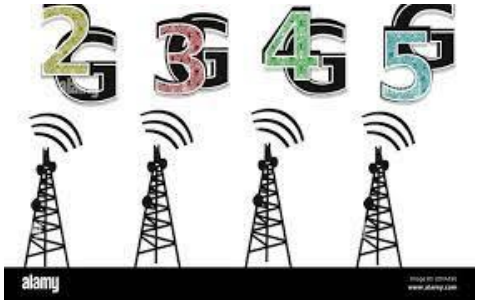
# Polycopié du Cours Réseaux Mobiles Master 2 RSD

*Université de Relizane*
*Département Informatique*




Guelta Bouchiba

Janvier 2022
1.0

# Table des matières

**Objectifs** 4

I - **Pré-requis** 5

II - **Carte Conceptuelle Mentale** 6

III - **Partie I :Introduction aux Réseaux : Mécanismes de base** 7

1. Les réseaux informatiques ..... 7

2. Les objectifs d'un réseau informatique ..... 8

3. Classification des réseaux ..... 8

*3.1. Classification des réseaux selon la distance* ..... 8
*3.2. Classification des réseaux selon la topologie* ..... 9

4. Les techniques de commutations ..... 11

5. L'architecture en couches ..... 13

*5.1. Principe de l'architecture en couches* ..... 13

6. Les modèles d'architecture réseaux ..... 15

*6.1. Le modele OSI* ..... 16
*6.2. Le modele TCP/IP* ..... 21
*6.3. Architectures Propriétaires* ..... 22
*6.4. Réseaux Locaux et Couche Liaison de données* ..... 23

IV - **Partie II** 31

1. Réseaux sans Fil ..... 32

*1.1. Qu'est-ce qu'un réseau sans fil ?* ..... 32
*1.2. Techniques de transmission dans les réseaux sans fil* ..... 32
*1.3. Les avantages et les inconvénients des réseaux sans fil* ..... 33
*1.4. Les catégories des réseaux sans fil* ..... 34
*1.5. Introduction au 802.11* ..... 36
*1.6. Le Standard 802.11* ..... 37
*1.7. Couche Physique dans Les Réseaux Sans Fil* ..... 39
*1.8. Wi-Fi5 ou 802.11a* ..... 40
*1.9. La Norme 802.11a* ..... 40
*1.10. OFDM (Orthogonal Frequency Division Multiplex)* ..... 41
*1.11. La norme 802.11e* ..... 41
*1.12. Wifi vs. Wifi 5* ..... 42
*1.13. Couche de liaison de données* ..... 42

2. Réseaux Cellulaires ..... 52

*2.1. Introduction* ..... 52
*2.2. Radiotéléphonie Cellulaire* ..... 52
*2.3. Concepts Cellulaires* ..... 52
*2.4. Déploiement des Réseaux Cellulaires* ..... 53

*2.5. Caractéristiques des Réseaux Cellulaires* ..... 54
*2.6. Constitution d'un Réseau Cellulaire* ..... 55
*2.7. Fonctionnement d'un Réseau Cellulaire* ..... 56
*2.8. Avantages & Inconvénient d'un Réseau Céllulaire* ..... 56
*2.9. Évolutions des Normes Cellulaires* ..... 56

3. GSM (Global System for Mobile Communications) ..... 57

*3.1. Architecture GSM* ..... 58
*3.2. Interfaces GSM :* ..... 59
*3.3. Identités dans un réseau GSM* ..... 61

4. Mobilité IP ..... 73

*4.1. Mobilité IP V4* ..... 73
*4.2. Mobilité IPV6* ..... 74

V - **Références Bibliographiques** 75

1. Abréviation ..... 75

2. Bibliographie ..... 76

# Objectifs

Cet enseignement couvre deux parties liées aux réseaux sans fil et mobiles. Dans la première, on traite les protocoles utilisés dans les réseaux de type LAN, MAN et WAN et elle permet aussi d'acquérir les compétences pour la conception de nouveaux protocoles. La seconde partie engendre les problèmes liés à la mobilité dans deux types d'infrastructure : les réseaux locaux sans fil (Wireless Local Area Networks) et les réseaux cellulaires de type GSM/GPRS/UMTS . On s'intéressera particulièrement aux protocoles de la couche MAC (médium radio) et la gestion de la mobilité des terminaux.

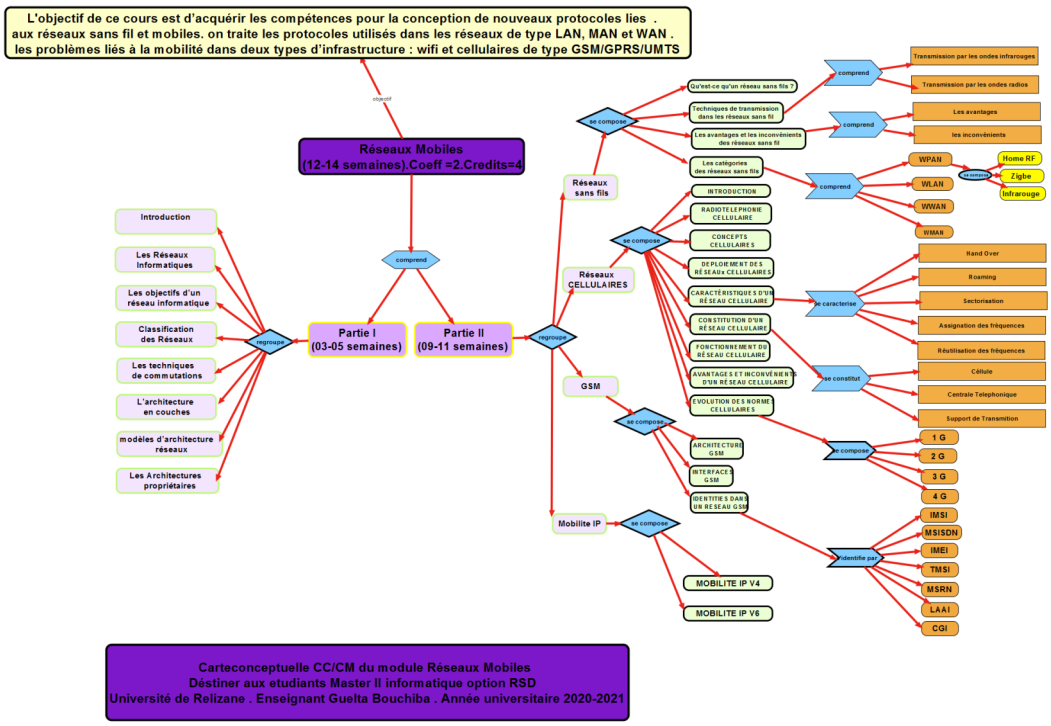
# Pré-requis

I

- connaissances solides en Traitement de Signal, en Electromagnétisme (en particulier la propagation des ondes électromagnétiques et le rayonnement des antennes).
- connaissance en Techniques de Transmission (modulations analogiques et numériques) et en Théorie de l'Information.
- La connaissance de prerequiss réseaux de télécommunications est un plus.

# Carte Conceptuelle Mentale

II




Carte Conceptuelle Mentale du Cours Réseaux mobiles

# Partie I :Introduction aux Réseaux : Mécanismes de base

III

Les réseaux informatiques sont nés à la fin des années 1960. C'est avec le projet ARPANET que la DARPA a lancé le premier réseau aux États-Unis. En adoptant ce point de vue, bien sûr, les terminaux passifs connectés aux ordinateurs centraux ne sont pas considérés comme des réseaux informatiques. De nos jours, les réseaux informatiques sont devenus une nécessité. Ce chapitre présente les bases des réseaux informatiques.

## 1. Les réseaux informatiques

Les réseaux informatiques sont le résultat de la combinaison de deux domaines : l'informatique et les télécommunications. En effet, les télécommunications recouvrent toutes les techniques (filaires, radio, optiques, etc.) de transmission d'informations, quelle que soit leur nature (symboles, polices, images fixes ou animées, sonores ou autres). L'histoire des télécommunications commence en 1832, lorsque le physicien américain Morse (1791-1872) a l'idée d'un système de transmission codé (code Morse). Cependant, le mot "télécommunications" a été introduit en 1904 par Estaurié (polytechnicien, ingénieur général des télégraphes 1862-1942). En 1932, lors de la conférence de Madrid, le terme est consacré en renommant l'Union internationale des télécommunications en Union internationale des télécommunications (IUT) .

Malgré les profondes similitudes entre les réseaux informatiques et les systèmes distribués, il est important de noter la différence entre les deux concepts. Un système distribué est en fait un ensemble de systèmes informatiques indépendants présentés aux utilisateurs comme un seul système cohérent.

