP** lorsqu'aucun serveur DHCP n'est joignable.

```
Carte Ethernet Ethernet0 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::31e6:980e:8e5f:f880%4
   Adresse d'autoconfiguration IPv4 . . . : 169.254.248.128
   Masque de sous-réseau. . . . . . . . . : 255.255.0.0
   Passerelle par défaut. . . . . . . . . :
```

La carte réseau du client envoie des requêtes sur l'adresse de broadcast pour tenter de communiquer avec un serveur DHCP. Si elle ne reçoit pas de réponse, **elle va s'attribuer automatiquement une adresse située dans le réseau APIPA**. **Attention**, le 169.254.0.0/16 est un **réseau privé, complètement isolé et non routable** ! C'est à dire que votre machine ne pourra pas communiquer avec d'autres et donc par conséquent, n'accédera pas à internet.

https://neptunet.fr/intro-dhcp/

JFA 27

Pourquoi je ne reçois pas d'adresse de mon DHCP ? :

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Les raisons pour lesquels un poste ne recevrait pas une adresse d'un DHCP sont nombreuses. En voici quelques-unes au hasard :
  - Il n'y a pas de serveur DHCP sur le réseau
  - Le service DHCP n'a plus d'adresses à fournir
  - Le serveur DHCP n'est pas joignable (problème réseau ou système)
  - Des stratégies de filtrage par adresses MAC sont appliquées sur le serveur DHCP et votre machine ne respecte pas les conditions
  - Le port du switch sur lequel est branché votre machine est désactivé
  - …

https://neptunet.fr/intro-dhcp/

JFA 28

Quelles sont les fonctionnalités principales d'un serveur DHCP ? :

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

Quand on déploie le service DHCP dans son infrastructure, la 1ère chose à faire c'est de **créer des étendues pour les réseaux que l'on veut desservir**, et d'y **définir des plages**, aussi appelées des **"*pools*" d'adresses IP** que le DCHP devra distribuer sur ladite étendue.

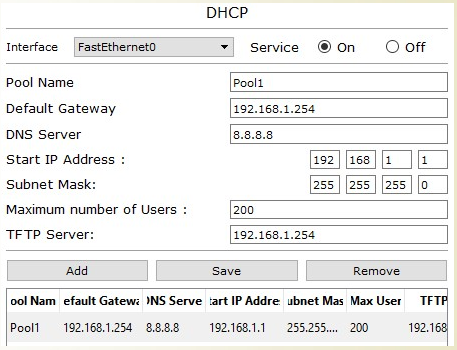
https://neptunet.fr/intro-dhcp/

JFA 29

Le Service DHCP : Le pool d'adresses

R 2.05

- On va donc pouvoir définir un Pool (Bloc) D'adresses IP dynamiques à distribuer à nos machines du réseau.



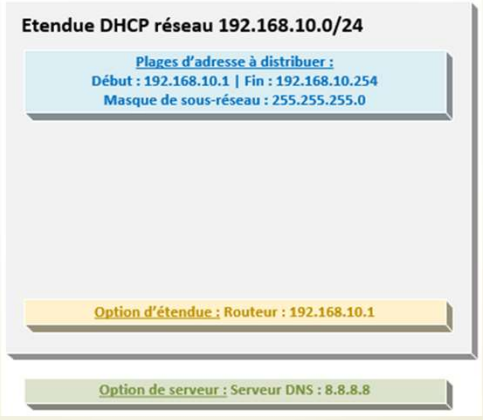
- Ce Pool contiendra :
  - Le nom du Pool ;
  - La passerelle (Gateway) à distribuer ;
  - Le serveur DNS à Distribuer ;
  - La première adresse IP du Pool ;
  - Le masque de réseau à distribuer ;
  - Le nombre d'utilisateurs max à distribuer ou l'adresse de Fin du Pool.

JFA 30

Quelles sont les options d'un serveur DHCP ? :

R 2.05

On peut également **attribuer des options à notre étendue** comme par exemple l'***option "Routeur"*** qui va définir l'adresse de passerelle de ce réseau. On parle d'une **"option d'étendue"** car **cette option ne va s'appliquer que sur l'étendue où elle est définie**.
Si l'on souhaite appliquer une **option à toutes les étendues** du serveur DHCP, il faudra alors utiliser une **"option de serveur"** comme par exemple l'option "Serveur DNS". Une option de serveur se gère **en dehors des étendues**.



https://neptunet.fr/intro-dhcp/

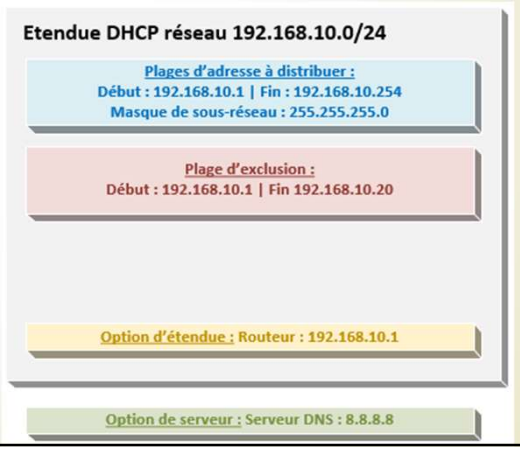
JFA 31

Quelles sont les options d'exclusion d'un serveur DHCP ? :

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

Autre possibilité, **ajouter des plages d'exclusions à l'intérieur de notre pool d'adresse**. Cela signifie que l'on peut **définir une plage d'adresses IP qui ne seront pas attribuées par le DHCP**. Par exemple, on peut définir le pool à distribuer sur 192.168.10.1 à 192.168.10.254 mais décider que les 100 premières adresses ne devront pas être distribuées mais qu'on souhaite les garder pour les attribuer manuellement. On devra alors exclure la plage d'adresses allant de 192.168.10.1 à 192.168.10.100.



https://neptunet.fr/intro-dhcp/

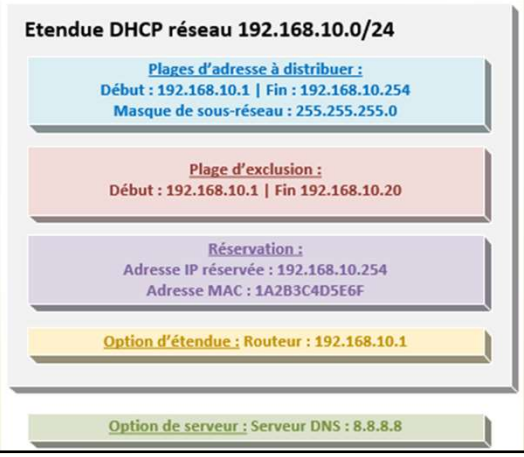
JFA 32

Quelles sont les options de réservation d'un serveur DHCP ? :

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

Autre fonctionnalité bien utile, **la fonction "Réservation"**, qui permet comme son nom l'indique de **réserver une adresse IP spécifique de l'étendue à un client particulier en spécifiant son adresse MAC.** On peut l'utiliser par exemple pour une imprimante. Le serveur DHCP saura que *si telle adresse MAC en fait la demande, elle devra recevoir telle adresse IP et non pas une autre*.



https://neptunet.fr/intro-dhcp/

JFA 33

Le Service DHCP : en statique ?

R 2.05

- *Le problème se pose si on a besoin d'adresses dynamiques et statiques dans le même réseau !*
- *En effet certains postes doivent avoir des adresses IP fixes :*
  - *Notre serveur : 192.168.1.1,*
  - *Notre passerelle : 192.168.1.254,*
  - *Notre imprimante : 192.168.1.210,*
  - *Le photocopieur réseau : 192.168.1.200,*
  - *…,*
- *Il suffit alors d'exclure les adresses IP statiques à attribuer du pool d'adresse IP du DHCP, et de les affecter en association avec leur adresse MAC.*
- *Cela permet en cas de panne de réaffecter toujours la même adresse IP au même matériel.*
- *De plus en cas de changements dans l'adressage IP, les adresses « statiques » se renouvelleront automatiquement dans votre nouveau réseau !*

JFA 34

Le Service DHCP : en statique ?

R 2.05

- *Exemple :*

Vous pouvez réserver une adresse IP statique à chaque équipement de votre réseau local. L'équipement aura donc systématiquement la même adresse sur votre réseau local.

Baux DHCP statiques

nom	adresse IP	adresse MAC	
Moulinsart	192.168.1.104		ajouter
gutemberg	IPv4 : 192.168.1.149	00:00:48:37:ef:bc	supprimer
inconnu	IPv4 : 192.168.1.150	ac:81:12:32:12:b8	supprimer

Vous pouvez visualiser les adresses IP dynamiques attribuées par le serveur DHCP de la Livebox.

Baux DHCP valides

nom	adresse IP	adresse MAC
PC_MLTV_IHD92	IPv4 : 192.168.1.11	D8:6C:E9:48:50:4B
gutemberg	IPv4 : 192.168.1.149	00:00:48:37:EF:BC
Midsommer	IPv4 : 192.168.1.104	
Midsommer	IPv4 : 192.168.1.18	
Spip	IPv4 : 192.168.1.19	38:F2:3E:34:A4:00

Introduction à la résolution de noms

JFA 35

R 2.05

- Pour pouvoir communiquer sur un réseau, chaque machine présente doit avoir un identifiant unique : ¨c'est l'adresse IP.
- Cependant pour un utilisateur, il est impensable de retenir les adresses IP de chaque ordinateur. C'est pourquoi des mécanismes de résolution de noms ont été mis en place. Un mécanisme de résolution de noms permet de traduire des noms en adresses IP et inversement.
- Les ordinateurs du réseau sont connus par leurs adresses IP, mais on ne va pas apprendre toutes les adresses IP disponibles pour naviguer dans le réseau :
  - 77.135.128.85 pour faire une recherche Google,
  - 216.58.204.101 pour lire mes mails,
  - 62.210.16.62 pour avoir le cours,
  - ……
- **Il est plus facile de retenir :**
  - www.google.fr faire une recherche Google,
  - www.gmail.fr pour lire mes mails,
  - www.jfanne.fr pour avoir le cours,
  - ….,
- **C'est la résolution de noms qui permet de faire cette conversion de Noms en adresses IP et inversement !**

Introduction à la résolution de noms

JFA 36

R 2.05

- Au départ, chaque machine stockait localement dans un fichier Hosts, les mappages noms / adresse IP (un mappage est une correspondance entre un nom et une adresse IP). Cependant ce système a l'inconvénient de demander une trop lourde charge administrative. En effet, à chaque ajout de machine dans le réseau ou bien à chaque modification de la configuration d'une machine, il faut éditer manuellement le fichier Hosts contenant les mappages noms / adresse IP.
- Le premier mécanisme de résolution de noms mis en place sous Windows est NetBIOS (NetBIOS Extended User Interface), un protocole crée par IBM dans les années 80. Cette méthode de résolution de noms a de nombreux inconvénients :
  - Les noms NetBIOS sont limités à 16 caractères (15 caractères pour le nom de la machine et un 16è caractère indiquant le type de services hébergés par la machine).
  - Le protocole NetBIOS utilise la diffusion (ou broadcast) pour résoudre les noms en adresses IP ce qui surcharge la bande passante du réseau.
  - Les noms NetBIOS ne possèdent pas de hiérarchie ce qui les rends inutilisables sur Internet.
  - Le protocole NetBIOS n'est pas utilisé sur les plateformes non Microsoft ce qui pose un problème d'interopérabilité.
- C'est pourquoi sous Windows 200X/XP, un nouveau système de résolution de noms appelé DNS (Domain Name System) a été adopté. Il corrige les inconvénients du protocole NetBIOS.

Le système DNS

JFA 37

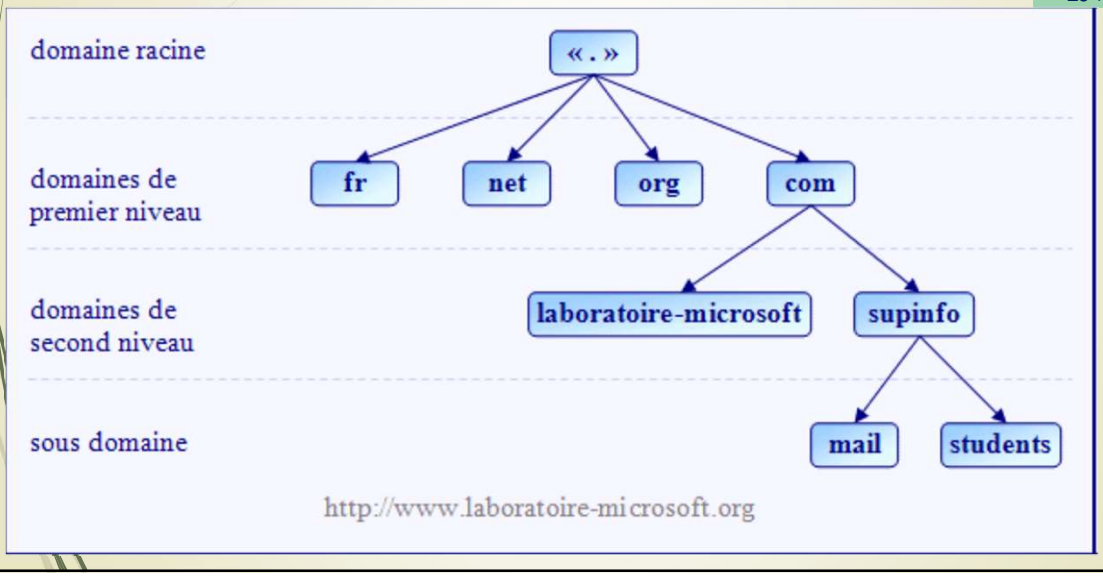
R 2.05

- Le DNS est une **base de données distribuée** qui fait correspondre le nom à une adresse IP (et à d'autres informations)
  - Administration partagée,
  - Charge partagée,
  - Robustesse avec la réplication,
  - Système de cache,
  - Faille critique possible de l'infrastructure internet,
- Le système DNS introduit **une convention de nommage hiérarchique** des domaines qui commence par un domaine racine appelé **"."**. Les domaines situés directement sous le domaine racine sont appelés domaines de premier niveau. Ils sont gérés par l'ICANN et représentent souvent la localisation géographique (fr, be, eu, ru, de ...) ou le type de service (museum, info, org, gov, mail, ...). Les domaines de second niveau sont disponibles pour les entreprises et les particuliers. Ils sont distribués et gérés par d'autres sociétés comme l'InterNIC (une filiale de l'ICANN) ou bien l'AFNIC (Association Française pour le Nommage Internet en Coopération) qui gère le domaine fr. Enfin une multitude de sous domaines peuvent être crée à l'intérieur d'un domaine de second niveau.

la hiérarchie du système DNS

JFA 38

R 2.05



Le système DNS

JFA 39

R 2.05

- Les noms de machine utilisant le système DNS sont appelés noms d'hôtes. Un nom d'hôte peut contenir jusqu'à 255 caractères alphanumériques (chiffres et lettres) et le caractère trait d'union "-". L'utilisation du caractère "." est interdite car il est réservé afin de séparer un domaine supérieur d'un domaine inférieur et pas de caractère underscore " _".
- En effet, on distingue deux types de noms avec le système DNS :
  - le nom d'hôte qui représente le nom d'une machine (un ordinateur, une imprimante ou bien encore un routeur).
  - le nom de domaine pleinement qualifié ou FQDN (Fully Qualified Domain Name).
- Le **FQDN** est en fait composé de deux parties : le nom d'hôte et le suffixe DNS. Le suffixe DNS défini la relation entre le domaine auquel appartient la machine et le domaine racine. Par exemple, si l'on considère une machine avec le nom d'hôte CLIENT-11 située dans le domaine students, son suffixe DNS est : students.supinfo.com. Le nom de domaine pleinement qualifié (FQDN) de la machine CLIENT-11 est donc :

CLIENT-11.students.supinfo.com.

Le Service DNS : résolution de noms

JFA 40

R 2.05

- Le Domain Name System (ou DNS, système de noms de domaine) est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.
- Un FQDN (Fully Qualified Domain Name) (Nom qualifié) est composé d'un nom d'hôte et d'un nom de domaine, par exemple :
  - www.google.com est un FQDN où
  - www est le nom d'hôte et
  - google.com le nom de domaine.
- Les noms de domaine sont organisés de manière hiérarchique, le domaine se trouvant le plus haut dans la hiérarchie est « . », il est omis dans les FQDN. En « dessous » dans la hiérarchie se trouvent les TLD (Top Level Domain).

Le Service DNS : résolution de noms

JFA 41

R 2.05

Résolution de noms directe

- Dans un réseau IP, lorsqu'une machine A veut communiquer avec une machine B, la machine A connaît le nom FQDN de B.
- Par exemple, lorsqu'on navigue sur le net, on connaît en général le nom FQDN des serveurs qu'on visite (exemple www.microsoft.fr.).
- Pour que A puisse communiquer avec B grâce au protocole IP, A va avoir besoin de connaître l'adresse IP de B.
- A doit posséder un moyen d'effectuer la résolution de noms directe, c'est-à-dire un moyen de trouver l'adresse IP de B à partir de son nom qualifié.
- Le résolveur est le programme chargé de cette opération.

Résolution de noms inverse

- La machine B reçoit un datagramme IP en provenance de A. Ce datagramme contient l'adresse IP de A. B peut avoir besoin de connaître le nom FQDN de la machine A.
- B doit donc être capable de trouver le nom FQDN de A à partir de son adresse IP. C'est ce qu'on appelle la résolution de noms inverse.
- Le résolveur est également chargé de cette opération.

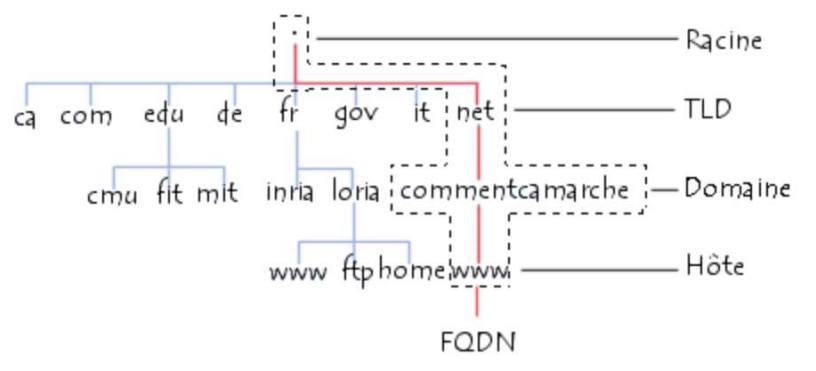
Le Service DNS : L'espace de noms

JFA 42

R 2.05

L'espace de noms

- La structuration du système DNS s'appuie sur une structure arborescente dans laquelle sont définis des domaines de niveau supérieurs (appelés TLD, pour Top Level Domains), rattachés à un nœud racine représenté par un point.
- Arborescence du Domain Name System :



Le Service DNS : L'espace de noms

JFA 43

R 2.05

- On appelle « nom de domaine » chaque nœud de l'arbre. Chaque nœud possède une étiquette (en anglais « label ») d'une longueur maximale de 63 caractères.
- L'ensemble des noms de domaine constitue ainsi un arbre inversé où chaque nœud est séparé du suivant par un point (« . »).
- L'extrémité d'une branche est appelée hôte, et correspond à une machine ou une entité du réseau. Le nom d'hôte qui lui est attribué doit être unique dans le domaine considéré, ou le cas échéant dans le sous-domaine. A titre d'exemple le serveur web d'un domaine porte ainsi généralement le nom www.
- Le mot « domaine » correspond formellement au suffixe d'un nom de domaine, c'est-à-dire l'ensemble des étiquettes de nœuds d'une arborescence, à l'exception de l'hôte.
- Le nom absolu correspondant à l'ensemble des étiquettes des nœuds d'une arborescence, séparées par des points, et terminé par un point final, est appelé adresse FQDN (Fully Qualified Domain Name, soit Nom de Domaine Totalement Qualifié). La profondeur maximale de l'arborescence est de 127 niveaux et la longueur maximale d'un nom FQDN est de 255 caractères. L'adresse FQDN permet de repérer de façon unique une machine sur le réseau des réseaux.
- Ainsi www.commentcamarche.net. représente une adresse FQDN.

Le Service DNS : Les serveurs de noms

JFA 44

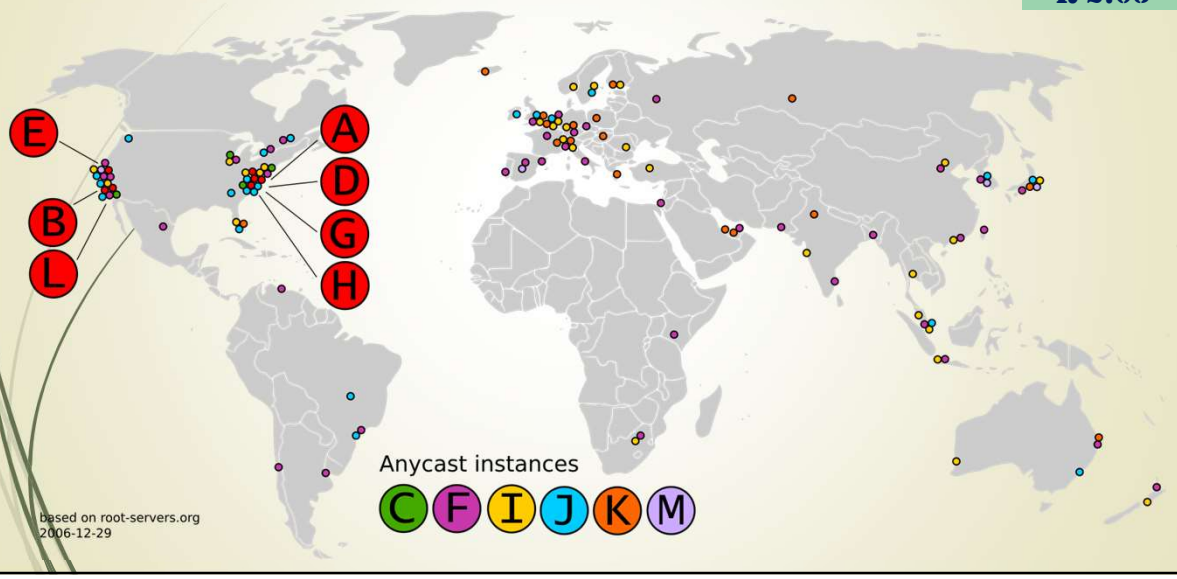
R 2.05

- Les machines appelées serveurs de nom de domaine permettent d'établir la correspondance entre le nom de domaine et l'adresse IP des machines d'un réseau.
- Chaque domaine possède un serveur de noms de domaines, appelé « serveur de noms primaire » (primary domain name server), ainsi qu'un serveur de noms secondaire (secondary domaine name server), permettant de prendre le relais du serveur de noms primaire en cas d'indisponibilité.
- Chaque serveur de nom est déclaré dans à un serveur de nom de domaine de niveau immédiatement supérieur, ce qui permet implicitement une délégation d'autorité sur les domaines. Le système de nom est une architecture distribuée, où chaque entité est responsable de la gestion de son nom de domaine. Il n'existe donc pas d'organisme ayant à charge la gestion de l'ensemble des noms de domaines.
- Les serveurs correspondant aux domaines de plus haut niveau (TLD) sont appelés « serveurs de noms racine ». Il en existe treize, répartis sur la planète, possédant les noms « a.root-servers.net » à « m.root-servers.net ».
- Neuf de ces serveurs ne sont pas de simples machines mais correspondent à plusieurs installations réparties dans des lieux géographiques divers, il y a ainsi au 19 juillet 2019 plus de 997 sites dans 53 pays qui hébergent un serveur racine du DNS. En 2007, on comptait 130 sites.

Le Service DNS : Les serveurs de noms

JFA 45

R 2.05



https://fr.wikipedia.org/wiki/Serveur_racine_du_DNS

Le Service DNS : Les serveurs DNS

JFA 46

R 2.05

- Un serveur de noms (Serveur DNS) définit une zone, c'est-à-dire un ensemble de domaines sur lequel le serveur a autorité. Le système de noms de domaine est transparent pour l'utilisateur, néanmoins il ne faut pas oublier les points suivants :
  - Chaque ordinateur doit être configuré avec l'adresse IP du DNS, une machine capable de transformer n'importe quel nom en une adresse IP. Cette machine est appelée Domain Name Server. Pas de panique: lorsque vous vous connectez à internet, le fournisseur d'accès va automatiquement modifier vos paramètres réseau pour vous mettre à disposition ces serveurs de noms.
  - L'adresse IP d'un second Domain Name Server (secondary Domain Name Server) doit également être définie : le serveur de noms secondaire peut relayer le serveur de noms primaire en cas de dysfonctionnement.
- Le serveur DNS le plus répandu s'appelle BIND (Berkeley Internet Name Domain). Il s'agit d'un logiciel libre disponible sous les systèmes UNIX, développé initialement par l'université de Berkeley en Californie et désormais maintenu par l'ISC (Internet Systems Consortium).

Le Service DNS : Résolution de noms

JFA 47

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

Résolution de noms de domaine :

- Le mécanisme consistant à trouver l'adresse IP correspondant au nom d'un hôte est appelé « résolution de nom de domaine ». L'application permettant de réaliser cette opération (généralement intégrée au système d'exploitation) est appelée « résolveur » (en anglais « resolver »).
- Lorsqu'une application souhaite se connecter à un hôte connu par son nom de domaine (par exemple « www.jfanne.fr »), celle-ci va interroger un serveur de noms défini dans sa configuration réseau. Chaque machine connectée au réseau possède en effet dans sa configuration les adresses IP de deux serveurs de noms de son fournisseur d'accès.
- Une requête est ainsi envoyée au premier serveur de noms (appelé « serveur de nom primaire »). Si celui-ci possède l'enregistrement dans son cache, il l'envoie à l'application, dans le cas contraire il interroge un serveur racine (dans notre cas un serveur racine correspondant au TLD « .fr »). Le serveur de nom racine renvoie une liste de serveurs de noms faisant autorité sur le domaine (dans le cas présent les adresses IP des serveurs de noms primaire et secondaire).

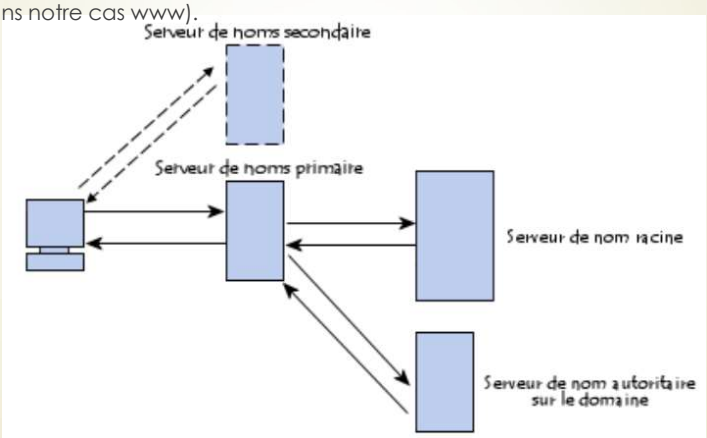
Le Service DNS : Résolution de noms

JFA 48

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Le serveur de noms primaire faisant autorité sur le domaine va alors être interrogé et retourner l'enregistrement correspondant à l'hôte sur le domaine (dans notre cas www).

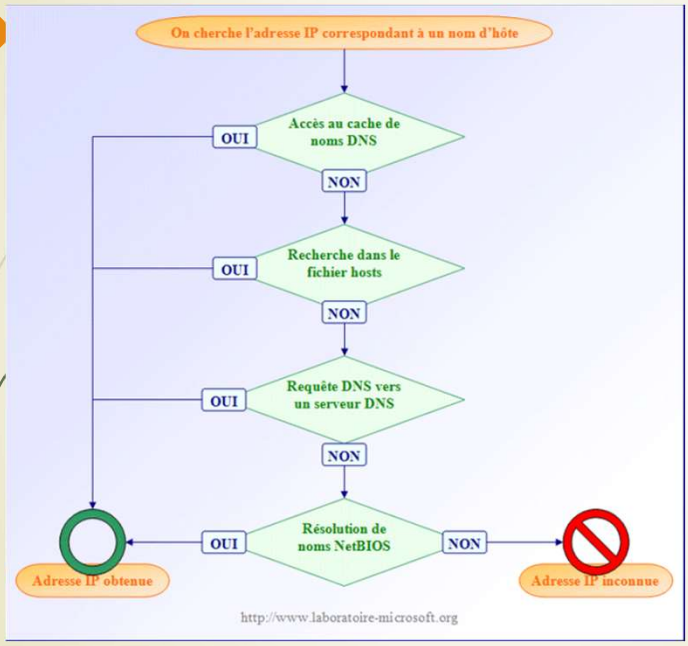


http://www.commentcamarche.net/contents/518-dns-systeme-de-noms-de-domaine

Le Service DNS : Fonctionnement côté client

JFA 49

R 2.05



- Lorsqu'un client souhaite résoudre un nom de domaine en adresse IP ou bien lors de l'accès à un dossier partagé, un processus décomposable en plusieurs étapes est exécuté :

Le Service DNS : Fonctionnement côté client

JFA 50

R 2.05

- <u>fonctionnement de la résolution de nom d'hôte</u>
- La première chose que doit faire le client avant de pouvoir se connecter, au serveur web ou bien au serveur de fichier, est de trouver son adresse IP à partir de son nom d'hôte. Le client commence par vérifier si une adresse IP correspondant au nom d'hôte est présente dans le cache de noms DNS. Le cache de noms DNS contient tous les mappages noms d'hôte / adresses IP qui ont été précédemment résolus. Le cache de noms DNS est stocké en mémoire vive ce qui permet d'accélérer le processus de résolution de noms d'hôte lorsque l'utilisateur accède souvent au même serveur. On peut afficher le cache de noms DNS en utilisant la commande :

  ipconfig /displaydns
- Il est aussi possible de vider cette mémoire cache grâce à la commande :

  ipconfig /flushdns
- Si l'adresse IP recherchée n'est pas présente dans le cache de noms DNS, alors le client consulte le fichier hosts. Ce fichier est situé dans le répertoire :
  - **c:\windows\system32\drivers\etc**
  - **/etc/hosts**
- Toutes les entrées sont faites de manières statiques. Par défaut, il contient uniquement le mappage entre le nom d'hôte localhost et l'adresse IP 127.0.0.1.

Le Service DNS : Le fichier Hosts sous Windows :

JFA 51

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- # Copyright (c) 1993-2009 Microsoft Corp.
- # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
- # This file contains the mappings of IP addresses to host names. Each
- # entry should be kept on an individual line. The IP address should
- # be placed in the first column followed by the corresponding host name.
- # The IP address and the host name should be separated by at least one
- # space.
- # Additionally, comments (such as these) may be inserted on individual
- # lines or following the machine name denoted by a '#' symbol.
- #
- # For example:
- # 102.54.94.97 rhino.acme.com # source server
- # 38.25.63.10 x.acme.com # x client host

- # localhost name resolution is handled within DNS itself.
- #127.0.0.1 localhost
- #::1 localhost

Le Service DNS : Suite

JFA 52

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Si le mappage n'a pas été trouvé dans le fichier hosts, alors le client va envoyer une requête DNS au premier serveur DNS dont l'adresse IP a été définie dans ses paramètres TCP/IP.
- Si le premier serveur DNS est injoignable alors le client envoie une requête au second
- et ainsi de suite...
- Si aucun serveur DNS n'a été paramétré dans les paramètres TCP/IP du client ou bien si aucun serveur DNS n'est capable de résoudre le nom en adresse IP alors le client passe à la quatrième et dernière étape.
- Si le client n'a pas trouvé le mappage recherché alors il considère que l'adresse IP recherchée ne correspond pas à un nom d'hôte mais à un nom NetBIOS et lance une résolution de nom NetBIOS.

Le Service DNS : Suite

JFA 53

R 2.05

- La résolution de noms NetBIOS se passe en plusieurs étapes :
  - 1. vérification de la présence de l'adresse IP dans le cache de noms NetBIOS.
  - 2. envoie d'une requête au premier serveur WINS dont l'adresse IP a été définie dans ses paramètres TCP/IP du client. (*)
  - 3. le client cherche l'adresse IP de la machine sur son sous-réseau en réalisant une diffusion (broadcast). (*)
  - 4. recherche d'une éventuelle entrée dans le fichier c:\Windows\system32\drivers\etc\lmhosts.
- (*) Les étapes 2 et 3 peuvent être inversées ou non présentes selon le type de nœud NetBT défini sur le client. Par défaut, le nœud NetBT H (Hybride) est utilisé et il réalise les étapes dans l'ordre ci-dessus. Le type de nœud NetBT peut se paramétrer au niveau du serveur DHCP (le type de nœud NetBT correspond à l'option DHCP numéro 46).
- Si à la fin de ce processus aucune adresse IP n'a été trouvée alors le client ne peut pas obtenir l'adresse IP correspondante et ne peut pas joindre la ressource (par exemple un serveur web ou un serveur de fichier). Dans tous les cas le résultat de la requête DNS sera mis dans le cache de noms DNS.

Les différents types de requêtes sur un serveur DNS

JFA 54

R 2.05

- Un serveur DNS peut recevoir deux types de requêtes DNS :
  - une requête **récursive** : Lorsqu'un serveur DNS reçoit une requête récursive, il doit donner la réponse la plus complète possible. C'est pourquoi le serveur DNS est souvent amené à joindre d'autres serveurs de noms dans le but de trouver la réponse exacte.
  - une requête **itérative** : Lorsqu'un serveur reçoit une requête itérative, il renvoie la meilleure réponse qu'il peut donner sans contacter d'autres serveurs DNS (c'est-à-dire en consultant uniquement sa propre base de données).
- Lorsqu'une machine cliente envoie une requête à un serveur DNS (étape 3 de la résolution de nom d'hôte), elle est toujours de type récursif !
- Dans l'exemple ci-dessous, l'ordinateur client nommé client23.laboms.lan cherche l'adresse IP correspondant au nom d'hôte websrever.laboms.lan. C'est pourquoi il envoie une requête récursive au serveur DNS nommé dns1.laboms.lan.
- A partir de cet instant dns1.laboms.lan a pour obligation renvoyer une réponse au client. Pour cela il va chercher dans sa mémoire cache, puis la base de données qu'il héberge et va éventuellement contacter d'autres serveurs DNS.
- Une fois qu'il a obtenu la réponse (la réponse peut être négative), il la renvoie au client. Dans notre exemple, le serveur DNS a trouvé l'adresse IP recherchée qui est : 172.16.104.30. L'ordinateur client peut ensuite contacter le serveur web nommé webserver.laboms.lan.

La requête récursive sur un serveur DNS

JFA 55

R 2.05

La requête vers les redirecteurs

JFA 56

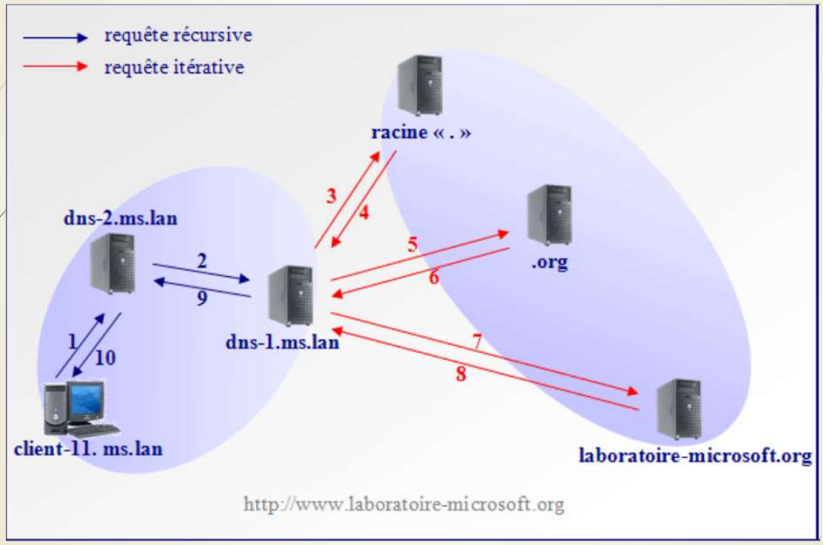
R 2.05

- Lorsqu'un serveur DNS ne peut pas répondre à la requête récursive d'un client, il va d'abord essayer de contacter ses redirecteurs. Si le serveur DNS est paramétré pour utiliser des redirecteurs alors il envoie une requête récursive au premier serveur DNS défini dans sa liste de redirecteurs. Par contre, si le serveur DNS n'a pas de redirecteurs, il va envoyer une requête itérative au premier serveur DNS situé dans sa liste de serveur DNS racine. Le serveurs DNS n'envoie donc des requêtes itératives que si il n'a pas de redirecteurs.

Les requêtes sur un serveur DNS

JFA 57

R 2.05



La requête complète

JFA 58

R 2.05

Dans l'exemple ci-dessus, un client nommé client-11.ms.lan souhaite accéder au site web du laboratoire Microsoft. La procédure de résolution de nom se passe en plusieurs étapes :

1. L'ordinateur client client-11.ms.lan commence par chercher l'adresse IP du serveur Web. Pour cela il envoie une requête récursive au premier serveur DNS de sa liste de serveurs DNS soit dns-2.ms.lan.

2. Le serveur dns-2.ms.lan ne connaît pas la réponse, il envoie donc une requête récursive à dns-1.ms.lan qui est le premier serveur DNS de sa liste de redirecteurs.

3. Dans le cas présent dns-1.ms.lan ne connaît pas l'adresse IP recherchée et n'est pas configuré pour utiliser des redirecteurs. Il envoie donc une requête itérative au premier serveur DNS racine parmi sa liste d'indications de racine.

4. Le serveur DNS racine ne connaît pas la réponse mais il sait quel serveur DNS fait autorité pour le domaine org. Il renvoie donc l'adresse IP du serveur DNS faisant autorité pour le domaine org à dns-1.ms.lan.

5. Le serveur dns-1.ms.lan envoie alors une requête itérative au serveur DNS du domaine org.

6. Le serveur DNS du domaine org ne connaît pas la réponse et renvoie l'adresse IP du serveur DNS faisant autorité pour le domaine laboratoire-microsoft au serveur dns-1.ms.lan.

7. Le serveur dns-1.ms.lan contacte alors le serveur DNS faisant autorité pour la zone laboratoire-microsoft au moyen d'une requête itérative.

8. Le serveur DNS faisant autorité pour la zone laboratoire-microsoft possède le mappage dans sa zone de recherche directe locale. Il envoie donc l'adresse IP recherché à dns-1.ms.lan.

9. dns-1.ms.lan transmet la réponse au serveur dns-2.ms.lan.

10. Le serveur dns-2.ms.lan fait suivre la réponse au client qui peut ensuite joindre le serveur HTTP et afficher le site du laboratoire Microsoft.

Détails du protocole

JFA 59

R 2.05

- DNS utilise en général UDP et le port 53. La taille maximale des paquets utilisée est de 512 octets. Si une réponse dépasse cette taille, la norme prévoit que la requête doit être renvoyée sur le port TCP 53. Ce cas est cependant rare et évité, et les firewalls bloquent souvent le port TCP 53.
- L'extension EDNS0 (RFC 267140) permet d'utiliser une taille de paquets plus élevée, sa prise en charge est recommandée pour IPv6 comme pour DNSSEC.
- La norme prévoit qu'il existe une classe associée aux requêtes. Les classes IN (Internet), CH (Chaos) et HS (Hesiod) sont définies, seule la classe IN étant réellement utilisée en pratique. La classe chaos est utilisée par BIND pour révéler le numéro de version.