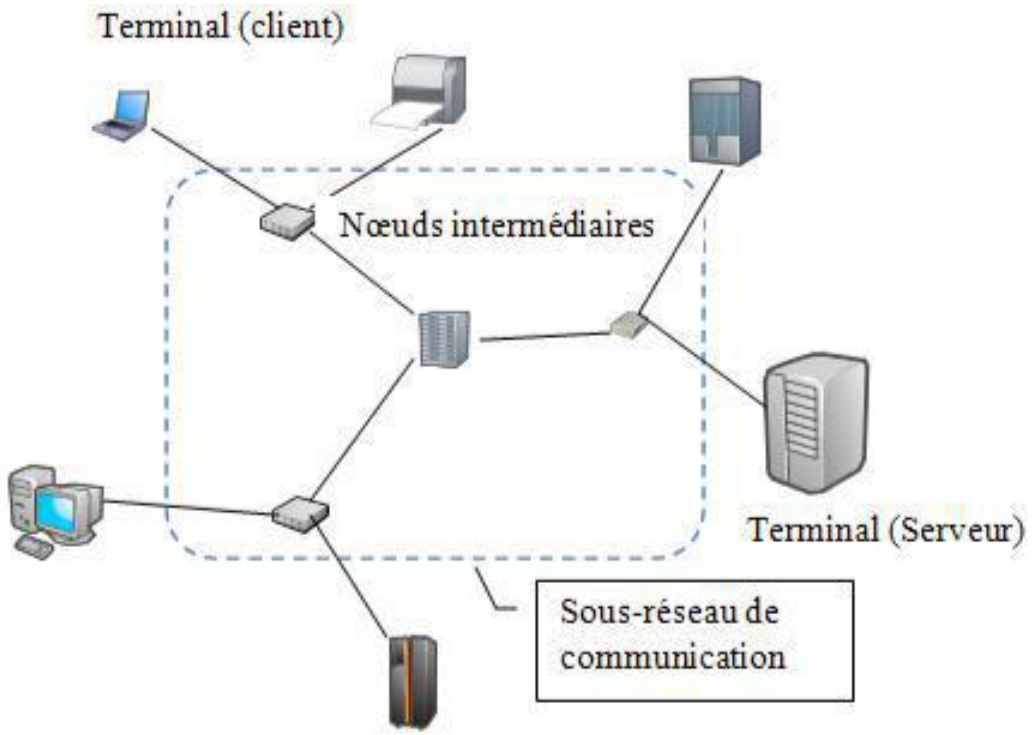
Un réseau informatique est constitué d'un ensemble de nœuds reliés par des chemins physiques (Figure suivante ). Un nœud est une machine ou toute entité qui peut être adressée par un numéro unique. Il existe deux types de nœuds :

. Terminaux (Hôtes) : sont des systèmes informatiques interconnectés capables d'échanger des données et d'exécuter des applications utilisateur. Dans une architecture client/serveur, ces terminaux peuvent être clients ou serveurs.

. Nœuds intermédiaires : il s'agit d'un ensemble de périphériques qui assure la communication réseau. Parfois, ces appareils sont appelés commutateurs ou routeurs.

Différents nœuds sont connectés aux canaux de communication par un dispositif spécial appelé MAU (Medium Access Unit).

L'ensemble des nœuds intermédiaires et des canaux de communication forme un sous-réseau de communication.




# 2. Les objectifs d'un réseau informatique

Les réseaux informatiques sont nés de la nécessité de faire communiquer des terminaux distants avec un ordinateur central. En fait, l'évolution des besoins va au-delà de la volonté de connecter les installations des grands laboratoires et des entreprises à la volonté de connecter tous nos appareils simples via des réseaux informatiques (notamment Internet). Un réseau informatique offre plusieurs avantages, par ex :

- Partage de ressources (Matériel : imprimante... ou logiciel : Fichier...).
- Transfert de données (fichiers, parole, vidéo...).
- Interaction avec les utilisateurs connectés : messagerie électronique, conférence électronique, ...
- Fiabilité (en dupliquant les ressources).
- Rapport qualité-prix (problème économique) : atteindre une puissance de calcul ou de calcul comparable à un multiprocesseur à des coûts réduits.

# 3. Classification des réseaux

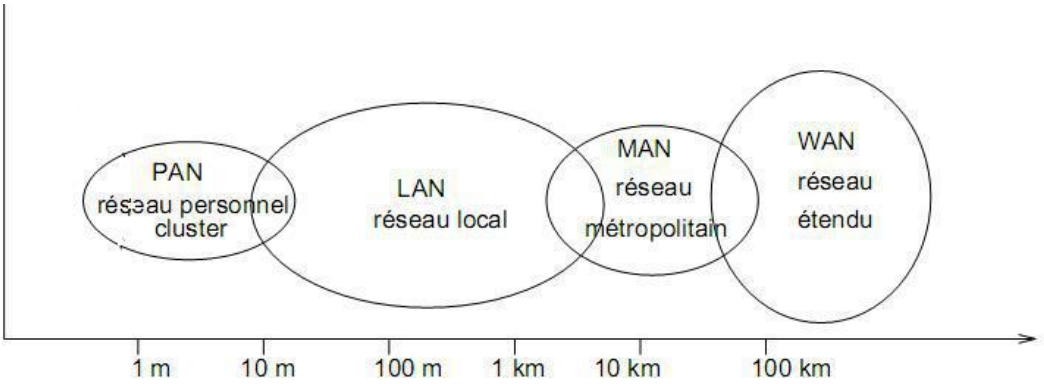
Plusieurs critères peuvent être utilisés pour la classification des réseaux comme : la taille, la topologie ou la technique de transmission.

## 3.1. Classification des réseaux selon la distance

Comme on peut le voir sur la figure suivante, les réseaux informatiques peuvent être divisés en quatre classes selon leur portée :

- PAN (Personal Area Network) est un réseau informatique centré sur les utilisateurs. Indique une connexion de plusieurs mètres autour de lui. Les connexions sans fil sont souvent utilisées dans ce type de réseau.

- LAN (Local Area Network) : peut aller de quelques mètres à quelques kilomètres et correspond au réseau de l'entreprise. Il peut être développé en plusieurs bâtiments et permet de répondre à tous les besoins internes de cette entreprise. Les LAN diffèrent des autres classes de réseaux par leur taille, leur technologie de transmission, leur vitesse de transmission et leur topologie. Avec un débit de plusieurs Mb/s avec support mutualisé.
- MAN (Metropolitan Area Network) : relie plusieurs sites situés dans la même ville, tels que différents sites universitaires ou administratifs, chacun avec son propre réseau local. Leur topologie est similaire à la topologie LAN, mais avec des normes différentes. Leur vitesse de transmission peut être de plusieurs centaines de kbit/s à plusieurs Mbit/s.
- WAN (Wide Area Network) : permet de communiquer à l'échelle terrestre ou planétaire avec des infrastructures physiques, qui peuvent être terrestres ou spatiales, à l'aide de satellites de télécommunications.




## 3.2. Classification des réseaux selon la topologie

La topologie détermine la manière dont les périphériques du réseau sont organisés. En fait, il convient de distinguer deux classes de topologies : la topologie logique de la topologie physique.

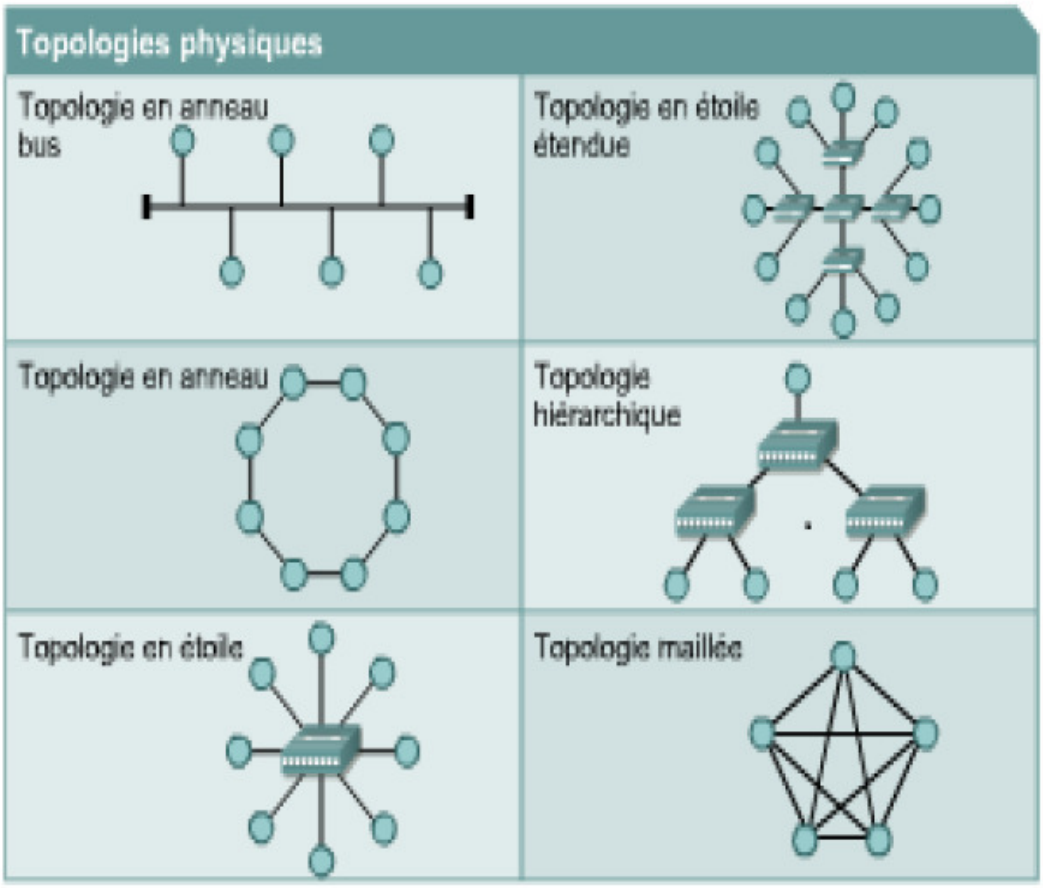
Dans une topologie logique, on considère le flux d'informations entre les différents éléments du réseau. Les aspects de partage des médias et les méthodes d'accès aux médias sont cruciaux dans ce type de topologie. D'autre part, la topologie physique traite de l'agencement spatial du dispositif. Cette topologie est choisie en fonction de l'environnement, de l'architecture et des exigences de débit technique de l'entreprise. En plus, elle a une importance extrême sur l'évolution de réseau, sur son administration et sur les compétences des personnelles qui seront amené à s'en servir.

Il existe plusieurs topologies possibles. De plus, il est possible de combiner différentes topologies pour créer une topologie hybride. Les principales topologies sont :

- Topologie en bus : dans ce type de réseau, différentes stations sont reliées par le même câble à l'aide de connecteurs spécialisés. Un capuchon (terminateur) est fixé à chaque extrémité du câble pour empêcher la réflexion du signal. Parce que le câble était partagée par toutes les stations, il n'y en a qu'une qui transmet les données à la fois. Les réseaux de bus sont simples, peu coûteux, faciles à mettre en place et à entretenir. Si la machine tombe en panne sur un réseau de bus, le réseau fonctionne toujours, mais si le câble est défectueux, l'ensemble du réseau ne fonctionne plus. L'augmentation du nombre de stations connectées au réseau réduit les performances du réseau.
- Topologie en étoile : dans ce type, plusieurs câbles sont centrés autour d'un nœud central. Les faisceaux et les réseaux de faisceaux sont faciles à gérer car la gestion des ressources est centralisée. De plus, les réseaux en étoile fonctionnent toujours même si la station tombe en panne ou si la connexion est perdue si le nœud central est opérationnel. Si le nœud central tombe en panne, tout le réseau tombe en panne.

D'un point de vue économique, les réseaux de faisceaux sont particulièrement coûteux pour les réseaux WAN. Il existe deux types de nœuds centraux : les concentrateurs et les commutateurs. Le fonctionnement du hub consiste à envoyer des informations à tous ses ports. D'autre part, le commutateur remplit la fonction de commutation (c'est-à-dire qu'il envoie des informations uniquement au port approprié).

- Topologie circulaire : Il s'agit d'une topologie en bus refermée sur elle-même. La direction dans laquelle le réseau fonctionne est déterminée - ce qui évite les conflits. Avec ce type, une collision est empêchée par une procédure basée sur le droit d'accès au média. Habituellement, l'anneau est placé à l'intérieur d'une boîte appelée unité d'accès multistation (MAU). Toutes les stations sont connectées au MAU. L'heure d'accès est précisée (la machine sait quand elle pourra envoyer l'information). Pour éviter une défaillance du réseau si le câble est détruit, une boucle de secours supplémentaire est ajoutée dans la topologie à double boucle.
- Topologie maillée : ce réseau est constitué d'un ensemble de stations reliées par des canaux. Selon le nombre de relations établies, on distingue les réseaux totalement interconnectés et les réseaux irrégulièrement interconnectés.




### 3.2.1. Classification des réseaux selon la technique de transmission

Il existe deux classes de réseaux selon les critères de la technologie de transmission :

- Mode diffusion : Le premier mode de fonctionnement consiste à partager un support de transmission. Chaque message envoyé par un appareil sur le réseau est reçu par tout le monde. Il s'agit d'une adresse de destination spécifique située dans le message qui permet à chaque appareil de déterminer si le message lui est adressé ou non. Si le message est destiné à toutes les machines, on parle de diffusion. Certains systèmes permettent également de transférer le paquet vers un sous-ensemble, ce qui est un multicast.

Un seul appareil a le droit d'envoyer un message au support à la fois. Il doit donc "écouter" à l'avance si la voie est dégagée ; sinon, il attend selon le protocole propre à chaque architecture. Ce mode est généralement utilisé pour les petits réseaux.

- Mode point à point : Dans ce mode, le support physique (câble) ne connecte qu'une seule paire d'appareils. Quand deux éléments non

directement connectés entre eux veulent communiquer ils le font par l'intermédiaire des autres noeuds du réseau. Il est possible de trouver plusieurs itinéraires de longueurs différentes pour atteindre la même destination. Choisir le meilleur chemin est crucial. Ce mode est généralement utilisé dans les réseaux étendus.

# 4. Les techniques de commutations

La commutation décrit la technique permettant d'acheminer des informations au travers d'un réseau composé de nœuds liés entre eux. Les informations sont transportées de nœud en nœud jusqu'au destinataire. Il existe deux techniques principales :

la commutation de circuit et la commutation de paquets.D'autres modes de commutation tels que la commutation de trames et la commutation de cellules s'inspirent de la commutation de paquets. Par ailleurs, la commutation de messages, l'ancêtre de la commutation de paquet, n'est plus utilisée.

- La commutation de circuit : Historiquement c'est la première à avoir été utilisée, par exemple dans le réseau téléphonique à l'aide des autocommutateurs. Elle consiste à créer dans le réseau un circuit physique entre l'émetteur et le récepteur avant que ceux-ci ne commencent à échanger des informations. Ce circuit sera propre aux deux entités communiquant et il sera libéré lorsque l'un des deux coupera sa communication. Par contre, si pendant un certain temps les deux entités ne s'échangent rien le circuit leur reste quand même attribué. C'est pourquoi, un même circuit (ou portion de circuit) pourra être attribué à plusieurs communications en même temps. Cela améliore le fonctionnement global du réseau mais pose des problèmes de gestion (files d'attente, mémorisation).

Les applications classiques de ce type de réseau sont celles à contrainte temporelle (délai de traversée du réseau constant) telles que le service téléphonique (RTC et RNIS) et toutes les applications "streaming". L'inconvénient majeur de cette technique est le gaspillage possible de la bande passante. En effet, les ressources réservées pour une communication ne sont pas toujours utilisées de façon optimale.

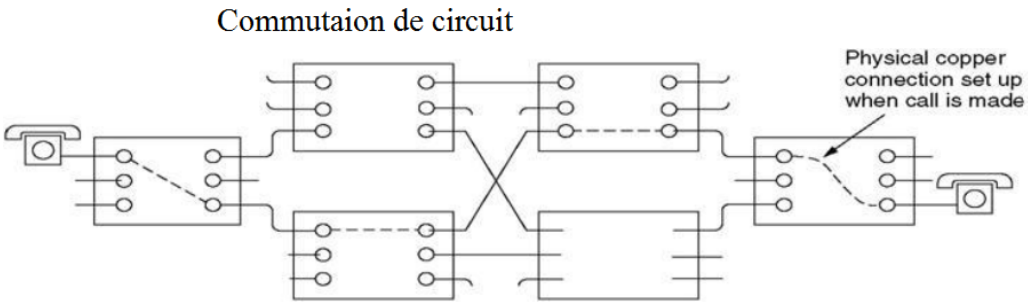
- La commutation de messages : Il s'agit d'une technique de commutation simple qui consiste à effectuer la communication entre les voisins. Un message est un ensemble d'information logique formant un tout (fichier, mail). Ainsi, cette technique consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de nœud de commutation en nœud de commutation. Chaque nœud attend d'avoir reçu complètement le message avant de le réexpédier au nœud suivant (Store & Forward). Cette technique nécessite de prévoir de grandes zones tampon dans chaque nœud du réseau, mais comme ces zones ne sont pas illimitées il faut aussi prévoir un contrôle de flux des messages pour éviter la saturation du

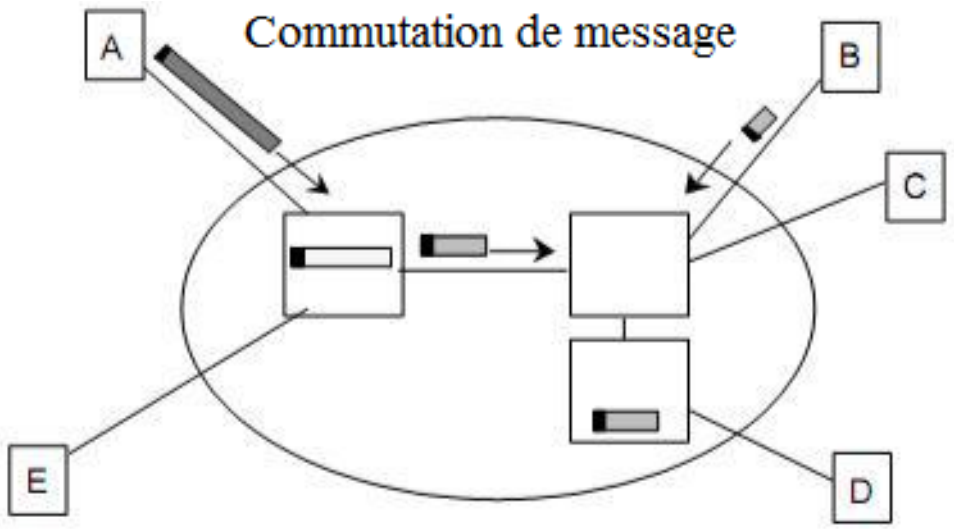
réseau. Dans cette approche il devient très difficile de transmettre de longs messages. En effet, comme un message doit être reçu entièrement à chaque étape si la ligne a un taux d'erreur de 10-5 par bit (1 bit sur 105 est erroné) alors un message de 100000 octets n'a qu'une probabilité de 0,0003 d'être transmis sans erreur.