Les outils d'administration en ligne de commande

JFA 60

R 2.05

- **Introduction**
- Il existe divers outils en ligne de commande permettant de vérifier le bon fonctionnement de la résolution de noms. On peut citer nslookup, DNScmd ou bien encore DNSlint. Seul nslookup est intégré au système d'exploitation. Les deux autres outils devront être installés avec les outils de support Windows 2000 server,
- **Utiliser nslookup**
  - nslookup permet de **tester la résolution des noms d'hôtes en adresses IP** et inversement. Lorsque l'on tape nslookup en mode texte, une invite de commande apparaît. En outre le nom d'hôte et l'adresse IP du serveur DNS par défaut sont affichés.

```
C:\>nslookup
Serveur par défaut :  dns-2.labomicrosoft.lan
Address:  172.16.16.2

>
```

Utiliser nslookup

JFA 61

R 2.05

- Lorsque l'on tape un nom d'hôte ou un FQDN, nslookup renvoie l'adresse IP correspondante et indique éventuellement si la réponse fait ou non autorité sur le domaine. Dans l'exemple ci-contre, lorsque l'on tape le nom d'hôte *client-7*, le serveur DNS nommé *dns-2.labomicrosoft.lan* renvoie l'adresse IP *172.16.16.16* et rappelle le nom de domaine pleinement qualifié : *client-7.labomicrosoft.lan*.

```
> client-7
Serveur :  dns-2.labomicrosoft.lan
Address:  172.16.16.2

Nom :    client-7.labomicrosoft.lan
Address:  172.16.16.16

> _
```

Utiliser nslookup

JFA 62

R 2.05

- Lorsque l'on tape une adresse IP, nslookup renvoie le nom de domaine pleinement qualifié correspondant et indique éventuellement si la réponse fait ou non autorité sur le domaine. Dans l'exemple ci-à-droite, lorsque l'on l'adresse IP 172.16.16.15, le serveur DNS nommé dns-2.labomicrosoft.lan renvoie le nom de domaine pleinement qualifié client-6.labomicrosoft.lan.

```
> 172.16.16.15
Serveur :  dns-2.labomicrosoft.lan
Address:  172.16.16.2

Nom :    client-6.labomicrosoft.lan
Address:  172.16.16.15

> _
```

Utiliser nslookup sous Windows

JFA 63

Par exemple sur Windows la commande nslookup est disponible via l'invite de commande :

R 2.05

```
> nslookup www.google.fr
Serveur : Livebox-6370
Address: 192.168.1.1
Réponse ne faisant pas autorité :
Nom : www.l.google.com
Adresses:
      209.85.229.104
      209.85.229.106
      209.85.229.103
      209.85.229.147
      209.85.229.105
      209.85.229.99
Alias: www.google.fr
       www.google.com
```

dig sur les systèmes UNIX :

JFA 64

R 2.05

```
> dig www.google.com aaaa
; <<>> DiG 9.7.0-P1 <<>> www.google.com aaaa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47055
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 4, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com.                        IN      AAAA
;; ANSWER SECTION:
www.google.com.         422901  IN      CNAME   www.l.google.com.
www.l.google.com.       77      IN      AAAA    2a00:1450:8004::67
www.l.google.com.       77      IN      AAAA    2a00:1450:8004::68
www.l.google.com.       77      IN      AAAA    2a00:1450:8004::69
www.l.google.com.       77      IN      AAAA    2a00:1450:8004::6a
www.l.google.com.       77      IN      AAAA    2a00:1450:8004::93
www.l.google.com.       77      IN      AAAA    2a00:1450:8004::63
;; AUTHORITY SECTION:
google.com.             155633  IN      NS      ns2.google.com.
google.com.             155633  IN      NS      ns1.google.com.
google.com.             155633  IN      NS      ns3.google.com.
google.com.             155633  IN      NS      ns4.google.com.

;; Query time: 0 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sun May 23 16:23:49 2010
;; MSG SIZE rcvd: 292
```

Le Service NAT : Principe du NAT :

JFA 65

R 2.05

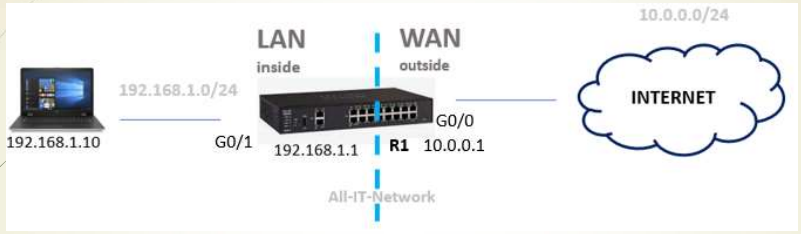
- Le mécanisme de translation d'adresses NAT (*Network Address Translation*) a été mis au point afin de répondre à la pénurie d'adresses IP avec le protocole IPv4.
  En effet, en adressage IPv4 le nombre d'adresses IP routables (donc uniques sur la planète) n'est pas suffisant pour permettre à toutes les machines le nécessitant d'être connectées à internet.
- Le principe du NAT consiste donc à utiliser une passerelle de connexion à internet, possédant au moins une interface réseau connectée sur le réseau interne et au moins une interface réseau connectée à Internet (possédant une adresse IP routable), pour connecter l'ensemble des machines du réseau.
- La translation d'adresses sert à faire correspondre une adresse IP à une autre adresse IP. La translation d'adresses permet de gagner en sécurité, vos adresses IP peuvent être dissimulées mais elle permet aussi un gain du nombre d'adresses IP grâce au PAT,

Le Service NAT : Translation d'adresses

JFA 66

R 2.05

- **Adresse IP Privée**
- **Adresse IP Publique**

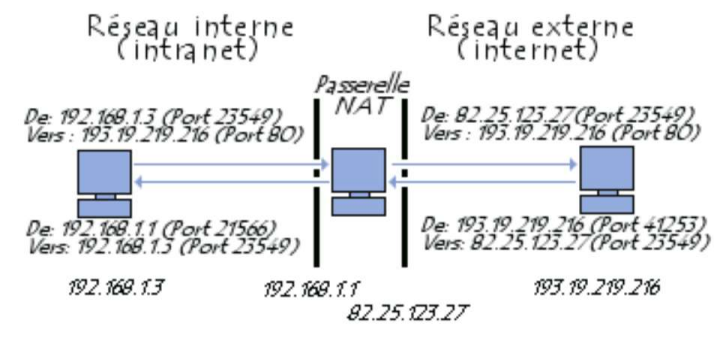


Le Service NAT : Translation d'adresses

JFA 68

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- Ainsi, chaque machine du réseau nécessitant d'accéder à internet est configurée pour utiliser la passerelle NAT (en précisant l'adresse IP de la passerelle dans le champ « Gateway » de ses paramètres TCP/IP). Lorsqu'une machine du réseau effectue une requête vers Internet, la passerelle effectue la requête à sa place, reçoit la réponse, puis la transmet à la machine ayant fait la demande.



http://www.commentcamarche.net/contents/527-nat-translation-d-adresses-port-forwarding-et-port-triggering

Le Service NAT : Translation d'adresses

JFA 69

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- Étant donné que la passerelle camoufle complètement l'adressage interne d'un réseau, le mécanisme de translation d'adresses permet d'assurer une fonction de sécurisation. En effet, pour un observateur externe au réseau, toutes les requêtes semblent provenir de l'adresse IP de la passerelle.

Le Service NAT : Translation d'adresses

JFA 70

R 2.05

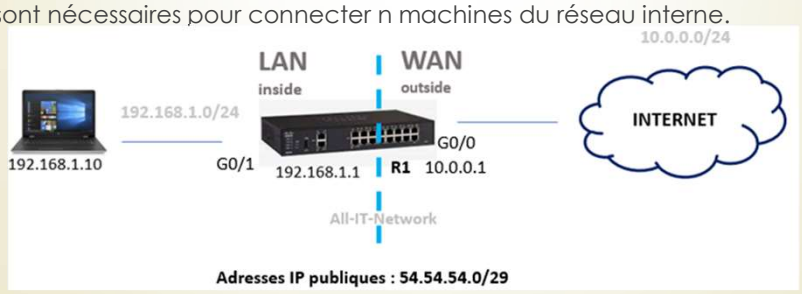
- ***Espaces d'adressage :***
- L'organisme gérant l'espace d'adressage public (adresses IP routables) est l'Internet Assigned Number Authority (IANA). La RFC 1918 définit un espace d'adressage privé permettant à toute organisation d'attribuer des adresses IP aux machines de son réseau interne sans risque d'entrer en conflit avec une adresse IP publique allouée par l'IANA. Ces adresses dites non-routables correspondent aux plages d'adresses suivantes :
  - Classe A : plage de 10.0.0.0 à 10.255.255.255 ;
  - Classe B : plage de 172.16.0.0 à 172.31.255.255 ;
  - Classe C : plage de 192.168.0.0 à 192.168.255.255 ;
- Toutes les machines d'un réseau interne, connectées à internet par l'intermédiaire d'un routeur et ne possédant pas d'adresse IP publique doivent utiliser une adresse contenue dans l'une de ces plages. Pour les petits réseaux domestiques, la plage d'adresses de 192.168.0.1 à 192.168.0.255 est généralement utilisée.

Le Service NAT : Translation statique :

JFA 71

R 2.05

- Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée (par exemple 192.168.0.1) une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.
- La translation d'adresse statique permet ainsi de connecter des machines du réseau interne à internet de manière transparente mais ne résout pas le problème de la pénurie d'adresse dans la mesure où n adresses IP routables sont nécessaires pour connecter n machines du réseau interne.

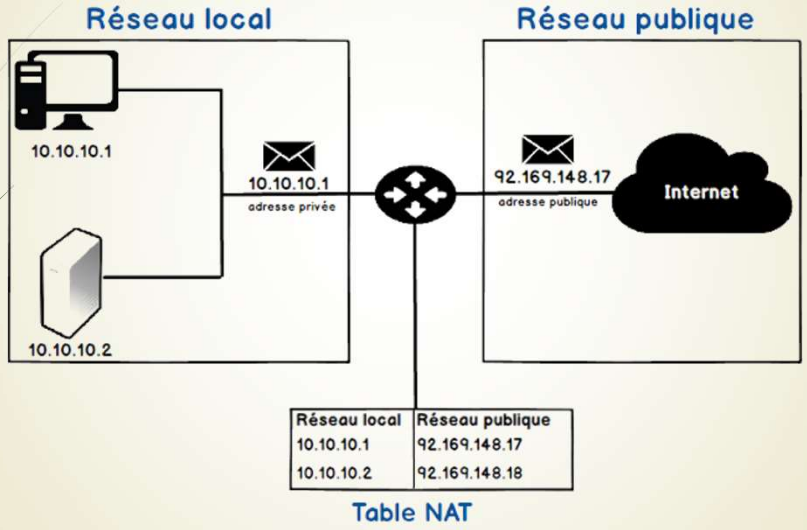


192.168.1.10 <=> 54.54.54.1

Le Service NAT : Translation statique :

JFA 72

R 2.05



https://waytolearnx.com/2018/07/difference-entre-nat-et-pat.html

Avantages et inconvénients du NAT statique :

JFA 73

R 2.05

- En associant une adresse IP publique à une adresse IP privée, nous avons pu rendre une machine accessible sur Internet. Par contre, on remarque qu'avec ce principe, on est obligé d'avoir une adresse publique par machine voulant accéder à Internet. Cela ne va pas régler notre problème de pénurie d'adresses IP... D'autre part, tant qu'à donner une adresse publique par machine, pourquoi ne pas leur donner cette adresse directement plutôt que de passer par un intermédiaire ? A cette question, on peut apporter plusieurs éléments de réponse. D'une part, il est souvent préférable de garder un adressage uniforme en interne et de ne pas mêler les adresses publiques aux adresses privées. Ainsi, si on doit faire des modifications, changements, interventions sur le réseau local, on peut facilement changer la correspondance entre les adresses privées et les adresses publiques pour rediriger les requêtes vers un serveur en état de marche.
- D'autre part, on gâche un certain nombre d'adresses lorsqu'on découpe un réseau en sous-réseaux (adresse de réseau, adresse de broadcast...), comme lorsqu'on veut créer une DMZ pour rendre ses serveurs publics disponibles. Avec le NAT statique, on évite de perdre ces adresses. Malgré ces quelques avantages, le problème de pénurie d'adresses n'a toujours pas été réglé. Pour cela, on va se pencher sur la NAT dynamique.

Le Service NAT Dynamique

JFA 74

R 2.05

- Le NAT (Network Address Translation) dynamique va lier une ou des adresse(s) IP à d'autres adresses IP externes de façon dynamique. La ou les adresses vont utiliser un pool d'adresses IP défini.
- Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Ainsi, toutes les machines du réseau interne possèdent virtuellement, vu de l'extérieur, la même adresse IP. C'est la raison pour laquelle le terme de « mascarade IP » (en anglais IP masquerading) est parfois utilisé pour désigner le mécanisme de translation d'adresse dynamique.
- La différence avec le NAT statique du chapitre précédent et que le PC ne va pas toujours sortir sur la même adresse IP externe. Avec cette configuration, si vous avez plus d'IP interne que d'IP externe et que les IP du pool externe sont toutes utilisées, les autres clients ne pourront pas sortir. Pour pallier à ce problème, il existe le PAT que nous allons voir après.

Le Service NAT Dynamique

JFA 75

R 2.05

- Afin de pouvoir « multiplexer » (partager) les différentes adresses IP sur une ou plusieurs adresses IP routables, le NAT dynamique utilise le mécanisme de translation de port (**PAT** - Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur.
- Le ***PAT*** (Port Address Translation) va permettre à plusieurs équipements réseaux d'utiliser la même adresse IP externe. La distinction des équipements va se faire grâce à l'ajout d'un numéro de port. Le ***PAT*** est par exemple utilisé par votre BOX, tous les équipements du LAN vont sortir sur la même adresse IP publique:

JFA 76

Définition de PAT

R 2.05

- Le PAT est la traduction d'adresse de port est un type de NAT dynamique grâce auquel la traduction d'adresse peut être configurée au niveau du port, et l'utilisation de l'adresse IP est optimisée. PAT met en correspondance plusieurs adresses locales et ports sources avec une adresse IP publique et un port à partir d'une liste d'adresses IP routables sur le réseau de destination. Ici, l'adresse IP de l'interface est utilisée en combinaison avec le numéro de port et plusieurs hôtes peuvent avoir la même adresse IP avec un numéro de port unique.
- Il utilise une adresse de port source unique sur l'adresse IP globale interne pour identifier des traductions distinctes. Le nombre total de traductions NAT pouvant être exécutées est 65536 car le numéro de port est codé sur 16 bits.

JFA 77

Le Service NAT Dynamique : PAT

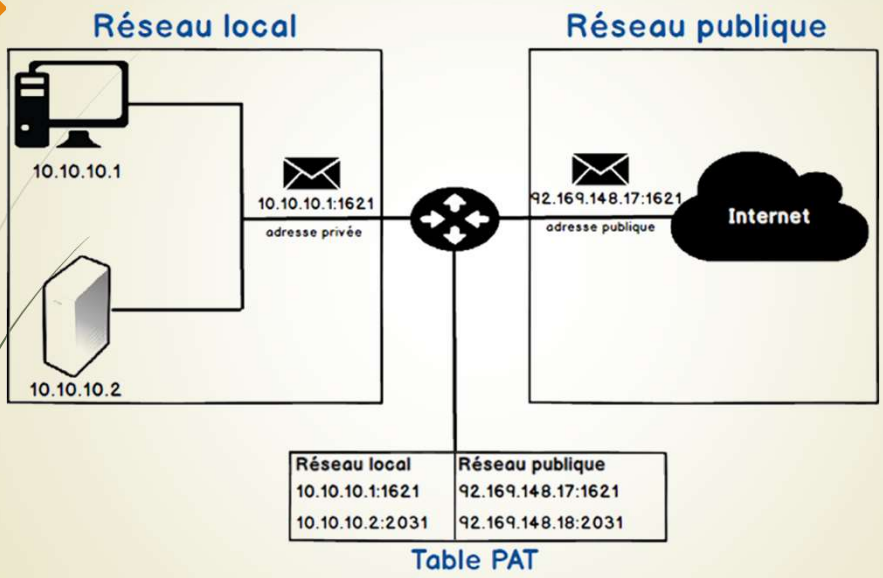
R 2.05

https://all-it-network.com/translation/

Le Service NAT Dynamique : PAT

JFA 78

R 2.05



https://waytolearnx.com/2018/07/difference-entre-nat-et-pat.html

Avantages et inconvénients du NAT dynamique

JFA 79

R 2.05

- Comme nous l'avons vu, le NAT dynamique permet à des machines ayant des adresses privées d'accéder à Internet. Cependant, contrairement au NAT statique, il ne permet pas d'être joint par une machine de l'Internet. Effectivement, si le NAT dynamique marche, c'est parce que le routeur qui fait le NAT reçoit les informations de la machine en interne (Adresse IP, port TCP/UDP). Par contre, il n'aura aucune de ces informations si la connexion est initialisée de l'extérieur... Le paquet arrivera avec comme adresse de destination le routeur, et le routeur ne saura pas vers qui rediriger la requête en interne.
- La NAT dynamique ne permet donc que de sortir sur Internet, et non pas d'être joignable. Il est donc utile pour partager un accès Internet, mais pas pour rendre un serveur accessible. De plus, étant donné que l'on peut "cacher" un grand nombre de machines derrière une seule adresse publique, cela permet de répondre à notre problème de pénurie d'adresses.
- Par contre, les machines n'étant pas accessibles de l'extérieur, cela donne un petit plus au niveau de la sécurité.

Le Service NAT : Port Forwarding

JFA 80

R 2.05

- La translation d'adresse ne permet de relayer que des requêtes provenant du réseau interne vers le réseau externe, ce qu'il signifie qu'il est impossible en tant que tel pour une machine externe d'envoyer un paquet vers une machine du réseau interne. En d'autres termes, les machines du réseau interne ne peuvent pas fonctionner en tant que serveur vis-à-vis de l'extérieur.
- Pour cette raison, il existe une extension du NAT appelée « redirection de port » (en anglais Port Forwarding ou Port mapping) consistant à configurer la passerelle pour transmettre à une machine spécifique du réseau interne, tous les paquets reçus sur un port particulier. Ainsi, si l'on souhaite pouvoir accéder de l'extérieur à un serveur web (port 80) fonctionnant sur la machine 192.168.1.2, il sera nécessaire de définir une règle de redirection de port sur la passerelle, redirigeant tous les paquets TCP reçus sur son port 80 vers la machine 192.168.1.2. .

Le Service NAT : Port Triggering :

JFA 81

R 2.05

- La plupart des applications client-serveur effectuent une requête sur un hôte distant sur un port donné et ouvrent un port en retour pour récupérer les données. Néanmoins, certaines applications utilisent plus d'un port pour échanger des données avec le serveur, c'est le cas par exemple du FTP, pour lequel une connexion est établie par le port 21, mais les données sont transférées par le port 20. Ainsi, avec le mécanisme NAT, après une demande de connexion sur le port 21 d'un serveur FTP distant, la passerelle attend une connexion sur un seul port et refusera la demande de connexion au port 20 du client.
- Il existe un mécanisme dérivé du NAT, appelé « déclenchement de port » (en anglais port triggering), permettant d'autoriser la connexion à certains ports (port forwarding) si une condition (requête) est remplie. Il s'agit donc d'une redirection de port conditionnelle, permettant de ne pas laisser ouvert un port en permanence, mais uniquement lorsqu'une application en a besoin.

Différences clés entre NAT et PAT :

JFA 82

R 2.05

- NAT traduit les adresses locales internes en adresses publique similaires, tandis que le PAT convertit les adresses IP non enregistrées privées en adresses IP publiques enregistrées, mais à la différence de NAT, il utilise également des numéros de port source et plusieurs hôtes peuvent être affectés avec la même adresse IP ayant des numéros de port différents.
- PAT est une forme de NAT dynamique.
- NAT utilise des adresses IP dans le processus de traduction tandis que PAT utilise des adresses IP avec des numéros de port.

Le VPN : réseau Privé

JFA 83

R 2.05

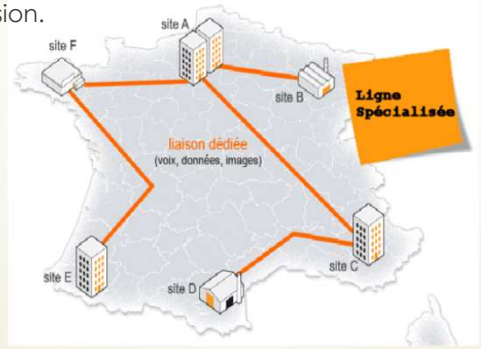
- **Qu'est-ce qu'un VPN ? :**
- Les réseaux locaux d'entreprise (LAN ou RLE) sont des réseaux internes à une organisation, c'est-à-dire que les liaisons entre machines appartiennent à l'organisation. Ces réseaux sont de plus en plus souvent reliés à Internet par l'intermédiaire d'équipements d'interconnexion. Il arrive ainsi souvent que des entreprises éprouvent le besoin de communiquer avec des filiales, des clients ou même du personnel géographiquement éloigné via internet.
- Pour autant, les données transmises sur Internet sont beaucoup plus vulnérables que lorsqu'elles circulent sur un réseau interne car le chemin emprunté n'est pas défini à l'avance, ce qui signifie que les données empruntent une infrastructure réseau publique appartenant à différents opérateurs. Ainsi il n'est pas impossible que sur le chemin parcouru, le réseau soit écouté par un utilisateur indiscret ou même détourné. Il n'est donc pas concevable de transmettre dans de telles conditions des informations sensibles pour l'organisation ou l'entreprise.

Le VPN : réseau Privé

JFA 84

R 2.05

- La première solution pour répondre à ce besoin de communication sécurisé consiste à relier les réseaux distants à l'aide de liaisons spécialisées. Toutefois la plupart des entreprises ne peuvent pas se permettre de relier deux réseaux locaux distants par une ligne spécialisée, il est parfois nécessaire d'utiliser Internet comme support de transmission.



Le VPN : réseau Privé

JFA 85

R 2.05

- Un bon compromis consiste à utiliser Internet comme support de transmission en utilisant un protocole d'"encapsulation" (en anglais tunneling, d'où l'utilisation impropre parfois du terme "tunnelisation"), c'est-à-dire encapsulant les données à transmettre de façon chiffrée. On parle alors de réseau privé virtuel (noté RPV ou VPN, Virtual Private Network) pour désigner le réseau ainsi artificiellement créé.
- Ce réseau est dit virtuel car il relie deux réseaux "physiques" (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent "voir" les données.
- Le système de VPN permet donc d'obtenir une liaison sécurisée à moindre coût, si ce n'est la mise en œuvre des équipements terminaux. En contrepartie il ne permet pas d'assurer une qualité de service comparable à une ligne louée dans la mesure où le réseau physique est public et donc non garanti. .

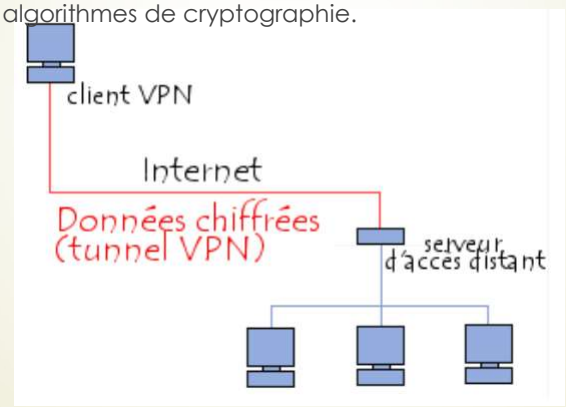
Le VPN : Fonctionnement d'un VPN

JFA 86

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Un réseau privé virtuel repose sur un protocole, appelé **protocole de tunnelisation** (*tunneling*), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie.



Le VPN : Fonctionnement d'un VPN

JFA 87

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Le terme de "tunnel" est utilisé pour symboliser le fait qu'entre l'entrée et la sortie du VPN les données sont chiffrées (cryptées) et donc incompréhensible pour toute personne située entre les deux extrémités du VPN, comme si les données passaient dans un tunnel. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de l'organisation.
- De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A réception sur le client VPN de l'utilisateur, les données seront déchiffrées, puis transmises à l'utilisateur ...

Le VPN : Les protocoles de tunnelisation

JFA 88

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Les principaux protocoles de tunneling sont les suivants :

- PPTP (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'*IETF* (RFC 2661) pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IPSec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

Le VPN : Les protocoles de tunnelisation

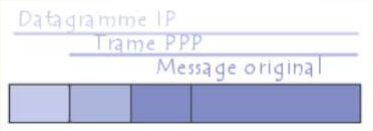
JFA 89

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Le protocole PPTP :

- Le principe du protocole PPTP (Point To Point Tunneling Protocol) est de créer des trames sous le protocole PPP et de les encapsuler dans un datagramme IP.
- Ainsi, dans ce mode de connexion, les machines distantes des deux réseaux locaux sont connectées par une connexion point à point (comprenant un système de chiffrement et d'authentification, et le paquet transite au sein d'un datagramme IP.



- De cette façon, les données du réseau local (ainsi que les adresses des machines présentes dans l'en-tête du message) sont encapsulées dans un message PPP, qui est lui-même encapsulé dans un message IP.

Le VPN : Les protocoles de tunnelisation

JFA 90

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

Le protocole L2TP :

- Le protocole L2TP est un protocole standard de tunnelisation (standardisé dans un RFC) très proche de PPTP. Ainsi le protocole L2TP encapsule des trames protocole PPP, encapsulant elles-mêmes d'autres protocoles (tels que IP, IPX ou encore NetBIOS).

Le VPN : Les protocoles de tunnelisation

JFA 91

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

Le protocole IPSec :

- IPSec est un protocole défini par l'IETF permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.
- Le protocole IPSec est basé sur trois modules :
  - *IP Authentification Header* (**AH**) concernant l'intégrité, l'authentification et la protection contre le rejeu des paquets à encapsuler,
  - *Encapsulating Security Payload* (**ESP**) définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejeu.
  - *Security Assocation* (**SA**) définissant l'échange des clés et des paramètres de sécurité. Les SA rassemblent ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP (les protocoles AH et/ou ESP, mode tunnel ou transport, les algorithmes de sécurité utilisés par les protocoles, les clés utilisées,...). L'échange des clés se fait soit de manière manuelle soit avec le protocole d'échange IKE (la plupart du temps), qui permet aux deux parties de s'entendre sur les SA.

JFA 92

Les notions des Qualité de Services

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Le terme de QoS (Quality of Service) désigne la capacité à fournir un service :

- en temps de réponse,
- en bande passante,
- À garantir un niveau acceptable de perte de données, pour un usage donné,

En effet contrairement à un circuit dédié, il est impossible de prédire le chemin et le temps mis pour un paquet de données pour traverser et parcourir un réseau de données.

JFA 93

Les niveaux de Services

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Le terme « **niveau de service** » (*Service level*) définit le niveau d'exigence pour la capacité d'un réseau à fournir un service point à point ou de bout en bout avec un trafic donné. On définit généralement trois niveaux de QoS :

- **Meilleur effort** (*best effort*), ne fournissant aucune différenciation entre plusieurs flux réseaux et ne permettant aucune garantie. Ce niveau de service est ainsi parfois appelé *lack of QoS*.
- **Service différencié** (*differenciated service* ou *soft QoS*), permettant de définir des niveaux de priorité aux différents flux réseau sans toutefois fournir une garantie stricte.
- **Service garanti** (*guaranteed service* ou *hard QoS*), consistant à réserver des ressources réseau pour certains types de flux. Le principal mécanisme utilisé pour obtenir un tel niveau de service est RSVP (*Resource reSerVation Protocol, Protocole de réservation de ressources*).

JFA 94

Les critères de qualité de service

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

Les principaux critères permettant d'apprécier la qualité de service sont les suivants :

- **Débit** (*Bandwidth*), parfois appelé *bande passante* par abus de langage, il définit le volume maximal d'information (bits) par unité de temps.
- **Gigue** (*Jitter*) : elle représente la fluctuation du signal numérique, dans le temps ou en phase.
- **Latence**, **délai** ou **temps de réponse** (*Delay*) : elle caractérise le retard entre l'émission et la réception d'un paquet.
- **Perte de paquet** (*Packet Loss*): elle correspond à la non-délivrance d'un paquet de données, la plupart du temps due à un encombrement du réseau.
- **Dé séquencement** (*Desequencing*) : il s'agit d'une modification de l'ordre d'arrivée des paquets.

JFA 95

Protocole HTTP

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- **Qu'est-ce que le HTTP ?**
  - Chaque adresse Internet commence par « http:// » (ou « https:// »). Ceci renvoie au protocole HTTP utilisé par votre navigateur Web pour consulter un site Internet. Nous vous présentons le concept de HTTP, vous expliquons les différences entre les versions et vous montrons à quels autres concepts le HTTP est associé.
- **Que signifie HTTP ?**
  - HTTP signifie « Hypertext Transfer Protocol ». Ce protocole a été développé par Tim Berners-Lee au CERN (Suisse) avec d'autres concepts qui ont servi de base à la création du World Wide Web : le HTML et l'URI. Alors que le HTML (Hypertext Markup Language) définit comment un site Internet est construit, le HTTP détermine comment la page est transmise du serveur au client. Le troisième concept, l'URL (Uniform Resource Locator), fixe la façon dont une ressource (par exemple un site Internet) doit être adressée sur le Web.
  - Mais que signifie exactement « hypertexte », ce terme qui revient dans les abréviations HTTP et HTML ? Il s'agit d'un concept que nous connaissons tous et qui désigne le fait de mettre en lien des fichiers. Les sites Internet contiennent en effet des hyperliens renvoyant à d'autres pages Web..

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 96

R 2.05

- **À quoi sert le protocole HTTP ?**
  - Lorsque vous saisissez une adresse Internet dans votre navigateur Web et qu'un site vous est affiché quelques secondes plus tard, cela signifie qu'une communication a été établie entre votre navigateur et le serveur Web via HTTP. On peut donc dire que le HTTP est la langue dans laquelle votre navigateur Web parle au serveur Web afin de lui communiquer ce qui est demandé.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 97

R 2.05

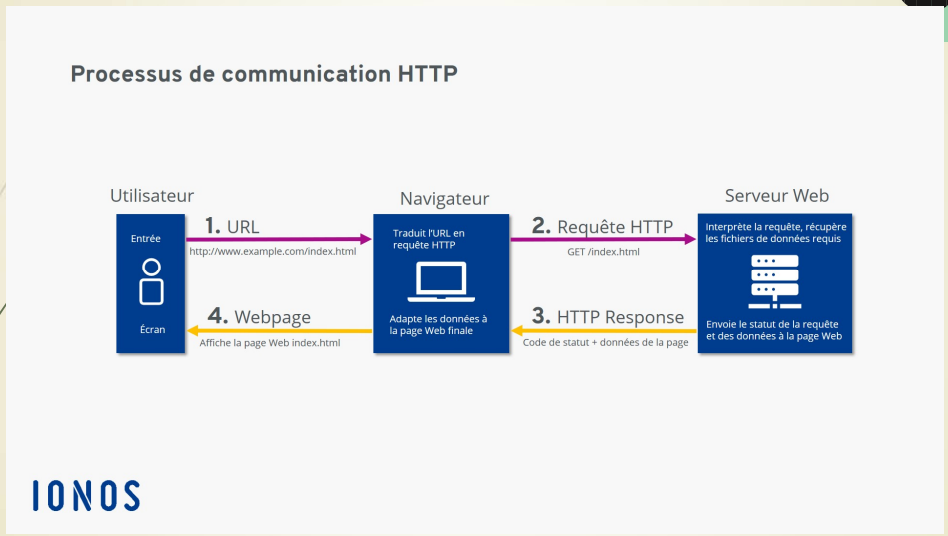
- **Comment fonctionne le HTTP ?**
  - Le fonctionnement du HTTP peut être expliqué très simplement à travers la consultation d'un site Internet :
    1. L'utilisateur saisit dans la barre d'adresse de son navigateur Internet : www.jfanne.fr
    2. Le navigateur envoie une requête correspondante, appelée requête HTTP, au serveur Web qui administre le domaine jfanne.fr. Normalement, cette requête est de type : « Merci de m'envoyer le fichier ». Mais le client peut également se contenter de demander : « As-tu ce fichier ? ».
    3. Le serveur Web reçoit la requête HTTP, cherche le fichier désiré (dans l'exemple : la page d'accueil de www.jfanne.fr, c'est-à-dire le fichier index.html) et envoie dans un premier temps l'en-tête qui informe le client à l'origine de la requête du résultat de sa recherche à l'aide d'un code de statut. Vous trouverez des détails concernant les codes de statut après.
    4. Si le fichier a été trouvé et si le client demande à l'obtenir (c'est-à-dire si le client ne souhaite pas uniquement savoir s'il existe), après l'en-tête, le serveur envoie le corps du message, à savoir le contenu à proprement parler. Dans notre exemple, il s'agit du fichier index.html.
    5. Le navigateur reçoit le fichier et l'affiche sous forme de page web.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 98

R 2.05



https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 99

R 2.05

- **Dans quel contexte le HTTP est-il utilisé ?**
  - À l'origine, le HTTP servait uniquement à demander un document HTML à un serveur Web. Aujourd'hui, ce protocole est utilisé de façons très diverses :
    - Le HTTP permet au navigateur de demander tous les types de médias utilisés sur les sites Internet modernes : texte, images, vidéos, code source, etc.
    - Les applications utilisent par ailleurs le HTTP pour charger des fichiers et des mises à jour de serveurs distants.
    - Le HTTP intervient également dans les API REST, une solution permettant de contrôler les services Web.
    - WebDAV est une autre technologie basée sur le HTTP.
    - Dans la communication de machine à machine, le HTTP est utilisé comme protocole pour la communication entre les services Web.
    - Le HTTP est également utilisé par les lecteurs de médias.
    - Les accès à une base de données en ligne, c'est-à-dire les opérations CRUD, peuvent également avoir lieu grâce au HTTP.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 100

- **La version initiale : HTTP/1**

En 1996, la version HTTP/1 fut décrite par l'Internet Engineering Task Force (IETF) dans le mémo RFC1945, mais elle n'était alors qu'une proposition non contraignante. Un en-tête fut ajouté afin de pouvoir spécifier aussi bien la requête du client que la réponse du serveur. Le champ d'en-tête « Content-Type », qui permet de transmettre d'autres fichiers que des documents HTML, a notamment été introduit. Pour résumer, cette version du HTTP présentait les propriétés suivantes :

- **Sans connexion :** le client établit la connexion avec le serveur, il présente sa requête à laquelle le serveur répond, puis la connexion est coupée. Pour la requête suivante, le client doit à nouveau établir la connexion. Ce processus est lourd car une page Web se compose généralement de plusieurs fichiers, et chacun d'entre eux doit être « récupéré » à l'aide d'une requête indépendante.
- **Sans statut :** les deux côtés, client et serveur, s'« oublient » mutuellement, immédiatement. Lorsque le client se reconnecte au serveur, ce dernier ne sait pas que le client lui a déjà envoyé une requête.
- **Indépendant du média :** le HTTP permet de transmettre n'importe quel type de fichier dans la mesure où les deux côtés savent comment ils doivent traiter le type de fichier en question.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 101

- **Le premier standard officiel : HTTP/1.1**

En 1997, la version HTTP/1.1, décrite dans le mémo RFC2068, a fait son apparition. Elle fut considérée comme le premier standard « officiel » et est encore utilisée aujourd'hui. Elle a apporté d'importantes nouveautés par rapport au HTTP/1 :

- **Keepalive :** le client a la possibilité de maintenir la connexion au-delà d'une requête (persistent connection) en envoyant un keepalive (littéralement « maintenir en vie ») dans l'en-tête de sa requête.
- **Le HTTP-Pipelining** permettant au client d'envoyer la requête suivante avant d'avoir reçu la réponse à la première requête.
- Dans les **chats**, le navigateur peut actualiser la fenêtre en utilisant le type MIME multipart/replace.
- Il est également possible de transmettre des données **du client au serveur**.
- La nouvelle **méthode TRACE** introduite permet de suivre le chemin du client au serveur Web.
- **Cache :** de nouveaux mécanismes pour mettre des contenus en mémoire tampon sont disponibles.
- **Host :** grâce à une spécification correspondante dans l'en-tête (host), les requêtes HTTP fonctionnent également lorsque plusieurs domaines différents sont hébergés sous une même adresse IP, comme c'est le cas aujourd'hui pour la majorité des sites Internet (Shared Webhosting).

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 102

R 2.05

- **HTTP/2 : une refonte bien nécessaire**

Au fil des ans, les sites Internet n'ont cessé de gagner en taille et en complexité. Pour être en mesure de charger un site Internet moderne dans un navigateur, celui-ci doit demander plusieurs mégaoctets de données et envoyer jusqu'à cent requêtes HTTP différentes. Comme le HTTP/1.1 prévoit que les requêtes soient traitées les unes après les autres dans une même connexion, plus un site Internet est complexe, plus l'établissement de la page demande du temps.

C'est pourquoi Google a développé un nouveau protocole expérimental intitulé **SPDY** (prononcé « Speedy »). Ce dernier a suscité un vif intérêt dans la communauté des développeurs et a abouti en 2015 à la publication de la version HTTP/2 du protocole. Ce nouveau standard apporte notamment des nouveautés ayant toutes pour objectif d'accélérer le chargement des sites Internet :

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 103

R 2.05

- **Binaire :** le protocole est basé sur des données binaires plutôt que sur des fichiers texte.
- **Multiplexe :** le client et le serveur peuvent envoyer et/ou traiter plusieurs requêtes HTTP en parallèle.
- **Compression :** les en-têtes sont compressés ; comme ils sont souvent quasiment identiques dans de nombreuses requêtes HTTP, la compression évite les redondances inutiles.
- **Serveur Push :** lorsque le serveur est en mesure de prévoir les données dont le client aura encore besoin, il peut les lui envoyer d'emblée dans une mémoire cache client – sans nécessité de requête HTTP préalable.

Le HTTP/2 pourrait rapidement devenir la norme ; les sites Internet présentant un trafic important n'ont en particulier pas attendu pour passer à cette nouvelle version. En mai 2022, on notait près de 46 % des sites Internet utilisant la version HTTP/2 selon les données de W3Techs :

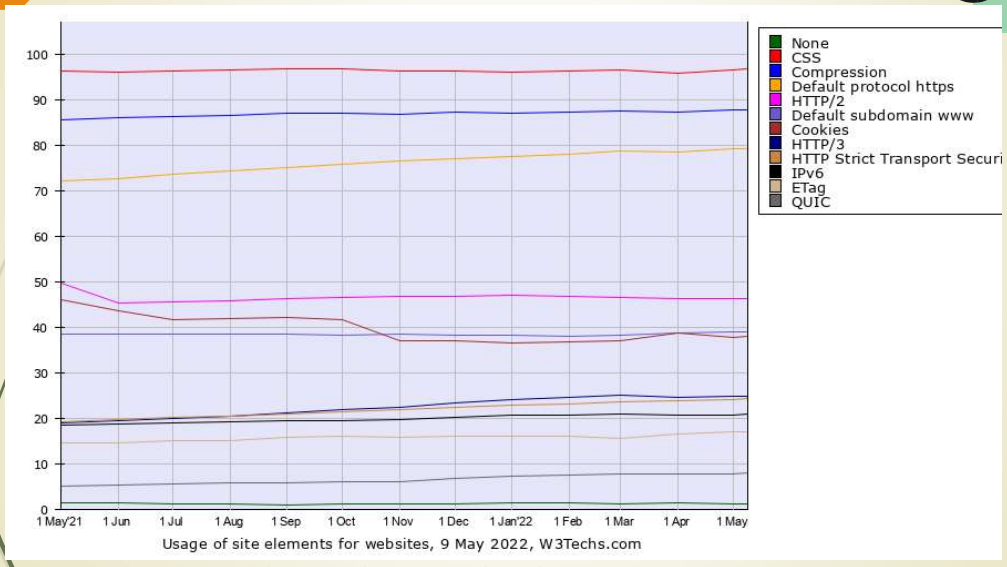
https://w3techs.com/technologies/history_overview/site_element/all

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 104

R 2.05



https://w3techs.com/diagram/history_overview/site_element/all/m

Protocole HTTP

JFA 105

R 2.05

- **L'avenir : le HTTP/3**

- Dans toutes les anciennes versions du protocole HTTP, le protocole de transport TCP sous-jacent constituait l'un des points faibles. Ce dernier exige que le destinataire de chaque paquet de données donne confirmation avant de pouvoir envoyer le paquet suivant. Mais si un paquet est perdu, tous les autres paquets doivent attendre que le paquet perdu soit à nouveau transféré. Dans ce cas, les experts parlent de « head-of-line blocking ».
- Par conséquent, le nouveau HTTP/3 ne doit plus reposer sur TCP mais sur UDP, qui ne nécessite aucune mesure corrective de ce type. Le protocole QUIC (Quick UDP Internet Connections) a été développé à partir du protocole UDP et doit servir de base au HTTP/3.
- Pour le moment, le HTTP/3 n'a pas encore été définitivement adopté par l'IETF. Mais d'après W3Techs, près de 25% des sites Internet utilisent QUIC ou le HTTP/3.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/definition-protocole-http/

Protocole HTTP

JFA 106

R 2.05

- **Codes de statut HTTP :**
- Les administrateurs de sites ont l'obligation de limiter les pages d'erreur HTML au minimum s'ils veulent garantir aux internautes une navigation agréable. Cela vaut particulièrement pour les boutiques en ligne et les sites d'informations dont les contenus varient constamment. Si une page n'existe plus, le navigateur affichera à l'utilisateur le code de statut **404** (introuvable). Souvent, ce phénomène incite les internautes à chercher autre part sur la Toile et à se rendre chez les sites concurrents. Il va donc de l'intérêt des éditeurs de sites Internet de prendre des mesures pour retenir les internautes sur leurs pages. De la même manière, il est difficile et long d'identifier les erreurs de type 404. Pour cela, il existe des outils pour webmasters proposés par Google qui permettent d'établir des statistiques de ces erreurs de crawl (d'indexation). Pour contrer les erreurs de type 404, il est bien vu de rediriger la page vers une autre cible. Ces pages d'erreur personnalisées permettent de réduire manuellement le taux d'abandon des internautes.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/apercu-des-codes-de-statut-http-principaux/

Protocole HTTP

JFA 107

R 2.05

- **Des pages d'erreur personnalisées :**
- Etant donné qu'il n'est pas toujours possible d'empêcher l'apparition des erreurs de type 404, il est conseillé de relier la page en question à un message personnalisé. Cette action est possible grâce au fichier de configuration .htaccess. En général, les messages 404 conservent le design du site Internet et proposent aux internautes d'autres informations, produits voire un aperçu global de l'offre du site. Voici des astuces .htaccess pour savoir comment relier ces pages d'erreur.

```
# Votre message d'erreur de l'emplacement local
ErrorDocument 404 / erreur/404.html
```

Si la page d'erreur se trouve au niveau supérieur du répertoire racine ou d'une URL externe, l'URL complète peut aussi être incorporée dans le .htaccess qui se trouve dans ce cas dans le répertoire racine :

```
# Votre message d'erreur de l'emplacement externe
ErrorDocument 404 / http://www.nom-de-votre-site.com/erreur/404.html
```

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/les-meilleures-astuces-htaccess/

Protocole HTTP

JFA 108

R 2.05

- **Que signifie un code de statut HTTP pour le moteur de recherche ?**
- Certains codes de statut HTTP sont très importants pour votre référencement. Le code 404, par exemple, indique non seulement au navigateur de l'internaute que la page est introuvable, mais aussi aux moteurs de recherche qui ne peuvent pas indexer la page. De la même manière que pour les visiteurs, les robots d'indexation se laissent rediriger vers les nouveaux liens cibles. Pour des raisons de SEO, le code HTTP 301 permet également de maintenir le PageRank du site à un niveau élevé. Si le robot d'indexation tombe sur une page contenant un code HTTP 301, celui-ci prendra en compte la redirection et effacera l'ancienne page de son index de recherche.
- Le niveau de PageRank de l'ancienne page n'est pas perdu mais transférée vers une autre page cible grâce au code HTTP 301. Ce processus est pertinent avant tout si l'ancienne page est la cible des liens entrants. Ainsi, l'autorité et la force acquise peuvent être transmises vers le site suivant. Le code de statut HTTP 302 entraîne un tout autre processus. En effet, le transfert n'est que temporaire, ce qui implique que la vieille adresse demeure indexée. Dans ce cas, le pouvoir des liens retour éventuels n'est pas transféré à la cible..

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/les-meilleures-astuces-htaccess/

Protocole HTTP

JFA 109

R 2.05

- **Les codes de statut HTTP et leur signification :**
- le navigateur Internet (aussi nommé « client ») démarre une requête sur le serveur, celui-ci répond avec un code de statut HTTP sous la forme d'un nombre à trois chiffres. A travers ce message, le serveur Internet nous informe si une requête est bien traitée, si une erreur est présente ou si l'authentification est nécessaire. Ainsi, le code de statut HTTP est une partie essentielle de la réponse transmise par le serveur Internet. Celui-ci l'intègre automatiquement dans chaque en-tête de réponse HTTP. En général, un utilisateur reçoit des codes de statut sous la forme d'une page HTML automatique si le serveur Web ne peut exécuter la requête du client.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/les-meilleures-astuces-htaccess/

Protocole HTTP

JFA 110

R 2.05

- **Les classes de statuts HTTP :**
- Les codes de statuts HTTP sont divisés en cinq classes différentes toutes déterminées par les premiers chiffres de leurs codes. 200 correspond à la classe 2xx tandis que le 404 correspond à la 4xx. Cette répartition repose sur la signification et la fonction des codes de statut. Voilà comment sont composées ces classes :

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/les-meilleures-astuces-htaccess/

Protocole HTTP

JFA 111

R 2.05

- **Les codes de statut HTTP et leur signification :**
  - **Classe 1xx**, codes d'information : si le code commence par 1, le serveur indique au client que la requête actuelle est en en train de se faire. Cette classe regroupe des codes en cours de traitement et d'envoi.
  - **Classe 2xx**, codes de succès : un code qui commence par 2 indique que la requête a abouti. Elle a été reçue par le client, comprise et acceptée. En conséquence, les codes 2xx du serveur sont envoyés en même temps que les informations des pages Web désirées. En général, l'utilisateur ne prend en compte que la page Web qu'il a chargé.
  - **Classe 3xx**, codes de redirection : un code 3xx indique que la requête a été reçue par le serveur. Cependant, le client doit encore provoquer une action complémentaire pour que le traitement soit conduit à sa résolution finale. Les codes qui commencent par 3 apparaissent en majorité en cas de transfert.
  - **Classe 4xx**, erreurs du client : le code 4xx renvoie à une erreur commise par le client. Le serveur a reçu la requête mais ne peut pas l'exécuter. En général, il s'agit d'une syntaxe erronée. En général, l'utilisateur est automatiquement dirigé vers une page HTML.
  - **Classe 5xx**, erreurs du serveur : Le code 5xx fait référence à une erreur commise par le serveur. Ces informations indiquent que la requête en question est complètement ou provisoirement impossible. Une page d'erreur HTML est également présentée.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/apercu-des-codes-de-statut-http-principaux/

Protocole HTTP

JFA 112

R 2.05

- **Aperçu des codes de statut HTTP importants :**
- Les codes de statut HTTP sont importants tant pour les administrateurs de sites que pour les professionnels du référencement. Les internautes sont pour leur part plus concernés par les codes d'erreur de client tels que 404 (not found) ou de serveur tels que 503 (service unavailable). En effet, ces pages, générées automatiquement, sont visibles de tous. Par ailleurs, de nombreux codes de statut HTTP ne peuvent être vus du premier coup. Des outils spécifiques ainsi que des extensions sont nécessaires à leur détection par les administrateurs. La découverte de ces erreurs est importante si on veut optimiser l'expérience utilisateur ainsi que le référencement de son site sur le Web. Vous trouverez dans la sélection suivante les codes de réponses les plus courants. Une liste complète est disponible sur le site codes HTTP.

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/les-meilleures-astuces-htaccess/

Protocole HTTP

JFA 113

R 2.05

- **Code HTTP 200**, OK : ce code indique que la requête a été traitée avec succès. Toutes les informations demandées ont été localisées par le serveur Web et ont été transférées au client. L'internaute ne peut normalement pas voir le code.
- **Code HTTP 301**, changement d'adresse définitif : ce code signifie que les informations demandées par le client ne se trouvent plus à l'adresse indiquée car celle-ci a définitivement changée. Etant donné que le lieu actuel du site demandé est aussi livré dans le statut, le navigateur Internet peut aussitôt rediriger l'utilisateur à la nouvelle adresse. L'ancienne adresse n'est plus valable. Ce code 301 est presque invisible pour les internautes car seul l'URL de la barre de saisie change.
- **Code HTTP 302**, changement d'adresse temporaire : contrairement au code 301 qui renvoie à un changement définitif, le code 302 indique que les informations demandées se trouvent temporairement sur une autre page. Dans ce cas de figure, le statut contient des informations pour permettre un transfert automatique. La vielle adresse reste valable.
- **Code HTTP 403**, interdit : le code de statut HTTP 403 signalise au client que l'accès aux contenus désirés est impossible car le client n'en a pas l'autorisation. En général, ce problème d'accès est indiqué à l'internaute via une page HTML automatique.
- **Code HTML 404**, non trouvé : la réponse 404 signifie que la page Internet est introuvable. En général, soit l'adresse n'existe plus, soit aucune redirection n'a été pas établie. L'utilisateur doit alors vérifier si l'adresse est correcte. Les liens qui renvoient à des pages inexistantes sont nommées « liens brisés ».
- **Code HTTP 500**, erreur interne du serveur : la réponse 500 sert à annoncer des erreurs inattendues du serveur. Si le serveur ne peut traiter la requête, ce statut HTTP est automatiquement affiché. Au-delà de la réponse du client, le serveur réalise en général un protocole d'erreur interne. Il faut que l'administrateur du site analyse la page pour pouvoir procéder à la réparation du logiciel.
- **Code HTTP 503**, service indisponible : le code 503 indique que le serveur en question est surchargé. Il se peut que cette réponse du serveur comporte aussi des informations sur le temps de traitement de la page. En règle générale, un utilisateur doit partir du principe qu'un administrateur est en train de travailler sur le problème et que le serveur est bientôt disponible. .

https://www.ionos.fr/digitalguide/hebergement/aspects-techniques/apercu-des-codes-de-statut-http-principaux/

Adressage IPv6

JFA 114

R 2.05

- Enjeux de l'adressage IPv6 (Version 6) :
  - Remplaçant de IPv4 avec une coexistence possible,
  - Peut supporter des milliards d'adresses,
  - Eviter la perte de plages d'adresses IP,
  - Simplifier le protocole de routage pour augmenter la rapidité,
  - Réduire la taille des tables de routage,
  - Faciliter la diffusion multidestinataire,
  - Apporter plus de sécurité et de services,
  - Possibilité de déplacement dans le réseau sans changer d'adresse,
  - Permettre des évolutions futures.

Adressage IPv6

JFA 115

R 2.05

- Les choix effectués :
  - Des adresses sur 128 bits (4 fois IPv4),
  - 2^{128} = 3,4.10^{38} adresses possibles,
  - 665.10^{21} adresses par m^2 de surface de la terre !,
  - Ce qui va permettre :
  - Plusieurs interfaces par hôte,
  - Plusieurs adresses par interface,
  - Différents types d'adresses :
    - Unicast, Multicast, Anycast;
  - des adresses par «fournisseur d'accès», propres à un site (site-local), propres à un lien de communication (link-local);
  - une partie de l'adresse IPv6 peut être l'adresse MAC (IEEE802) => auto-configuration !

Adressage IPv6 sur 128 bits

JFA 116

R 2.05

- Une nouvelle notation :

3FFE:085B:1F1F:0000:0000:0000:00A9:1234

- Une adresse composée en 8 groupes de 16 bits,
  - Séparés par des « : »,
  - Notée en hexadécimal,
  - Les zéros en début de séquence peuvent être omis,
  - Une séquence de zéros peut être omise une seule fois !

3FFE:85B:1F1F::A9:1234

Adressage IPv6 sur 128 bits

JFA 117

R 2.05

- Pour la compatibilité avec IPv4 :
  - on peut laisser les 32 derniers bits en notation IPv4,

    ::192.50.185.25
- Pour l'adresse de Bouclage (LoopBack) :
  - => 0:0:0:0:0:0:0:1 => ::1 ou ::1/128 en CIDR
- Dans une URL, on l'encadre entre crochets :
  - => http://[2001:1:4F3A::206:AE14]:8080/index.html

JFA 118

Décomposition d'une Adressage IPv6

R 2.05

- Comme pour IPv4, une adresse IPv6 peut-être découpée en une partie réseau et une partie hôte.

  <partie réseau>.<partie machine>

- Plusieurs structures d'adresses ont été définies :
  - En divisant en 2 les adresses :
    - les 64 premiers bits désignant la partie réseau,
    - les 64 derniers bits désignant la machine hôte;
  - En utilisant les N premiers bits de la partie réseau (/N) comme un préfixe pour indiquer le type d'adresses (comme IPv4 pour les classes d'adresses).

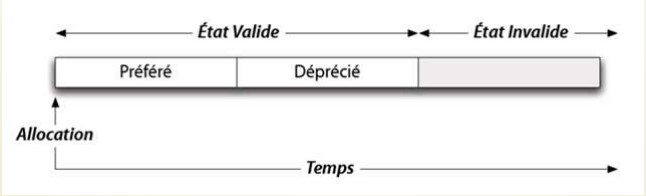
    xxxx:yyyy:: /N

JFA 119

Portée d'une adresse IPv6

R 2.05

- 3 types d'adresses :
  - Unicast : Désigne une interface unique
    - adresse à usage local (Lien local, Site local)
    - adresse globale (Agrégée, Compatible, etc.)
  - Anycast : Désigne un seul membre du groupe
  - Multicast : Désigne un groupe d'interfaces
- Durée de vie d'une Adresse IPv6 :
  - Une adresse IPv6 associée à une interface a une durée de vie de 30 jours par défaut.
  - Elle change d'état au cours du temps :



JFA 120

Préfixes d'une Adresse IPv6

R 2.05

- En IPv6, on définit un certain nombre de préfixes qui permettent de définir les types d'adresses

Adress Type	Type d'adresse	Préfixe binaire	Notation IPv6
Unspecified	Non spécifiée	00……0 (128 bits)	::/128
LoopBack	Bouclage	00…….1 (128 bits)	::1/128
Global Unicast	Globales	001	2000::/3
Unique Local (ULA)	Locales Uniques	1111110	FC00::/7 remplacement
Link Local Unicast	Lien Local Unicast	11111110 10	FE80::/10
Site local Unicast	Locales au site	11111110 11	FEC0::/10 obsolètes
Multicast	Multicast	11111111	FF00::/8

JFA 121

Adresse IPv6 réservée

R 2.05

- Comme en IPv4 certaines adresses sont réservées pour un usage particulier :
- ::/128 ou 0000:0000:0000:0000:0000:0000:0000:0000
  - Adresse non spécifiée. Celle-ci n'est jamais assignée à un hôte mais peut être utilisée comme adresse source dans une phase d'acquisition de l'adresse IPv6.
- ::1/128 ou 0000:0000:0000:0000:0000:0000:0000:0001
  - Adresse de Bouclage (loopback), c'est-à-dire la machine elle-même, équivalent de 127.0.0.1 en IPv4,

Conversion d'Adresse IPv6 en IPv4

JFA 122

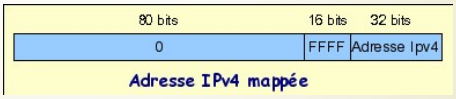
R 2.05

- L'adresse IPv4 mappée :
- Une machine IPv6 doit être capable de communiquer aussi bien avec une machine IPv4 qu'avec une machine IPv6. Elle utilise :
  - des adresses IPv4 mappées pour communiquer avec les autres machines IPv4,
  - utilise des adresses IPv6 « normales » pour communiquer avec les machines IPv6.
- Lors de l'émission d'un paquet vers un destinataire ayant une adresse IPv4 mappée, la machine formate un paquet IPv4 et l'envoie sur le réseau. Elles sont utilisées par des programmes IPv4 et IPv6 mais ne doivent pas se trouver sur le réseau. Ces adresses sont de la forme ::ffff:a.b.c.d.

Par exemple :

::ffff: 147.30.20.10 ou

::ffff:931E:140A

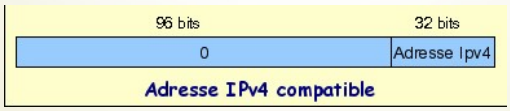


Adresse IPv6 en IPv4

JFA 123

R 2.05

- L'adresse IPv4 compatible : (obsolète)
- Une machine IPv6 communiquant avec une autre machine IPv6 via un tunnel automatique IPv6/IPv4 utilise des adresses IPv4 compatibles. En fait, le paquet IPv6 ayant pour adresse de destination une adresse IPv6 compatible (exemple :: 147.30.20.10) est encapsulé dans un paquet IPv4 ayant pour adresse destination l'adresse IPv4 ex:147.30.20.10 . Le paquet IPv4 peut éventuellement être routé avant d'atteindre son destinataire. Le destinataire recevant le paquet IPv4 retire le paquet IPv6 qui y est encapsulé.
- Ces adresses sont de la forme ::a.b.c.d . Par exemple ::147.30.20.10



Adresse IPv6 unicast : Unique Local Address (ULA)

JFA 124

R 2.05

- fc00::/7
  - Ces adresses sont utilisées pour les communications locales et ne sont routables que sur les sites qui le souhaitent. C'est l'équivalent des plages d'adresses privées de IPv4 (10.0.0.0/8, 172.16.0.0/12 et 192.168.0.0/16) (RFC 4193).
- est divisé en 2 blocs /8
  - Le bloc fc00::/8 n'est pas encore défini !
  - Le bloc fd00::/8 (avec le 8e bit fixé à 1)
    - complété avec une séquence de 40 bits pseudo-aléatoire pour d'éviter les conflits d'adresses identiques, et est donc défini avec un préfixe /48,

      Ex : fd00::/8 + 26:44e1:8c70 = fd26:44e1:8c70 ::/48
    - 16 bits sont réservés pour le sous-réseau.

      Permet 65536 sous-réseaux de taille /64 pour un réseau privé :

      de fd26:44e1:8c70::/64 à fd26:44e1:8c70:ffff::/64.

Adresse IPv6 unicast : Unique Local Address (ULA)

JFA 125

R 2.05

- 64 bits sont réservés pour l'adresse de l'hôte.

  On utilise l'adresse MAC (Interface ID) pour remplir ce champ :

  MAC : b8:27:eb:59:70:f3

  fd26:44e1:8c70:fd00:ba27:ebff:fe59:70f3
- Utilisée par la configuration automatique d'adresses et la découverte de voisins.

- Synthèse :

Préfixe	L	Global ID	Subnet ID	Interface ID
7 bits	1 bit	40 bits	16 bits	64 bits
FC00/7	1	Aléatoire	Sous-réseau	Adresse MAC

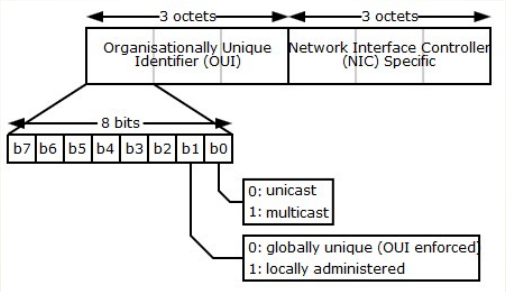
JFA 126

Adresse de l'interface ID : adresse MAC

R 2.05

- Adresse MAC
  - Une adresse MAC est un numéro unique au monde qui est attribué à toute interface réseau.
  - Elle est constituée de 48 bits (6 octets) ou 64 bits (8 octets) notée sous la forme hexadécimale :

5E:FF:56:A2:AF:15



JFA 127

Adresse de l'interface ID : adresse MAC

R 2.05

Ces 48 bits (64 bits) sont répartis de la façon suivante :

- 1 bit I/G : indique si l'adresse est individuelle:
  - le bit sera à 0 (pour une machine unique, unicast) ou
  - le bit sera à 1pour un groupe (multicast ou broadcast) ;
- 1 bit U/L : indique si l'adresse est
  - 0 : universelle (conforme au format de l'IEEE),
  - 1 pour une adresse administrée localement ;
- 22 bits réservés :
  - tous les bits sont à zéro pour une adresse locale,
  - sinon ils contiennent l'adresse du constructeur ;
- 24 bits (40 bits) : adresse unique (pour différencier les différentes cartes réseaux d'un même constructeur).

JFA 128

Conversion de l'interface ID en Adresse IPv6

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

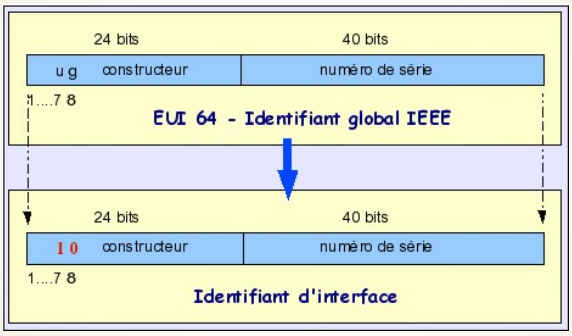
- *1er cas: Format EUI-64 de l'EEE : (standard revisité)*
  - Les **24** premiers bits identifient toujours par un numéro le constructeur de la carte réseau et
  - les **40** derniers bits identifient par un numéro de série la carte fabriquée par ce constructeur.
- Le concept du bit "u" et "g" est repris au standard EUI-48 et est identique.
  - Si le bit u=0, il s'agit d'un identifiant universel,
  - Si le bit u=1, il s'agit d'un identifiant local,
  - Si le bit g=0, il s'agit d'une adresse individuelle (unicast), dans ce cas le 1er octet est toujours pair,
  - Si le bit g=1, il s'agit d'une adresse de groupe (multicast), dans ce cas l'octet est impair.
- La construction de l'identifiant de l'adresse IPv6 est alors simple, il suffit de reprendre entièrement ces 64 bits et d'inverser le bit "u" en lui attribuant la valeur "1".

JFA 129

Conversion de l'interface ID en Adresse IPv6

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- *Synthèse de construction :*



JFA 130

Conversion de l'interface ID en Adresse IPv6

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

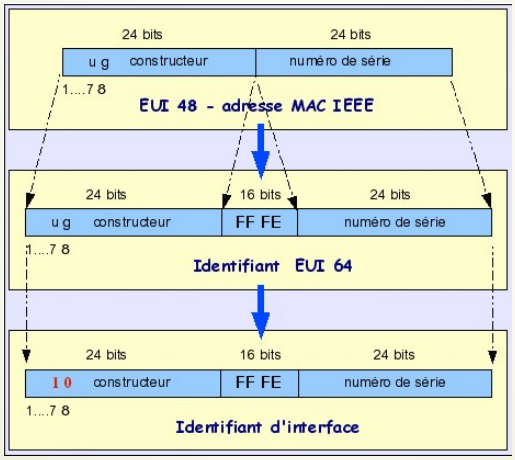
- 2ème ***cas: Format EUI-48 de l'EEE :***
  - C'est le cas de nos cartes réseaux Ethernet actuelles. L'identifiant d'interface IPv6 va donc être conçu à partir de l'adresse Mac.
  - On va donc recourir à une petite astuce qui consiste à rajouter les 16 bits manquants entre les 24 premiers bits (qui identifient par un numéro le constructeur de la carte réseau) et les 24 derniers bits (qui identifient le numéro de série de cette carte fabriquée par ce constructeur).
  - Les 16 bits rajoutés ont pour valeur: **FFFE**.

JFA 131

Conversion de l'interface ID en Adresse IPv6

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- ***Synthèse de construction :***

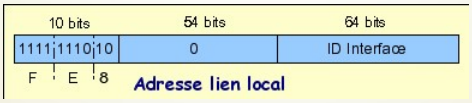


JFA 132

Adresse IPv6 unicast : Link-Local (ULL)

R 2.05

- fe80::/10
  - Les adresses de lien local (utilisables uniquement au sein d'un réseau local, non routables) appartiennent à fe80::/64.
  - La validité de ces adresses est restreinte à un lien, c'est-à-dire à l'ensemble de interfaces directement connectées sans routeur intermédiaire, Elles sont configurées automatiquement à l'initialisation de l'interface et permettent la communication entre nœuds voisins.
  - Ces adresses sont utilisées par les protocoles de configuration d'adresse globale, de découverte de voisins (*neighbor discovery*) et de découverte de routeurs (*router discovery*).
  - L'adresse est obtenue en concaténant le préfixe FE80::/64 aux 64 bits de l'identifiant d'interface (MAC Address).



JFA 133

Adresse IPv6 unicast Link-Local (ULL)

R 2.05

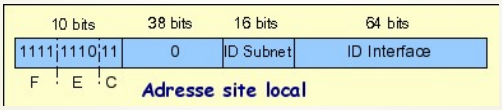
- Elles désignent une et une seule machine.
- Elles comportent une partie réseau "préfixe" et une partie hôte "suffixe":
- **La partie réseau ou préfixe** est codée sur 64 bits : les 48 bits **publics** "Global Routing Prefix" et les 16 bits de **site** définissant le **sous-réseau**
- **La partie hôte ou suffixe** est codée aussi sur 64 bits, fabriquée à partir de l'adresse MAC de l'interface, elle permet d'identifier la machine dans un réseau donné.
- Prenons par exemple cette adresse **fe80::ba27:ebff:fe59:70f3**
  - **fe80::** ,en réalité **fe80:0000:0000:0000** correspond au préfixe ou partie réseau
  - **ba27:ebff:fe59:70f3** correspond au suffixe ou partie hôte

Adresse IP v6 de site local (Obsolète)

JFA 134

R 2.05

- fec0::/10
  - Cette adresse de site local est restreinte au site. Par exemple un site non relié sur Internet.
  - L'idée consiste à reprendre le concept des adresses IPv4 confinées au site et ne pouvant être routées sur internet (par exemple les adresses 10.0.0.0 /8, 172.16.0.0 /12 et 192.168.0.0 /16) . Un routeur de sortie de site ne doit pas router ce type d'adresse.

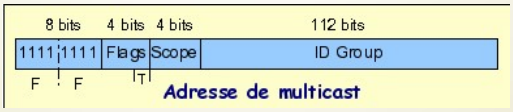


Adresse IP v6 multicast

JFA 135

R 2.05

- ff00::/8
  - Cette adresse spécifie un groupe d'interfaces appartenant au groupe de diffusion.
  - Cette adresse peut être permanente (T=0) ou temporaire (T=1), le bit T du champ flags marque cette différence. Les trois premiers bits du champ flags sont nuls (réservés). Typiquement, une vidéo-conférence est temporaire, dans ce cas les membres de ce groupe se verront attribuer ce type d'adresse temporaire avec le T à 1.
  - L'étendue de la diffusion est définie par le champ scope de l'adresse. Pour l'exemple de notre vidéo-conférence, sa diffusion peut être confinée au lien local, au site, ou au-delà selon la valeur du champ scope.



JFA 136

Adresse IP v6 multicast

R 2.05

- ff00::/8
- Les adresses multicast (remplacent les adresses "broadcast" en IP v4 qui était très pénalisante pour toutes les machines se trouvant sur un même lien).
- Une adresse multicast est une adresse désignant un groupe d'interfaces donné. Une interface est libre de s'abonner à un groupe ou de le quitter à tout moment.
- Le format des adresses multicast permanentes est le suivant :
  - ff01:: => nœud local, les paquets ne quittent pas l'interface.
  - ff02:: => lien local, les paquets ne quittent pas le lien .
  - ff03:: => sous-réseau local, les paquets restent dans le sous réseau .
  - ff05:: => site local, les paquets ne quittent pas le site .
  - ff08:: => L'organisation
  - ff0e:: => Global

JFA 137

Adresse IP v6 multicast réservées

R 2.05

- Voici quelques adresses réservées par l'IANA[9] :

Bloc	Description
ff02::1	Tous les hôtes sur un segment
ff02::2	Tous les routeurs sur un segment
ff02::1:FF00:0000/104	*Solicited Node* utilisé par Neighbor Discovery Protocol
ff02::1:2	Tous les agents DHCP sur un segment
ff05::1	Tous les hôtes d'un site
ff0x::fb	Multicast DNS
ff0x::101	Network Time Protocol
ff05::1:3	Tous les serveurs DHCP du réseau local.

Adresse IP v6 multicast Exemple

JFA 138

R 2.05

Voici un exemple intéressant d'utilisation d'adresse multicast qui vous permet de détecter les hôtes actifs sur le lien local :

```
# ping6 -I eth0 ff02::1
  PING ff02::1(ff02::1) from fe80::20e:35ff:fe8f:6c99 eth2: 56 data bytes
  64 bytes from ::1: icmp_seq=1 ttl=64 time=0.048 ms
  64 bytes from fe80::20d:61ff:fe22:3476: icmp_seq=1 ttl=64 time=9.05 ms (DUP!)
  64 bytes from ::1: icmp_seq=2 ttl=64 time=0.045 ms
  64 bytes from fe80::20d:61ff:fe22:3476: icmp_seq=2 ttl=64 time=3.33 ms (DUP!)
  64 bytes from ::1: icmp_seq=3 ttl=64 time=0.037 ms
```

- Vous pouvez identifier 2 hôtes actifs :
  - fe80::20e:35ff:fe8f:6c99 (celui d'où est passée la commande)
  - fe80::20d:61ff:fe22:3476 (qui correspond à un autre poste du réseau local).

Adresse IP v6 multicast sollicité

JFA 139

R 2.05

- Cette adresse est utilisée par une station du réseau qui connaît l'adresse IPv6 d'une station à joindre mais en ignore son adresse physique (Mac). En utilisant l'adresse multicast sollicité, il sera possible de joindre le destinataire. ICMPv6, entre autre, utilise ce type de mécanisme.
- La construction d'une adresse IPv6 multicast sollicité concatène le préfixe **ff02::1:ff00:0 /104** avec les trois derniers octets d'une adresse Mac.

JFA 140

Adresse IP v6 Anycast

R 2.05

- L'adresse anycast est ni plus ni moins qu'une adresse multicast, à la différence qu'un paquet émis avec cette adresse de destination ne sera remis qu'à un seul membre du groupe, même si plusieurs interfaces ont répondu au message de sollicitation des voisins d' ICMPv6. Pour l'instant, une seule adresse anycast est définie et est réservée au routeur mais dans l'avenir, d'autres pourraient être définies.
- La construction d'une adresse IPv6 anycast d'un sous-réseau (la seule définie actuellement) concatène le préfixe du sous réseau de l'interface et la valeur nulle pour la dernière partie de l'adresse.

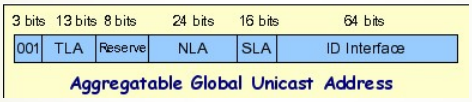
Adresse anycast

JFA 141

Adresse IP v6 Agrégé Globales unicast

R 2.05

- L'adressage IPv6 est structuré en plusieurs niveaux selon un modèle dit "agrégé".
- représente 1/8ème de l'espace adressable total d'IPv6.
- Cette composition devrait permettre une meilleure agrégation des routes et une diminution de la tailles des tables de routage.



Aggregatable Global Unicast Address

Cela permet d'établir un plan d'adressage hiérarchisé en trois niveaux.

1- la topologie publique utilisant 48 bits
2- la topologie de site sur 16 bits
3- la topologie d'interface sur 64 bits.

Les deux premiers niveaux identifient le réseau tandis que le troisième identifie l'hôte sur le réseau.

Adresse IP v6 Agrégé Globales unicast

JFA 142

R 2.05

FP	TLA ID	RES	NLA ID	SLA ID	Interface ID
3 bits	13 bits	8 bits	24 bits	16 bits	64 bits
Topologie Publique				Site	Interface

Ainsi:

1- la topologie publique (48 bits)

- le préfixe 2000::/3 identifie le plan d'adressage agrégé,
- le 13 bits suivants identifient l'unité d'agrégation haute (TLA Top Level Aggregator), assignés aux FAI ou à des zones géographiques,
- les 8 bits suivants sont réservés pour l'évolution de l'adressage. Ces bits pourront être réattribués aux TLA ou NLA dans l'avenir car pour l'instant, ces besoins sont difficilement quantifiables.
- les 24 bits suivants identifient l'unité d'agrégation basse (NLA Next Level Aggregator) assignés à des zones géographiques restreintes (régionales).

Adresse IP v6 Agrégé Globales unicast

JFA 143

R 2.05

2- la topologie de site (16 bits)

- les 16 bits suivants (SLA Site Level Aggregator) sont sous la responsabilité du gestionnaire de site. Cette partie peut être hiérarchisée par le gestionnaire et définir ses propres sous réseaux dans cette plage.

Pour résumer, les 48 premiers bits + les 16 bits suivants identifient la partie réseau de l'adresse IPv6, c'est-à-dire 64 bits,

3- la topologie d'interface site (64 bits)

- les derniers 64 bits identifient l'interface, c'est-à-dire l'hôte sur le réseau identifié par les 64 premiers bits.
- Elle peut être configurée de la façon suivante :
  - Par auto-configuration et en utilisant l'adresse MAC de son interface,
  - Par un nombre pseudo-aléatoire généré automatiquement.
  - Assignée via DHCP.
  - Configurée manuellement.

Adresse IP v6 Agrégé Globales unicast

JFA 144

R 2.05

- Exemples de TLA assignés :

IPv6 Prefix	FP	TLA	Assignment
2000/16	001	0 0000 0000 0000	Reserved
2001::/16	001	0 0000 0000 0001	Assignement du Sub TLA
2002::/16	001	0 0000 0000 0010	« v6tov4 »
3FFE::/16	001	1 1111 1111 1111	6Bone Testing

Adresse IP v6 Globales unicast

JFA 145

R 2.05

Parmi ces adresses, on distingue :

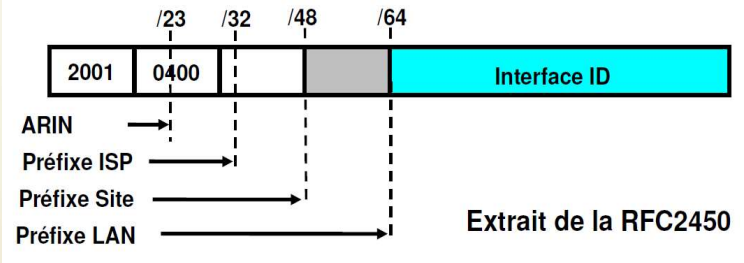
- Les adresses unicast globales (2001::/16. Ces adresses sont allouées par bloc de /23 à /12 par l'IANA à un RIR : registre Internet régional.
- Certains blocs sont réservés à un usage particulier[13] :
  - 2001::/32 utilisé pour le protocole Teredo (RFC 4380[14])
  - 2001:2::/48 pour des tests de performance (RFC 5180[15])
  - 2001:10::/28 pour le protocole Orchid (RFC 4843[16])
  - 2001:db8::/32 est réservé pour la documentation (RFC 3849[17])
- Les adresses 6to4 (2002::/16) permettant d'acheminer le trafic IPv6 via un ou plusieurs réseaux IPv4,
- Toutes les autres adresses routables sont actuellement réservées pour usage ultérieur (plus des trois quarts),

Adresse IP v6 Globales unicast

JFA 146

R 2.05

- Les adresses qui commencent par 2001 sont déléguées aux FAI.
- Les préfixes fournis aux FAI ont un préfixe d'une longueur de 32.
- Tout client peut obtenir de son FAI un préfixe d'une longueur de 48.



Adresse IPv6 synthèse

JFA 147

R 2.05

Type	Préfixe	L	Global ID	Subnet ID	Interface ID
unicast Unique Local (ULA)	7 bits	1 bit	40 bits	16 bits	64 bits
	FC00/7	1	Aléatoire	Sous-réseau	Adresse MAC
unicast Link-Local	10 bits		54 bits		64 bits
	FE80/10		0		Adresse MAC
unicast Site local Obsolète	10 bits		54 bits		64 bits
	FEC0/10		Sous-réseau		Adresse MAC

Adresse IPv6 synthèse

JFA 148

R 2.05

Type	Préfixe			Group ID
Multicast	8 bits	4 bits	4 bits	112 bits
	FF	000T T=0 : Permanent, T=1 : Temporaire	Scope : 1 : Interface Local 2 : Link Local 4 : Admin Local 5 : Site Local 8 : Organisation Local e : Global	
Anycast	N bits			128-N bits
	Préfix sous réseau			0

Adresse IPv6 synthèse

JFA 149

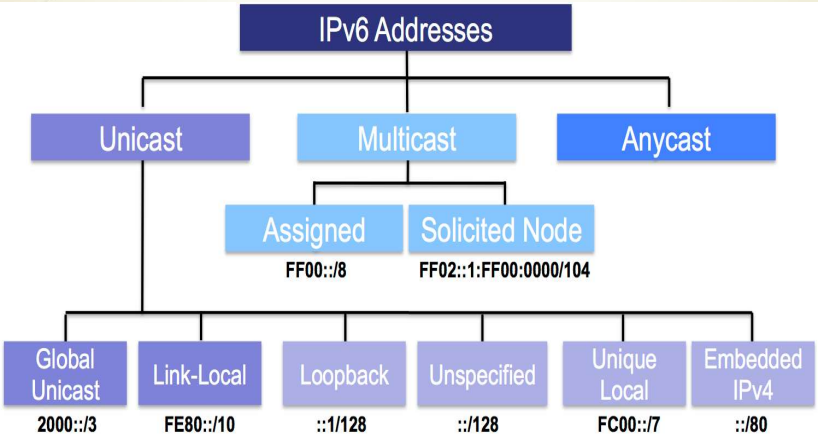
R 2.05

Type	Préfixe	TLA	Global ID	Subnet ID	Interface ID
Aggregatable Global Unicast Address	3 bits	13 bits	112 bits		
	2000/3	0000	réservé		
		0001	Global Unicast		
		0002	6to4		

JFA 150

Adresse IPv6 synthèse

R 2.05



http://www.iplogos.fr/ipv6-les-differentes-adresses/

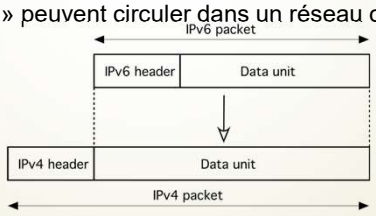
JFA 151

Communication IPV6 à travers un réseau IPv4

R 2.05

Lorsqu'un réseau IPv6 veut joindre un autre réseau IPv6 séparé par un réseau en IPv4, le problème consiste à offrir une connectivité IPv6 entre ces 2 réseaux. La connectivité s'établit par des mécanismes de niveau réseau reposant sur le principe du tunnel. Ainsi, le tunnel est la solution pour utiliser une infrastructure IPv4 existante pour acheminer du trafic IPv6.