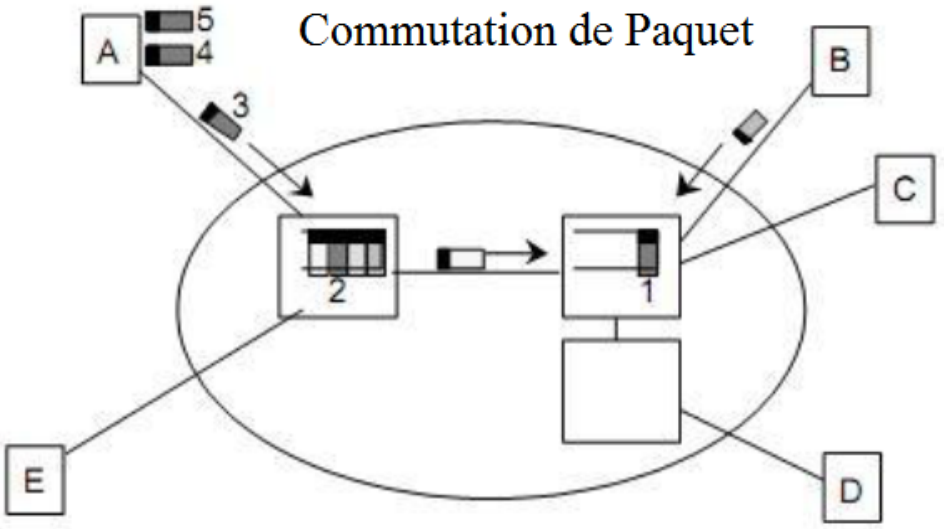
- La commutation de paquets : Elle est apparue au début des années 70 pour résoudre les problèmes d'erreur de la commutation de messages. Un message émis est découpé en paquets et par la suite chaque paquet est commuté à travers le réseau comme dans le cas des messages. Les paquets sont envoyés indépendamment les uns des autres et sur une même liaison on pourra trouver les uns derrière les autres des paquets appartenant à différents messages. Chaque noeud redirige chaque paquet vers la bonne liaison grâce à une table de routage. La reprise sur erreur est donc ici plus simple que dans la commutation de messages, par contre le récepteur final doit être capable de reconstituer le message émis en réassemblant les paquets. Ceci nécessitera un protocole particulier car les paquets peuvent ne pas arriver dans l'ordre initial, soit parce qu'ils ont emprunté des routes différentes, soit parce que l'un d'eux a du être réémis suite à une erreur de transmission.

Technique de commutation de paquets

- La commutation de trames : La commutation de trames ou relais de trames est une évolution de la commutation par paquets et peut être considérée comme une technique intermédiaire en attendant l'arrivée des techniques à commutation ATM. En fait, l'amélioration de fiabilité de voies de communication montrée avec le temps nécessite l'optimisation des performances en allégeant les procédures de contrôle de flux et le routage. Cette technique permet de diminuer le volume de données émis et d'augmenter les débits. En effet, les commutateurs à ce niveau acheminent les trames vers le récepteur en utilisant des références, également appelés identificateurs ou étiquettes (en anglais labels). Une référence est une suite de chiffres, accompagnant une trame pour lui permettre de choisir une porte de sortie, suivant une table de commutation. Par contre, les routeurs acheminent les paquets vers le destinataire en utilisant son adresse complète et une table de routage, qui lui permet de diriger les paquets vers les bonnes sorties.
- La commutation de cellules : Une cellule est un paquet particulier dont la taille est toujours fixée à 53 octets (5 octets d'en-tête et 48 octets de données). C'est la technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode) qui opèrent en mode connecté où avant toute émission de cellules, un chemin virtuel est établi par lequel passeront toutes les cellules. Cette technique mixe donc la commutation de circuits et la commutation de paquets de taille fixe permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés.






# 5. L'architecture en couches

La transmission de données entre les stations du réseau nécessite sans doute une infrastructure composée de canaux de communication et d'un ensemble de nœuds. Cependant, l'existence même de cette infrastructure ne permet pas d'offrir un service de transfert de données de la qualité requise. L'existence d'un logiciel contrôlant toutes les fonctions du réseau (telles que l'adressage, le contrôle des erreurs et le contrôle du flux) est plus que nécessaire. Un logiciel réseau est en fait un logiciel complet avec de nombreuses fonctionnalités. Afin de maîtriser sa complexité, le logiciel réseau est organisé en couches dont le nombre, les noms et les fonctions varient d'une conception à l'autre.

## 5.1. Principe de l'architecture en couches

Une couche est un ensemble homogène destiné à accomplir une tâche ou à fournir un service. Le layering doit en effet respecter les principes suivants :

Une couche doit être créée lorsqu'un nouveau niveau d'abstraction est nécessaire.

Chaque couche remplit une fonction définie avec précision.

Le choix des frontières entre les couches doit minimiser le flux d'informations aux interfaces.

Le nombre de couches doit être :

- assez grand pour empêcher la coexistence dans une même couche de fonctions très différentes et
- suffisamment petit pour éviter que l'architecture ne devienne difficile à gérer.

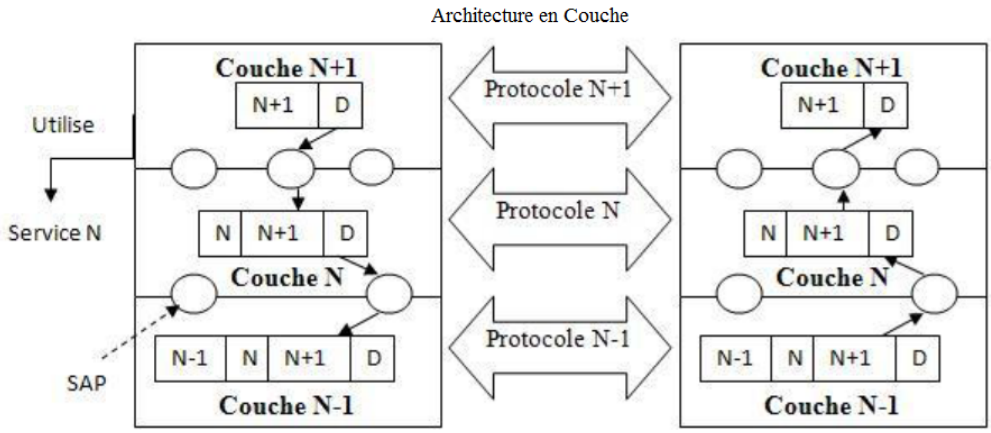
Cette superposition de logiciels réseau offre des avantages supplémentaires tels que : l'évolutivité, la portabilité et l'interopérabilité.

Le principe de fonctionnement des logiciels hiérarchisés repose sur cette règle : chaque niveau offre des services au niveau supérieur immédiat en cachant les détails de l'implémentation (le premier niveau est situé au-dessus du support de communication). Un service désigne un ensemble de primitives ou d'opérations qu'une couche fournit à la couche supérieure. Les éléments actifs de chaque couche ou niveau sont appelés entités, qu'elles soient logicielles (processus) ou matérielles (puce d'E/S intelligente), les entités d'un même niveau sur différentes machines sont appelées entités homologues ou homologues.

Les primitives peuvent être divisées en quatre classes : les primitives de demande, les primitives de réponse, les primitives d'indication et les primitives d'accusé de réception.

La couche (N) offre des services à la couche (N + 1) via l'interface. En effet, l'échange de données et de primitives entre ces couches se fait via des points d'accès aux services (SAP Service Access Points). Chaque SAP est identifié par un numéro unique. Pour SAP vous pouvez trouver d'autres noms comme : port, porte et socket...etc.

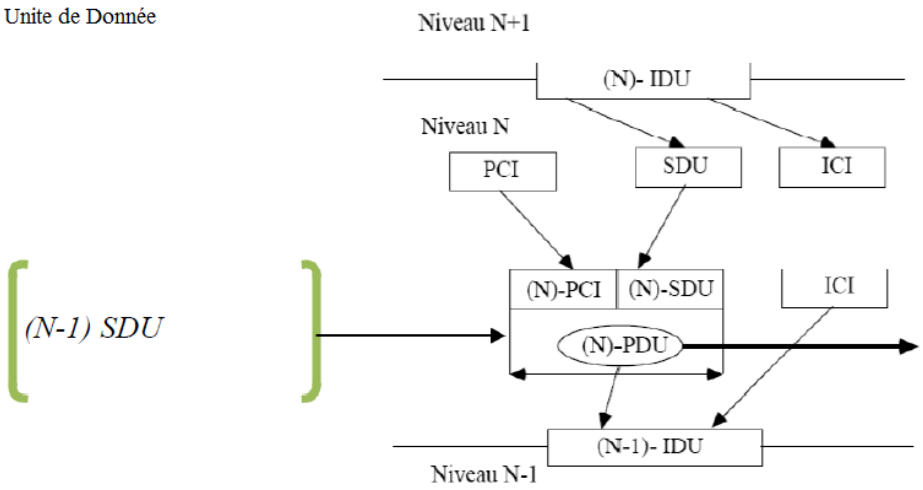
Chaque entité de la couche N peut communiquer indirectement avec son homologue d'une autre machine en respectant le protocole. Le protocole est un ensemble de règles qui déterminent le format et la signification des messages échangés. Un ensemble de couches et de protocoles forme une architecture réseau. Par pile de protocoles, nous entendons les protocoles utilisés par un système particulier avec un protocole dans chaque couche.