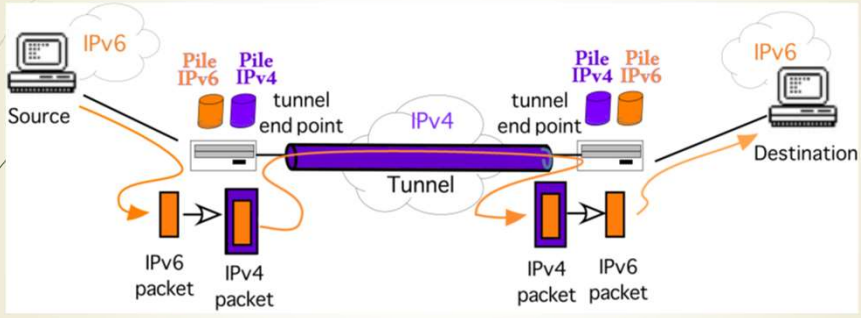
Le tunnel est un mécanisme bien connu dans le domaine des réseaux, qui consiste à faire qu'une unité de transfert d'un protocole (PDU Protocol Data Unit) d'une couche se trouve encapsulée dans la charge utile de l'unité de transfert (PDU) d'un autre protocole de la même couche. Ainsi, des protocoles « transportés » peuvent circuler dans un réseau construit sur un protocole encapsulant.



Communication IPV6 à travers un réseau IPv4

JFA 153

R 2.05

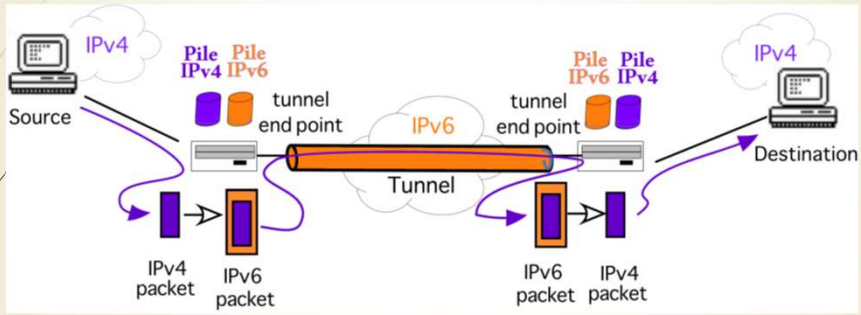


http://livre.g6.asso.fr/index.php/File:43-fig2-hd.png

Communication IPV4 à travers un réseau IPv6

JFA 154

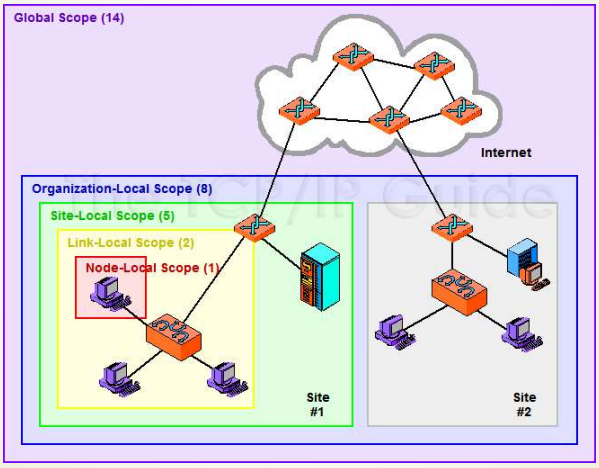
R 2.05



http://livre.g6.asso.fr/index.php/File:43-fig2-hd.png

Adresse IPv6 Scope

JFA 155



http://www.tcpipguide.com/free/t_IPv6MulticastandAnycastAddressing-2.htm

Exemple d'adresse IPv6 d'une machine

JFA 156

```
IP Configuration
Ethernet adapter Ethernet0:
Connection-specific DNS Suffix  . : lan.org
IPv6 Address. . . . . . . . . . . : 2001:db8:acaf:fd00::2ae
IPv6 Address. . . . . . . . . . . : 2001:db8:acaf:fd00:b48a:c5e2:e5a3:1f3e
IPv6 Address. . . . . . . . . . . : fd26:44e1:8c70:fd00::2ae
IPv6 Address. . . . . . . . . . . : fd26:44e1:8c70:fd00:b48a:c5e2:e5a3:1f3e
Temporary IPv6 Address. . . . . . : 2001:db8:acaf:fd00:61a9:365c:2d95:898
Temporary IPv6 Address. . . . . . : fd26:44e1:8c70:fd00:61a9:365c:2d95:898
Link-local IPv6 Address . . . . . : fe80::b48a:c5e2:e5a3:1f3e%3
IPv4 Address. . . . . . . . . . . : 192.168.1.195
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::12fe:edff:fee5:a266%3
192.168.1.1

C:\Users\user1>netsh int ipv6 show add
 Interface 3: Ethernet0
Addr Type  DAD State   Valid Life Pref. Life Address
---------  ----------- ---------- ---------- ------------------------
Dhcp       Preferred   23h15m46s   2001:db8:acaf:fd00::2ae
Temporary  Preferred    1h53m48s   23m48s     2001:db8:acaf:fd00:61a9:365c:2d95:898
Public     Preferred    1h53m48s   23m48s     2001:db8:acaf:fd00:b48a:c5e2:e5a3:1f3e
Dhcp       Preferred   23h15m46s   fd26:44e1:8c70:fd00::2ae
Temporary  Preferred    1h53m48s   23m48s     fd26:44e1:8c70:fd00:61a9:365c:2d95:898
Public     Preferred    1h53m48s   23m48s     fd26:44e1:8c70:fd00:b48a:c5e2:e5a3:1f3e
Other      Preferred    infinite   infinite   fe80::b48a:c5e2:e5a3:1f3e%3
```

JFA 157

Client de messagerie : quelle solution choisir ?

R 2.05

- Un client de messagerie est un logiciel qui sert à lire, à envoyer et à recevoir des emails transférés par le serveur de messagerie. On peut le retrouver installé localement sur votre poste mais aussi sur votre téléphone ou accessible via un navigateur web.
- Depuis 2013, plus de la moitié des mails sont ouverts sur mobile (téléphone ou tablette). Les clients emails pour mobile d'iPhone, de l'iPad et d'Android font partie des solutions les plus utilisées. Il reste tout à fait possible de les synchroniser avec n'importe quel client de messagerie.
- Sur desktop (PC ou Mac), les principaux clients de messagerie (Mail User Agent, MUA) connus sont Microsoft Outlook, Mozilla Thunderbird ou Mail pour Apple. Les autres programmes comme Windows Live Mail, Opera Mail, eM Client, Zimbra ou Incredimail ne représentent pas de véritables solutions professionnelles.

JFA 158

Comprendre la différence entre les protocoles de messagerie SMTP, POP3 et IMAP

R 2.05

- Les trois principaux protocoles utilisés par un serveur de messagerie sont le SMTP (Simple Mail Transfer Protocol), le POP (Post Office Protocol) et l'IMAP (Internet Message Access Protocol). Il en existe encore un autre, le MAPI (Messaging Application Programming Interface) mais qui n'est employé que dans le cadre de l'utilisation de Microsoft Exchange.

JFA 159

Le protocole de messagerie SMTP

R 2.05

- Ce protocole de communication est utilisé pour le transfert des messages électroniques (emails) sur le réseau. Il est de type client / serveur. Chaque demande d'envoi par le client est suivie par une réponse de la part du serveur. Il s'agit d'un protocole simple qui utilise le protocole de contrôle de transmissions TCP pour le transfert des données.
- Les échanges de mails sur un serveur de messagerie se font via des ports (un port pour le serveur) et le protocole SMTP écoute, par défaut, le port 25 avec pour objectif de router les messages.

JFA 160

Tout savoir sur le protocole SMTP (Simple Mail Transfer Protocol)

R 2.05

Le protocole Simple Mail Transfer Protocol, plus connu sous le nom de SMTP, est un protocole de messagerie qui a pour objectif de faire transiter les mails vers les serveurs de messagerie afin que les utilisateurs puissent consulter leurs mails.

- **Principe de fonctionnement du SMTP**
  - L'envoi et la réception de mails se font via des ports, par défaut, c'est le port 25 qui est utilisé par les serveurs de messagerie électronique et le port 587 par les clients de messagerie. Différentes commandes composent le scénario d'envoi de mails afin qu'ils puissent transiter directement de l'expéditeur au destinataire.
  - Ici, tout est question de syntaxe, la moindre erreur dans le code pourrait générer un blocage des mails. Si le protocole de messagerie SMTP est le plus utilisé, il rencontre malgré tout certaines limites. De fait, il ne permet pas d'identifier l'expéditeur des mails et ne permet pas de lutter contre le spam, un fléau depuis quelques années sur le web.

JFA 161

Tout savoir sur le protocole SMTP (Simple Mail Transfer Protocol)

R 2.05

- **Les agents de transferts (MTA)**
  - Les agents de transferts Mail (MTA) ou serveurs de messagerie sont les programmes qui permettent le transfert des courriers entre les serveurs. Un mail peut très bien être relayé entre plusieurs MTA. Il est possible de connaitre tous les MTA par lesquels le mail est passé en affichant la source du message.

  En voici quelques-uns des plus courants :

  - **Sendmail**
    - C'est Sendmail qui fut le premier serveur de messagerie à avoir recours au SMTP en 1983. Aujourd'hui, c'est le MTA le plus utilisé du monde avec environ 55% des serveurs SMTP. Très fiable, Sendmail est le MTA le plus puissant mais aussi sûrement le plus critiqué pour sa lenteur et sa complexité dans sa mise en place et dans son maintien.
  - **Postfix**
    - Postfix est une des meilleures alternatives à Sendmail. Publié sous licence libre, il reste cependant incompatible avec la licence GPL.
  - **Autres MTA**
    - Il existe d'autres serveurs de moins connus comme Exim (EXperimental Internet Mailer) et qmail.

JFA 162

Le protocole de messagerie POP

R 2.05

- Le protocole POP (Post Office Protocol) est aujourd'hui disponible dans sa version 3, aussi appelé POP3. Il s'agit du protocole standard qui permet la récupération des mails situés sur un serveur distant (serveur POP). L'objectif de ce protocole est de relever le courrier électronique depuis un hôte qui ne contient pas sa boite aux lettres. Il vient tout simplement télécharger les messages à partir du serveur et les stocke sur le poste de travail.
- L'avantage de ce protocole est de permettre la consultation de sa messagerie en mode « hors connexion », sans avoir besoin d'une connexion internet permanente. L'inconvénient, par contre, est qu'il n'est pas adapté aux supports de mobiles (smartphones, tablettes, SaaS) et que les messages ne sont pas synchronisés en permanence avec le serveur.

JFA 163

Tout savoir sur le protocole de messagerie POP3 (Post Office Protocol)

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- Le **POP est le Post Office Protocol**, un des trois principaux protocoles de messagerie. Aujourd'hui, c'est la version 3 qui est utilisée. Il s'agit ici de se connecter à un serveur TCP/IP afin de collecter les messages sur le serveur puis de les effacer et se déconnecter. On utilise pour cela le port 110. Il existe également le POP3S ou POP3 over SSL qui est plus sécurisé que l'original.
- Tout l'intérêt de ce protocole est de permettre aux utilisateurs de pouvoir consulter les mails qu'ils ont reçus lorsqu'ils n'étaient pas connectés. Le POP3 et le SMTP fonctionnent sur le même principe, à savoir que des commandes textuelles sont utilisées pour faire transiter les mails. La différence fondamentale entre ces deux systèmes est l'authentification.
- De fait, si le **SMTP** ne permet pas d'identifier l'expéditeur, le protocole de messagerie POP3 est à même de gérer cela grâce à l'utilisation d'un identifiant et d'un mot de passe. Les utilisateurs de gestionnaires de courrier électronique, à l'image de Microsoft Outlook qui peut paramétrer leurs comptes de messagerie, sont familiers avec ce système. En revanche, la sécurité n'est pas sans faille puisque les mots de passe ne sont pas cryptés.

JFA 164

Le protocole de messagerie IMAP

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- Le protocole IMAP (Internet Message Access Protocol) c'est un peu l'inverse du protocole POP, c'est à dire qu'il une connexion constante au serveur de messagerie pour pouvoir consulter ses mails. Ce protocole synchronise en permanence les messages contenus sur le serveur et sur le poste de travail. Son avantage réside donc dans la possibilité de consulter ses mails depuis n'importe quel endroit et de pouvoir synchroniser et sauvegarder ses messages sur le serveur.

JFA 165

Tout savoir sur le protocole de messagerie IMAP (Internet Message Access Protocol)

R 2.05

- Internet Message Access Protocol ou IMAP, est l'un des trois protocoles de messagerie. Il permet de collecter les mails sur un serveur de messagerie à l'image du POP3 via le port 143. En revanche, si le POP3 efface les courriers électroniques avant de se déconnecter, l'IMAP les conserve sur le serveur. L'intérêt principal de ce protocole est de permettre aux utilisateurs de consulter leurs mails à divers endroits et sur des webmails différents.
- Outre la possibilité de consulter ses mails partout, cela laisse la possibilité aux administrateurs de faire des sauvegardes avec pour seule limite la capacité de stockage allouée sur le serveur. C'est la garantie de retrouver tous ses mails en cas de dysfonctionnement de votre poste de travail.

JFA 166

Beaucoup d'avantages à utiliser le protocole IMAP

R 2.05

- Mais là où le protocole de messagerie IMAP se démarque, c'est au niveau des différentes possibilités qu'il offre, notamment en sauvegardant les messages sur le serveur. De fait, il est possible de **trier les mails directement sur le serveur** et de créer des dossiers pour mieux gérer ses courriers électroniques. Ces sous-dossiers se retrouvent synchronisés aussi bien sur le serveur que sur votre poste de travail.
- En outre, avec l'IMAP**, il est possible de gérer plusieurs boîtes aux lettres**. Mais parce que chaque protocole possède également des inconvénients, celui-ci a le désavantage de nécessiter une connexion permanente, même si certains clients de messagerie ont peu à peu développé un mode « off-line ».

JFA 167

Quel protocole choisir entre POP et IMAP ?

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

La grande différence entre les protocoles de messagerie POP et IMAP est que POP télécharge les messages sur le serveur et vient les stocker en local, sur votre poste de travail, alors que le protocole IMAP opère une synchronisation constante entre votre poste de travail et le serveur.

- **Le protocole IMAP s'avère souvent plus pertinent pour plusieurs raisons :**
  - Les messages restent stockés sur le serveur, ils donc sont sauvegardés dans la limite du stockage existant sur votre serveur. En cas de problème sur votre poste de travail, aucun de vos mails ne sera perdu.
  - IMAP gère les sous-dossiers distants, c'est à dire que vous retrouvez votre organisation de boîte aux lettres partout.
  - La synchronisation permanente permet une gestion très fine de vos messages. Par exemple, si sur votre mobile vous passez un message en « non lu », il le sera aussi automatiquement sur votre poste de travail.

JFA 168

Le webmail : un client de messagerie sur le web

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Le webmail est un client de messagerie qui sert d'interface entre le serveur de messagerie et un navigateur web, contrairement au client classique qui s'installe directement sur le disque de l'ordinateur ou sur un smartphone. Les webmails les plus utilisés sont Gmail, Outlook.com (anciennement Hotmail) et Yahoo! Mail.
- L'avantage principal est bien évidemment de ne pas devoir installer de logiciel et de ne pas avoir besoin d'effectuer de configuration spécifique. Dès que vous êtes connectés à Internet, vous êtes en mesure d'accéder à vos courriers électroniques. Ce système représente aussi des inconvénients liés à la qualité de connexion au réseau Internet.

JFA 169

Et la sécurité dans tout cela ?

IUT GRAND OUEST NORMANDIE
INFO
R 2.05

- Les deux protocoles POP et IMAP existent en version sécurisés, POPs (POP3 over SSL) et IMAPs (IMAP over SSL). Ce type de sécurisation est conseillé notamment dans le cadre d'une utilisation WiFi, y compris chez vous, pour éviter la récupération malveillante de vos données d'identifications (login et mot de passe).

JFA 170

Serveur de messagerie : Client et protocoles

IUT GRAND OUEST NORMANDIE
INFO
R 2.05

- Si l'infrastructure informatique de votre entreprise comporte un service de messagerie électronique, un logiciel serveur s'occupe alors de la gestion des transferts des messages. L'utilisateur final que vous êtes n'est jamais directement en contact avec ce serveur. Découvrez comment, en interne, le serveur de votre système informatique procède lors d'un envoi de mail…

JFA 171

Les différents services d'un serveur de courriel

R 2.05

Le protocole global de la messagerie électronique est divisé en plusieurs services avec, à chaque fois, une fonction associée :

- **MUA (Mail User Agent) :** c'est le logiciel qui sert à lire et à envoyer les messages électroniques : le client de messagerie (Exemples : Microsoft Outlook, Mozilla ThunderBird, Apple Mail, IBM Lotus Notes, etc.)
- **MTA (Mail Transfert Agent) :** c'est le logiciel pour serveur de transmission. Il s'occupe d'envoyer les mails entre les serveurs.
- **MDA (Mail Delivery Agent) :** c'est le logiciel de distribution du courrier électronique et représente la dernière étape de la chaîne d'envoi d'un mail. Il est plutôt associé aux protocoles POP et IMAP.

JFA 172

Fonctionnement du courrier électronique

R 2.05

Le fonctionnement du courrier électronique est basé sur l'utilisation d'une boîte à lettres électronique. Lors de l'envoi d'un email, le message est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire. Plus exactement, le message est envoyé au serveur de courrier électronique chargé du transport (nommé MTA pour Mail Transport Agent), jusqu'au MTA du destinataire. Sur internet, les MTA communiquent entre eux grâce au protocole SMTP et sont logiquement appelés serveurs SMTP (parfois serveur de courrier sortant).

- **MUA (Mail User Agent) :** c'est le logiciel qui sert à lire et à envoyer les messages électroniques : le client de messagerie (Exemples : Microsoft Outlook, Mozilla ThunderBird, Apple Mail, IBM Lotus Notes, etc.)
- **MTA (Mail Transfert Agent) :** c'est le logiciel pour serveur de transmission. Il s'occupe d'envoyer les mails entre les serveurs.
- **MDA (Mail Delivery Agent) :** c'est le logiciel de distribution du courrier électronique et représente la dernière étape de la chaîne d'envoi d'un mail. Il est plutôt associé aux protocoles POP et IMAP.

JFA 173

Fonctionnement du courrier électronique

R 2.05

Le fonctionnement du courrier électronique est basé sur l'utilisation d'une boîte à lettres électronique. Lors de l'envoi d'un email, le message est acheminé de serveur en serveur jusqu'au serveur de messagerie du destinataire. Plus exactement, le message est envoyé au serveur de courrier électronique chargé du transport (nommé MTA pour Mail Transport Agent), jusqu'au MTA du destinataire. Sur internet, les MTA communiquent entre eux grâce au protocole SMTP et sont logiquement appelés serveurs SMTP (parfois serveur de courrier sortant).

Le serveur MTA du destinataire délivre alors le courrier au serveur de courrier électronique entrant (nommé **MDA** pour *Mail Delivery Agent*), qui stocke alors le courrier en attendant que l'utilisateur vienne le relever. Il existe deux principaux protocoles permettant de relever le courrier sur un MDA :

JFA 174

Fonctionnement du courrier électronique

R 2.05

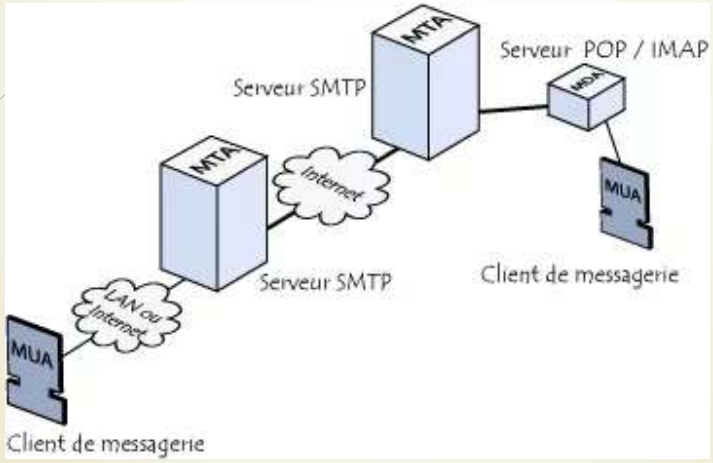
- le protocole POP3 (Post Office Protocol), le plus ancien, permettant de relever son courrier et éventuellement d'en laisser une copie sur le serveur.
- le protocole IMAP (Internet Message Access Protocol), permettant une synchronisation de l'état des courriers (lu, supprimé, déplacé) entre plusieurs clients de messagerie. Avec le protocole IMAP une copie de tous les messages est conservée sur le serveur afin de pouvoir assurer la synchronisation.

JFA 175

Fonctionnement du courrier électronique

R 2.05

Ainsi, les serveur de courrier entrant sont appelés serveurs POP ou serveurs IMAP, selon le protocole utilisé.



JFA 176

Fonctionnement du courrier électronique

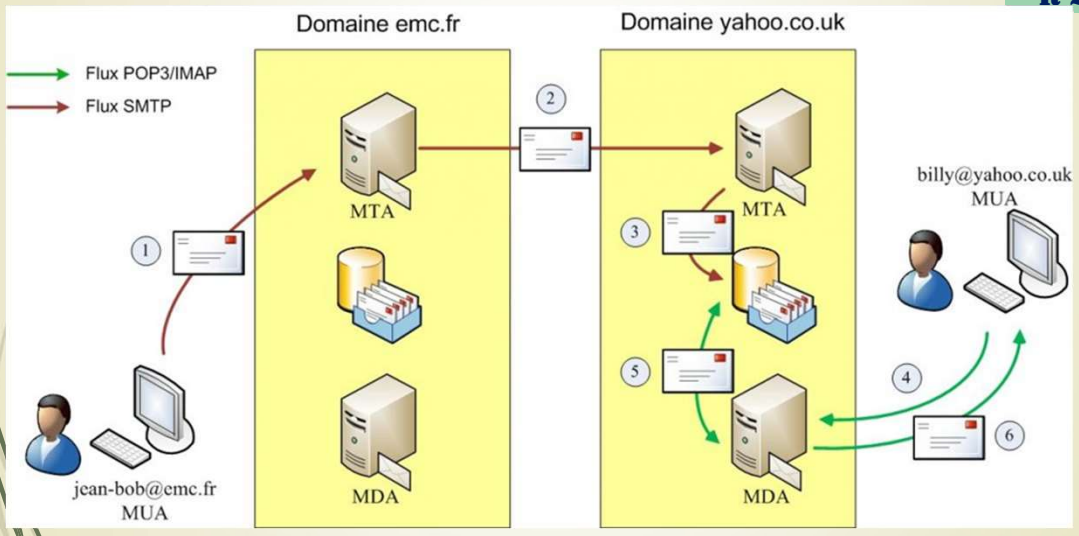
R 2.05

- Par analogie avec le monde réel, les MTA font office de bureau de poste (centre de tri et facteur assurant le transport), tandis que les MDA font office de boîte à lettres, afin de stocker les messages (dans la limite de leur capacité en volume), jusqu'à ce que les destinataires relèvent leur boîte. Ceci signifie notamment qu'il n'est pas nécessaire que le destinataire soit connecté pour pouvoir lui envoyer du courrier.
- Pour éviter que chacun puisse consulter le courrier des autres utilisateurs, l'accès au MDA est protégé par un nom d'utilisateur appelé identifiant (en anglais login) et par un mot de passe (en anglais password).
- La relève du courrier se fait grâce à un logiciel appelé MUA (Mail User Agent).
- Lorsque le MUA est un logiciel installé sur le système de l'utilisateur, on parle de client de messagerie (par exemple Mozilla Thunderbird, Microsoft Outlook, Eudora Mail, Incredimail ou Lotus Notes).
- Lorsqu'il s'agit d'une interface web permettant de s'interfacer au serveur de courrier entrant, on parle alors de webmail.

B. Itinéraire détaillé d'un message

JFA 177

R 2.05



https://blog.slashroot.fr/?p=22

B. Itinéraire détaillé d'un message

JFA 178

R 2.05

1. Jean-Bob rédige son message et l'envoie grâce à son MUA. Le message est acheminé au serveur SMTP de son domaine.
2. Le MTA du domaine emc.fr reçoit le message et constate que le destinataire n'est pas dans ses destinations. Il cherche alors grâce à DNS si un MTA existe pour le domaine yahoo.co.uk. Une fois qu'il l'a trouvé il envoie le message à ce MTA.
3. Le serveur SMTP de yahoo.co.uk reçoit le message et constate que le destinataire est bien dans ses destinations. Il dépose alors le message dans la boite aux lettres de Billy par l'intermédiaire du MDA.
4. Billy souhaite relever son courrier et envoie donc une requête à son serveur POP via son MUA.
5. Le serveur POP consulte la boite aux lettres de Billy et constate qu'il y a un message.
6. Il envoie alors le message au MUA de Billy.

JFA 179

Relais ouverts

R 2.05

- Par défaut et pour des raisons historiques, il n'est pas nécessaire de s'authentifier pour envoyer du courrier électronique, ce qui signifie qu'il est très facile d'envoyer du courrier en falsifiant l'adresse électronique de l'expéditeur.
- Ainsi, la quasi-totalité des fournisseurs d'accès verrouillent leurs serveurs SMTP afin de n'en permettre l'utilisation qu'à leurs seuls abonnés ou plus exactement aux machines possédant une adresse IP appartenant au domaine du fournisseur d'accès. Ceci explique notamment la nécessité qu'ont les utilisateurs nomades de modifier les paramètres du serveur sortant dans leur client de messagerie à chaque changement entre le domicile et l'entreprise.
- Lorsque le serveur de messagerie d'une organisation est mal configuré et permet à des tiers appartenant à des réseau quelconques d'envoyer des courriers électronique, on parle alors de **relais ouvert** (en anglais *open relay*).
- Les relais ouverts sont ainsi généralement utilisés par les spammeurs, car leur utilisation permet de masquer l'origine des messages. Par conséquent, de nombreux fournisseurs d'accès tiennent à jour une liste noire contenant une liste des relais ouverts, afin d'interdire la réception de messages provenant de tels serveurs.

JFA 180

Les différents types de serveur de messagerie

R 2.05

Il existe deux types de serveur de messagerie :

- **un serveur sortant, le serveur SMTP**
- **serveur entrant, le serveur POP/IMAP**.

JFA 181

Les principaux protocoles de messagerie

R 2.05

SMTP, POP et IMAP sont les protocoles de messagerie qui définissent le moyen de transfert et de réception d'un mail. En un mot, vous pouvez envoyer un courrier électronique grâce au protocole SMTP et vous pouvez le réceptionner sur votre ordinateur grâce au protocole POP ou au protocole IMAP.

Suivez ce lien pour savoir plus sur le principe de fonctionnement et de navigation des principaux protocoles de messagerie.

JFA 182

Le client de messagerie

R 2.05

Le client de messagerie est le programme serveur qui sert d'interface pour l'utilisateur. Il permet l'envoi et la réception d'un message électronique. Ces logiciels de messagerie instantanée nécessitent parfois une bonne configuration afin d'en tirer le meilleur parti.

Il existe deux catégories de client de messagerie :

- **les clients mail**, installés sur votre poste informatique, appelés « lourds »
- **les clients web**, accessible à partir d'une connexion sur votre navigateur, appelés « webmails ».

JFA 183

Le client de messagerie

R 2.05

Pour bien choisir son client mail, il faut bien entendu prendre en considération votre système d'exploitation (OS) : Windows, Mac OS X, Linux (système UNIX), etc.

Il existe deux catégories de client de messagerie :

- **Exemples de clients installés sur votre machine en local** : Microsoft Outlook (avec la possibilité de le coupler avec Microsoft Exchange Server), Mozilla ThunderBird, Apple Mail, IBM Lotus Notes, etc.
- **Exemples de clients web en ligne :** Google Gmail, Outlook.com (ex Hotmail), GMX, Free, Yahoo!, La Poste.net, etc.

JFA 184

Fonctionnement d'une messagerie et de sa boîte aux lettres électronique (BAL)

R 2.05

- Élément incontournable du service de messagerie d'un système informatique professionnel, le compte de messagerie est une adresse électronique grâce à laquelle on peut recevoir de la messagerie électronique (emails). Cela peut être un compte personnel ou un compte d'entreprise suivant l'utilisation que vous en faites. Il d'ailleurs souvent conseillé de créer plusieurs adresses afin de ne pas mélanger les emails professionnels, les emails privés et les mails dits « poubelles ».

- **La boîte aux lettres électronique (BAL)** est la boîte de réception de vos adresses de messagerie. C'est le conteneur de tous les messages reçus et envoyés. Cette BAL est accessible via un identifiant (votre adresse mail) et un mot de passe. Elle est tout à fait comparable à une boite postale classique. En 2014, tout le monde, ou presque, en possède une. Les plus connues et les plus utilisées sont Gmail, Outlook.com (ex Hotmail), Yahoo! Mail, GMX, Mail Orange, etc.

JFA 185

Composition d'une adresse de messagerie

R 2.05

Une adresse de messagerie est composée des trois éléments suivants :

- **Un identifiant** comme le nom, le prénom ou une information qui peut comporter des points ou des tirets.
- **Le séparateur arobase (@).**
- **Le nom de domaine** qui peut être celui de l'entreprise ou celui du fournisseur.

JFA 186

Alias de messagerie : Comment faire pour gérer plusieurs adresse mail ?

R 2.05

- Comme tout utilisateur de boîte aux lettres électronique, vous disposez d'un compte de messagerie principal. Si vous souhaitez ajouter une adresse, il existe deux façons de procéder : vous pouvez créer un nouveau compte de messagerie ou créer un alias de messagerie.
- Un alias est une adresse mail supplémentaire qui redirige les messages vers votre boîte de réception. Il existe certains cas où la création d'alias est préconisée et d'autres cas où la création d'une nouvelle adresse est plus judicieuse.

JFA 187

Quelles sont les différences entre un alias et une boîte aux lettres électronique (BAL) ?

R 2.05

- Un **alias de messagerie** se présente sous la forme d'une adresse mail qui sert à rediriger les messages reçus vers votre compte de messagerie principal. La boîte aux lettres électronique (BAL ou boîte de réception) est le conteneur de réception de l'ensemble des mails provenant de votre compte de messagerie principal comme des alias. **Cela revient à créer une deuxième identité pour une seule BAL.**
- Avec le système d'alias de messagerie, plusieurs adresses peuvent pointer vers la même boîte de réception, autrement dit, vers le même conteneur (BAL). L'inverse est aussi possible : un alias peut pointer vers plusieurs BAL.
- Avec votre **identité alias**, vous pouvez aussi envoyer des emails et conservez votre liste de contacts ainsi que vos paramètres à l'identique pour tous les comptes de messageries de votre boîte de réception.

JFA 188

Quel est l'intérêt de créer un alias de messagerie ?

R 2.05

- L'intérêt principal d'un alias est de créer une ou plusieurs adresses supplémentaires qui servent à communiquer différemment selon vos besoins sans avoir à changer de boîte de réception.
- Prenons un cas concret pour illustrer son utilisation : Au sein de votre société, vous avez plusieurs commerciaux qui possèdent chacun une boite aux lettres avec une adresse personnelle.
  - jean.dupont@votresociete.fr
  - martin.duval@votresociete.fr
  - …

JFA 189

Quel est l'intérêt de créer un alias de messagerie ?

R 2.05

- Pour plus de facilité, vous préférez communiquez d'autres adresses de messagerie plus génériques et plus thématiques à vos clients et prospects comme :
  - commercial@votresociete.fr
  - contact@votresociete.fr
  - …
- Ces deux dernières adresses mail sont des alias et peuvent être redirigées suivant vos règles. Ainsi l'adresse commercial@votresociete.fr peut être redirigée vers la boîte aux lettres électronique de tous les commerciaux et l'adresse contact@votresociete.fr peut, elle, être dirigée uniquement vers la boîte de réception de Jean Dupont.
- En vous connectant à une seule boîte mail, vous pouvez récupérer les messages de plusieurs adresses.

JFA 190

Dans quel cas est-il plus adapté de créer une nouvelle adresse mail ?

R 2.05

- Si votre société est divisée en service qui comporte plusieurs personnes assignées aux mêmes tâches, il peut être très utile de crée une boîte de réception différente pour chaque service afin de favoriser le travail en commun.
- Cette façon de gérer les messages nécessite une configuration différente de votre client de messagerie. Vous avez accès à plusieurs boîtes de réception mais qui sont partagées avec plusieurs utilisateurs.
- La création de plusieurs BAL est la solution la plus adaptée pour travailler en équipe et partager les tâches. Toute l'équipe ou le service a accès à la même boîte et peut gérer les messages. Si l'un des collaborateurs marque un courrier en non lu, il prend cette forme pour tout le reste des utilisateurs.
- La messagerie partagée permet également d'éviter la duplication inutile de mails. Si un des membres de l'équipe répond à un mail, tous les autres peuvent voir sa réponse et peuvent classer le message. Attention cependant à ne pas supprimer un message par erreur car il serait alors irrécupérable.

JFA 191

Vers la fin des comptes de messagerie nominatifs ?

R 2.05

- Cette manière de partager votre messagerie amène à se poser question sur l'avenir des adresses de messagerie personnelle comme jean.dupont@votresociete.fr. La gestion en équipe à partir d'adresses collaboratives paraît être une solution particulièrement adaptée pour beaucoup d'entreprises. L'intérêt de posséder une adresse personnelle peut, dans de nombreux cas, être remis en question.

JFA 192

Une réponse automatique par mail pendant votre absence

R 2.05

- Un autorépondeur est un outil qui vous permet de garder le contact avec vos clients et vos prospects en leur envoyant des messages de manière automatisée. On distingue deux grandes catégories de répondeurs automatiques :
  - le répondeur automatique de votre compte de messagerie qui se déclenche en cas d'absence et
  - l'auto répondeur marketing qui lui permet de programmer des envois de mails en masse.
- Dans ce deuxième cas, on sort complètement du sujet des comptes mail (il s'agit plutôt d'une fonctionnalité pour l'emailing.

JFA 193

Répondre automatiquement à vos clients pendant vos absences et vos congés

IUT GRAND OUEST NORMANDIE – iNFO

R 2.05

- En cas d'absence courte ou prolongée, de congés ou dans une période très chargée, il est très pratique de pouvoir répondre à vos correspondants de manière automatique. Grâce à une configuration spécifique de votre compte de messagerie, il est possible de préparer un message qui sera envoyé en réponse à tous les mails que vous recevrez pendant votre absence.
- Afin d'avertir au mieux vos correspondants, il est important de renseigner un maximum d'informations utiles en configurant votre autorépondeur. Pensez à faire figurer la durée de votre absence et éventuellement une personne à prévenir en cas d'urgence.
- Dans le cas d'un client de messagerie évolué, l'assistant de gestion des messages peut vous permettre de préciser des règles de fonctionnement ou de renseigner des exceptions. Ainsi vous pouvez décider de ne pas répondre automatiquement si le message contient des mots spécifiques, suivant le destinataire ou si le mail est marqué comme important.

JFA 194

L'autorépondeur comme outil marketing

IUT GRAND OUEST NORMANDIE – iNFO

R 2.05

- Cette fonctionnalité, un peu différente de la précédente, peut s'avérer très puissante pour convaincre de nouveaux prospects ou fidéliser des clients. Cette manière d'utilisation de l'autorépondeur ne se contente pas d'une simple réponse automatique mais peut être programmé de façon plus fine et plus évoluée. Maîtriser le processus d'envoi de mails commerciaux est un gage de réussite et d'efficacité pour une société.
- Ce service existe dans la plupart des solutions d'emailing et d'email marketing et se déclenche en fonction de plusieurs situations : inscription à une newsletter, confirmation d'une souscription, en réponse au message, …

JFA 195

SPAM : Comment lutter efficacement contre les courriers indésirables ?

R 2.05

- Le SPAM est un courrier indésirable (ou pourriel), c'est-à-dire un courriel non sollicité. Son coût d'envoi très faible continue d'inciter de nombreuses « spammeurs » à utiliser cette technique pour diffuser des contenus commerciaux, de la publicité ou pire encore pour tenter de tromper le dentinaire dans le but de lui soutirer des informations ou de transmettre un programme malveillant. Il représente près de 90% du trafic global des emails.

- Les expéditeurs de SPAM font souvent preuve de beaucoup d'ingéniosité pour détourner les filtres anti SPAM installés sur les boites aux lettres électroniques. Les techniques d'envoi s'avèrent de plus en plus sophistiquées. Pour lutter efficacement contre ces messages intempestifs, il est absolument nécessaire de mettre en place un filtrage anti SPAM pertinent et régulièrement mis à jour.

JFA 196

Protéger votre messagerie des courriers indésirables (SPAM)

R 2.05

- Le SPAM ou spamming est un courrier indésirable, autrement dit une technique d'envoi de mails à but publicitaire ou frauduleux à des personnes qui ne l'ont pas demandé. Il s'agit de la pollution la plus importante pour votre boîte aux lettres électronique.
- Souvent envoyé de manière massive et parfois à multiples reprises, le spamming est tellement important qu'il peut très vite saturer votre communication. Les SPAMs représentent près de 90% de l'ensemble des courriers électroniques, soit environ 150 milliards de mails par jour (chiffres 2013).
- La plupart des messages indésirables sont heureusement filtré en amont par les outils antispam mis en place par les fournisseurs d'accès à Internet et de messagerie, si bien qu'ils ne vous parviennent presque jamais. C'est pourquoi il est primordial que sa boîte aux lettres électronique soit parfaitement protégée, faute de quoi vous seriez envahi de mails non désirés.
- Il existe plusieurs types de courriers indésirables que l'on peut cependant classé en deux grandes catégories : les SPAMs publicitaires (plus de 80%) et les SPAMs pour escroquerie (moins de 20%)..

JFA 197

Pour la petite histoire

R 2.05

- Le mot SPAM est à l'origine une marque américaine de corned-beef (Spiced Pork And Meat), célèbre pour avoir été utilisée par les forces américaines pour nourrir les soldats pendant la seconde guerre mondiale. L'association du terme SPAM avec les courriers abusifs est due à un sketch des Monty Python.
- Alors déguisés en Vikings amateurs de SPAM (le jambon épicé), les comiques britanniques parodient une publicité en chantant « Spam, Spam, Spam, Spam, lovely Spam, wonderful Spam ». Certains des premiers utilisateurs d'Internet étant des fans des humoristes, ils reprirent ce terme pour désigner le fait de poster des messages de manière abusive.

JFA 198

Quelles sont les bonnes pratiques à adopter quand on reçoit un courrier indésirable ?

R 2.05

- Les SPAMs peuvent aujourd'hui prendre des formes diverses : une image, un document pdf, un mp3 ou n'importe quel autre type de fichiers peut contenir un message indésirable. Pour s'en prémunir, il est important d'adopter des bons réflexes.
- La première des bonnes pratiques consiste à éviter d'afficher ces courriers en configurant votre client de messagerie ou votre webmail pour empêcher l'affichage automatique. Une autre consigne des plus logiques reste bien sûr de ne **jamais répondre aux messages** et de **ne pas cliquer sur les liens proposés**.
- Dernier conseil, et pas des moindres, ne tentez jamais de cliquer sur les liens de désinscriptions. Ceux-ci servent en fait à valider votre adresse mail, votre geste n'aura alors pour conséquence que de multiplier le nombre de courriers indésirables que vous recevrez.

JFA 199

Comment se protéger des courriers indésirables ?

R 2.05

- Outre les bonnes pratiques énumérées plus haut pour éviter d'augmenter les risques, la solution la plus efficace est de faire appel à la fonction antiSPAM de votre boite aux lettres électronique.
- L'utilisation du mode SaaS de la messagerie de votre entreprise permet une gestion en amont, directement au niveau du serveur, ce qui évite de contaminer tout le réseau. Le taux de détection des menaces est plus élevé et protège plus efficacement sans perte de performance.

JFA 200

Les techniques de détection de messages SPAM

R 2.05

- Plusieurs techniques permettent de détecter au mieux un courrier électronique « spammy » :
  - **Le filtre bayésien,**
  - **Les listes noires,**
  - **Le filtrage heuristique**
  - **L'anti-spoofing pour lutter contre l'usurpation d'identité**
  - **Listes blanches**
  - **Bases collaboratives de spams**
  - **Enregistrement DNS inversé**
  - **Adresses URL**
  - **SPF (Sender Policy Framework)**
  - **Teergrubing**
  - **Greylisting**

JFA 201

Les techniques de détection de messages SPAM

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- **Le filtre bayésien :**

Le filtrage bayésien est une méthode pour filtrer les courriers indésirables basée sur le principe des probabilités. Grâce à l'analyse des messages considérés comme indésirables et en comparaison de ceux qui ne le sont pas, l'algorithme calcule la probabilité de chaque terme d'appartenir à la catégorie des expressions suspectes. Si la fréquence de mots « spammy » dépasse un seuil le mail est classé automatiquement en SPAM.

- **Les listes noires :**

Les listes noires (RBL ou DNSBL) sont des listes de serveurs qui recense des SPAMs collectifs. Elles servent à bloquer certains expéditeurs reconnus comme spammeurs. Cette technique aide à fournir un service pour éviter de les délivrer.

- **Le filtrage heuristique :**

L'analyse heuristique des messages est basée sur un examen complet du contenu d'un mail. En analysant des centaines, voire des milliers de règles, l'algorithme détermine la probabilité qu'un message soir considéré comme du SPAM. Les paramètres étudiés sont par exemple les en-têtes, les déclinaisons de certains mots, l'utilisation d'images au lieu du texte ou la présence de sigles monétaires.

JFA 202

Les techniques de détection de messages SPAM

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- **L'anti-spoofing pour lutter contre l'usurpation d'identité :**

L'email spoofing est une technique que certains spammeurs utilisent pour envoyer des messages à partir d'une adresse mail trouvée sur le web ou falsifiée pour l'occasion. L'intérêt est bien sûr de masquer l'identité du véritable expéditeur et de se faire passer pour une adresse mail de confiance.

- **Listes blanches :**

Afin de détecter les messages SPAM, il existe aussi la technique des listes blanches qui consiste à établir un inventaire des sites, des domaines ou des adresses IP sûres et certifiées.

- **Bases collaboratives de spams :**

Alimentées par les utilisateurs de solutions anti-spam, ce sont des bases de données de signatures de SPAM. Les plus utilisées sont : Razor, Pyzor ou Distributed Checksum Clearinghouses (DCC).

JFA 203

Les techniques de détection de messages SPAM

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- **Enregistrement DNS inversé :**

L'enregistrement DNS consiste à vérifier la corrélation entre l'adresse IP du serveur et son nom via une requête DNS inverse. En effet, une adresse IP peut être associée à plusieurs noms de domaine différents via l'enregistrement de plusieurs entrées PTR mais généralement les serveurs de messagerie possèdent une adresse IP fixe avec un nom de domaine associé.

- **Adresses URL :**

Cette technique compare les URL trouvées dans les corps des messages avec les sites de spammeurs.

- **SPF (Sender Policy Framework) :**

La technique SPF utilise un champ DNS pour définir les serveurs de messagerie qui seront autorisés à expédier des courriers électroniques pour le domaine dont il est question.

JFA 204

Les techniques de détection de messages SPAM

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- **Teergrubing :**

Le Teergrubing est une technique antispam proactive qui réduit de manière significative la vitesse de réponse du serveur SMTP, sur certaines connexions suspectes. Cette méthode sert à contraindre le serveur émetteur de SPAM mais n'est utilisée que dans le cas où on est sûr d'avoir à faire à du SPAM.

- **Greylisting :**

La méthode du Greylisting consiste à rejeter temporairement un message électronique en renvoyant un code de refus au serveur émetteur. S'il s'agit d'un véritable serveur de messagerie, il réexpédiera le mail au bout de quelques minutes. S'il s'agit d'un serveur de SPAM, ce ne sera pas le cas.

JFA 205

Le filtre bayésien pour protéger sa messagerie des SPAM

R 2.05

Le filtrage bayésien est une des techniques utilisée pour détecter et se protéger des SPAM. Issue du théorème de Bayes, cette méthode consiste à comparer les mots d'un mail. Chaque terme est associé à une probabilité qui correspond au nombre de fois où ce mot apparaît dans un SPAM. Si la probabilité dépasse un certain seuil, alors le message est considéré comme un message indésirable..

JFA 206

Le filtre bayésien pour protéger sa messagerie des SPAM

R 2.05

- **Une méthode antispam par apprentissage :**

Le calcul de la probabilité de chaque mot est issu d'un apprentissage grâce aux expériences passées. En classant un mail manuellement dans le dossier des SPAM, une analyse des mots est effectuée. Plus un terme apparaît fréquemment dans ces courriers non désirés, plus sa probabilité augmente en tant que chaîne suspecte.

Par exemple, le mot viagra a une probabilité de 100% et le mot sécurité 20%. A chaque détection de SPAM, les probabilités deviennent plus précises et le filtre bayésien s'améliore.

Au final, si la probabilité dépasse un serveur seuil, le mail est considéré comme étant indésirable, autrement dit si certains mots apparaissent souvent dans un mail dit SPAM, il est alors légitime de le considérer comme tel à l'avenir..

JFA 207

Les listes noires :

R 2.05

Les listes noires de SPAM servent à bloquer certains expéditeurs connus comme étant des spammeurs avérés (producteurs de courriers indésirables) ou des distributeurs de programmes malveillants. Elles peuvent être locales ou publiques et sont composées d'adresses IP de serveurs ou de réseaux ou dans certains cas de domaines. Pour rappel, une adresse IP est un numéro d'identification unique attribué à chaque ordinateur connecté au web...

JFA 208

Les listes noires :

R 2.05

- **Les RBL (Realtime Blackhole List) ou DNSBL (Black List DNS) :**

Les listes noires publiques sont appelées RBL ou DNSBL. Disponibles gratuitement sur Internet ou par abonnement, ce sont des listes composées de d'adresses IP reconnues comme étant des sources d'envoi de courriers indésirables. Il en existe un grand nombre mais toutes ne se valent pas. La principale source provient de Spamhaus, une organisation internationale non gouvernementale basée à Genève et à Londres.

Pour une sécurité accrue, une méthode consiste à constituer une liste à partir de plusieurs listes RBL et de bloquer les adresses IP présentes dans au moins deux listes.

Différents types de listes noires de SPAM :

JFA 209

R 2.05

Si on décompose un peu le système, on comprend que les RBL sont divisées en plusieurs catégories :

- **SBL (Spamhaus Block List) :** Base de données d'adresses IP fournie par Spamhaus.
- **XBL (Exploits Block List) :** Base de données d'adresses IP d'ordinateurs infectés pour lutter contre le piratage informatique.
- **PBL (Policy Block List) :** C'est une liste DNSBL d'adresses IP qui ne délivrent pas de mails authentifiés SMTP. Il s'agit de lutter contre le routage malveillant.
- **DBL (Domains Block List) :** Depuis mars 2010, cette liste recense les domaines suspects.
- **SURBL (Spam URI RBL) :** Cette liste détermine les sites web considérés comme suspects et permet de bloquer les messages issus de ces noms de domaines.

Différents types de listes noires de SPAM :

JFA 210

R 2.05

Voici une liste des principaux sites où trouver des listes noires réputées comme sérieuses :

- **http://www.dnsbl.info/dnsbl-list.php**
- **http://www.spamhaus.org/**
- **http://www.spamcop.net/**
- **http://www.sorbs.net/**
- **http://www.dsbl.org/**

JFA 211

Le filtrage heuristique des mails pour protéger sa messagerie des SPAM:

R 2.05

L'analyse heuristique est une technique de détection et de protection contre les SPAM. Il s'agit d'un filtre basé sur l'analyse du contenu d'un message et non sur la comparaison avec des bases de données comme les listes noires. Il s'agit d'examiner un mail grâce à un très grand nombre de paramètres (de quelques centaines à plusieurs milliers) comme la proportion de code HTML, le nombre d'images, la présence de signes monétaires ou l'absence de sujet de mail.

JFA 212

Le filtrage heuristique des mails pour protéger sa messagerie des SPAM

R 2.05

- **L'analyse par expressions régulières :**

Le filtrage heuristique est constitué sur le principe des expressions régulières. (plus d'informations pour comprendre les expressions régulières). Une expression régulière (ou rationnelle) est une chaîne de caractères permettant d'interpréter ou de réaliser des actions sur une autre chaîne de caractère. Ainsi, il est possible d'effectuer une recherche, de traiter des éléments ou de les remplacer.

Voici à quoi peut ressembler une expression régulière :

(\W|^)[\w.+\-]{0,25}@(yahoo|hotmail|gmail)\.com(\W|$)

JFA 213

Le filtrage heuristique des mails pour protéger sa messagerie des SPAM

R 2.05

- **L'analyse heuristique pour la recherche de virus :**

L'analyse heuristique est une des méthodes les plus employées pour la recherche de nouveaux virus informatique et qui permet une détection de plus de 90% des virus inconnus. L'analyse permet d'évaluer la structure d'une application afin de détecter si elle présente des caractéristiques semblables à celles d'un virus.

JFA 214

Email Spoofing (ou Address Spoofing) : Le SPAM par usurpation d'adresse IP

R 2.05

L'Email Spoofing ou Address Spoofing est une technique d'usurpation d'identité qui consiste à envoyer des messages en se faisant passer pour quelqu'un d'autre. L'objectif des spammeur est de cacher l'origine réelle de l'expéditeur, la plupart du temps pour faire croire à une adresse de confiance. La conséquence d'une telle pratique peut conduire au blacklistage de votre mail.

Cette technique d'usurpation d'identité est appelée spoofing. Elle peut être utilisée pour envoyer des SPAM mais aussi pour mettre en place des attaques contre la sécurité du réseau.

JFA 215

Email Spoofing (ou Address Spoofing) : Le SPAM par usurpation d'adresse IP

R 2.05

Les mails de retour qui saturent votre boîte de messagerie :

Avec cette technique d'email spoofing, les spammeurs peuvent envoyer des SPAM à de très nombreux destinataires. Ces messages ont de grandes chances d'être refusés par les serveurs de messagerie à cause des anti-spam. Ils vont alors renvoyer un mail de retour à l'expéditeur qui n'est pas le vrai.

Dans le cas où c'est votre adresse mail qui sert de faux expéditeur, c'est vous qui allez recevoir les retours d'emails non-délivrés et ça peut vite être très embêtant. En effet, la conséquence est que votre boîte de messagerie peut très rapidement se retrouver saturée sans que vous n'ayez jamais envoyé de message à personne.

JFA 216

Email Spoofing (ou Address Spoofing) : Le SPAM par usurpation d'adresse IP

R 2.05

Les solutions à adopter après un spoofing de mail

Il y a plusieurs cas à distinguer :

- Soit le spammeur a réussi à collecter vos identifiants : dans ce cas, il ne vous reste plus qu'à changer de mot de passe, ce qui devrait résoudre le problème.
- Soit le spammeur a réussi a infecté votre ordinateur : la solution est alors de sécuriser votre machine en trouvant le virus en question.
- S'il s'agit d'une usurpation ponctuelle, il n'y a malheureusement pas grand-chose à faire.
- Si toutefois vous avez un catch all ou collecteur d'email, vous pouvez annuler la redirection afin de limiter les retours de mails non-délivrés

La conséquence peut être un blacklistage de votre email.

Mise en place d'un Réseau

JFA 217

R 2.05

- **Etudes des différentes étapes pour mettre en place un réseau d'entreprise :**
  - Recenser les différents équipements réseau à mettre en place,
  - Répartir les différents équipements en réseaux indépendants,
  - Recenser les réseaux qui doivent communiquer entre eux,
  - Dresser un plan d'adressage, en fonction du nombre de machines dans chaque réseau.
  - Calculer les masques de sous-réseau de chacun des réseaux prévus.

JFA 218

Contenu du cours Wifi

R 2.05

- Introduction & Historique
- Le Wifi : 802.11
- Le Bluetooth : 802.15
- Le Wimax : 802.16
- Le WifiMAX : 802.11
- Le ZigBEE : 802.15.4

JFA 219

Introduction

- Plusieurs protocoles
  - Ethernet, Fast-Ethernet, Gigabit-Ethernet
  - IP, ICMP, IGMP, ARP, DHCP
  - TCP/UDP
  - Netbios (SMB/CIFS)
  - FTP, NFS, SSH
  - …
- Câbles :
  - 10Base2, 10Base5 : coaxial (cuivre)
  - 10BaseT, 100BaseT, 1000BaseTx : UTP
  - 100BaseF, 1000BaseF : fibre optique

IUT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 220

Introduction (2)

- Une machine est connectée par
  - Câble secteur
  - Câble vidéo
  - Câbles série (clavier, souris, modem, réseau)
  - Câbles parallèles (imprimante)
  - Câbles USB (imprimantes, disques, …)
  - Câbles réseau
  - …
- ➔ encombrant, ➔ peu pratique,
- ➔ peu déplaçable
- ➔ infrastructure coûteuse (tirer câbles)

IUT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 221

Historique

- Technologie ancienne
  - Radio-transmission ~ années 50
  - Initiative des armées
- Innovations (relativement) récentes
  - GSM : 1982
  - Bluetooth : 1994…maintenant
  - Hiperlan : 1996
  - Wifi : 1997…maintenant
  - HomeRF : 1998…2003 (abandonné)
  - Wimax : 2002

IUT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 222

Le Wifi

- WIreless Fidelity en référence à High Fidélity
- Groupement de constructeurs
  Wireless Ethernet Compatibility Alliance
- Normes ISO :
  - 802.11 : 1 → 2Mbit/s (1997)
  - 802.11a : jusqu'à 54Mbit/s (1999)
  - 802.11b : 11Mbit/s (1999)
  - 802.11g : jusqu'à 54Mbit/s (2003)
    compatible 802.11b
  - 802.11h : compatibilité Hiperlan2
  - 802.11i : cryptage
  - 802.11j : compatibilité réseaux japonais

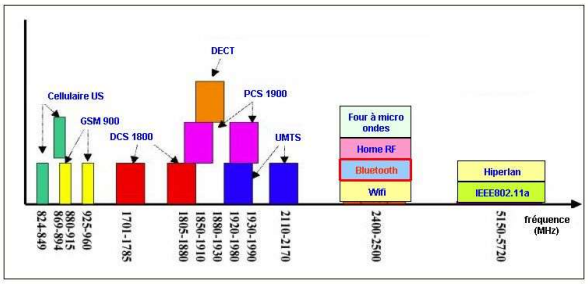
IUT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 223

Un problème de fréquences

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- Fréquences allouées par l'état
  - ARCEP (Autorité de Régulation communications électronique et des postes) ancinnement : Autorité de Régulation des Télécommunications
  - European Telecommunications Standard Institute
  - Federal Communication Commission
- Ex : 2400-2500 MHz : Wifi, Bluetooth, et Four à micro ondes !



JFA 224

Un problème de fréquences (2)

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

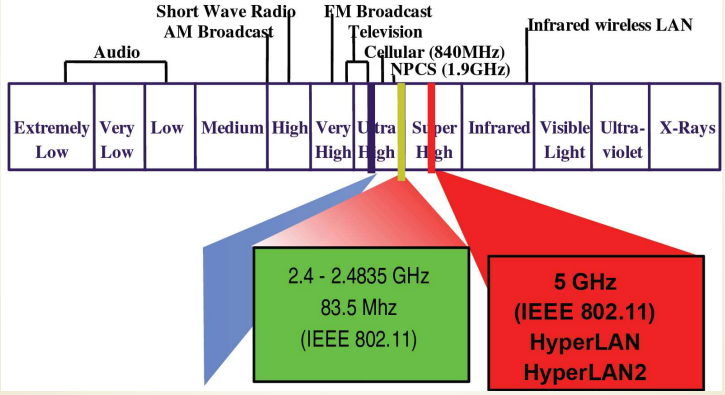
- Un réseau sans fil fournit un support radio partagé par les utilisateurs afin de communiquer entre eux et d'accéder à un réseau IP (Internet par exemple, un réseau d'entreprise, un fournisseur de services Internet, ou un fournisseur Internet d'Application). Les WLANs par exemple, existent en 900 MHz (902-928 MHz), 2,4 GHz (2400-2483.5MHz) et 5 GHz (5150-5850MHz) ISM (industriel, scientifique médical, sans licence) en bandes radio de fréquence. Les graphiques ci-dessous illustre le cas dans le spectre des bandes de fréquences sans licence utilisées pour LAN sans fil résident.

JFA 225

Un problème de fréquences (2)

R 2.05

- La bande Industry-Science-Medical
- Sans autorisation



JFA 226

Un problème de fréquences (4)

R 2.05

- **2.4 GHz ISM Band**
- La bande ISM sans licence à 2,4 GHz est disponible à l'échelle mondiale. Il est cependant utilisé par de nombreux systèmes différents, y compris les fours à micro-ondes, téléphones sans fil (USA), WLAN IEEE 802.11b, Bluetooth WPAN. Les fréquences autorisées sont 2.4-2.4835 GHz. Certains pays limitent le nombre de canaux disponibles et la largeur de bande de canal pour des sauts de fréquence. Les normes IEEE 802.11 prennent en compte les différents domaines réglementaires permettant ces paramètres à définir par l'utilisateur.

JFA 227

Un problème de fréquences (4)

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- **5 GHz ISM Band**
- 5,15 à 5,25 GHz: Cette bande est disponible dans de nombreuses régions du monde, et est partagé seulement avec les service de connexion primaire de liaisons terre-espace. En Europe, cette bande est limitée au service primaire partagé avec High Performance Radio Local Area Networks (RLAN).
- 5,25 à 5,35 GHz: Cette bande est partagée avec les services de radio-localisation / navigation et exploration de la Terre par satellite. Il est également disponible pour les RLAN dans la plupart des régions de 5,15 à 5,25 GHz, à l'exception du Japon.
- 5,470 à 5,725 GHz: Cette bande est partagée de manière similaire en Europe. Par conséquent, l'ingérence dans ces bandes en Europe est limitée à d'autres RLAN et aux services primaires seulement. L'Europe est la seule région à ce jour à avoir permis de 5,470 à 5,725 GHz pour les RLAN, mais la répartition dans les autres régions est un sujet abordé par la prochaine Conférence mondiale des radiocommunications.
- 5,725 à 5,825 GHz: Cette bande est actuellement adapté pour une utilisation RLAN aux Etats-Unis et au Canada. C'est une bande ISM, mais dans d'autres régions les applications à courte portée sont limitées à une faible puissance, par exemple 50 mW en Europe
- *La bande des 5 GHz semble être le spectre où le déploiement de masse des produits WLAN s'intensifie. !!*

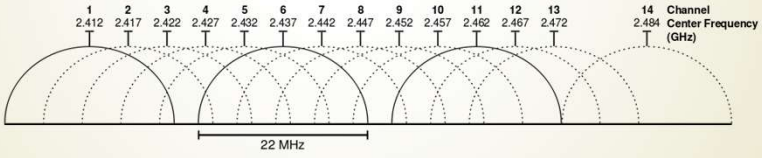
JFA 228

Un problème de fréquences (4)

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Dans le standard 802.11b/g, le WiFi utilise une bande de fréquence étroite (de 2,3995 GHz à 2,4845 GHz, soit 85 MHz) de type partagée. Pour simplifier les choses, cette bande de fréquence a été découpé en 13 canaux de 25 MHz séparés de 5 MHz.
- En France, le canal 1 commence à 2,412 MHz et le 13 ferme la marche à 2,472 MHz (varie suivant la loi imposée dans chaque pays).



JFA 229

Un problème de fréquences (4)

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Toutefois, pour une transmission de 11 Mbps correcte il est nécessaire de transmettre sur une bande de 22 MHz car, d'après le théorème de Shannon, la fréquence d'échantillonnage doit être au minimum égale au double du signal à numériser. Ainsi certains canaux recouvrent partiellement les canaux adjacents, c'est la raison pour laquelle des canaux isolés (les canaux 1, 6 et 11) distants les uns des autres de 25MHz sont généralement utilisés.
- Ainsi, si deux points d'accès utilisant les mêmes canaux ont des zones d'émission qui se recoupent, des distorsions du signal risquent de perturber la transmission. Ainsi pour éviter toute interférence il est recommandé d'organiser la répartition des points d'accès et l'utilisation des canaux de telle manière à ne pas avoir deux points d'accès utilisant les mêmes canaux proches l'un de l'autre.

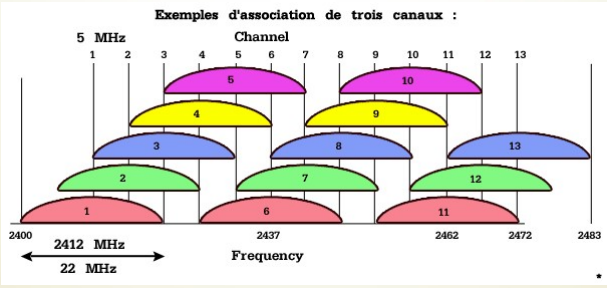
JFA 230

Un problème de fréquences (4)

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Bande des 2400MHz-2483,5MHz
- 13 canaux de 22MHz (chevauchement)
  - Théorème de Shannon → 11M bit/s
  - 1-11 aux USA, 1-13 en France, 1-14 au Japon



JFA 231

Structure du réseau

R 2.05

3 niveaux :

- Independant Basic Service Set (IBSS)
  - Machines connectées ensembles
- Basic Service Set (BSS)
  - 1 point d'accès (AP)
  - Machines connectées à cet AP
- Extended Service Set (ESS)
  - Plusieurs BSS, Reliés entre eux
    - En filaire
    - En sans-fil

JFA 232

Structure du réseau

R 2.05

- Ad-Hoc :

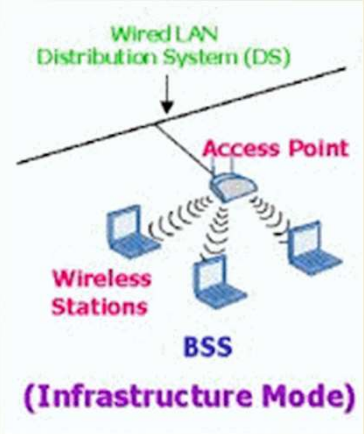
➢ Le fonctionnement de ce mode est totalement distribué, il n'y a pas d'élément permettant une structure hiérarchique. Ce mode permet la communication entre deux machines sans l'aide d'une infrastructure. Les stations se trouvant à portée de radio forment un IBSS (Independant Basic Service Set).

JFA 233

Structure du réseau

R 2.05

- Infrastructure :
  - Le mode infrastructure se base sur une station spéciale appelée Point d'Accès (PA). Ce mode permet à des stations wifi de se connecter à un réseau (généralement Ethernet) via un point d'accès. Elle permet à une station wifi de se connecter à une autre station wifi via leur Point d'Accès commun. Une station wifi associée à un autre Point d'Accès peut aussi s'interconnecter. L'ensemble des stations à portée radio du Point d'Accès forme un BSS (Basic Service Set). Chaque BBS est identifié par un BSSID (BSS Identifier) de 6 octets qui correspond à l'adresse MAC du Point d'Accès.

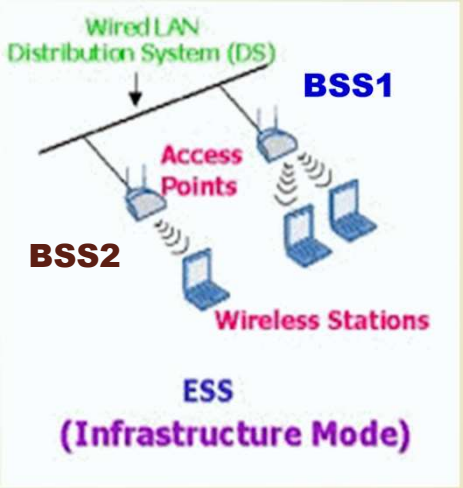


JFA 234

Structure du réseau

R 2.05

- Infrastructure étendue:
  - On peut composer un réseau avec plusieurs BSS. Ceux-ci sont reliés entre eux par un Système de Distribution (DS) connecté à leurs points d'accès. Ce DS est généralement le réseau Ethernet sur lequel le PA se connecte mais il peut correspondre à du token ring, FDDI ou un autre réseau 802.11. Ces différents BSS interconnectés via un DS forme un ESS (Extended Service Set). Un ESS est identifié par un ESSID (abrégé en SSID) qui est constitué d'un mot de 32 caractères qui représente le nom du réseau.
  - On peut associer un IBSS au sein d'un ESS.



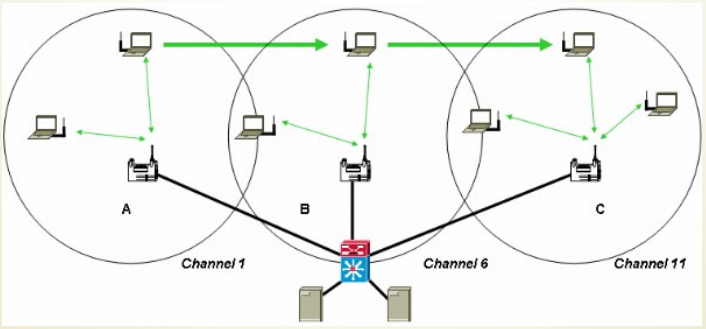
JFA 235

Structure du réseau

R 2.05

Application de l'ESS:

- Par l'extension d'un BSS (avec le même SSID) qui forme un ESS, La station peut alors se déplacer du point d'accès A au point d'accès C. Cela permet de faire du Wifi itinérant sur une petite distance,



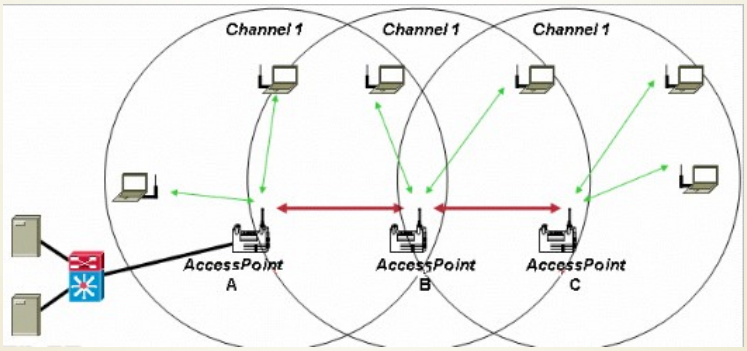
JFA 236

Structure du réseau

R 2.05

Application : Etendre la zone de réception

- Point d'accès en mode répéteur : permet d'étendre la zone de couverture du BSS, partage de la bande passante totale sur toute la zone.,



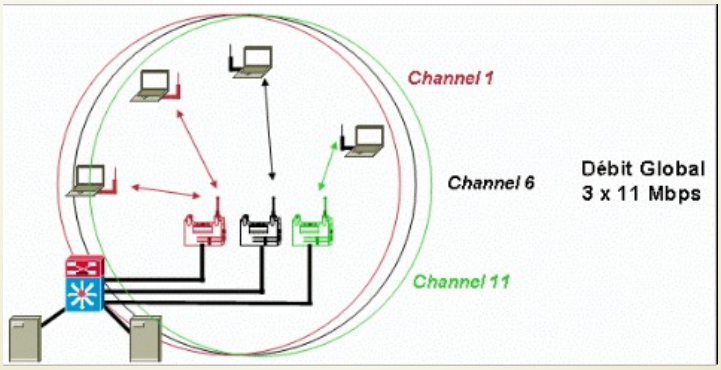
JFA 237

Structure du réseau

R 2.05

Application : Partage de charge

- trois canaux recouvrent la même zone et augmentent ainsi le débit. La station détermine le meilleur point d'accès suivant le signal et la charge de l'AP.



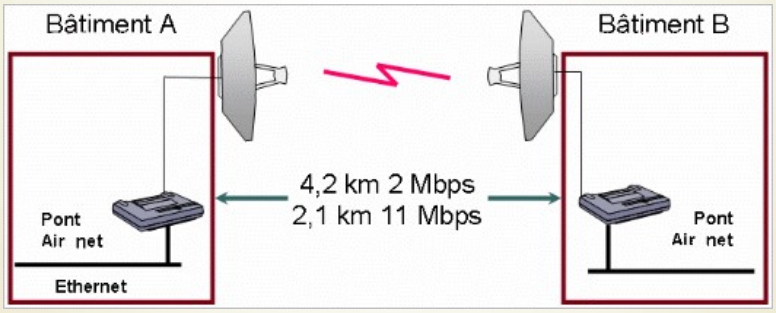
JFA 238

Structure du réseau

R 2.05

Application : Interconnexion à distance

- Interconnexion à distance de réseaux privés : ici la norme Wi-Fi permet d'interconnecter deux bâtiments.

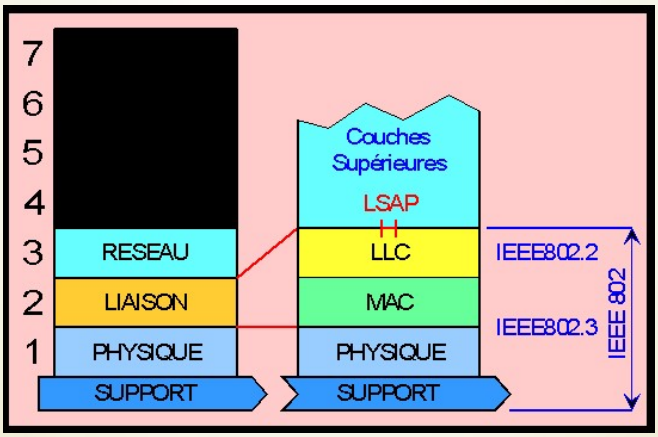


JFA 240

Architecture logicielle 802.11

R 2.05

- Correspondance Modèle OSI pour le WI-FI



JFA 241

Architecture logicielle 802.11

R 2.05

- Pour la couche 2 :
- Elle est découpée en 2 couches :
  - Couche LLC
    - Adressage & liaison de données
  - Couche MAC
    - CSMA/CA (collision avoidance) ou Accès par priorité (802.12)
    - Association à un AP
    - Confidentialité

JFA 242

Architecture logicielle 802.11

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Pour la couche 1 : Couche physique
  - Elle peut utiliser 3 codages différents :
    - FHSS (saut de fréquence)
    - DSSS (séquence de Barker)
    - IR (codage par position)

JFA 243

Couche Physique : FHSS

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Étalement de spectre par saut de fréquence (Frequency Hopping Spread Spectrum)
  - est une méthode de transmission de signaux par ondes radio qui utilise alternativement plusieurs canaux (sous-porteuses) répartis dans une bande de fréquence selon une séquence pseudo-aléatoire connue de l'émetteur et du récepteur.
  - Cette méthode est utilisée dans les torpilles radio-guidées, qui permettait au système émetteur-récepteur de la torpille de changer de fréquence, rendant pratiquement impossible la détection de l'attaque sous-marine par l'ennemi. Il s'agit aussi du principe de transmission toujours utilisé pour le positionnement par satellites (GPS, GLONASS…), les liaisons chiffrées militaires, les communications des navettes spatiales avec le sol et dans les techniques Wi-Fi.

JFA 244

Couche Physique : FHSS

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Les réseaux Wifi actuels utilisant cette technologie sont définis par des standards ce qui signifie que la séquence des fréquences utilisée est connue de tous (et n'assure donc plus cette fonction de sécurisation des échanges) : le FHSS était utilisé dans les premières versions des standards IEEE 802.11 afin de réduire les interférences entre les transmissions des diverses stations d'une cellule.
- Norme 802.11 :
- La bande de fréquence 2,4 - 2,485 GHz permet de créer jusqu'à 79 canaux de 1 MHz chacun. La transmission se faisait ainsi, à l'aide des méthodes FHSS, en émettant successivement sur un canal puis sur un autre pendant une courte période de temps (maximum 400 ms) en utilisant une combinaison, connue de toutes les stations, d'une partie des canaux regroupés dans une bande de 80 MHz, ce qui permet à un instant donné de transmettre un signal facilement reconnaissable sur une fréquence donnée. Les versions plus récentes des normes 802.11 (g, n et ac) utilisent une autre méthode de codage sans « saut de fréquence », mais permettant des débits plus élevés : l'OFDM.

JFA 245

Couche Physique : FHSS

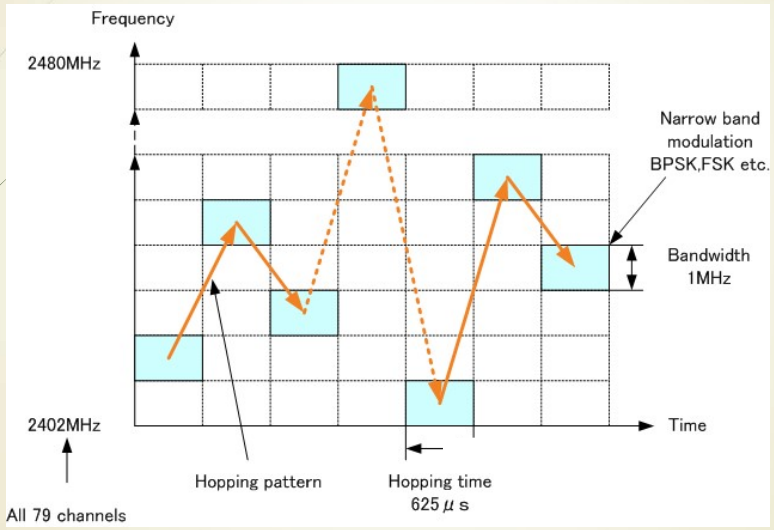
IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Plages de fréquences utilisées par les normes 802.11, b, g et n :
  France : 2,4 à 2,483 GHz ;
- Une variante est aussi utilisée dans les normes Bluetooth[2].
- L'étalement de spectre offre trois avantages par rapport à l'utilisation d'une fréquence unique :
  - il rend le signal transmis plus résistant aux interférences,
  - le signal est plus difficile à intercepter,
  - les signaux transmis de cette manière peuvent partager des bandes de fréquence avec d'autres types de transmission, ce qui permet d'utiliser plus efficacement la bande passante ; le partage des fréquences ajoute un minimum de bruit à l'un et à l'autre types de transmission.

JFA 246

Couche FHSS

R 2.05

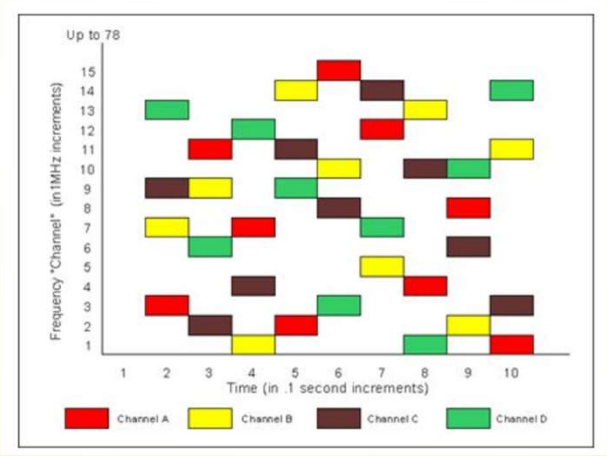


JFA 247

Couche FHSS

R 2.05

- Transmission de plusieurs canaux :



JFA 248

Couche FHSS : Synthèse

R 2.05

- Frequency Hopping Spread Spectrum
- 79 canaux de 1MHz
- 78 séquences de canaux ≠
- Au moins 2,5 sauts par seconde
- Avantages
  - Résistance aux perturbations
  - Propagations multiples
- Inconvénients
  - Matériel cher
  - Propagation multiple (Pls réceptions/émission)
  - Faible débit, faible portée

JFA 249

Couche Physique : DSSS

R 2.05

- DSSS : Direct-Sequence Spread Spectrum
- Le but du DSSS est de rendre les signaux occupant une bande de fréquence plus résistants aux brouillages et aux interférences rencontrés lors de la transmission ; et d'autre part de permettre à plusieurs équipements de partager la même fréquence porteuse (accès multiple par répartition par code). Pour cela, ils sont combinés avec un signal pseudo-aléatoire de fréquence beaucoup plus élevée. En conséquence, le signal résultant occupe une bande de fréquence plus large, déterminée par la fréquence du signal pseudo-aléatoire. Cette technique s'applique essentiellement à des liaisons numériques; le signal d'étalement est dans ce cas une séquence de code pseudo-aléatoire.
- Le fait d'étaler la puissance du signal émise sur une bande de fréquence plus large diminue la densité de puissance émise et dans le cadre d'applications militaires, le DSSS peut être utilisé dans un tout autre but : dissimuler le signal en augmentant sa ressemblance avec un bruit aléatoire.

JFA 250

Couche Physique : DSSS

R 2.05

- La technique DSSS consiste à transmettre pour chaque bit une séquence Barker (bruit pseudo-aléatoire) de 11 bits. Ainsi chaque bit valant 1 est remplacé par une séquence de 11 bits et chaque bit valant 0 par son complément.
- La couche physique de la norme 802.11 définit une séquence de 11 bits « 10110111000 » pour représenter un 1 et « 01001000111 » pour coder un 0. On appelle chip ou chipping code chaque bit encodé à l'aide de la séquence. Cette technique de chipping revient donc à moduler chaque bit avec la séquence barker.

- Grâce au chipping, de l'information redondante est transmise, ce qui permet d'effectuer des contrôles d'erreurs sur les transmissions, voire de la correction d'erreurs (Distance de Hamming de 11).

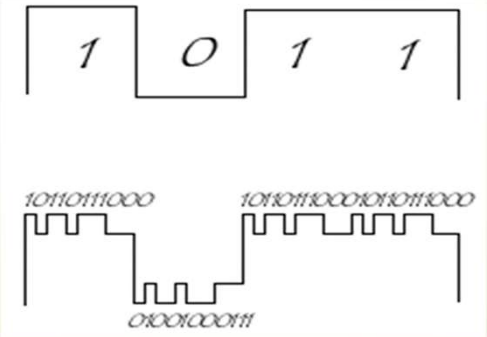
JFA 251

Couche Physique : DSSS

R 2.05

- ***Exemple :***

  Envoi de 11 bits pour 1 bit (802.11) (6 « 1 » et 5 « 0 »)
  - 10110111000 = 1
  - 01001000111 = 0 (complément)

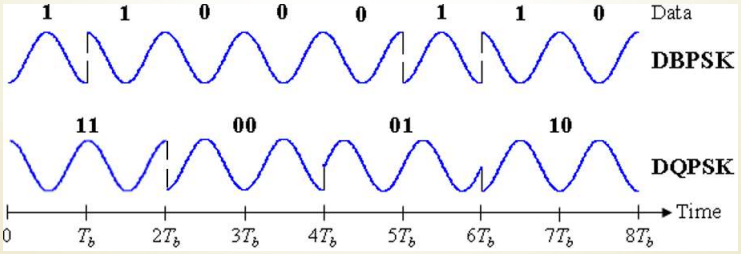


JFA 252

Couche Physique : DSSS

R 2.05

- Avantage :
  - Matériel simple
  - Peu sensible aux interférences
  - Détection/Correction d'erreurs
- Inconvénients :
  - 1Mbit/s (modulation en 2 phases : DBPSK)
  - 2Mbit/s (modulation en 4 phases : DQPSK)



JFA 253

Couche Physique : Optimisation

R 2.05

- La norme 802.11b propose d'autres types d'encodage permettant d'optimiser le débit de la transmission. Les deux séquences Barker ne permettent de définir que deux états (0 ou 1) à l'aide de deux mots de 11 bits.
- Une méthode alternative appelée CCK (complementary code keying) permet d'encoder directement plusieurs bits de données en un seul chip en utilisant 8 séquences de 64 bits. Ainsi en codant simultanément 4 bits, la méthode CCK permet d'obtenir un débit de 5.5 Mbps et elle permet d'obtenir un débit de 11 Mbps en codant 8 bits de données.
- La technologie PBCC (Packet Binary Convolutionnary Code) permet de rendre le signal plus robuste vis-à-vis des distorsions dues au cheminement multiple des ondes hertziennes. Ainsi la société Texas Instrument a réussi a mettre au point une séquence tirant avantage de cette meilleure résistance aux interférences et offrant un débit de 22 Mbit/s. Cette technologie baptisée 802.11b+ est toutefois non conforme à la norme IEEE 802.11b ce qui rend les périphériques la supportant non compatibles avec les équipements 802.11b.