### 5.1.1. Les unités de données

Lorsqu'un service de niveau (N) est invoqué, le niveau (N + 1) fournit l'ensemble des informations nécessaires au bon traitement de l'unité de données. Une partie de ces informations est destinée à l'usage exclusif de l'entité de niveau N, en précisant les traitements qui doivent être effectués localement sur les données. Ces informations de contrôle d'interface (ICI) sont attachées au SDU et forment l'unité de données de contrôle d'interface (IDU). L'ICI de couche N à usage exclusif n'est pas transmis.

La couche N ajoute aux données de service, appelées (N) SDU, les informations de service nécessaires à l'homologue de la couche N pour traiter et transmettre correctement les données à sa couche distante (N + 1). Ces informations de protocole forment les informations de contrôle de la couche Protocol Control Information (N), appelées (N) PCI. Les données sont acheminées vers un pair via une connexion de niveau (N-1). La couche distante N recevant le (N) SDU extrait (N) PCI, l'interprète, et fournit les données (N) SDU à la couche (N + 1) ; ces données deviennent alors le (N + 1) PDU.




### a) Les types de services

Les couches fournissent au niveau supérieur deux types de services différents :

Mode connexion : dans ce mode, une entité de niveau N ne peut envoyer un bloc d'information qu'après avoir demandé au partenaire avec lequel elle souhaite communiquer l'autorisation de le faire. Pour établir la connexion, le protocole de niveau N envoie donc un bloc d'information contenant la connexion de niveau N. Le récepteur a le choix d'accepter ou de refuser la connexion en envoyant un bloc de données indiquant sa décision. Dans certains cas, la demande de connexion peut être arrêtée par l'administrateur du service, qui peut refuser de transmettre la demande de connexion au récepteur, par exemple en raison d'un manque de ressources internes (comme un espace mémoire de nœud insuffisant). La mise en place du mode connexion, qui permet la communication entre entités homologues, se déroule en trois phases différentes :

1. Établir une connexion.

2. Transfert de données d'utilisateur d'un sujet à un autre.

3. Libérez la connexion.

Mode sans connexion : en mode sans connexion, les blocs de données sont transmis sans qu'il soit nécessaire de s'assurer au préalable de la présence d'une entité distante. Cependant, l'existence de connexions à n'importe quel niveau d'architecture est nécessaire pour s'assurer que le service fourni n'est pas complètement inutile.

## 6. Les modèles d'architecture réseaux

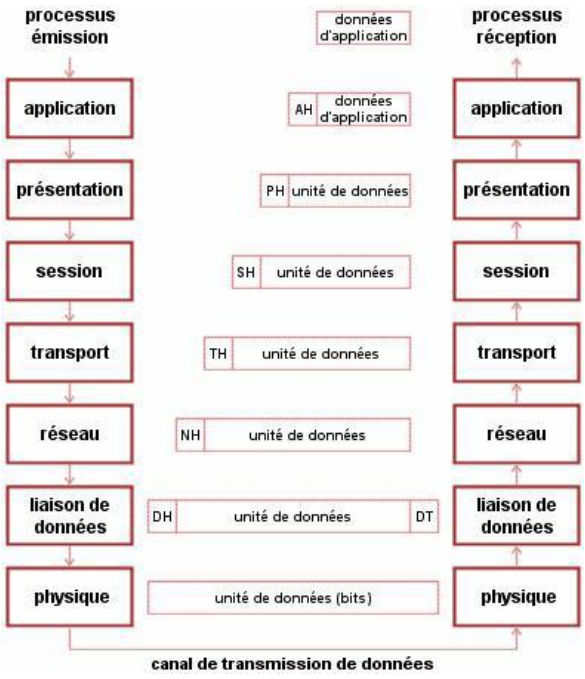
Au début des années 1970, chaque fournisseur a développé sa propre solution réseau basée sur une architecture et des protocoles privés, tels que : SNA "System Network Architecture" d'IBM, DECnet de DEC "Digital Network Architecture", DSA "Distributed System Architecture" de Bull, DoD TCP/IP, etc. Il est vite apparu qu'il serait impossible d'interconnecter ces différents réseaux hétérogènes sans un standard international.

La normalisation est en fait un ensemble de règles techniques résultant de l'accord des fabricants et des utilisateurs, visant à clarifier, unifier et simplifier quelque chose en vue d'une meilleure performance dans tous les domaines de l'activité humaine. Il existe deux types de normes : les normes de facto et les normes de jure. La norme de facto survient lorsqu'un ensemble de producteurs s'accorde sur des règles communes (ou que l'un d'eux impose certaines règles aux autres). En revanche, les normes de jure ont une plus grande valeur juridique car elles sont imposées par des organisations internationales ou nationales.

Il existe de nombreux organismes de normalisation dans le monde des réseaux informatiques tels que : ISO, IEEE, ITU, EIA et W3C.

## 6.1. Le modele OSI

Cette norme, développée en 1978/1979 par l'Organisation internationale de normalisation (ISO), est une norme d'interconnexion de systèmes ouverts (OSI). En fait, il y avait 02 projets. Le second est celui initié par le CCITT (ou actuellement IUT-T) publié sous le nom X.200. Les deux projets ont fusionné en une seule norme publiée en 1983 appelée ISO 7498.Le premier objectif de la norme OSI était de définir un modèle d'architecture de réseau quelconque basé sur la division en sept couches, chacune de ces couches correspondant à la fonctionnalité spécifique du réseau. Les couches 1, 2, 3 sont dites basses (ou couches orientées transmission) et les couches 5, 6 et 7 sont dites hautes (couches orientées processus). Notez que les nœuds de sous-réseau n'ont que les trois premières couches car ils ne fournissent que le routage des données.

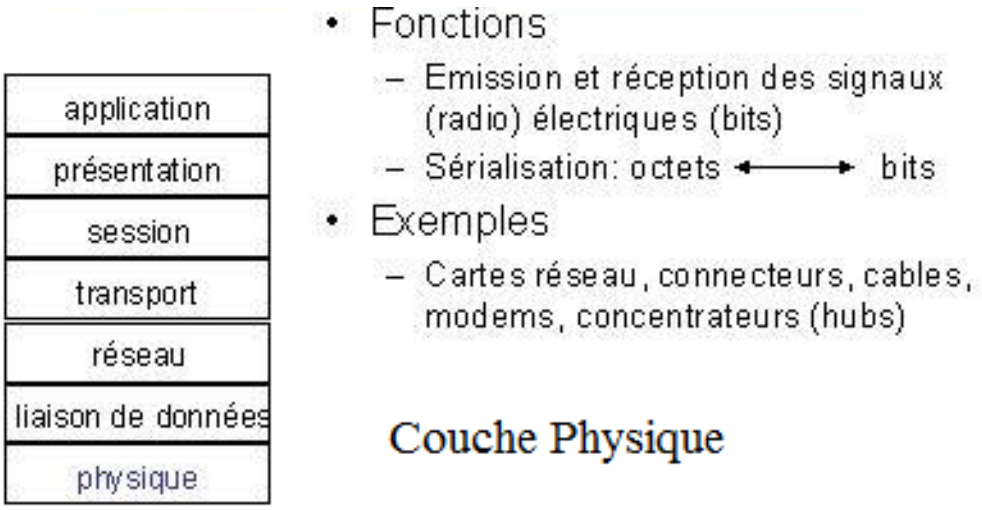



### 6.1.1. Couche physique

La fonction principale de la couche physique est de matérialiser l'interface entre l'ordinateur et le réseau pour pouvoir émettre et recevoir des signaux de communication. Ces signaux peuvent être de nature électrique, ectromagnétique (radio) ou optique. La définition de connecteurs, des câbles ou antennes font partie de cette couche. En général on considère que les cartes réseau, les modems et les concentrateurs (hubs) en font aussi partie.

Une autre fonction de cette couche est de sérialiser l'information, c-à-d transformer les octets en éléments binaires (bits) ou vice versa pour pouvoir émettre ou recevoir sur les canaux de communication. Cette transformation doit être effectué à un rythme qui est imposé par la vitesse (débit binaire) de l'interface.

Beaucoup d'autres fonctions peuvent être réalisées par cette couche; la détection de l'existence d'une communication en cours (Carrier Sense) ou d'une collision (Collision Detect) sur un réseau local Ethernet en sont deux exemples.