JFA 254

Couche Physique : OFDM

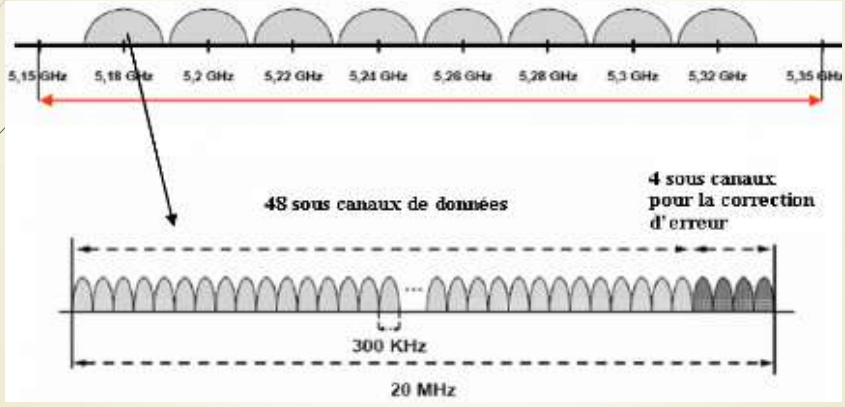
R 2.05

- OFDM (Orthogonal Frequency Division Multiplexing)
- La norme 802.11a opère dans la bande de fréquence des 5 GHz, qui offre 8 canaux distincts, c'est la raison pour laquelle une technique de transmission alternative tirant partie des différents canaux est proposée. L'OFDM (Orthogonal Frequency Division Multiplexing) permet d'obtenir des débits théoriques de 54 Mbps en envoyant les données en parallèle sur les différentes fréquences. De plus la technique OFDM fait une utilisation plus rationnelle du spectre.
- Le principe de cette technique consiste à diviser le signal que l'on veut transmettre sur différentes bandes porteuses, comme si l'on combinait ce signal sur un grand nombre d'émetteurs indépendants, fonctionnant sur des fréquences différentes. Un canal est constitué de 52 porteuses de 300 KHz de largeur, 48 porteuses sont dédiées au transport de l'information utile et 4 pour la correction d'erreurs appelées porteuses pilote, Huit canaux de 20 MHz sont définis dans la bande de 5 GHz

JFA 255

Couche Physique : OFDM

R 2.05



JFA 256

Couche Physique : MIMO

R 2.05

- Deux autres éléments importants ont fait leurs apparition avec la norme 802.11n : le MIMO et la largeur de canal. Commençons avec le MIMO, il s'agit en fait d'un nouveau type d'antenne bien plus performant. Jusqu'ici les routeurs sont équipés d'une ou deux antennes : Une pour émettre et une pour recevoir les informations. Ces antennes sont maintenant dépassées et leurs mode de fonctionnement est sur le point de changer !

- MIMO signifie "Multiple Inputs, Multiple Outputs" cela signifie en anglais "entrées multiples, sorties multiples", ces antennes sont donc capables d'émettre et de recevoir à destination de plusieurs sources. Les antennes les plus répandues de ce type sont les MIMO 2×2 (2 entrées et 2 sorties) mais pour les réseaux chargés il est possible d'utiliser une antenne 3×3 par exemple ou encore 4×4. Quoi qu'il en soit cette révolution du monde des antennes Wifi a permis de multiplier le débit maximal de la norme utilisée, en utilisant une antenne MIMO 2×2 on peut théoriquement doubler la bande passante du réseau !

JFA 257

Couche Physique : MIMO

R 2.05

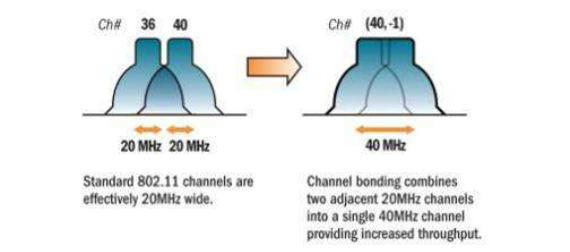
https://siam.lyon.archi.fr/index.php/informatique/materiels/431-wifi-normes

JFA 258

Couche Physique : Largeur de bande

R 2.05

Le deuxième élément qui a été ajouté sur la norme 802.11n c'est la largeur de bande. Jusqu'ici celle-ci était systématiquement autours des 20 Mhz, cependant les concepteurs de la nouvelle norme 802.11n se sont rendu compte que plus la largeur de bande était importante plus les débits qui y transitent pouvaient être élevés. Un canal plus large permet en effet de faire transiter plus de données sur le même intervalle de temps. Sur la norme 802.11n on retrouve donc 2 largeurs de canaux différentes : 20 Mhz ou 40 Mhz. Comme vous vous en doutez le débit de la bande large de 40 Mhz est l'équivalent du double de celui sur la bande 20 Mhz.



https://siam.lyon.archi.fr/index.php/informatique/materiels/431-wifi-normes

JFA 259

Couche Physique : Beamforming

R 2.05

- Le BeamForming est une technologie utilisée par les constructeurs de routeurs wifi pour améliorer la stabilité et la puissance du signal, donc d'améliorer considérablement la portée et le débit de leur signal Wifi.
- La technologie BeamForming permet au routeur de concentrer le signal vers une direction précise : celle du récepteur ! Comme avec la technologie QoS, le signal va être envoyé plus ou moins fort en fonction de la distance entre le routeur et le récepteur, permettant ainsi une meilleure gestion des ressources du routeur, une meilleure connexion internet et une utilisation plus réfléchie de l'énergie.
- Cette technologie n'est accessible qu'en choisissant un routeur utilisant la norme 802.11ac.

JFA 260

Couche Physique : Beamforming

R 2.05

- Voilà donc le résultat final du Beamforming – Un signal plus puissant et stable émis directement dans la direction de vos appareils connectés. Je vous propose un petit graphique proposé par Netgear sur le Beamforming :

https://le-routeur-wifi.com/beamforming/

JFA 261

Couche Physique : Synthèse

R 2.05

Technique	Avantages	Inconvénients
DSSS	- Elle propose des vitesses de transmissions plus importantes.	- L'utilisation d'un seul canal pour la transmission, rend le système DSSS plus sensibles aux interférences.
FHSS	- Elle empêche une perte totale du signal, grâce à la technique de transmission par saut. - Elle constitue une solution efficace dans un environnement où il y a beaucoup de multi trajets.	- faible largeur de bande par canal ne lui permettant pas d'atteindre des vitesses de transmissions élevées. - Utilisation de toute la largeur de bande, ce qui implique une charge supplémentaire sur le réseau.
Infrarouge		- La transmission se fait avec une longueur d'onde très faible. - Une traversée des obstacles (murs, plafonds, cloisons...) n'est pas possible.
OFDM	- Permet d'atteindre des vitesses de transmission jusqu'à 54 Mbps pour la 802.11a et la 802.11g. - Elle offre un mécanisme de correction d'erreurs sur l'interface physique.	

JFA 262

Synthèse en 802.11

R 2.05

Technologie	Codage	Type de modulation	Débit
802.11b	DSSS (2 phases)	BPSK	1 Mbps
802.11b	DSSS (4 phases)	QPSK	2 Mbps
802.11b	CCK (4 bits)	QPSK	5,5 Mbps
802.11b	CCK (8 bits)	QPSK	11 Mbps
802.11a	CCK (8 bits)	OFDM	54 Mbps
802.11g	CCK (8 bits)	OFDM	54 Mbps

JFA 263

Synthèse en 802.11

R 2.05

Protocole 802.11	date	F (GHz)	Largeur de bande (MHz), (GHz)	Débit binaire (Mbit/s), (Gbit/s)	Nombre maximum de flux MIMO	Codage / Modulation	Portée Intérieur (mètres)	Portée Extérieur (mètres)
802.11-1997 (d'origine)	juin 1997	2,4	79 ou 22 MHz	1, 2 Mbit/s	NC	FHSS, DSSS	20 m	100 m
802.11b (Wi-Fi 1)	sept 1999	2,4	22 MHz	1, 2, 5,5, 11 Mbit/s	1	DSSS	38 m	140 m
802.11a (Wi-Fi 2)	sept 1999	5	20 MHz	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	1	OFDM	35 m	120 m
802.11g (Wi-Fi 3)	juin 2003	2,4	20 MHz	6, 9, 12, 18, 24, 36, 48, 54 Mbit/s	1	OFDM	70 m (2,4 GHz) 12-35 m (5 GHz)	250 m
802.11n (Wi-Fi 4)	oct 2009	2,4 / 5	20 MHz	7,2 à 72,2 Mbit/s[B] (6,5 à 65)[C]	4	OFDM	70 m (2,4 GHz) 12-35 m (5 GHz)	250 m
			40 MHz	15 à 150 Mbit/s[B] (13,5 à 135)[C]			12-35 m	300 m
802.11ac (Wi-Fi 5)	déc 2013	5	20 MHz	6,5 à 346,8 Mbit/s[D]	8	OFDM	12-35 m 10 m	300 m
			40 MHz	13,5 à 800 Mbit/s[D]				
			80 MHz	19,3 Mbit/s à 1,7 Gbit/s[D]				
			160 MHz	58,5 Mbit/s à 3,4 Gbit/s[D]				
802.11ad	déc 2012	57 à 71	1,7 à 2,16 GHz	jusqu'à 6,75 Gbit/s	NC	OFDM ou porteuse unique	100 m	1000 m
802.11af	fév 2014	0,054 à 0,79	6 à 8 MHz	1,8 à 568,9 Mbit/s	1, 2, 4	OFDM	100 m	
802.11ah	mai 2017	0,9	1 à 8 MHz	0,6 à 8,6 Mbit/s	4	OFDM	12-35 m	300 m
802.11ax (Wi-Fi 6)	fév 2021	1 à 7,1	20 MHz	8 Mbit/s à 1,1 Gbit/s[D]	8	OFDM, OFDMA	12-35 m 100 m	300 m 500
			40 MHz	16 Mbit/s à 2,3 Gbit/s[D]				
			80 MHz	34 Mbit/s à 4,8 Gbit/s[D]				
			160 MHz	68 Mbit/s à 10,5 Gbit/s[D]				
802.11ay	mars 2021	58,3 à 70,2	2,16 à 8,64 GHz	20 à 176 Gbit/s	4	OFDM ou single carrier		

https://fr.wikipedia.org/wiki/IEEE_802.11g

JFA 264

Couche Physique : Infra Rouge

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- ***La technologie infrarouge :***
- Le standard IEEE 802.11 prévoit également une alternative à l'utilisation des ondes radio : la lumière infrarouge. La technologie infrarouge a pour caractéristique principale d'utiliser une onde lumineuse pour la transmission de données. Ainsi les transmissions se font de façon uni-directionnelle, soit en "vue directe" soit par réflexion. Le caractère non dissipatif des ondes lumineuses offre un niveau de sécurité plus élevé.
- Il est possible grâce à la technologie infrarouge d'obtenir des débits allant de 1 à 2 Mbit/s en utilisant une modulation appelé PPM (Pulse Position Modulation).
- La modulation PPM consiste à transmettre des impulsions à amplitude constante, et à coder l'information suivant la position de l'impulsion (sur l'axe des temps). Le débit de 1 Mbps est obtenu avec une modulation de 16-PPM, tandis que le débit de 2 Mbps est obtenu avec une modulation 4-PPM permettant de coder deux bits de données avec 4 positions possibles :

JFA 265

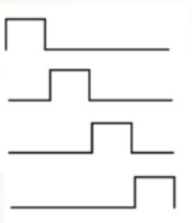
Couche Physique : IR

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Exemple :

  2 bits par modulation : 4 PPM : 2 Mbps

  - 00
  - 01
  - 10
  - 11



JFA 266

La couche MAC :

R 2.05

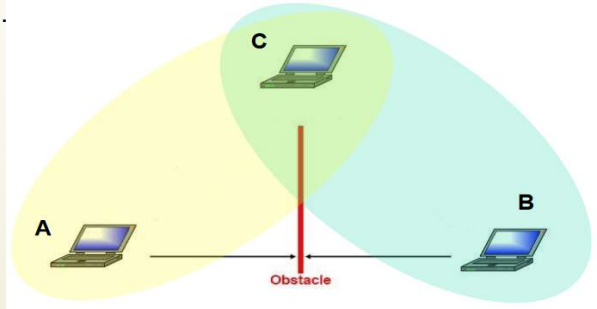
- La sous-couche MAC (Media Access Control) est spécifique à la norme Wi-Fi et définit deux nouveaux mécanismes qui assurent la gestion d'accès de plusieurs stations à un support partagé dans lequel chaque station écoute le support avant d'émettre, elle assure aussi le contrôle d'erreur permettent de contrôler l'intégrité de la trame à partir d'un CRC.
- Elle utilise deux modes de fonctionnement :
  - DCF
  - PCF

JFA 267

DCF : Le problème de la station cachée

R 2.05

- 3 stations : A, B et C;
  - La station C peut communiquer avec chacune des 2 autres stations (A et B) ;
  - Mais A et B ne se voient pas entre elles (obstacle, distance, ..)
  - ⇒ Les 2 stations A et B détectent une porteuse libre et émettent.
  - ⇒ Il y a collision au niveau de la station C, qui ne peut jamais émettre.

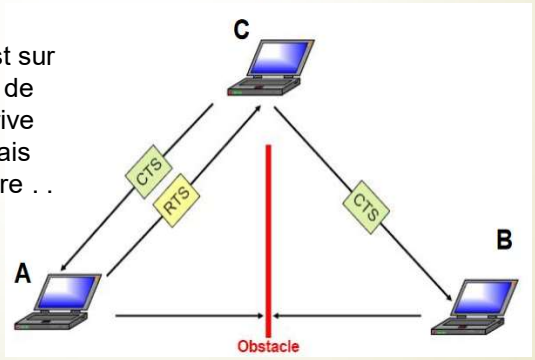


JFA 268

DCF : Le problème de la station cachée

R 2.05

- Résolution du problème par réservation du canal :
  - envoi d'une trames RTS (Request To Send) par A (ou B)
  - le destinataire (station C) répond par une CTS (Clear To Send)
  - la station B (et A) reçoit le CTS et comprend qu'il y a une station cachée.
  - s'il y a collision, c'est sur le RTS. Mais moins de chance que cela arrive car trame courte. Mais overhead protocolaire . .



JFA 269

La couche MAC : DCF

R 2.05

- Distributed coordination fonction (DCF) :
  - C'est un mode qui peut être utilisé par tous les mobiles, et qui permet un accès équitable au canal radio sans aucune centralisation de la gestion de l'accès (mode totalement distribué). Il met en œuvre un certain nombre de mécanismes qui visent à éviter les collisions et non pas à les détecter. Dans ce mode tous les nœuds sont égaux et choisissent quand ils veulent parler. Ce mode est accessible sans point d'accès lorsqu'il n'y a pas de station de base (mode ad hoc) aussi bien que lorsqu'il y a un point d'accès (mode infrastructure).
  - Ce mode s'appuie sur le protocole CSMA/CA.

JFA 270

La couche MAC : CSMA/CA

R 2.05

- La méthode d'accès de base CSMA/CA :
  - Un protocole CSMA/CA (Carier Sense Multiple Access with Collision Avoidance) utilise un mécanisme d'esquive de collision en imposant un accusé de réception systématique des paquets (ACK), ce qui signifie que pour chaque paquet de données arrivé intact, un paquet ACK est émis par la station de réception.
  - Ce protocole fonctionne de la manière suivante : Une station voulant émettre, doit d'abord écouter le support de transmission, s'il est occupé (i.e. une autre station est en train d'émettre), alors, la station remet sa transmission à plus tard différée. Dans le cas contraire, la station est autorisée à transmettre.
  - La procédure de vérification se fait en utilisant deux types de messages, le premier est appelé RTS (Ready To Send) qui est envoyé par la station et contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond par un deuxième message qui est le CTS (Clear To Send), puis la station commence l'émission des données :

JFA 271

La couche MAC : CSMA/CA

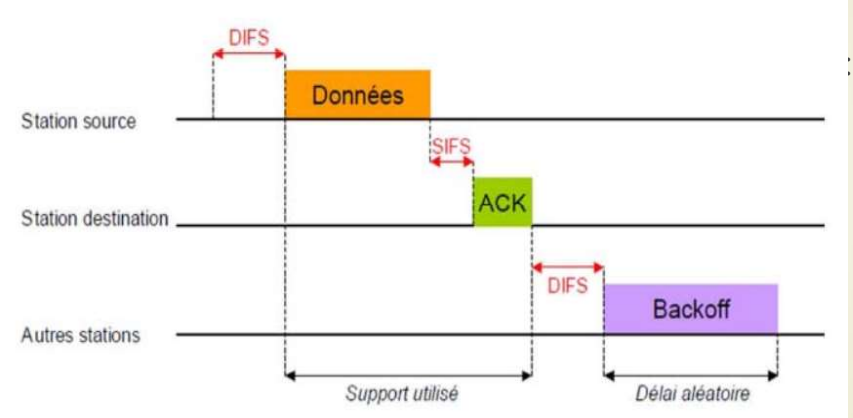
R 2.05

- A chaque paquet envoyé, l'émetteur doit recevoir un accusé de réception ACK (ACKnowledgement), qui indiquera qu'aucune collision n'a eu lieu.
- Si l'émetteur ne reçoit pas de l'accusé de réception, alors il retransmet la trame après un ACK_TIMEOUT jusqu'à ce qu'il obtienne un accusé réception ou abandonne au bout d'un certain nombre de transmission.
- Ce type de protocole est très efficace quand le support n'est pas surchargé, mais il y a toujours une chance que des stations émettent en même temps (collision). Cela est dû au fait que les stations écoutent le support, repèrent qu'il est libre, et finalement décident de transmettre, parfois en même temps qu'un autre, exécutant cette même suite d'opération.
- Ces collisions doivent être détectées pour que la couche MAC puisse retransmettre le paquet sans avoir à repasser par les couches supérieures, ce qui engendrerait des délais significatifs.

JFA 272

La couche MAC : CSMA/CA

R 2.05



JFA 273

La couche MAC : CSMA/CA

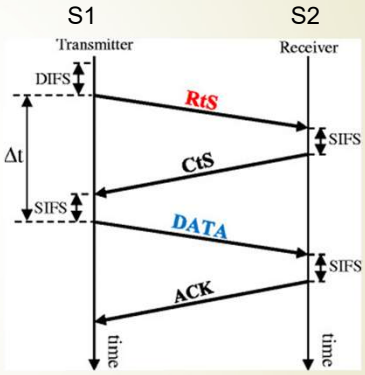
R 2.05

- Schéma : Mécanisme de vérification du canal :
- La station voulant émettre écoute le réseau. Si le réseau est occupé, la transmission est différée. Dans le cas contraire, si le média est libre pendant un temps donné (appelé DIFS pour *Distributed Inter Frame Space*), alors la station peut émettre. La station transmet un message appelé *Ready To Send* (ou *Request To Send*, noté RTS signifiant prêt à émettre) contenant des informations sur le volume des données qu'elle souhaite émettre et sa vitesse de transmission. Le récepteur (généralement un point d'accès) répond un *Clear To Send* (CTS, signifiant *Le champ est libre pour émettre*), puis la station commence l'émission des données. Toutes les stations avoisinantes patientent pendant un temps calculé à partir du CTS (ou du RTS, mais tous les voisins ne reçoivent pas forcément le RTS de la station émettrice en raison des rayons de portée radio).
- À réception de toutes les données émises par la station, le récepteur envoie un accusé de réception (ACK).

JFA 274

DCF
Réservation du canal

- Mécanisme RTS/CTS
  - *Ready To Send* : « Je veux te parler »
  - *Clear To Send* : « Je t'écoute »
- Une station S1 envoie RTS à S2
  - Trame très courte suivie d'un SIFS
- S2 envoie CTS
  - Trame très courte suivie d'un SIFS
  - Toutes les autres stations se taisent et attendent
- S1 envoie les données
  - Trames suivies de SIFS
- S2 accuse réception
  - 1 DIFS d'attente
  - Toutes les stations recommencent à émettre



JFA 275

Couche MAC
Point Coordination Function

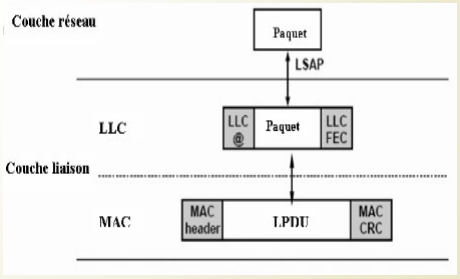
- Point Coordination Fonction (PCF):
  - Le (PCF) appelée mode d'accès contrôlé, est fondé sur l'interrogation à tour de rôle des stations, contrôlé par le point d'accès qui indiquera a chacune des stations qui lui sont rattachées quand elles doivent émettre leurs paquets. Durant la phase où le point d'accès impose l'ordre des transmissions, il n'y a pas de contention pour l'accès au canal (pas de collisions).
  - Une station ne peut émettre que si elle est autorisée et elle ne peut recevoir que si elle est sélectionnée. Cette méthode est conçue pour les applications temps réel (vidéo, voix) nécessitant une gestion du délai lors des transmissions de données. Cette méthode est optionnelle et ne fonctionne qu'en mode infrastructure.

JFA 276

La couche LLC

R 2.05

- La couche LLC a été définie par le standard IEEE 802.2, elle permet d'établir un lien logique entre la couche MAC et la couche réseau du modèle OSI. Ce lien se fait par l'intermédiaire du Logical Service Access Point (LSA P).
- La trame LLC contient une adresse en en-tête ainsi qu'une zone de détection d'erreur en fin de trame : le *forward error correction* (FEC) comme le montre la figure suivante :
- Son rôle principal réside dans son système d'adressage logique, qui permet de masquer aux couches hautes les informations provenant des couches basses. Cela permet de rendre interopérables des réseaux complètements différents dans la conception de la couche physique ou la couche MAC possédant la couche LLC.



JFA 277

La sécurité du Wifi

R 2.05

Les menaces du sans fil :

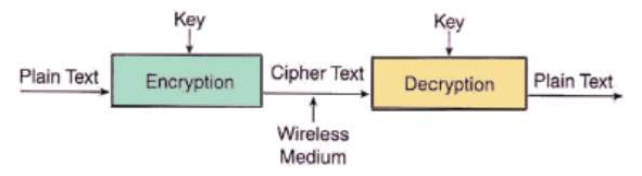
- Utilisation des ondes électromagnétiques :
  - Problème de sécurisation géographique des zones d'émission
  - Technologie "accessible" (il suffit d'une antenne)
- Attaques passives :
  - ⇒ Espionnage
  - ⇒ Interception
- Attaques actives :
  - ⇒ Modification des messages
  - ⇒ Déguisement
  - ⇒ Brouillage de toutes les communications

JFA 278

La sécurité du Wifi : 1ères Solutions

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- SSID (Service Set ID) : transmission régulière d'un ID qui définit le réseau. Permet la gestion de la mobilité et la synchronisation des stations.
- ACL (Access Control List) : dans l'AP, liste des @MAC autorisées à se connecter.
- WEP (Wired Equivalent Privacy) : clé secrète et partagée, confidentialité par cryptage. WEP = authentification + chiffrement (aléatoire) des données.



- Authentification : deux modes prévu en 802.11
  - Authentification en système ouvert : une station souhaitant se joindre envoie une trame spécifique à l'AP qui renvoie un ACK.
  - Authentification par clé partagée : utilisation du WEP,

JFA 279

La sécurité du Wifi : Les réponses

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

- **WPA** (2003) : amélioration du WEP

Version temporaire de la norme 802.11i

  - 128 bits
  - clé dynamique : contrôleur + serveur authentification
  - vecteur d'initialisation plus grand

- **RADIUS**, **serveur 802.1x** : serveur global d'authentification, avec login et password (utilisable avec WAP, WAP2..)

- **802.11i & WPA 2** (2004 + certification) : amélioration du système de chiffrement % WAP; overhead

- **VPN** (tunneling) : encapsulation et cryptographie des données transmises.

JFA 280

La sécurité du Wifi : Le WPA et WPA2

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- **WPA** a été prévu comme une solution intermédiaire pour remplacer le WEP en attendant que la norme 802.11i soit terminée. WPA a été conçu pour fonctionner, après mise à jour du micro-logiciel, de toutes les cartes Wi-Fi, mais pas nécessairement avec la première génération des PA.
- **WPA2**, son successeur, comprend tous les éléments obligatoires de la norme 802.11i[1]. C'est la version de la norme IEEE 802.11i certifiée par la Wi-Fi Alliance. En particulier, la norme WPA2 impose de prendre en charge le mécanisme CCMP, lequel s'appuie sur le cryptage AES. Le protocole CCMP est considéré comme complètement sécurisé ; en mai 2004, le NIST (National Institute of Standards and Technology) l'a approuvé. Il est pris en charge depuis 2005.

JFA 281

La sécurité du Wifi : Le WPA et WPA2

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Les deux mécanismes fournissent une bonne sécurité, si l'on respecte deux points importants :

- l'utilisateur doit faire le choix explicite d'activer WPA ou WPA2 en remplacement du WEP, car le WEP reste habituellement le choix de chiffrement par défaut sur la plupart des équipements ;
- lorsque le mode « WPA personnel » (*WPA-Personal*) est utilisé, ce qui est le choix le plus probable pour les particuliers et les PME, une phrase secrète plus longue que les classiques mots de passe de six à huit caractères utilisés par les utilisateurs est nécessaire pour assurer une sécurité complète.
- On peut classer les technologies WPA selon trois axes :
  - la version (1 ou 2),
  - le groupe d'utilisateurs visés (Personal ou Entreprise)
  - le protocole de chiffrement (TKIP ou CCMP)

JFA 282

La sécurité du Wifi : La version

R 2.05

selon la version :

- **WPA :** la version initiale de WPA, qui améliore la sécurité offerte par l'ancien protocole WEP. WPA utilise en général le protocole de chiffrement TKIP.
- **WPA2** : également connu sous le nom IEEE 802.11i-2004, ce successeur de WPA remplace le chiffrement TKIP par CCMP pour plus de sécurité. La compatibilité WPA2 est obligatoire pour les équipements certifiés Wi-Fi depuis 2006.

JFA 283

La sécurité du Wifi : Le WPA

R 2.05

selon le groupe d'utilisateurs visés :

- **WPA personnel** (*WPA-Personal*) : connu également sous le nom de mode à secret partagé ou WPA-PSK (Pre-shared key), WPA personnel est conçu pour les réseaux personnels ou de petites entreprises, car il n'y a pas besoin d'utiliser un serveur d'authentification. Chaque équipement du réseau sans fil s'authentifie auprès du point d'accès en utilisant la même clé sur 256 bits.
- **WPA entreprise** (*WPA-Enterprise*) : connu également sous le nom de mode WPA-802.1X ou WPA-EAP, WPA entreprise est conçu pour les réseaux d'entreprise et demande que l'on installe un serveur d'authentification RADIUS. C'est plus compliqué à mettre en place, mais offre plus de sécurité, car cette méthode ne repose pas sur des phrases secrètes, vulnérables aux attaques par dictionnaire. Le protocole EAP (Extensible Authentication Protocol) est utilisé pour l'authentification. EAP existe en plusieurs variantes, dont EAP-TLS, EAP-TTLS et EAP-SIM.
- Remarque : WPA personnel et WPA entreprise concernent à la fois WPA et WPA2.

JFA 284

La sécurité du Wifi : Le chiffrement

R 2.05

selon le protocole de chiffrement :

- **TKIP** (Temporal Key Integrity Protocol) : une clé de 128 bits est utilisée pour chaque paquet. On génère une nouvelle clé pour chaque paquet. TKIP est utilisé par WPA.
- **CCMP** : un mécanisme de chiffrement qui s'appuie sur AES et qui est plus fort que TKIP. On fait parfois référence à cette méthode de chiffrement sous le nom d'AES plutôt que sous le nom de CCMP. CCMP est utilisé par WPA2.
- De nos jours, bon nombre de points d'accès Wi-Fi utilisés à titre personnel sont réglés par défaut soit en WPA en mode clé partagée (PSK) avec le chiffrement TKIP, soit en WPA2 en mode clé partagée avec chiffrement CCMP, et prennent également en charge le mode entreprise.

JFA 285

Contenu du cours

R 2.05

- Introduction & Historique
- Le Wifi : 802.11
- Le Bluetooth : 802.15

JFA 286

Introduction

- IEEE 802.15.1, Inventé par Ericsson (1994)
- www.bluetooth.com
- Special Interest Group (SIG)
  - Ericsson, IBM, Intel, ….
  - >4000 entreprises
- Normes
  - 1.0 (1999)
  - 1.1 (2000) : + non-cryptage + Mesure force du signal
  - 1.2 (2003) : + saut de fréquence + débit > + qualité >
  - 2.0 (2004) : + débit > + consommation < + multipoint

JFA 287

Quelques éléments

- Faible portée, faible consommation
- Dans la bande ISM 2,4GHz
  - FHSS, 79 canaux de 1MHz
  - Changement pseudo-aléatoire
- Architecture en couches,
- Deux modes de connections:
  - Piconet (ad_hoc)
  - Scatternet (réseau)

JFA 288

Quelques éléments

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Architecture : Piconet
  - Ensemble de périphériques connectés de manière ad-hoc
  - Une unité se comporte en maître, les autres en esclaves, pour la durée de la connexion piconet
  - Le maître définit l'horloge et le saut de fréquence
  - Chaque piconet a un unique motif/ID de saut
  - Chaque maître peux connecter jusqu'à 7 esclaves simultanément ou +200 esclaves inactifs (parqués)

JFA 289

Quelques éléments

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

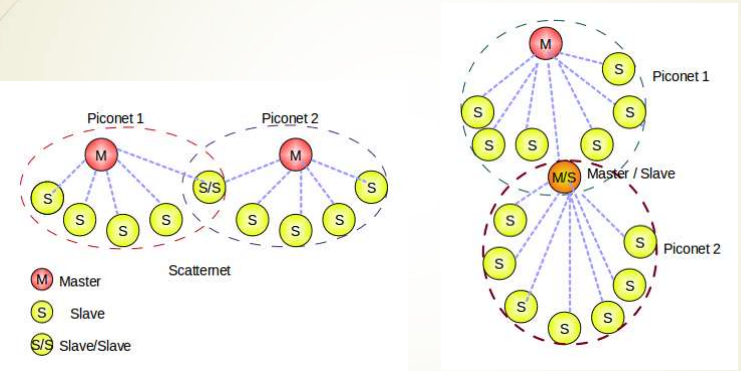
- Architecture : Scatternet
  - Liaison de piconets co-localisés partageant des périphériques maîtres ou esclaves
  - Un périphérique peut être à la fois maître et esclave
  - Canaux Radios symétriques (Le même canal peut être maître ou esclave)
  - Système haute capacité : chaque piconet a une capacité maximale (720 Kbps),

JFA 290

Quelques éléments

IUT GRAND OUEST NORMANDIE – INFO – R 2.05

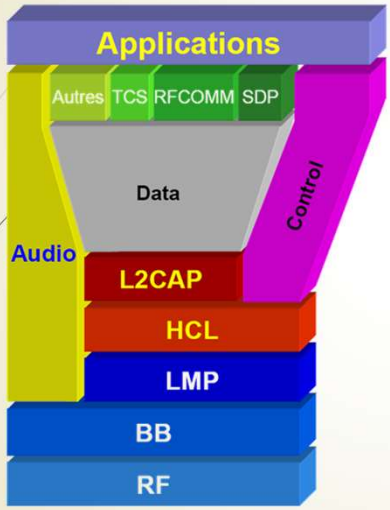
- Schéma architecture :



JFA 291

Architecture Bluetooth

IUT GRAND OUEST NORMANDIE – INFO – R 2.05



Application Framework & Support

Logical Link Control & Application Protocol

Host Controller Layer

Link Manager Protocol

Bande de base

Radio

JFA 292

Architecture (2)

R 2.05

- Couche RF : 2,4GHz sur 83,5 Mhz
  - S'occupe de l'émission et de la réception (bande, canaux, caractéristiques, modulation, …
  - Modulation FHSS : 79 canaux de 1 Mhz,
    - Commutation rapide pseudo aléatoire des canaux,
  - 3 *classes* de puissance :
    Classe I : 100 mW (20 dBm), Portée : 100 mètres
    Classe II : 2,5 mW (4 dBm)), Portée : 15-20 mètres
    Classe III : 1 mW (0 dBm)), Portée : 10 mètres
  - La classe II est la plus courante.

JFA 293

Architecture (2)

R 2.05

- Couche Bande de Base (BB)
  - Définition des adresses matérielles (eq MAC) :
  - BD_ADDR (Bluetooth Device Address), codée sur 48 bits (gérées par la IEEE Registration Authority)
  - 2 modes de communication : Les connexions peuvent être synchrones ou asynchrones. La bande de base peut donc gérer deux liens de connexions:
    - Les liaisons SCO (Synchronous Connection-Oriented)
    - Les liaisons ACL (Asynchronous Conection-Less)
    - Les liaisons de base

JFA 294

Architecture (3)

R 2.05

- Couche Link Management Protocol
  - Gestion des pico-réseaux
  - Gestion Maître/Esclave
  - Gestion Économie énergie
  - Supervision des différentes connexions
    - l'authentification, l'appairage
    - la création et la modification des clés, le cryptage
    - Qualité de service
    - Authentification des esclaves

JFA 295

Architecture (4)

R 2.05

- **L'interface HCI (Host Controller Interface)**
  - Fournit une méthode uniforme pour accéder aux couches matérielles
  - Composée de commandes et d'évènements
    - Le périphérique envoie des commandes à la puce Bluetooth et reçoit des évènements en retour.

JFA 296

Architecture (4)

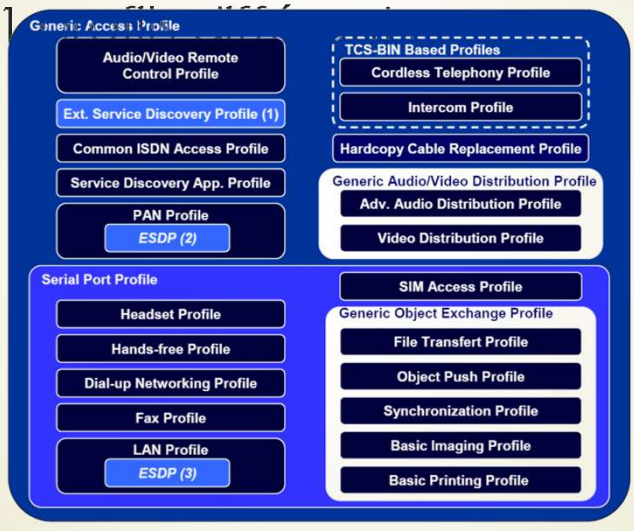
R 2.05

- L2CAP : *Logical Link Control & Application Protocol*
  - Protocole minimum d'échange de données.
  - Accessible par la couche application,
  - Protocole relativement simple à mettre en œuvre,
  - SDP : protocoles de recherche de services,
  - RFCOMM : émulation d'une liaison série.
  - Majoritairement en mode connecté, mais possibilité de mode non connecté,

JFA 297

Les profils Bluetooth

21



R 2.05

JFA 298

Les profiles Bluetooth (2)

R 2.05

- Les profiles Bluetooth : (21 profiles) : autant de fonctions possibles :
  - Generic Access Profile : couches basses
    - Ce profil est LE profil de base.
    - Il définit les procédures génériques de découverte d'équipement, et de gestion de connexion
    - Un utilisateur Bluetooth doit pouvoir se connecter à n'importe quel autre appareil Bluetooth, même si ils n'ont aucune application en commun en utilisant les fonctions basiques de Bluetooth. Ce profil est celui dont tous les autres dépendent, et tous les profils « héritent » de ses caractéristiques.

JFA 299

Les profiles Bluetooth (3)

R 2.05

GAP (*Generic Access Profile*) : assure le fonctionnement des couches de liaison basses.

- **AVRCP (*A/V Remote Control Profile*)**
- **ESDP (*Extended Service Discovery Profile*)**
- **CIP (*Common ISDN Acces Profile*)**
- **SDAP (*Service Discovery Application Profile*)** : permet à une application au sein d'un équipement Bluetooth de découvrir les services Bluetooth d'autres équipements et d'acquérir les données nécessaires à l'établissement d'une connexion.
- **PAN (*Personal Area Network Profile*)**
- **HCRP (*Hardcopy Cable Replacement Profile*)**

JFA 300

Les profiles Bluetooth (4)

R 2.05

GAVDP (*Generic Audio/Video Distribution Profile*)

- Advanced Audio Distribution Profile
- Video Distribution Profile

TCS-BIN Based Profiles

- **CTP (*Cordless Telephony Profile*)** : permet aux téléphones cellulaires de fonctionner comme téléphones sans fil avec un PC ou une station de base.
- **IP (*Intercom Profile*)** : offre une utilisation en mode interphone ou talkie-walkie.

JFA 301

Les profiles Bluetooth (5)

R 2.05

SPP (*Serial Port Profile*) : permet l'émulation d'un connecteur série. 3HS (Headset) : communication sur oreillette.

- **HP (*Headset Profile*)** : permet l'utilisation de casques sans fil avec les dispositifs audio (téléphones, lecteurs MP3)
- **HFP (*Hands Free Profile*)** : permet l'utilisation en mode mains libres de dispositifs audio (téléphones, interphones, etc.)
- **DNP (*Dial-Up Networking Profile*)** : autorise la connexion à un modem, ou l'utilisation d'un tél. mobile comme modem.
- **FP (*Fax Profile*)** : service fax.
- **LAP (*Local Area Network Profile*)** : donne accès au réseau local ou permet le fonctionnement en mode réseau local.
- **SAP (*SIM Access Profile*)**

JFA 302

Les profiles Bluetooth (6)

IUT GRAND OUEST NORMANDIE – iNFO

R 2.05

GOEP (*Generic Object Exchange Profile*) : profile générique d'échange d'objets pour synchronisation, FTP, Push...