### a) Couche Liaison de données

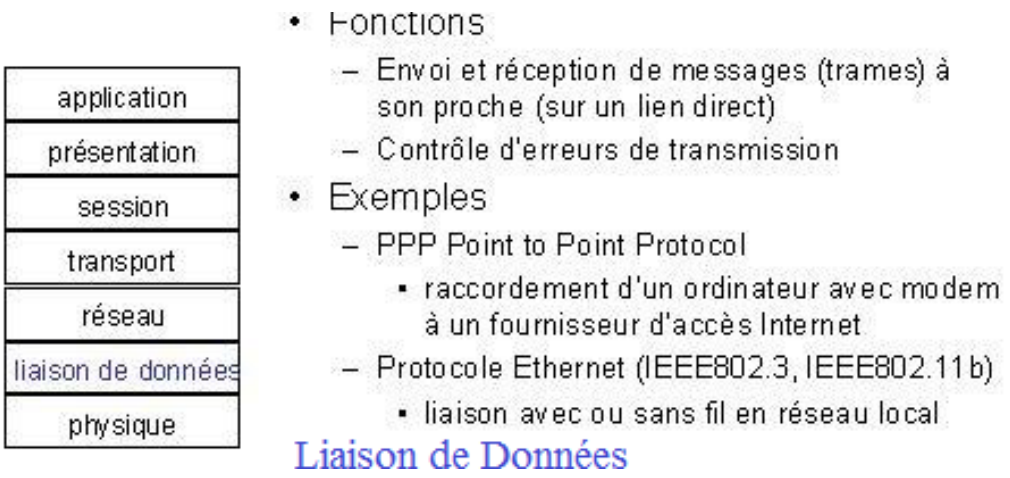
La fonction de la couche liaison de données est l'envoi et la réception de messages, souvent appelés trames à ce niveau, à son proche, c-à-d à un ordinateur qui se trouve sur un lien direct (sans faire appel des systèmes intermédiaires, les fameux routeurs). Ce lien direct peut être permanent comme dans le cas le plus simple des réseaux locaux où les ordinateurs sont tous raccordés au même câble (ou au même concentrateur, qui peut être vue comme une prise multiple de réseau!) ou bien peut avoir été créé au préalable, par exemple, par une commutation de circuit sur le réseau téléphonique en appelant un fournisseur d'accès à Internet. Dans ce dernier cas le lien direct est temporaire.

Cette couche peut aussi faire un contrôle d'erreurs de transmission, en utilisant, par exemple, dans le cas des trames Ethernet les derniers quatre octets de la trame appelés Frame Check Sequence (FCS).

Deux protocoles très utilisés à ce niveau sont:

Point to Point Protocol (PPP) pour la communication d'un ordinateur avec modem à un fournisseur d'accès Internet (en utilisant le réseau téléphonique)

IEEE802.3, IEEE802.11b (protocoles Ethernet) pour le raccordement en réseau local avec ou sans fils.




**i Couche Réseau**

La fonction de la couche réseau est d'acheminer les messages, souvent appelés soit paquets, soit datagrammes, de proche en proche jusqu'à destination en fonction de leur adresse. Cette fonction est appelé le routage; elle fait typiquement appel à des ordinateurs spécialisés, appelés routeurs, qui sont des systèmes intermédiaires sur la route qui va de la source à la destination.

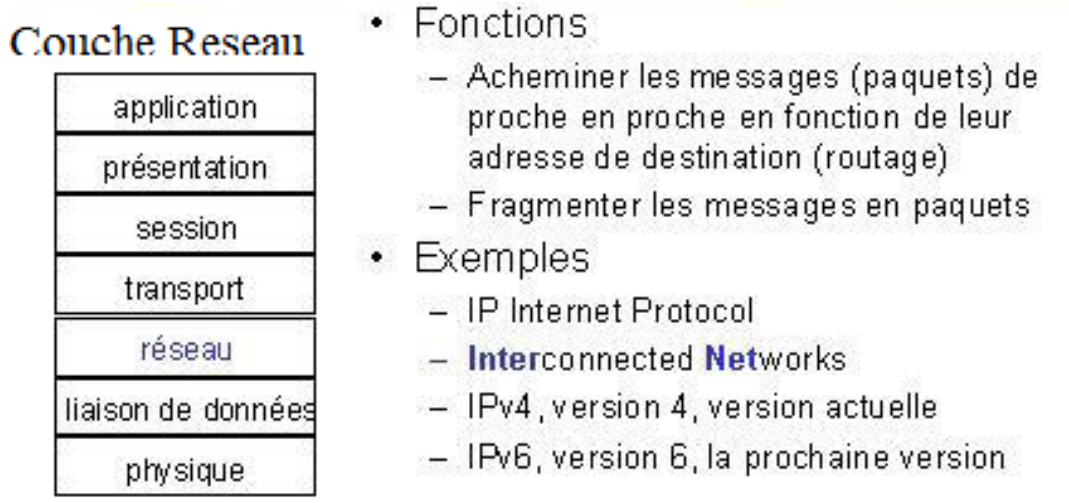
Question: Quel est le chemin, c-à-d la liste des systèmes intermédiaires, entre votre ordinateur et le serveur de l'universite de relizane www.univ-relizane.dz ?

Pour réaliser l'interconnexion de tous les réseaux d'ordinateurs à travers le monde entier il faut que ce protocole soit unique. Aujourd'hui il s'agit bien du protocole Internet IP (Internet Protocol). Ce protocole est dans sa version 4, caractérisée par des adresses sur 32 bits. L'évolution de l'Internet requiert le passage à la version 6 (la version 5 a été définie, mais n'a pas été adoptée), qui est caractérisée par des adresses beaucoup plus longues, représentées sur 128 bits.

Questions

1. Un espace d'adressage qui utilise des adresses représentées sur 32 bits permets de définir combien d'adresses différentes ?

2. Et si les adresses sont représentées sur 128 bits ?




**i Couche Transport**

Le rôle du service de transport est de transporter les messages de bout en bout, c-à-d de la source jusqu'à la destination, donc d'un bout à l'autre du réseau, sans se préoccuper du chemin à suivre car ce problème a déjà été traité par la couche inférieure de réseau.

Il y a plusieurs exemples de protocoles de transport. Dans le monde Internet les plus connus sont:

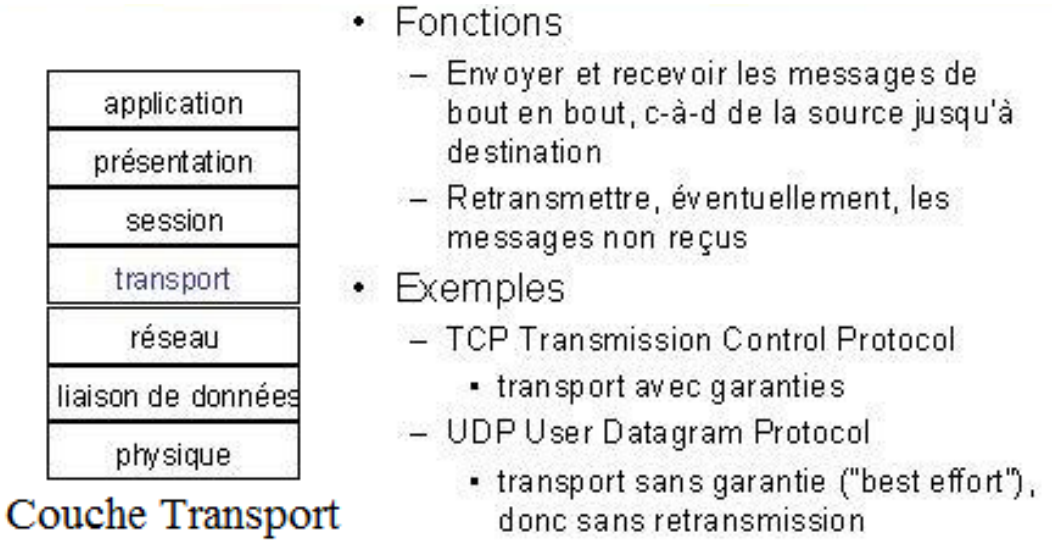
- TCP Transmission Control Protocol
- UDP User Datagram Protocol
- RTP Realtime Transport Protocol

Le choix dépend du type d'application et des services demandés.

Les applications de transfert de fichiers, de courrier électronique et de navigation sur le web requièrent des garanties de transmission sans erreurs et de retransmission en cas d'erreur. Dans le cas de messages longs, le fait de découper un message en paquets plus courts peut donner lieu à la remise des paquets à l'ordinateur de destination dans le désordre. Le protocole TCP s'occupe de résoudre ces problèmes, au prix d'une certaine complexité du protocole.

D'autres applications comme les requêtes aux annuaires éléctroniques ( pour obtenir la correspondance entre un nom d'ordinateur et son adresse) ou les applications de gestion de réseau préfèrent utiliser un protocole plus léger mais plus rapide car les messages sont typiquement très courts et en cas d'erreurs ou d'absence de réponse, ils peuvent être répétés sans problèmes. Le protocole UDP est typiquement utilisé dans ces cas.

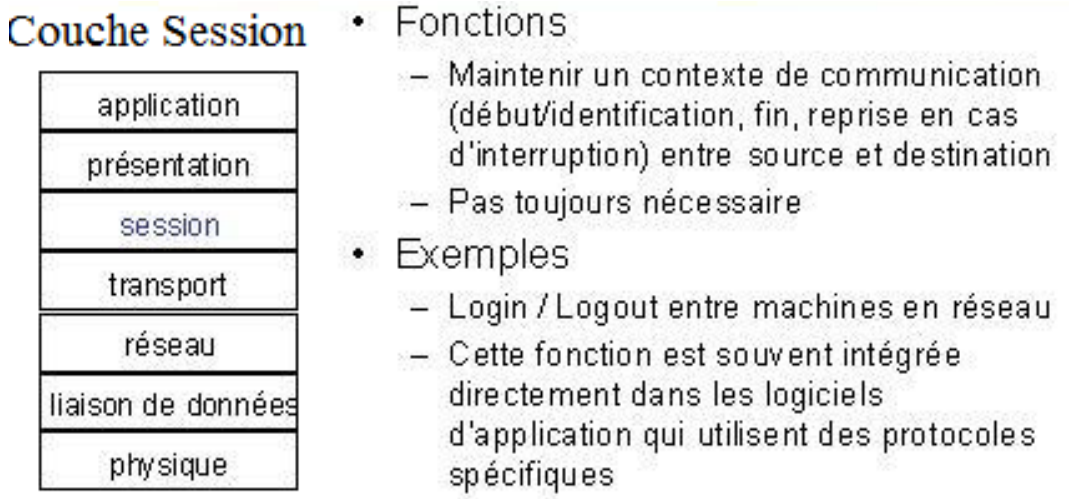
D'autres applications encore comme la téléphonie et la vidéoconférence sur Internet ont des contraintes de temps réel. La transmission de la voix et de la vidéo ne peuvent pas tolérer les variations de délais, appelées gigue, dans l'acheminement des paquets car les accélérations et ralentissements qui en résulteraient dans la restitution de la voix ou de l'images nuiraient gravement à la qualité de la transmission. Le protocole RTP, qui est utilisé en complément du protocole UDP, traite ces problèmes.