- **FTP (*File Transfer Profile*)** : service situé du côté de l'application qui provoque un transfert de fichiers vers un équipement Bluetooth.
- **OPP (*Object Push Profile*)** : service situé du côté de l'application qui fait du Push vers un appareil Bluetooth, typiquement pour l'expédition d'une carte de visite.
- **SP (*Synchronisation Profile*)** : service situé du côté de l'application qui lance une opération de synchronisation vers un équipement BT.
- **BIP (*Basic Imaging Profile*)** :
- **BPP (*Basic Printing Profile*)** :

JFA 303

La sécurité

IUT GRAND OUEST NORMANDIE – iNFO

R 2.05

- Communications cryptées par couche LMP
- Cryptage basé sur 4 valeurs
  - Adresse dispositif (public)
  - Clé privée sur 128 bits
  - Code PIN (8 → 128 bits, privé)
  - Nombre aléatoire
- Technique du challenge
  - Envoi une donnée non cryptée
  - Reçoit la donnée cryptée
  - Vérifie la donnée reçue

JFA 304

Conclusion

- Wifi ou Bluetooth ?
  - Même bande de fréquence, protocole différent
  - ➔ Interférence
- Wifi = Haut débit
  - Bluetooth promet du 100Mbit/s pour 2013
- Bluetooth = Basse consommation
  - ➔ Surtout pour périphériques embarqués
  - PDA, téléphones, lecteurs MP3

JFA 305

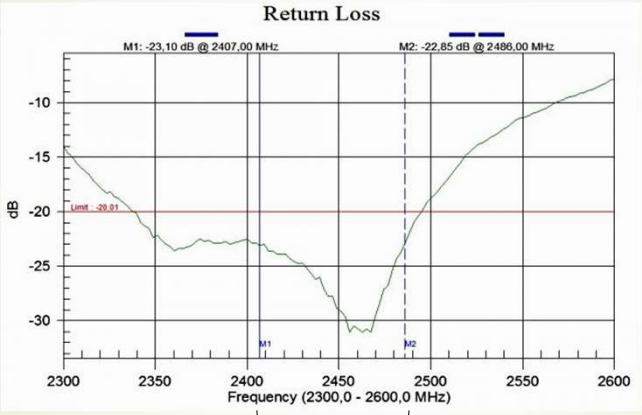
Retour sur les interférences

- Radio-diffusion : Interférences multiples
- Bande ISM
  - Libre
  - Très utilisée
  - Puissance limitée (10mW en France)
- Exemple : Un four à micro-ondes
  - Émet à 2450MHz environ…
    - milieu de la bande 2,4GHz
    - Large spectre (>100MHz)
  - Environ 1000 fois plus fort que le wifi ou le bluetooth
    - ➔ Toute communication est brouillée
    - sur plusieurs mètres de distance

JFA 306

Le micro-ondes

R 2.05



Bande WIFI / Bluetooth

JFA 307

Le WIMAX
Wifi de demain ?

R 2.05

- Apparu en janvier 2003, WiMax (Worldwide Interoperability for Microwave Access) est le nom commercial de la technologie sans fil 802.16 pour l'accès au réseau de l'opérateur
- Cette technologie pour opérateurs s'avère plus performante et plus solide que Wi-Fi. Son domaine d'action est le réseau métropolitain et plus spécialement le « dernier kilomètre » , c'est-à-dire entre le central de rattachement et l'abonné. Il est prévu pour fournir des services de type DSL, liaison louée et le raccordement de réseaux radio publics.
- « Le WiMAX est une technologie qui va désenclaver les régions touchées par la fracture numérique. »
- Altitude Télécom, seul détenteur en France d'une licence de réseau sans fil dans la bande des 3,5 GHz (proposant des services sur WiMAX) ,

JFA 308

Le WIMAX
Wifi de demain ?

- *Worldwide Interoperability for Microwave Access*
  - *Supporté par le « Wimax Forum » (différents fabricants)*
- Norme IEEE 802.16 (2001)
  - Fréquences initiales de 10GHz à 66GHz (134Mbit/s)
  - Fréquences de 2 GHz à 11 GHz (2004, IEEE 802.16d)
  - 70 Mbit/s sur 45 km (théorique)
  - 12 Mbit/s sur 20 km (pratique)
- Allocation de fréquences à la demande
  - Une seule licence Française (Attitude-Telecom→Free)
  - Plusieurs licences régionales (divers organismes)

JFA 309

Le WIMAX
Wifi de demain ?

- Le **WiMax** (Worldwide Interoperability for Microwave Access) :
  - Ensemble de normes techniques basées sur le standard de transmission radio 802.16 permettant la transmission de données IP haut débit par voie hertzienne. Le débit théorique maximum supporté par le WiMax est de 70 Mbits/s sur une distance théorique de plusieurs dizaines de kilomètres.
  - Le Wimax permet une utilisation à la fois sédentaire et nomade d'Internet haut-débit. D'un côté, les communes, les entreprises et les particuliers se connectent à Internet sans-fil à partir d'un poste fixe qui communique en hertzien via une antenne-relais appelée station de base. Les internautes peuvent alors bénéficier d'une connexion rapide où qu'ils se trouvent dans la zone couverte.

JFA 310

Le WIMAX
Wifi de demain ?

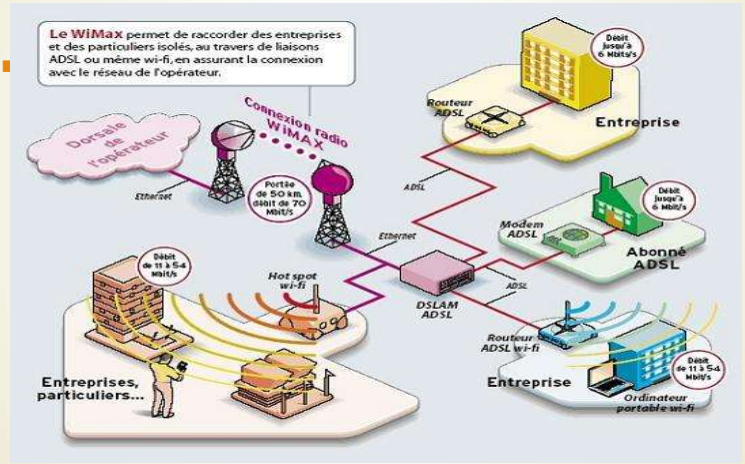
R 2.05

- Un réseau de stations émettrices est installé sur des points hauts de plusieurs départements pour les couvrir en Wimax. Pour recevoir le signal émis par les stations WiMAX, sur la bande de fréquences de 3,5 Ghz, il faut s'équiper d'une antenne radio. Cette antenne est orientée vers une station de base pour permettre un accès à l'internet haut débit en illimité mais également à la téléphonie par la technologie VoIP. La technologie WiMAX ne nécessite pas en effet l'installation d'une ligne de téléphone fixe filaire.
- La portée, les débits et la nécessité ou non d'être en ligne de vue de l'antenne émettrice dépendent de la bande de fréquences utilisée. Celle retenue en Europe de 3,5 Ghz permet de recevoir le signal radio sans la nécessité d'une ligne visuelle directe et peut franchir de petits obstacles. Cependant, les reliefs ou végétation peuvent avoir un impact sur les ondes radio.

JFA 311

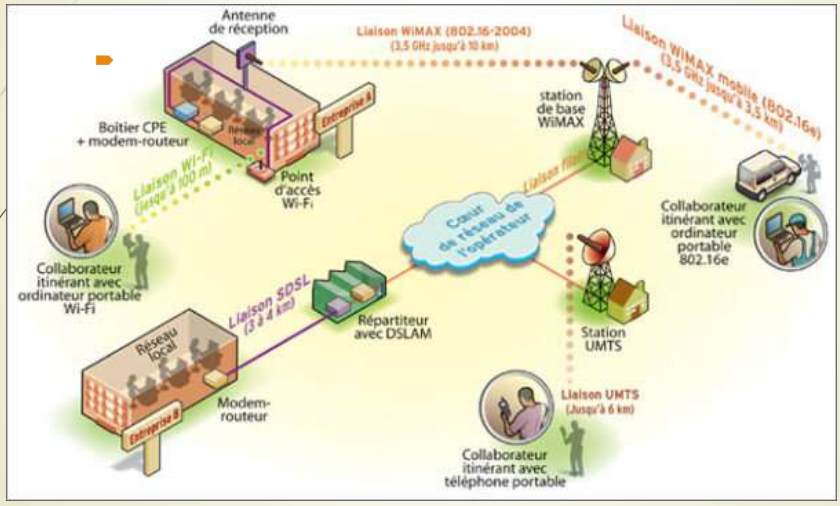
Le WIMAX
Wifi de demain ?

R 2.05



JFA 312

Le WIMAX
Parmi d'autres



JFA 313

Le WIMAX
Wifi de demain ?

- *Licences WiMax*
  - France Métropolitaine : Altitude Telecom
  - portée de plusieurs kilomètres(45 km théorique)
  - débits symétriques de plusieurs Mbit/s,:
    - 70 Mb/s Théorique, 10 Mb/s sur 8 à 10 km
  - WiMAX Mobile (802,16e), nomadisme.
  - Norme IEEE 802.16-2004
- Points faibles
  - nécessité de disposer d'un point haut et d'une licence,
  - éligibilité d'un site liée à de nombreux paramètres,
  - débit partagé entre les usagers d'une même station,
  - coût de l'abonnement élevé.
  - coût d'une station de base moins de 10 000 euros.

JFA 314

Le WIMAX
Wifi de demain ?

Standard	Bande de fréquence	Etat
IEEE std 802.16	Définit des réseaux métropolitains sans fil sur des bandes de fréquences supérieures à 10 GHz.	Octobre 2002
IEEE std 802.16a	Définit des réseaux métropolitains sans fil sur des bandes de fréquences comprises entre 2 et 11 GHz.	9 octobre 2003
IEEE 802.16b	Définit des réseaux métropolitains sans fil dans les bandes de fréquences comprises entre 10 et 60 GHz.	Fusionné avec 802.16a
IEEE std 802.16c	Définit des options (profils) pour les réseaux métropolitains sans fil dans les bandes de fréquences libres.	juillet 2003
IEEE 802.16d (IEEE std 802.16-2004)	Révision intégrant les standards 802.16, 802.16a et 802.16c.	1er octobre 2004 Actif
IEEE std 802.16e	Définit la possibilité d'utilisation de réseaux métropolitains sans fil avec des clients mobiles.	
IEEE std 802.16f	Définit la possibilité d'utilisation de réseaux sans fil maillés (mesh network).	

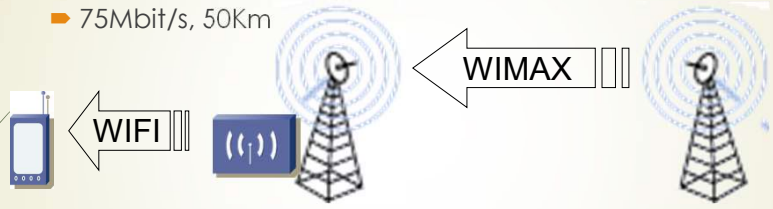
ILIT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 315

Le WIMAX (2)

Évolution de la norme

- IEEE 802.16d : Connexion via antenne relais
  - 75Mbit/s, 50Km



- IEEE 802.16f : Connexion directe Machine-Wimax
  - 30Mbit/s, 3,5Km

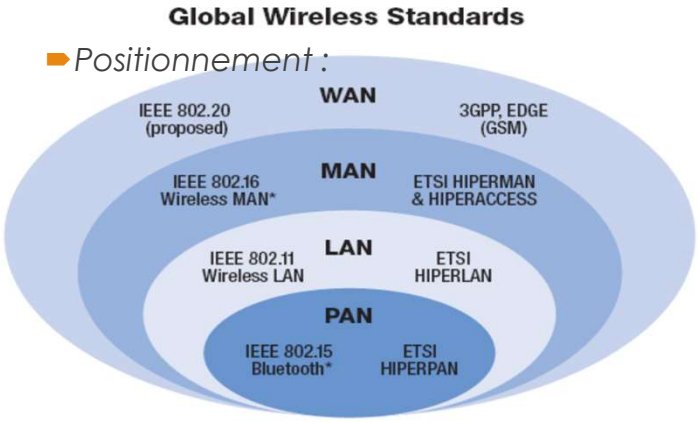
ILIT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 316

Le WIMAX
Wifi de demain ?

R 2.05

- *Positionnement :*

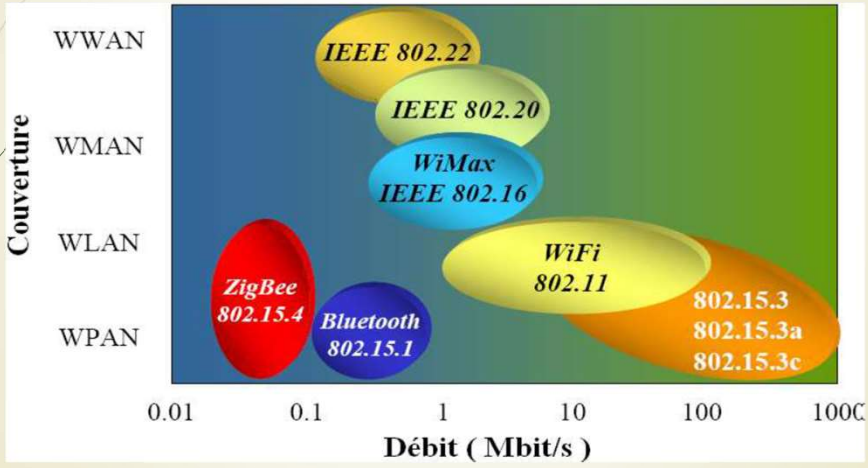


JFA 317

Le WIMAX
Wifi de demain ?

R 2.05

- *Comparaisons :*



JFA 318

Le WIMAX
Exemple dans l'orne ?

R 2.05

JFA 319

Le WIMAX
Wifi de demain ?

R 2.05

- *Synthèse :*
  - norme 802.16
  - Complémentaire de la norme Wi-Fi
  - une nouvelle forme de la "**boucle locale radio**" (BLR)
  - Avec une antenne parabolique sur le toit d'un bâtiment, permet l'internet et la téléphonie à haut débit,
  - 35 fois plus rapide qu'ADSL... et sans fil, et 1,54 fois plus que la norme 802.11g (54 Mb/s théoriques)
  - **débit théorique de 70Mb/s** (ou 8,75 Mo/s) sur un rayon de **45 kilomètres**
  - bande hertzienne comprise entre 10 et 66GHz
  - la largeur des canaux pour l'Europe (28 MHz) autorise un débit de 132 Mbit/s

JFA 320

Le WifiMAX (Nomotech) Nouveau WiMAX ?

R 2.05

- Le principe du WifiMax utilise la norme WIFI :
  - La qualité de service est améliorée afin que plusieurs clients puissent **se raccorder simultanément dans de bonnes conditions**.
- infrastructure WifiMax, deux types d'émetteurs :
  - **Les émetteurs de collecte** pour raccorder les sites entre eux afin de constituer un unique réseau sur le département, relié ensuite à Internet via un noeud d'accès.
  - **Les émetteurs de diffusion** pour raccorder les clients finaux (particuliers ou professionnels) au réseau.
  - Pour profiter de ce dispositif, l'utilisateur final doit disposer d'une antenne de réception extérieure pointée en direction de l'émetteur de diffusion le plus proche.

JFA 321

Le WifiMAX (Nomotech) Nouveau WiMAX ?

R 2.05

- C'est la solution idéale lorsque les systèmes WiFi traditionnels ne sont pas assez puissants, avec une portée de 5 à 10 km entre les relais émetteurs et l'abonné. Les équipements WifiMax permettent de gérer de multiples canaux radio sur les fréquences libres 2,4 GHz et 5,4 GHz, afin de réaliser une réelle infrastructure maillée dans un environnement aussi bien urbain que rural..
- La sensibilité des émetteurs et antennes de diffusion permet de réaliser de proche en proche des liaisons de l'ordre de 10 km, ce qui n'est pas possible avec des équipements Wi-Fi standards.
- Outre la rapidité des débits Internet dans les deux sens (jusqu'à 6 Mbps symétriques selon les infrastructures) et la facilité de l'installation domestique, la technologie WifiMax assure une bonne qualité de service à ses utilisateurs, et une sécurisation des transferts de données (cryptage, authentification).

JFA 322

Le WifiMAX (Nomotech) Nouveau WiMAX ?

- Outre la rapidité des débits Internet dans les deux sens (jusqu'à 6 Mbps symétriques selon les infrastructures) et la facilité de l'installation domestique, la technologie WifiMax assure une bonne qualité de service à ses utilisateurs, et une sécurisation des transferts de données (cryptage, authentification).
- La technologie WifiMax évolue avec le développement de la technologie WifiMax MIMO (Multiple Input Multiple Output) permettant d'utiliser plusieurs canaux radio simultanément pour atteindre des débits allant jusqu'à 20 Mbps (selon infrastructures et départements). Cette technologie dernière génération est en cours de déploiement.

JFA 323

Le WifiMAX (Nomotech)

En finir avec la fracture numérique ?

- Dans le Calvados, le réseau WifiMAX a pour objectif d'en finir avec la fracture numérique. Quelle que soit la localisation de son domicile, aucun calvadosien ne doit donc désormais être inéligible à l'Internet haut-débit. Les offres s'adressent en priorité aux habitants dont la ligne téléphonique n'est pas compatible avec l'ADSL. Trop éloignées du noeud de raccordement (parfois à plus de 6 kilomètres), ces lignes ne sont en effet pas en mesure de supporter une connexion Internet... autre que l'antique bas-débit à 56 Kbit/s.
- Rappelons que sur les 175 000 lignes du Calvados, 4 000 sont complètement inéligibles à l'ADSL et plus de 30 000 (presque 20% !) doivent se contenter d'un débit ADSL inférieur à 2 Mbit/s. Outre la technologie satellitaire, le WifiMAX est une alternative pour améliorer la couverture Internet du territoire. Amener le haut-débit dans des communes mal desservies en ADSL, ce n'est pas seulement lutter contre les inégalités d'accès, c'est aussi combattre celles liées aux usages.

JFA 324

Le ZigBee :
IEEE 802.15.4

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

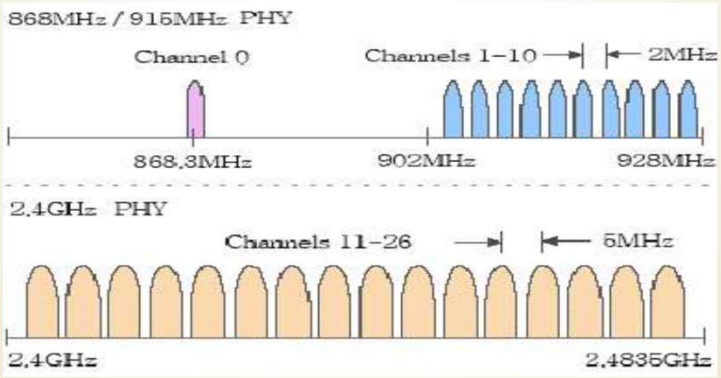
- *Généralités*
  - bas débits (maxi 250 kbit/s): 250 ou 40 ou 20 kbit/s selon la bande de fréquence, faible portée (50 m typique),
  - **WPAN** (Wireless Personnal Area Network) comme Bluetooth (802.15.1) et non WLAN
- Caractéristiques :
  - Robuste malgré parasites
    - (étalement de spectre DSSS, 2 Mchips/s à 2,4 GHz).
  - 2 modes d'adressage: Court (16 bits) et 64 bits IEEE.
  - Sait gérer les appareils à faible latence.
  - Résolution de collision CSMA-CA .
  - Echanges fiables par acquittement (handshake).

JFA 325

Le ZigBee :
IEEE 802.15.4

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Canaux :
  - 1 canal dans la bande 868MHz, 10 dans la bande 915MHz et 16 canaux dans la bande 2,4 GHz ISM band.



JFA 326

Le ZigBee :
IEEE 802.15.4

- Canal 0: 868 MHz
  - Europe, 20 kbit/s
  - Modulation BPSK
- Canaux 1 à 10: 915 MHz
  - USA, 40 kbit/s
  - Modulation BPSK, canaux de 2 MHz
- Canaux 11 à 26: 2,4 GHz
  - Monde entier, 250 kbit/s
  - Modulation QPSK, Canaux de 5 MHz
  - FC = 2405 + (5 * ch) MHz

IUT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 327

Le ZigBee :
IEEE 802.15.4

- 2 modes de fonctionnement: Avec ou sans voie balise (Beacon channel)
  - En mode voie balise,
    - le coordinateur joue son rôle en tant que maître: Périodiquement, il interroge les éléments du réseau via une trame balise.
  - En mode sans voie balise (non beacon),
    - un élément du réseau peut prendre l'initiative de contacter le coordinateur =>
      - moins de coordination, risque de collision,
      - mais plus rapide.

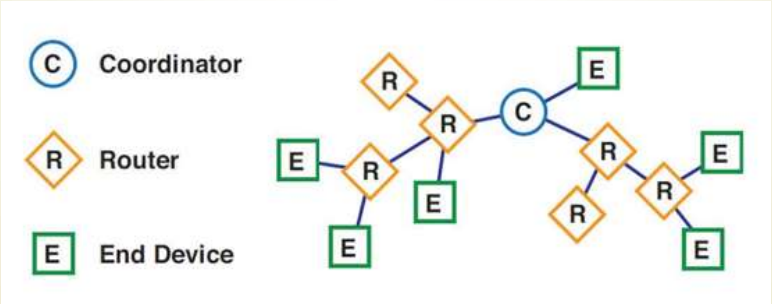
IUT GRAND OUEST NORMANDIE iNFO R 2.05

JFA 328

Le ZigBee :
IEEE 802.15.4

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Le réseau ZigBee :
  - il existe trois types de périphériques dans le réseau ZigBee : le coordinateur, le routeur et les « End-Devices »

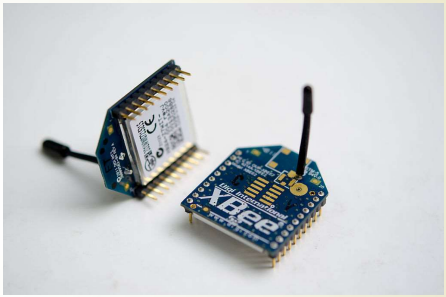


JFA 329

Le XBee :
IEEE 802.15.4

IUT GRAND OUEST NORMANDIE – iNFO – R 2.05

- Le module XBee
  - C'est un composant :
    - Deux modèles
    - XBee « Normal »
    - XBee « Pro »
  - Avec une interface :
    - API Interchangeable
  - Différents groupes de protocoles :
    - 802.15.4 , ZNet 2.5, ZB Zigbee, Wifi



JFA 330

Le XBee :

IEEE 802.15.4

R 2.05

- Les modules peuvent fonctionner dans deux modes principaux distincts :
  - - le mode transparent
    - qui permet le remplacement immédiat de n'importe quelle liaison série asynchrone filaire par une liaison radio sans aucune manipulation particulière au niveau des modules Xbee, ce mode peut supporter ou non, au gré de l'utilisateur, la programmation d'un certain nombre de fonctions du modem au moyen de commande dites commandes AT.
  - - le mode API
    - qui permet d'accéder aux possibilités plus fines de mise en réseau des modules mais ne se justifie vraiment que lorsque l'on veut gérer tout un groupe de modules avec des possibilités de diffusion multiple, d'adressage, etc.

JFA 331

Les Réseaux Mobiles

R 2.05

Les réseaux mobiles 2G, 3G, 4G, 4G+… 5G !

https://www.dzigue.com/wp-content/uploads/2015/11/reseaux-mobiles.jpg

JFA 332

Les Réseaux Mobiles

R 2.05

Réseaux mobiles 1G, 2G, 3G, 4G et 5G : l'essentiel à savoir

- Vous êtes-vous déjà demandé ce que signifie exactement le sigle (1G, 2G, G, E, 3G, H+ ou 4G) affiché dans le coin supérieur de votre téléphone ? En fait, ce sigle vous indique le type de réseau mobile auquel vous avez accès. De lui dépendent notamment :
  - La qualité de vos communications téléphoniques.
  - Le débit et la performance de votre connexion Internet mobile.
- Depuis l'avènement du téléphone portable, 4 générations de réseaux mobiles se sont succédé : 1G, 2G, 3G, 4G. Quant à la 5G, elle frappe déjà à notre porte, avec à la clé des débits dépassant les 10 Gbit/s !

JFA 333

Les Réseaux Mobiles

R 2.05

- Une histoire de génération !

  1G, 2G, 3G, 4G… un « G » pour Génération de réseaux mobile.
  - La 1G : C'est l'ancien Radiocom 2000 de France Télécom.
  - La 2G : C'est le réseau GSM (Global System for Mobile Communication) qui fonctionne toujours et qui permet uniquement des échanges de type voix. Débit inférieur à 10 Kbit/s.
  - Il existait le GSM 900 et le DSC 1800 (Digital Cellular System) utilisé par Bouygues Telecom.
  - La 2.5G : C'est le GPRS (Global Packet Radio Service), premier réseau pour la donnée. Débits théoriques de 114 Kbit/s, mais bien plus proche de 40 Kbit/s en réalité !
  - La 2.75G : C'est la norme EDGE (Enhanced Data Rate for GSM Evolution) qui offre des débits théoriques de 384 Kbit/s, ouvrant ainsi la porte aux applications multimédias.

JFA 334

Les Réseaux Mobiles

R 2.05

- La 3G : C'est l'UMTS, la principale norme 3G utilisée en Europe. Elle permet de transférer de la voix et de la données avec des débits pouvant aller de 384 Kbit/ss à 2 Mbit/s (dans des conditions idéales).
- 3.5G ou 3G+ : Norme HSPA (High Speed Packet Access) une évolution de l'UMTS permettant d'atteindre des débits de l'ordre de 8 à 10 Mbit/s.
- 3.75G ou 3G++ : Toujours une évolution de l'UMTS, c'est la norme HSPA+ (High Speed Packet Access +) pour atteindre des débits théoriques de 20 Mbit/s.
- Il existe aussi une petite évolution avec le DC-HSPA+ (Dual-Carrier High Speed Packet Access +) qui permet d'atteindre les 42 Mbit/s (toujours en théorie)

JFA 335

Les Réseaux Mobiles

R 2.05

- 4G : Parfois appelée par les puristes la 3.9G, cette nouvelle génération utilise la norme LTE (Long Term Evolution) et offre des échanges de données à plus 100 Mbit/s.
- 4G+ : Ou la « vrai » 4G pour les puristes, utilise la norme LTE-Advanced, une évolution de la LTE qui permet des débits bien supérieur à la 4G pouvant atteindre 1 Gbit/s (sur le papier).
- 5G : Ce sera un réseau mobile ultra haut débit. La norme ne semble pas encore définie mais on peut espérer des débits de plusieurs dizaines de Gbit/s... avec une commercialisation autour de 2020 !

On voit donc beaucoup de débits « *théoriques* » car concrètement sur le terrain, les débits sont plus bas voire beaucoup plus faibles. Il faut savoir que pour émettre en 3G, ou en 4G, les opérateurs ont **besoins de fréquences**. Et en fonction de celles-ci, les débits ne sont pas les mêmes (1800, 2600, 800 Mhz). De plus, les smartphones ne sont pas tous égaux. Ils font qu'ils soient compatibles. On parle par exemple pour la 4G de « *catégorie* » et un mobile de catégorie 4 ne pourra pas atteindre les débits d'une catégorie 5 (300 Mbit/s en 4G+).

JFA 336

Les réseaux de première génération

R 2.05

- Le réseau 1G, basé sur une technologie analogique
  - Apparue dans les années 70, la 1G, qui est la première génération de réseaux mobiles est uniquement dédiée aux appels vocaux. Elle repose sur une technologie dite « analogique ». Ceci à la différence des générations suivantes de téléphonie mobile (2G, 3G, 4G, 5G) qui, elles, exploitent la technologie « numérique ».
  - La 1G présente toutefois de nombreux défauts : service de communication mobile médiocre, non sécuritaire (appels non cryptés) et coûteux.
  - Le réseau 1G a commencé à céder la place à la 2G dans de nombreux pays vers la fin des années 80. Il est désormais obsolète.
  - Notons que la France a abandonné la 1G au profit exclusif de la 2G à partir du 28 juillet 2000.

JFA 337

Les réseaux de première génération

R 2.05

- La téléphonie cellulaire est un premier pas vers une utilisation réellement mobile. Elle impose de mailler le territoire de manière plus serrée avec un tapis d'antennes définissant des cellules, mais permet à plusieurs utilisateurs de passer un appel en même temps sans encombrer la ligne et est moins soumise à perturbations en fonctionnant sur des bandes de fréquences plus élevées. Cerise sur le gâteau : on peut passer d'une cellule à une autre sans que la communication ne soit coupée.
- Le téléphone mobile devenant commun, les premiers usages détournés apparaissent. Comme l'Autotel, les réseaux 1G utilisent un signal numérique pour les opérations techniques et la modulation analogique pour la voix — un canal non sécurisé qui peut être observé avec un scanner radio. Les pirates, notamment aux États-Unis, récupèrent ainsi les identifiants uniques des téléphones et les clonent dans un autre : on peut alors téléphoner avec l'identifiant d'un autre… et donc sur sa facture.

Le Motorola Dynatac 8000x. Commercialisé pour 3995 $, il dispose d'une autonomie d'une heure, la recharge en prenant pas moins de dix heures.

JFA 338

Les réseaux de première génération

R 2.05

- Chaque pays ou presque développe son propre système : **AMPS** aux États-Unis (Advanced Mobile Phone System, 1978), **NMT** en Scandinavie (Nordic Mobile Telephone, 1981), **TACS** en Grande-Bretagne et au Japon (Total Access Communication System, 1983), **Radiocom 2000** en France (1986). Ces réseaux sont incompatibles entre eux, et se font parfois concurrence à l'intérieur d'un même pays : la Société française du radio-téléphone contre le Radiocom de France Télécom dès 1987 avec un réseau… NMT ! Ces réseaux sont encore utilisés majoritairement en voiture (90 % des abonnés Radiocom).
- Le progrès des antennes et des batteries aidant, le marché des téléphones mobiles naît : le modèle le plus emblématique est sans doute le Motorola Dynatac 8000x (1983). On le présente souvent comme le « premier téléphone mobile », sans doute à cause de sa ressemblance avec le prototype utilisé par Martin Cooper en 1973 pour passer le premier appel sur un réseau 1G. Mesurant 25 cm sans l'antenne pour 780 grammes, c'est en fait le premier téléphone mobile suffisamment petit pour être transporté dans une sacoche commercialisé à grande échelle.

JFA 339

Les réseaux de première génération

R 2.05

- De nombreux standards du réseau 1G ont eu cours à travers le monde depuis son apparition en 1976, parmi lesquels :
  - La norme AMPS (Advanced mobile phone system) utilisée aux États-Unis (à partir de 1976), en Russie, en Australie et dans plusieurs pays asiatiques.
  - La norme NMT (Nordic Mobile telephone), exploitée au début des années 80 dans les pays nordiques et dans de nombreux pays européens, en Russie, au Moyen-Orient et en Asie.
  - La norme TACS (Total access communication system), qui la version européenne de la technologie AMPS, largement utilisée au Royaume-Uni, à Hong-kong et au Japon.
  - Les normes TZ-801, TZ-802, TZ-803 et JTACS (Japan Total Access Communications System) utilisées au Japon à partir de 1979.
  - La norme Radiocom 2000 déployée en France par France Telecom à partir de 1986, ainsi que la NMT-F (Nordic Mobile Telephone « Français ») lancée en 1988.

JFA 340

Les réseaux de deuxième génération

R 2.05

- Le réseau 2G ou l'avènement des technologies de la téléphonie mobile numérique.
- Déployée dans l'Hexagone dans les années 1990, la 2G (deuxième génération de réseaux mobiles) est le tout premier réseau de téléphonie mobile à utiliser une technologie numérique, plus fiable (grâce à un cryptage des données transmises) et plus performante que la 1G.
- Dotée d'un débit de transmission de 9,6 kbps maximum (GSM), la 2G permet de :
  - Passer des appels vocaux.
  - Envoyer des SMS (Short Message Service), voire des MMS (Multimedia Message Service).
- Par rapport à la 1G, la 2G a l'avantage d'être moins coûteuse pour l'utilisateur.

JFA 341

Les réseaux de deuxième génération

R 2.05

- La Conférence européenne des administrations des postes et télécommunications se penche dès 1982 sur un nouveau type de réseau mobile censé combler les failles des systèmes précédents. Le Groupe spécial mobile, installé à Paris, définit en l'espace de cinq ans un standard européen de transmission numérique, aux informations chiffrées avec un lien au réseau par carte à puce, et beaucoup plus léger dans sa gestion des ressources réseau.
- Au début des années 1990, France Télécom veut aussi passer au numérique, mais n'adopte pas le GSM : c'est la naissance du Bi-Bop. Les téléphones et les communications sont bon marché et l'opérateur convainc même Apple d'équiper une série de PowerBook 180 d'une connexion Bi-Bop, qui permet alors d'envoyer des faxs et de se connecter au minitel. Mais le Bi-Bop est construit sur la norme CT2, lointain ancêtre du DECT de nos téléphones domestiques sans-fil : il faut se trouver à proximité immédiate d'une des bornes déployées dans quelques villes pour pouvoir téléphoner, et on ne peut passer d'une borne à l'autre sans déconnexion. Le réseau est abandonné en 1997.

Le Nokia 1011, le premier téléphone GSM produit en masse. Haut de 19,5 cm, il pèse 476 grammes.

JFA 342

Les réseaux de deuxième génération

R 2.05

- Ce réseau, qui couvrait plus de 99 % du territoire français, exploite essentiellement les standards :
- GSM (Global System for Mobile Communication), norme apparue et très utilisée aux États-Unis (bande de fréquence 850 MHz et 1900 MHz). C'est le système le plus répandu en Europe (bandes de fréquences 900 MHz et 1800 MHz) et aussi en Afrique. Son débit maximal est de 9,6 kbps.
- CDMA (Code Division Multiple Access), aussi appelé CDMAOne ou IS-95, lancé à Hong-kong en 1994 et utilisé surtout aux États-Unis et en Asie. Notons que l'évolution du CDMA, dénommée CDMA2000, est reconnue par l'UIT (Union Internationale des Télécommunications) comme étant de troisième génération (3G).
- TDMA (Time Division Multiple Access), principalement utilisé en Amérique du Nord, en Nouvelle-Zélande et en Asie-Pacifique.

JFA 343

Les réseaux de deuxième génération

R 2.05

- Le GSM (Global System for Mobile communications) est formalisé en 1990 (Phase 1), les bandes des 900 et 1800 MHz lui étant réservées : le premier appel est passé en 1991, le premier SMS est envoyé en 1992. Il dépasse rapidement le cadre européen : il est adopté en Australie dès 1993. Il n'est pourtant pas universel. Le GSM emploie le multiplexage temporel (TDMA) : on découpe le temps disponible entre les différents utilisateurs, une bande de fréquence donnée pouvant ainsi être utilisée par plusieurs utilisateurs en même temps.
- Chacun de leur côté, les militaires américains et russes développent des réseaux utilisant le CDMA, une technique qui partage une bande de fréquence entre plusieurs utilisateurs en utilisant un système d'encodage et une technique d'étalement de spectre (on retrouve ce fonctionnement dans le GPS, le Bluetooth ou le Wi-Fi). L'IS-95, incompatible avec le GSM, utilise ce système et est notamment déployé aux États-Unis.

JFA 344

Les réseaux de deuxième génération

R 2.05

- Le GSM est à ce moment doté d'une couche réseau, comme l'IS-95, limitée à 14,4 kbit/s, puis augmenté par le GPRS (General Packet Radio Service), qui permet d'atteindre 115 kbit/s. En 1999, Nokia présente le 7110, le premier téléphone doté d'un navigateur WAP : les pages sont certes allégées, mais l'on peut désormais surfer en mobilité. L'EDGE (Enhanced Data Rates for GSM Evolution) ne tarde pas à suivre : avec ses 235 kbit/s de débit maximal, il permet de rêver de regarder des vidéos sur un mobile.

Le Nokia 7110, premier téléphone avec un navigateur WAP.

JFA 345

Les réseaux intermédiaires

R 2.05

- Avant l'arrivée de la 3G, la 2G évolue d'abord vers des réseaux intermédiaires :
  - Le réseau GPRS (General Packet Radio Service), aussi appelé 2,5G ou 2G+, améliore notablement le débit maximal de transfert de données (171,2 Kbit/s, avec un débit moyen de 48 Kbit/s) par rapport à la 2G. Permettant le transfert de datas de volume modéré, le GPRS est le précurseur sur l'internet mobile. Notons que tous les téléphones portables sont aujourd'hui au moins compatibles au réseau 2,5G.
  - Le réseau EDGE (Enhanced Data Rate for GSM Evolution), aussi appelé 2,75G, offre un débit maximal de 384 Kbit/s, et un débit moyen de 100 Kbit/s, ouvrant ainsi la porte aux applications multimédias. Certains opérateurs comme Orange et Bouygues Telecom ont déployé EDGE afin de faciliter la transition entre 2G et 3G.
- Les standards GPRS (sigle « G » dans le coin supérieur de l'écran du téléphone) et EDGE (E) constituent de ce fait une évolution du GSM. Ils permettent un accès à l'internet et à une consultation de mails à partir d'un téléphone mobile ou d'un micro-ordinateur.

JFA 346

Les réseaux de troisième génération

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Le réseau 3G ou l'Internet haut débit
- La 3G (troisième génération de réseaux mobiles), qui en Europe utilise la norme UMTS (Universal Mobile Telecommunications System), offre un accès à l'Internet haut débit, entre 144 kbit/s et 2 Mbit/s, avec un débit moyen de quelques centaines de Kbit/s. Ce qui vous permet notamment de :
  - Télécharger plus rapidement des données, des applications ou bien des jeux.
  - Envoyer des vidéos.
  - Regarder des vidéos en streaming sur YouTube, Dailymotion, etc.
  - Faire de la visio-conférence.
  - Accéder à la TV mobile.
  - Bénéficier du GPS.
- En France, le réseau 3G fonctionne sur les bandes de fréquences 900 MHz et 2100 MHz.

JFA 347

Les réseaux de troisième génération

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Le CDMA2000 a l'avantage d'être une évolution de l'IS-95 et donc de n'avoir nécessité que peu de nouveaux investissements. Ses premières évolutions ne répondent néanmoins pas aux spécifications 3G (moins de 200 kbit/s) et ne permettent pas l'utilisation de la voix et des données en même temps : on parle d'ailleurs de 1xRTT (voix seulement) et de 1xEv-DO (données seulement). Techniquement, l'EDGE répond lui à la définition d'un réseau de troisième génération — mais il ne permet pas non plus d'utiliser voix et données en même temps.

L'iPhone original exploitait à fond les capacités des réseaux EDGE.

JFA 348

Les réseaux de troisième génération

R 2.05

- Les opérateurs CDMA auraient pu choisir de régler le problème avec la norme Ev-DO Rev. B, mais ont pour la plupart choisi de ne pas la déployer. Ceci explique pourquoi aux États-Unis, Sprint ou Verizon ont très tôt pris le chemin des réseaux de quatrième génération : imaginez-vous que la moitié des Américains disposent d'un réseau similaire à notre EDGE, simplement plus rapide (jusqu'à 3,1 Mbit/s). On retrouve ce problème dans certains pays asiatiques et d'Amérique latine.
- En Europe, les opérateurs ont fait l'effort de déployer un nouveau réseau, basé sur le système UMTS, pour permettre l'utilisation simultanée de la voix et des données. Il est incompatible avec les réseaux GSM (les téléphones sont donc compatibles avec les deux types de réseau), mais offre des capacités d'évolution bien différentes des réseaux Ev-DO, ce qui explique que la 3G soit si présente en Europe.

JFA 349

Les réseaux de troisième génération

R 2.05

- Le 3GPP (3rd Generation Partnership Project), qui gère cette norme, l'a constamment amélioré, notamment pour augmenter les débits :
  - **UMTS** (Release 99, 2000) à 1,92 Mbit/s ;
  - **HSPA** (Release 5 et 6, 2002 et 2004) jusqu'à 14,4 Mbit/s en download (**HSDPA**) et 5,8 Mbit/s en upload (**HSUPA**) ;
  - **HSPA+** (Release 7, 2007) qui monte à 21,6 Mbit/s en download ;
  - **DC-HSPA+** (Release 8 et 9, 2008 et 2009), qui atteint 42 Mbit/s en download et 11 Mbit/s en upload.
- Ces débits sont théoriques, et dépendent d'ailleurs des bridages imposés par les opérateurs : la HSPA a longtemps été limitée à 7,2 Mbit/s, et la DC-HSPA+ peut théoriquement atteindre 128 Mbit/s.