### i Couche Session

La fonction de la couche session est de négocier et de maintenir un contexte de communication entre la source et la destination. En début de communication il s'agit de définir le mode de communication (half duplex ou full duplex) et les règles de la communication. En cas de problème de communication, par exemple d'interruption momentanée, les services de points de reprise devraient permettre de reprendre la conversation là ou elle avait été interrompue.

En pratique ces fonctions sont souvent intégrées directement dans les logiciels d'application qui utilisent des protocoles spécifiques adaptés à chaque application particulière.




**i Couche Présentation**

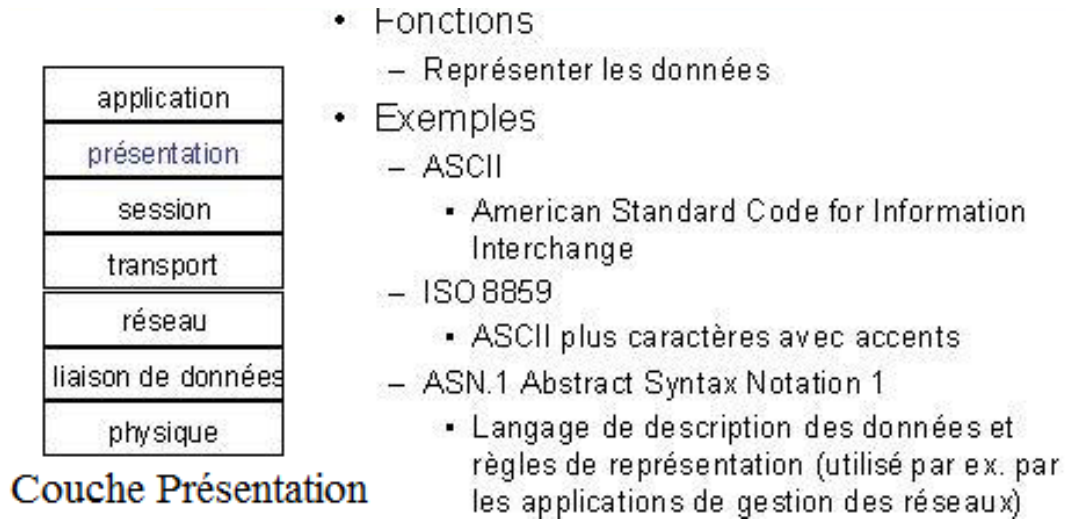
Le rôle de cette couche est d'aider les différentes applications à représenter les données de manière indépendante des plates-formes/systèmes d'exploitation (Macintosh/Mac OS, Intel/Windows, etc.).

Il existe plusieurs standards pour représenter les données (caractères, chiffres, booléens, mais aussi des données plus complexes construites à partir de données simples, comme les dates, les énumérations (par exemple, lundi, mardi, etc.), jusqu'aux données d'applications spécifiques comme une feuille de calcul, une présentation, un document incluant texte, tables et images).

Certaines applications se limitent à l'utilisation du standard ASCII pour représenter les caractères sans accents. D'autres applications peuvent utiliser le standard international ISO 8859 pour pouvoir représenter les caractères avec accents.

D'autres applications encore peuvent utiliser un véritable langage de description de données (simples et complexes) avec des règles de représentation des données pour le transfert entre applications en réseau. Le standard ISO ASN.1 est un exemple utilisé dans le cadre des application de gestion de réseau.

La couche de présentation pourrait aussi fournir des services de cryptage de l'information.Mais encore une fois cette couche est souvent intégrée directement dans les logiciels d'application.



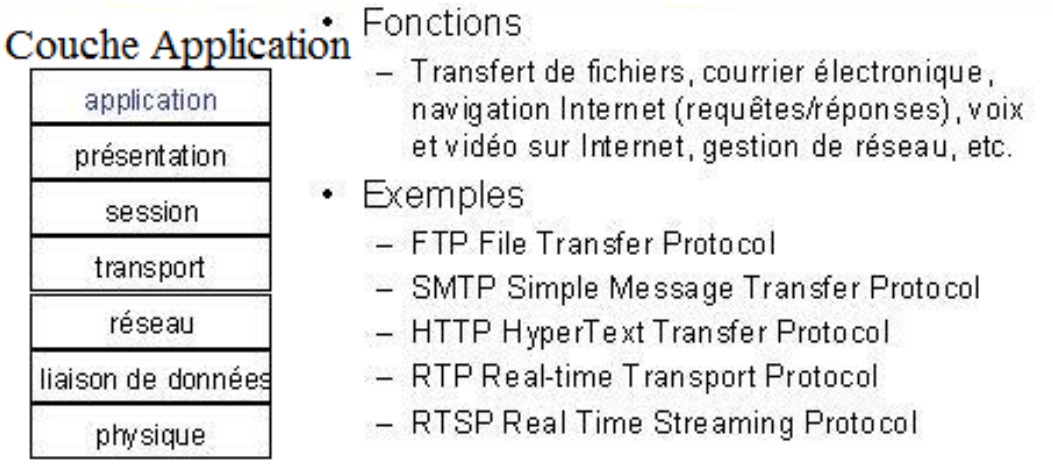

**i Couche Application**

Le rôle de la couche application est de fournir les services et les protocoles nécessaires aux applications qui souhaitent s'ouvrir sur le réseau. Il faut noter que les applications elles mêmes ne font pas partie de la couche application.

Les exemples de protocoles que nous pouvons classer dans cette couche sont très nombreux car les applications sont nombreuses et ne cessent de se développer.

Les protocoles les plus connus sont HTTP, FTP et SMTP pour naviguer sur le web, transférer des fichiers ou envoyer des messages électroniques.

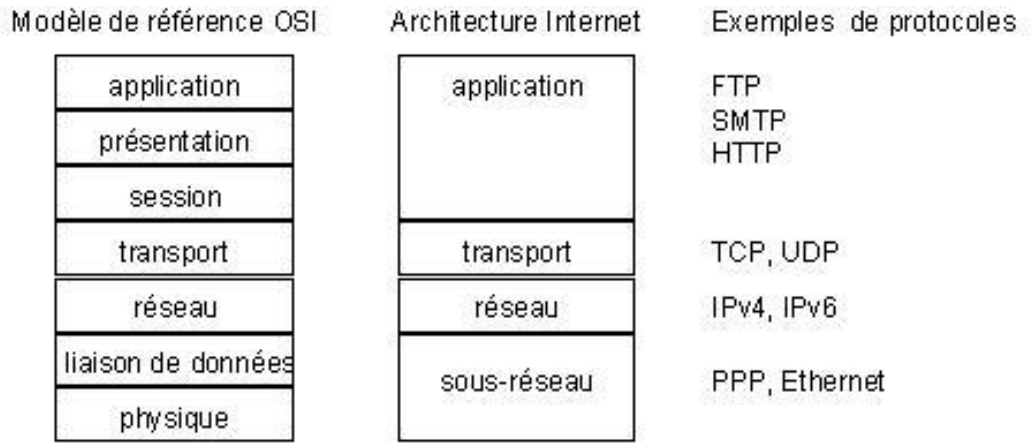
Le protocole RTP (Realtime Transport Protocol) dont nous avions parlé à-propos de la couche transport peut aussi être classé dans la couche application (voir architecture Internet).




## 6.2. Le modele TCP/IP

Utilisé dans le réseau ARPANET du ministère de la défense des états unis, un réseau de recherche devenu actuellement Internet. Le grand souci du DoD était de garantir la fiabilité du réseau en cas de panne d'un élément du sou réseau et fonctionner tant que les ordinatrices sources et destination fonctionnent. En outre, cette architecture permet de résoudre les problèmes d'interconnexion en milieu hétérogène. À cet effet, TCP/IP décrit un réseau logique (réseau IP) au-dessus du ou des réseaux physiques réels, auxquels sont effectivement connectés les ordinateurs.