JFA 350

Les réseaux de troisième génération

R 2.05

- Ces acronymes, moins faciles à retenir que GSM ou EDGE, ont souvent été masqués derrière des marques commerciales. L'UMTS a souvent été simplement désigné par **3G** ; les réseaux **3G+** sont des réseaux HSPA. Le terme **H+** d'Orange désigne les réseaux HSPA+ (HSPA+ et DC-HSPA+), alors que l'expression **Dual Carrier** de SFR ne désigne que les réseaux DC-HSPA+. Bouygues Telecom appelle un chat un chat et parle tout simplement de « 3G jusqu'à 42 Mbit/s ». On les désigne parfois sous le nom de réseaux **3.75G**.
- Notons que la 3G a connu trois évolutions successives avec :
  - La 3G+ aussi appelée « H » pour HSPA (High Speed Packet Access), avec un débit compris entre 300 kbit/s et 14,4 Mbit/s, pour une moyenne de 3,6 Mbit/s. Bref, la 3G+ est 7 fois plus rapide que la 3G.
  - Le H+ (ou HSPA+), avec un débit moyen de 5 Mbit/s, pour un débit théorique maximal de 21 Mbit/s.
  - Le H+ Dual Carrier (ou DC-HSPA+), doté d'un débit moyen de 10 Mbit/s, et un débit plafond de 42 Mbit/s.
- Bref, la 3G et ses évolutions ont permis de démocratise complètement l'utilisation de l'Internet mobile.

JFA 351

Les réseaux de quatrième génération

R 2.05

Le réseau 4G ou l'Internet très haut débit

- Déployée en France en 2013, la 4G (quatrième génération de réseaux mobiles) donne aux utilisateurs l'opportunité d'accéder à l'Internet très haut débit. Elle permet, entre autres, de :
  - Transférer rapidement des fichiers volumineux (photos, musiques, vidéos, etc.).
  - Visionner des vidéos en HD.
  - Faire des appels vidéo de meilleure qualité.
- La 4G est basée sur la norme LTE (Long Term Evolution) dont le débit théorique atteint les 150 Mbit/s.

Les réseaux de quatrième génération

JFA 352

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Ces réseaux HSPA+ sont si rapides que certains n'hésitent pas à les commercialiser sous le nom de 4G : c'est par exemple le cas d'AT&T aux États-Unis. Même la LTE qui est si à la mode ces derniers mois est techniquement un réseau de troisième génération : elle n'atteint pas le seuil du gigabit, mais se limite à 300 Mbit/s (et sera la plupart du temps déployée en 100 Mbit/s). On l'appelle donc parfois 3.9G.

- Cette « fausse » 4G est néanmoins le premier standard qui sera déployé dans le monde entier. Les opérateurs utilisant la CDMA ont sauté dessus : quitte à déployer un nouveau réseau, ils ont choisi le plus pérenne. Bien qu'elle nécessite des antennes-relais spécifiques, elle est aussi un choix naturel pour les opérateurs GSM/UMTS en tant que standard défini par la 3GPP.

L'iPhone 5 prend en charge la LTE.

Les réseaux de quatrième génération

JFA 353

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

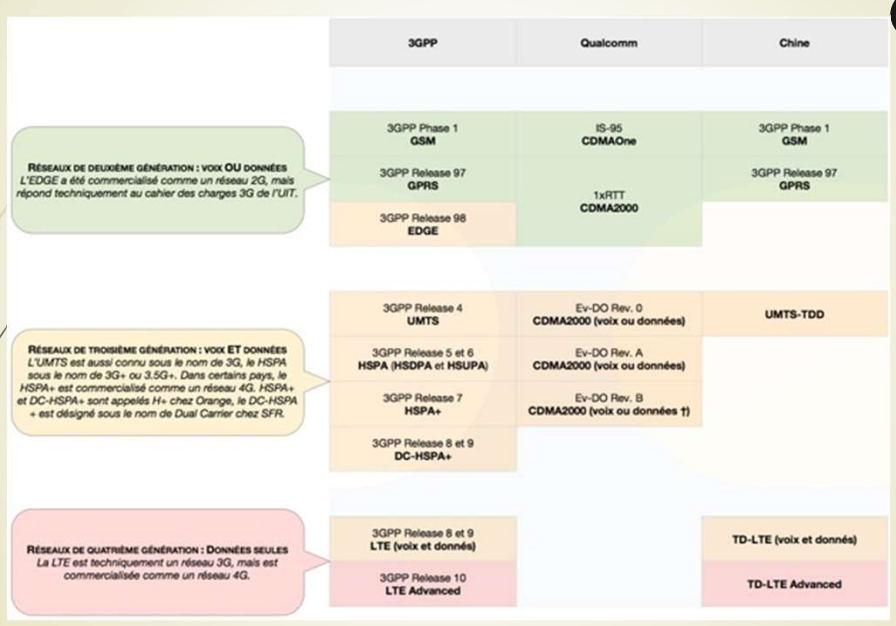
- La LTE utilise néanmoins un grand nombre de bandes de fréquences que les téléphones ne pourront pas toutes prendre en charge : un téléphone pouvant se connecter n'importe où dans le monde est encore un rêve. L'iPhone 5 distribué par AT&T aux États-Unis ne peut se connecter au réseau de Verizon, alors que tous deux utilisent la LTE. L'iPhone 5 distribué en Europe pourra se connecter aux réseaux LTE britanniques ou allemands, mais pas aux réseaux LTE scandinaves ou français.

- La 4G est définie non seulement par un seuil de débits, mais aussi par l'abandon total du mode commuté, c'est-à-dire du canal voix. Il n'y a plus qu'un seul canal de données, la voix passant sur IP (VoIP), avec comme avantage une augmentation drastique de sa qualité. La LTE-Advanced sera le premier réseau à répondre techniquement à la définition originale des réseaux de quatrième génération, mais il a fallu attendre quelques années avant d'y goûter.

JFA 354

Les réseaux de quatrième génération

R 2.05



JFA 355

Les réseaux de quatrième génération

R 2.05

- Les réseaux LTE commencent en effet à être exploités aux États-Unis, en Europe, au Japon ou encore en Chine. Une nouvelle norme pourrait d'ailleurs prolonger l'intérêt de la LTE en lui offrant la VoIP : VOLTE (Voice Over LTE).

Les réseaux de quatrième génération

JFA 356

R 2.05

- Les bandes de fréquences utilisées par les 4 opérateurs (Bouygues Telecom, Orange, Free Mobile et SFR) en France métropolitaine pour la 4G sont les suivantes :
  - 700 MHz (bande 28 ou B28).
  - 800 MHz (bande 20 ou B20).
  - 1,8 GHz (bande 3 ou B3).
  - 2,1 GHz (bande 1 ou B1).
  - 2,6 GHz (bande 7 ou B7).
- D'après l'ARCEP (Autorité de régulation des communications électroniques et des postes), avec la 4G, « *l'utilisateur dispose ainsi d'une connexion environ **3 fois plus rapide qu'en 3G** (résultat constaté sur les débits médians)* ».
- Notons que l'Hexagone commence à déployer une évolution de la 4G+, une évolution de la 4G basée sur la norme LTE-Advanced (Long Term Evolution Advanced). La **4G LTE-Advanced** offre un **débit maximal théorique** de l'ordre de **1 Gbit/s**.

Les réseaux de cinquième génération

JFA 357

R 2.05

Le réseau 5G ou l'ultra haut débit mobile

- La 5G (cinquième génération de réseaux mobiles), est une « ***génération de rupture** [qui] permettra un saut de performance* », affirme l'ARCEP. Elle ambitionne en effet d'offrir aux usagers l'**ultra haut débit mobile**, avec des **débits dépassant les 10 Gbit/s** ! En tous les cas, Orange, SFR ou encore Bouygues Telecom rivalisent déjà dans leurs effets d'annonce.
- Pour l'heure, la 5G en est dans sa phase expérimentale dans **plusieurs villes françaises** : Belfort, Bordeaux, Douai, Grenoble, Lannion, Lille, Lyon, Marseille, Nantes, Toulouse, Sophia-Antipolis et en Île-de-France.
- L'objectif fixé par la Commission européenne étant la couverture 5G d'au moins une grande ville de chaque État membre dès 2020.

JFA 358

Les réseaux de cinquième génération

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Le réseau 5G ou l'ultra haut débit mobile

- La 5G (cinquième génération de réseaux mobiles), est une « ***génération de rupture*** *[qui] permettra un saut de performance* », affirme l'ARCEP. Elle ambitionne en effet d'offrir aux usagers l'**ultra haut débit mobile**, avec des **débits dépassant les 10 Gbit/s** ! En tous les cas, Orange, SFR ou encore Bouygues Telecom rivalisent déjà dans leurs effets d'annonce.
- Pour l'heure, la 5G en est dans sa phase expérimentale dans **plusieurs villes françaises** : Belfort, Bordeaux, Douai, Grenoble, Lannion, Lille, Lyon, Marseille, Nantes, Toulouse, Sophia-Antipolis et en Île-de-France.
- L'objectif fixé par la Commission européenne étant la couverture 5G d'au moins une grande ville de chaque État membre dès 2020.

JFA 359

Les réseaux de cinquième génération

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Qu'est-ce que c'est ?

- La 5G est, comme son sigle le laisse deviner, la cinquième génération des standards en matière de téléphonie mobile. Elle succédera à la 4G, qui est toujours en cours de déploiement en France en 2019. Cette norme apportera des débits plus importants encore, mais aussi un temps de latence bien plus faible qu'aujourd'hui, et pourra supporter énormément de connexions en simultané.
- Mais la 5G ne doit pas être vue comme une simple évolution de la 4G. C'est en réalité une technologie de rupture. Elle « *se distingue des générations précédentes en ce qu'elle vise, dès sa conception, à intégrer un nombre de cas d'usages inédit* », relève l'Agence nationale des fréquences. Dès lors, son employabilité promet d'être très étendue et pourra donc servir dans des secteurs variés, notamment industriels.

JFA 360

Les réseaux de cinquième génération

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Quels atouts ?

- « Avec la 4G, un film de 800 Mo prend environ 40 secondes à télécharger ; avec la 5G ça serait réduit à une seule seconde », disait en 2014 l'ex-Premier ministre David Cameron.
- Voilà quel est son premier point fort : la capacité de téléchargement. Les débits en 5G seront jusqu'à 10 fois plus élevés que ceux de la 4G. Si l'on ose un parallèle, la 5G sera une sorte de fibre optique « sans fil » : elle pourrait même atteindre dans certaines situations jusqu'à 20 Gbit/s. En pratique, il faut plutôt s'attendre à une expérience de navigation entre 100 Mbit/s et quelques Gbit/s.

JFA 361

Les réseaux de cinquième génération

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Quels atouts ?

- Autre atout de la 5G : la latence. Cela désigne le délai de transit d'une donnée entre le moment où elle est envoyée et celui où elle est reçue. Celui-ci sera divisé par 10 par rapport à la 4G, avec un temps de réponse d'à peine une milliseconde. Cette réactivité est cruciale pour l'industrie, car des échanges constants et quasi-immédiats sont requis pour faire émerger des usages comme le transport autonome.
- Troisième point fort de la 5G : la densité. Avec elle, la 5G supportera « *un nombre très important de connexions mobiles simultanées* », commente le régulateur des télécoms. Cela va « *multiplier par 10 le nombre d'objets connectés au réseau simultanément* », confirme l'agence nationale des fréquences. En clair, il s'agit d'éviter l'engorgement des réseaux à l'heure où tout devient connectable et que les capteurs pullulent.

Les réseaux de cinquième génération

JFA 362

R 2.05

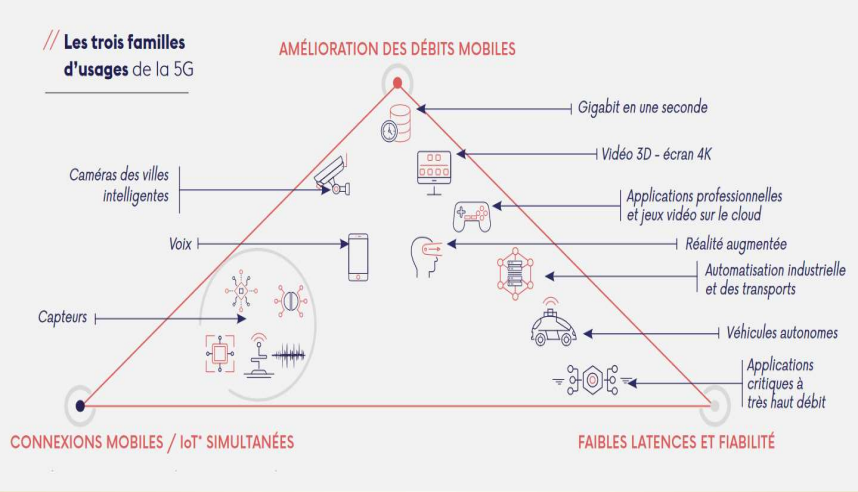
Quels services espérer ?

- Les performances annoncées de la 5G sont telles que les domaines qui vont en profiter sont très nombreux. Pour le mobinaute, la 5G permettra de charger instantanément n'importe quel contenu audiovisuel en haute et en très haute définition (vidéo 4K, vidéo en 3D…) ou de profiter du jeu à la demande (cloud gaming), avec les parties qui sont diffusées directement en streaming entre le joueur et les serveurs du service. C'est ce que proposent Shadow, GeForce Now ou Google Stadia par exemple.
- « La 5G continuera d'améliorer les services existants dans le domaine grand public en donnant par exemple l'accès à des contenus vidéo de meilleures définitions et en favorisant le développement d'applications de réalité augmentée ou virtuelle », anticipe l'Agence nationale des fréquence. Mais c'est surtout du côté de l'industrie que la 5G est intéressante.

Les réseaux de cinquième génération

JFA 363

R 2.05



https://www.numerama.com/tech/147723-5g-tout-savoir-sur-le-reseau-mobile-du-futur.html

Les réseaux de cinquième génération

JFA 364

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Pour quand ?

- Tout dépend de quoi on parle : si c'est le lancement de la 5G en France, le rendez-vous est fixé fin 2020. C'est en effet à cette date que les premiers déploiements auront lieu et que seront ouverts les premiers services 5G. On ne sait pas encore quelle sera la première ville qui sera desservie en ultra haut débit mobile, ni par qui : un opérateur ? Plusieurs ? Chacun se lancera-t-il dans une ville différente ?
- En principe, la prochaine grande échéance est fixée à 2025 : à ce moment-là, il faudra que les opérateurs couvrent les grandes villes et les principaux axes de transport (on suppose les autoroutes et les lignes TGV au minimum, mais aussi, possiblement, tout ou partie des voies secondaires, comme les RER).

Les réseaux de cinquième génération

JFA 366

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

- Ce qu'il va se jouer cette année, c'est la définition des modalités d'attribution des blocs de fréquences, ainsi que le lancement de la procédure qui permettra aux opérateurs de candidater pour récupérer des nouvelles ressources en fréquences. On s'attend bien sûr à ce que Orange, SFR, Bouygues Telecom et Free Mobile concourent. Les lauréats seront connus en 2020.
- Pour acquérir les licences 5G, les opérateurs devront collectivement dépenser au moins 2,17 milliards d'euros. Quatre blocs à prix fixe (350 millions d'euros chacun) seront proposés, assortis d'obligations précises. Ensuite, onze blocs à prix variable (à partir de 70 millions d'euros l'unité) seront mis aux enchères, avec toutefois des limites pour éviter qu'un opérateur ne rafle tout.

Les réseaux de cinquième génération

JFA 367

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Et mon smartphone ?

- Pour accéder à un réseau 5G, il faut posséder un smartphone compatible à la 5G ! Certes, les premiers modèles arrivent cette année, mais il n'y a aucune raison de se précipiter dessus… tout simplement parce que le réseau 5G n'existe pas encore ! De plus, il ne faut pas perdre de vue qu'il faudra des années avant d'avoir un degré de couverture du territoire correct.
- En France, SFR a annoncé le 16 octobre la vente de smartphones 5G en France. Seul problème (et pas des moindres) : il n'existe aucun réseau 5G en France qui soit prêt pour un usage commercial : ce n'est qu'à partir de 2020 que les opérateurs vont pouvoir vraiment s'y mettre.
- Au cours des derniers mois, des constructeurs ont promis le lancement de terminaux prêts pour la 5G. Il n'est toutefois pas urgent de se précipiter sur ces mobiles si vous n'êtes pas encore dans une zone 5G.

Les réseaux de cinquième génération

JFA 368

IUT GRAND OUEST NORMANDIE iNFO

R 2.05

Quelles bandes de fréquences ?

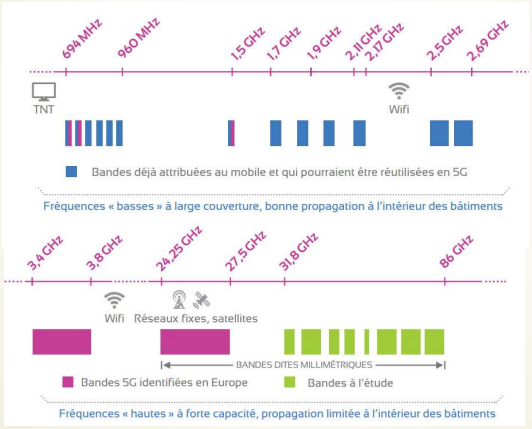
- Il est prévu de dégager au profit de la 5G des fréquences situées pratiquement sur tout le long du spectre radioélectrique. L'Agence nationale des fréquences (ANFR) précise qu'elles peuvent être classées en deux grandes catégories. Les fréquences dites « basses » ont une large couverture et une bonne propagation à l'intérieur des bâtiments. Quant aux fréquences dites « hautes », elles ont une forte capacité, mais une propagation limitée dans les bâtiments.
- Ceci étant dit, la stratégie consiste à utiliser à la fois de nouvelles fréquences dans la bande du spectre radioélectrique, mais aussi celles déjà attribuées pour faire passer des données en 2G, 3G et 4G. Pour l'heure, deux nouveaux blocs seront utilisés pour la 5G : celui de la bande 3,5 GHz (3,4 – 3,8 GHz) et celle, plus haute, de la bande 26 GHz (24,25 - 27,5 GHz). Cette dernière appartient à la catégorie des ondes millimétriques (voir ci-après).

Les réseaux de cinquième génération

JFA 369

R 2.05

Quelles bandes de fréquences ?



Les bandes de fréquence 5G identifiées. Et les autres. // Source : ANFR

Les réseaux de cinquième génération

JFA 370

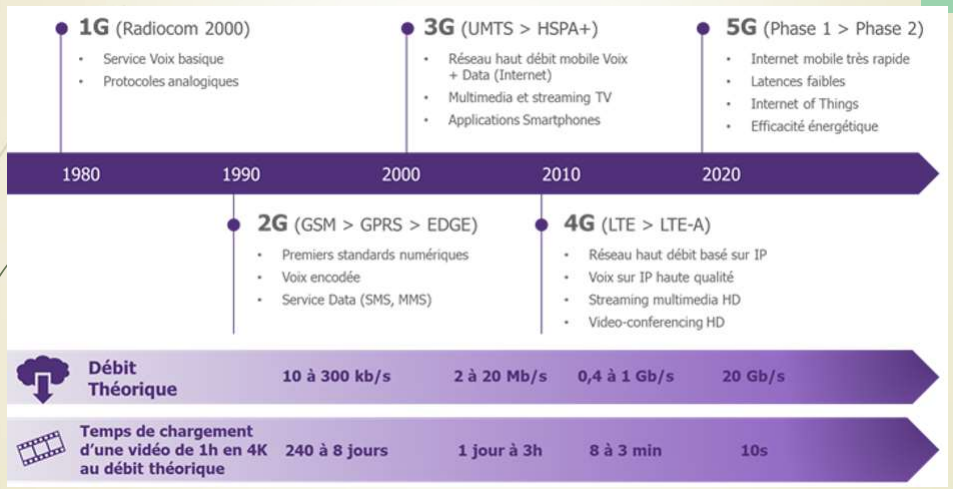
R 2.05

- D'autres fréquences ont aussi été identifiées comme adaptées à la 5G. C'est le cas des bandes situées dans la tranche des 700 et des 800 MHz, ainsi que celle à 1,5 GHz. Celles-ci sont idéales pour la pénétration dans les bâtiments et sont complémentaires des autres citées plus haut, davantage taillées pour apporter des capacités accrues en termes de vitesse de téléchargement.
- À mesure que le déploiement de la 5G se fera, les opérateurs pourront demander au régulateur des télécoms de recycler les bandes de fréquences utilisées pour la 2G, 3G et la 4G afin que les opérateurs disposent de plus de ressources pour l'ultra haut débit mobile. Cette réassignation n'est pas une nouveauté : Bouygues Telecom, Orange et SFR utilisent la bande 1 800 MHz pour faire de la 4G au lieu de la 2G.
- Enfin, la dernière conférence mondiale des radiocommunications, survenue en novembre, a été l'occasion de désigner de nouvelles bandes de fréquences. Y figurent les bandes 37 à 43,5 GHz, des portions 45,5 à 47 GHz, du segment 47,2 à 48,2 et de la tranche 66 à 71 GHz. « *Ces fréquences sont inédites en utilisation terrestre pour un service destiné au grand public* », dit-elle.
- Dans tous les cas de figure, la libération de ces bandes devra être organisée pour que l'on puisse y les faire migrer sur la 5G.

JFA 371

Synthèse des réseaux mobiles

R 2.05



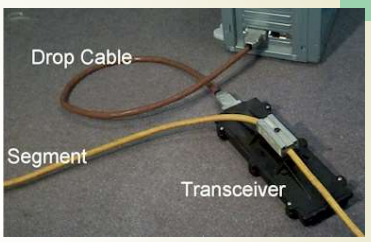
https://www.digitalcorner-wavestone.com/wp-content/uploads/2020/01/Image12.png

JFA 372

La structure physique

R 2.05

- Gros câble jaune « thicknet »
  - Coaxial, 10Base5
  - Topologie en Bus
  - 500m maxi
  - Postes espacés de 2,5 m
  - Peu maniable
  - Ajout de stations à la volée
    - Pas d'interruption
  - **Pas de retrait possible**

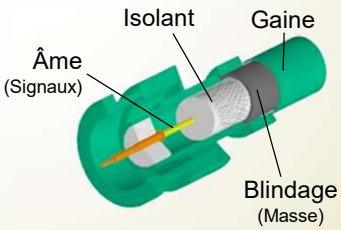


La structure physique (2)

JFA 373

R 2.05

- Petit câble noir (fin)
  - Coaxial, 10Base2
  - Topologie en Bus
  - 185m maxi
  - Postes espacés d'au moins 0,5 m
  - 30 stations maxi
  - Ajout grâce à un « T »
    - Interruption du réseau
  - Retrait aisé
    - Interruption du réseau
  - Sensible aux perturbations



JFA 374

Câble coaxial

R 2.05

- Caractéristiques : vitesse 10-100 Mbit/s pour une longueur de câble inférieure à 500m, connecteur BNC, coût moyen, peu flexible.
- Utilisation : câble TV (ex : Numéricâble), de moins en moins utilisé.
- Composition du câble : conducteur central (âme) - isolant – conducteur externe - gaine protectrice.

Plusieurs catégories de câbles existent suivant l'épaisseur de l'âme et la matière constituant la gaine (PVC ou téflon).

JFA 375

Câble à paires torsadées

R 2.05

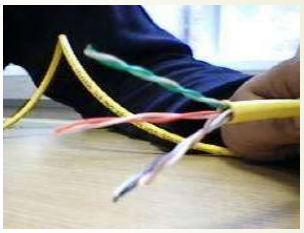
- Caractéristiques : vitesse 10-100 Mbit/s ou 1Gbit/s pour une longueur de câble inférieure à 100m, raccordement RJ-45, coût faible, facile à installer, problèmes d'atténuation / distorsion / diaphonie.
- Utilisation : réseau LAN, mais aussi sur l'interface d'accès WAN.
- Différents types de paires torsadées : ils résistent plus ou moins bien aux interférences électromagnétiques et à la diaphonie. Cependant, le coût est plus ou moins élevé. On distingue les paires torsadées :
  - non blindées (UTP, Unshielded Twisted Pair) : les plus courantes
  - écrantées (FTP ou ScTP, Foiled/Screened TP) : utilisées en France
  - blindées (STP, Shielded Twisted Pair) : peu utilisées

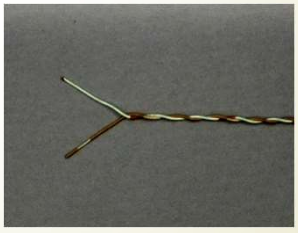
JFA 376

La structure physique (3)

R 2.05

- Paires Torsadées
  - Différentes normes
    - 10BaseT, cat. 3
    - 100BaseT, cat. 5
    - 1000BaseTX, cat. 6,7
  - Topologie en Etoile
  - 100m maxi
  - 2 stations maxi
  - Ajout sur le hub
    - Sans Interruption
  - Retrait aisé
    - Sans Interruption
  - Moins sensible aux perturbations si cat. Elevée
  - Facile d'emploi et résistant (aux manips)
  - Organe central obligatoire

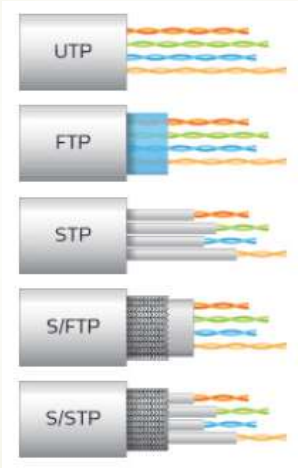




JFA 377

Câble à paires torsadées

R 2.05

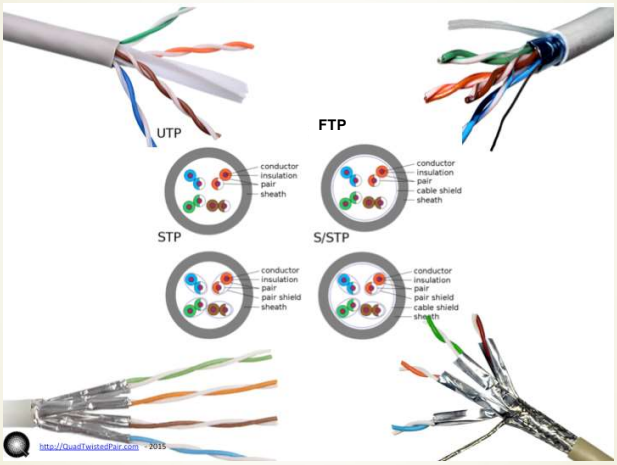


https://www.alliancelec.fr/img/cms/1361018345.jpg

JFA 378

Câble à paires torsadées

R 2.05



http://quadtwistedpair.com/wp-content/uploads/2015/02/Slide16.png

JFA 379

Fibre optique (FDDI)

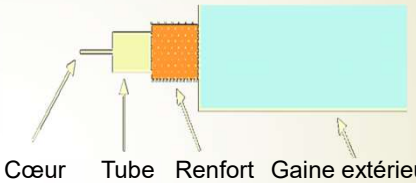
- Caractéristiques : 100Mbit/s ou 1Gbit/s dans les LAN, fonctionne par impulsions lumineuses, insensible aux interférences électromagnétiques, rayon de courbure faible, très coûteux, connectique délicate.
- Utilisation : pour les réseaux très hauts débits, les grandes distances et les environnements perturbes.
- Deux types de fibres :
  - multimodes (MMF), utilises dans les LAN 100Mbit/s et 1Gbit/s.
  - monomodes (SMF), utilises dans les LAN très haut débit et pour les applications WAN.

Composition de la fibre : fibre optique (cœur) et gaine optique en verre - revêtement - armature en fibre - enveloppe protectrice externe.

JFA 380

La structure physique (4)

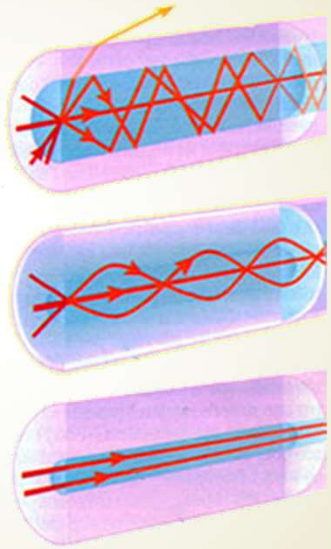
- Fibre Optique
  - Câble rond, xxxBaseYY
  - Topologie en BUS/Etoile
  - 1,5 km maxi
  - transceiver obligatoire à chaque extrémité de chaque fibre
  - Ajout sur une étoile optique
    - Sans Interruption
  - Ajout sur un bus
    - Interruption du réseau
  - Insensible aux bruits électromagnétiques



La structure physique (4b)

JFA 381

- Fibre Optique : deux types :
  - Multimode (base LX)
    - Cœur de 50-62m
    - Plusieurs ondes
    - 2 variétés :
    - Saut d'indice:
    - Transmission en zigzag
    - Gradient d'indice
    - Transmission parabolique
  - Monomode (base SX)
    - Transmission axiale
    - Cœur de 5-10m
    - 1 seule onde
    - Transmission selon axe
    - Peu de pertes => Longues distances



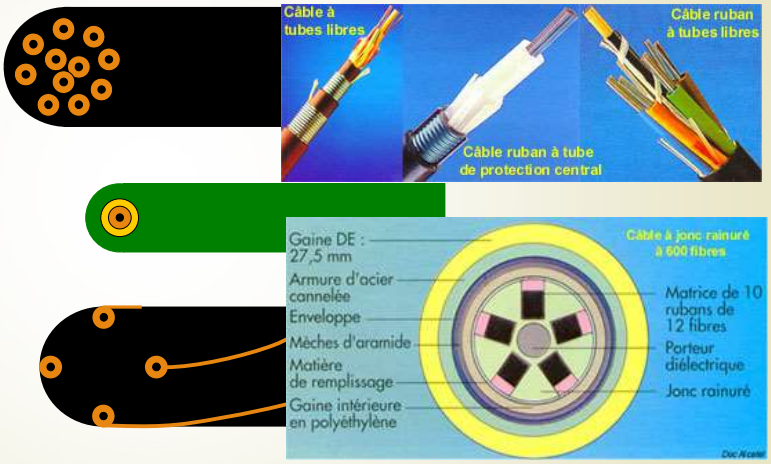
IUT GRAND OUEST NORMANDIE iNFO

R 2.05

La structure physique (4c)

JFA 382

- Fibre Optique : trois classes
  - Tubée Libre
    - Gros tube rigide contenant plusieurs fibres
    - Fibres bien protégées
    - **Encombrant...**
  - Tubée serré
    - 1 câble, 1 fibre
    - A base de silice (le cœur), de kevlar (le renfort)
    - Relativement fragile
    - Léger et flexible
    - Fibre gainée (plastique)
    - **Manipulation !**
  - Jonc rainuré
    - Gros câble flexible
    - Structure hélicoïdale
    - Dispositif de sortie
    - 1 fibre (nue) par rainure
    - **Pb pour câblage**



IUT GRAND OUEST NORMANDIE iNFO

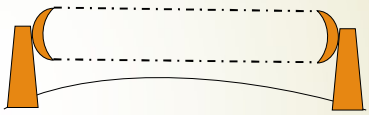
R 2.05

La structure physique (5)

JFA 383

R 2.05

- Sans fil
  - Faisceau hertzien
    - Quelques km
    - 2 → 30 Mb/s
    - Perturbations !
    - Courbure terrestre !
  - Radio
    - 30 m → quelques km
    - → 11 Mb/s
    - Loi stricte
    - Norme IEEE 802.11

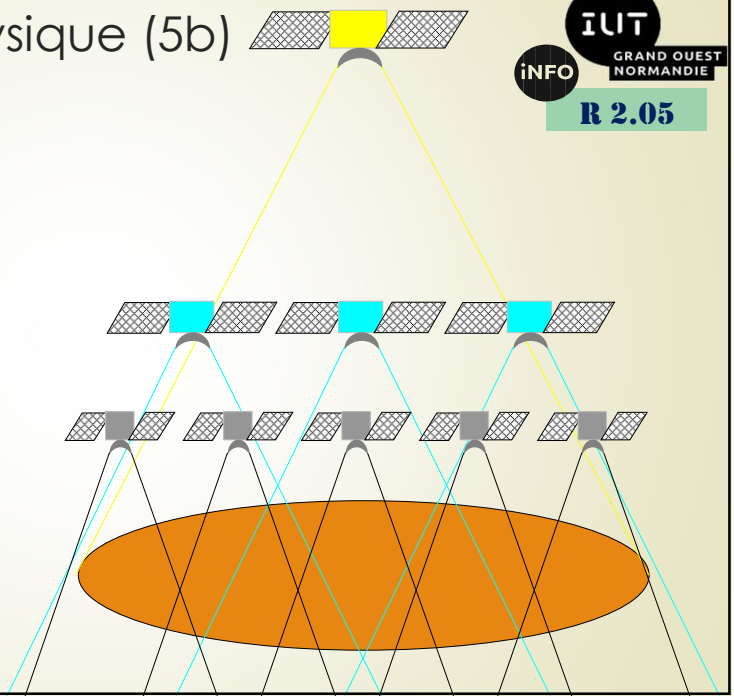


La structure physique (5b)

JFA 384

R 2.05

- Sans fil
  - Satellites
    - Géostationnaire
      - 36000 km
      - 150 Mb/s
      - 1s aller-retour !
    - Orbite moyenne
      - 5000 km
      - 10 → 40 Kb/s
      - 0,2s aller-retour
    - Orbite basse
      - 250 → 600 km
      - → 150 Mb/s
      - 0,1s aller-retour

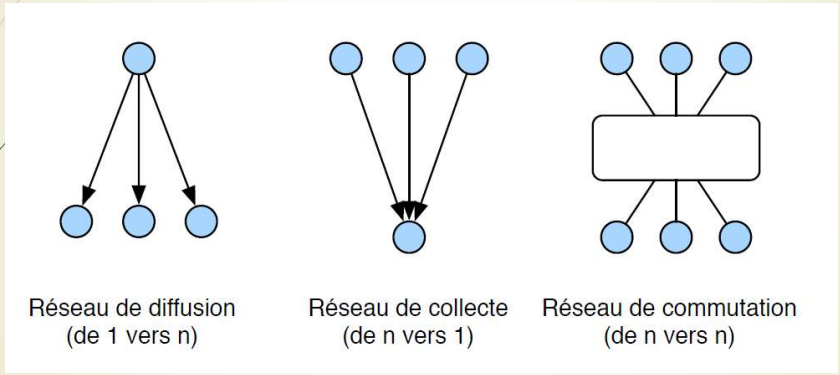


JFA 385

Qu'est-ce qu'un réseau à commutation ?

R 2.05

- Différents types de réseaux

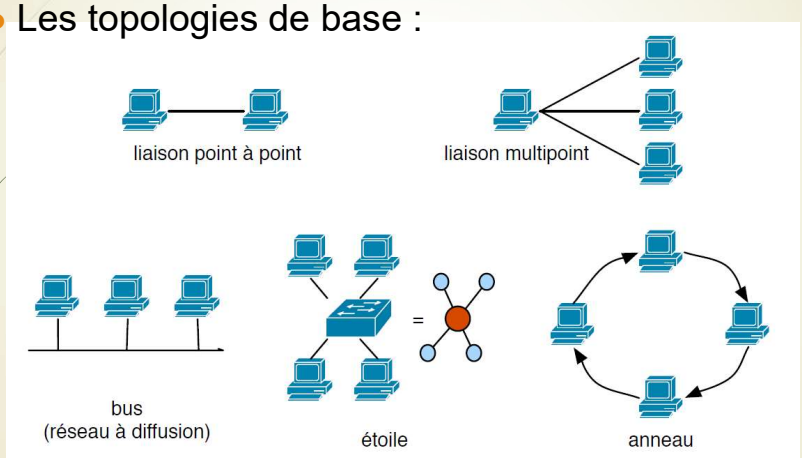


JFA 386

Topologie physique des réseaux à commutation

R 2.05

- Les topologies de base :

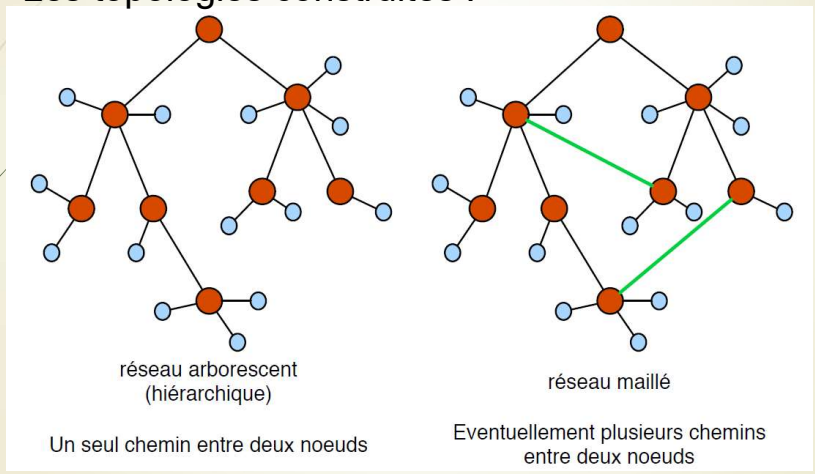


JFA 387

Topologie physique des réseaux à commutation

R 2.05

- Les topologies construites :



JFA 388

Webographie :

R 2.05

- https://fr.wikipedia.org/
- http://easytp.cnam.fr/terre/images/WiFi.pdf
- http://www.commentcamarche.net
- https://www.memoireonline.com/07/09/2324/m_Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite1.html
- http://w3.polytech.univ-montp2.fr/~karen.godary/Info_Indus/reseau/Cours_Wifi.pdf
- https://fr.wikipedia.org/wiki/Wi-Fi_Protected_Access
- https://www.macg.co/ios/2012/09/3g-h-4g-lte-un-guide-des-normes-reseau-77128
- https://www.dzigue.com/2015/11/11/reseaux-mobiles-2g-3g-4g-4g-5g/
- https://www.numerama.com/tech/147723-5g-tout-savoir-sur-le-reseau-mobile-du-futur.html

JFA 389

WEBOGRAPHIE

IUT GRAND OUEST NORMANDIE – INFO

R 2.05

- Liens Web :
  - http://www.commentcamarche.net/contents/532-qos-qualite-de-service
  - http://csud.educanet2.ch/3oc-info/3_Internet/3_Reseaux/page2.html
  - http://si.lycee-desfontaines.eu/userfiles/image/images_cours/buscan-cr1.gif
  - http://www.sen-av.net/IMG/jpg/LCD_Gestion_synoptiq1.jpg
  - http://www.loriotpro.com/ServiceAndSupport/How_to/WAN_Simulation_FR.php
  - http://slideplayer.com/slide/4919385/
  - https://www.sebastienadam.be/connaissances/cours/adressage_ip/les_adresses_ip_v4.php
  - https://www.inetdoc.net/articles/adressage.ipv4/adressage.ipv4.class.html
  - http://slideplayer.fr/slide/1322647/
  - https://www.sebastienadam.be/connaissances/cours/adressage_ip/les_sous-reseaux.php
  - https://openclassrooms.com/courses/apprenez-le-fonctionnement-des-reseaux-tcp-ip/le-routage-1
  - http://www.linux-france.org/~openingault/gulliveripv6/theorie/addr.html
  - http://www.lalitte.com/index.php?title=Le_routage
  - http://www.gipsa-lab.grenoble-inp.fr/~christian.bulfone/MIASS/
  - https://www.it-connect.fr/routage-statique-et-routage-dynamique/
  - https://web.maths.unsw.edu.au/~lafaye/CCM/internet/nat.htm
  - Cours de M. JEANPIERRE L.