Précédant le modèle OSI, TCP en diffère fortement. La figure suivante présente les couches de deux modèles. Ainsi, le modèle TCP/IP est constitué de deux protocoles essentiels TCP et IP et de quatre couches:




les deux modèles OSI & TCP/IP

### 6.2.1. Couche Matérielle (hostto Network)

La couche qui intègre les réseaux physiques LAN et MAN (Ethernet, physiques et liaison du modèle OSI. Ce modèle ne spécifie pas de détails sur cette couche sauf la manière d'encapsuler

**a) Couche Internet ou Réseau**

La couche permettant d'interconnecter plusieurs réseaux physiques différents, elle paquet et un protocole IP (Internet Protocol), son fonctionnement ressemble à la couche réseau du modèle

**i Couche Transport (host to host)**

c'est la couche qui fournit les services de transport fiables orientés connexion Protocol) ou non-fiables sans connexion qui est UDP (User Datagram Protocol) à travers le réseau internet,

**i Couche Application**

intégrant différents services applicatifs. Au plus haut niveau les utilisateurs permettent l'accès au réseau. Chaque programme d'application interagit avec la couche de transport pour En fonction des caractéristiques de l'échange, le programme a choisi un mode de transmission à la couche

<table>
<tr><td>Application</td><td rowspan="3">Application</td></tr>
<tr><td>Présentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport (Host to Host)</td></tr>
<tr><td>Réseau</td><td>Réseau (Internet)</td></tr>
<tr><td>Liaison de données</td><td rowspan="2">Matérielle (Host to Internet)</td></tr>
<tr><td>Physique</td></tr>
</table>

les Couches des Deux Modèles

## 6.3. Architectures Propriétaires

Les réseau d'ordinateurs se sont développés à partir des années 1970s. Pendant vingt ans les architectures constructeur ont dominé le paysage des réseaux. Les plus importantes de ces architectures sont:

1. SNA Systems Network Architecture de IBM

2. DSA Distributed Systems Architecture de Bull

3. DNA/DECNET DEC (Digital Equipment Corporation) Network Architecture

Dans le domaine des réseaux locaux d'entreprise l'architecture de Novell a dominé pendant une dizaine d'années.

Avec l'arrivée d'Internet en début des années 1990s (bien que sa conception remonte à l'année 1969 dans les laboratoires des universités américaines) toutes les architectures se sont ouvertes sur Internet soit en intégrant ses protocoles, soit en créant au moins des passerelles qui permettent aux données de passer d'un réseau qui utilise une architecture propriétaire aux réseaux qui utilisent l'architecture Internet.

## 6.4. Réseaux Locaux et Couche Liaison de données

pour comprendre les mécanismes de gestion d'accès au canal Allocations statique, déterministe, aléatoire on doit connaître le fonctionnement d'Ethernet classique et ses supports et les grands principes du Wifi on se basant sur les Liaisons louées, commutation de paquet, réseaux locaux CSMA/CD et Ethernet Format, protocole, supports CSMA/CA et Wifi .

Dans les Réseaux locaux LAN (Local Area Network) :

-Nombre de machines et couverture limitée .

-Débit très important (jusqu'à la dizaine de Gigabits/s).

-Possibilité d'utiliser la diffusion => support partagé.

-Normes gérées par le groupe IEEE 802 (février 1980) (Institute of Electrical and Electronic Engineers).

par exemple 802.3 Ethernet, 802.4 Token Bus, 802.5 Token Ring,802.11 Wifi

-Différentes topologies (bus, étoile, anneau, arbre...).

-Différents moyens de gérer la répartition du temps de parole interrogation, jeton, accès aléatoire.

-Différents formats de trame.

### 6.4.1. Méthode d'accès

Méthode statique :Chaque station utilise pour toute une session une partie allouée des ressources.

● TDMA (Time Division Multiple Access) ➢ Chacun a droit à un laps de temps

(temps de transmission, bande de fréquence...) Exemple: téléphone fixe, GSM.

● FDMA (Frequency Division Multiple Access) ➢ Chacun a droit à une bande de fréquence qui lui est propre.

●CDMA (Code Division Multiple Access) Chaque signal est soumis à un code => étalement de spectre.

Remarque : Accès statiques mal adaptés à l'arrivée/départ de stations Sousoptimisation si les stations n'ont pas un débit uniforme.

Méthode déterministe :Une station (contrôleur) est chargée d'attribuer dynamiquement des ressources (contrôleur centralisé ou distribué) Exemple: Bluetooth, Token Ring, GPRS.

● Allocation dynamique permettant de garantir un temps d'accès chaque station

Une certaine équité (comme méthodes statiques) mais qui prend en compte le fait que certaines stations peuvent n'avoir rien à dire.

● Contrôle centralisé par interrogation (polling) Un superviseur scrute toutes les stations et les invite à transmettre chacune à leur tour en fonction de leurs besoins.

● Contrôle décentralisé par passage de jeton (token passing) Un jeton (droit d'accès) circule de station en station Une station qui souhaite émettre retient le jeton le temps d'émettre sa trame, puis le libère.

● Nécessite un contrôle, et implique donc plus d'administration

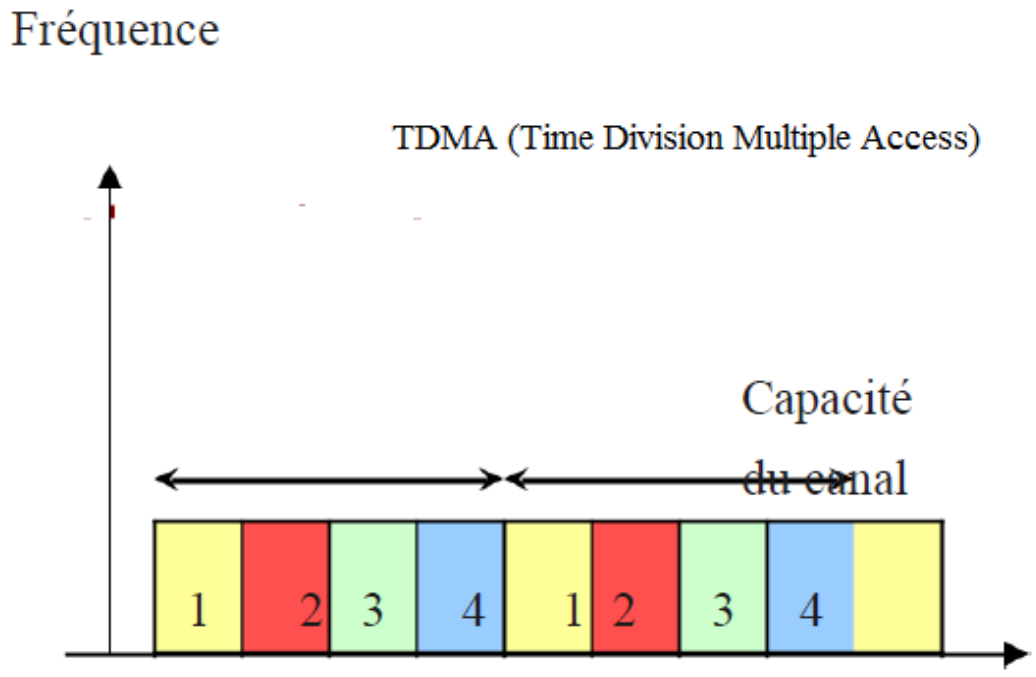
Méthode aléatoire :Toutes les stations tentent d'accéder simultanément au support et risquent de provoquer des collisions Exemple: Ethernet, WiFi.

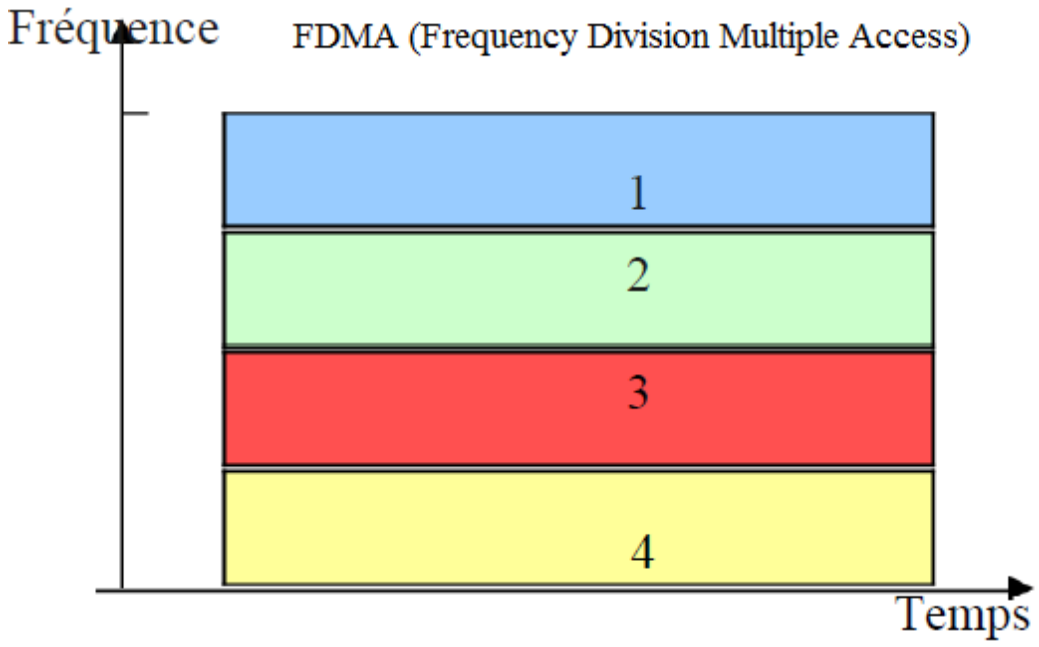
● Pas d'administration centralisée; « plug and play »chacun essaye d'émettre, avec le risque de provoquer des collisions (plusieurs trames se superposent)

● CSMA (Carrier Sense Multiple Access) L'écoute du canal (Carrier Sense) permet de n'émettre que si le canal est libre.

● CSMA/CD (Collision Detection) – Ex: Ethernet La détection d'une collision indique aux émetteurs qu'il faut attendre (un temps aléatoire) avant d'essayer de réémettre

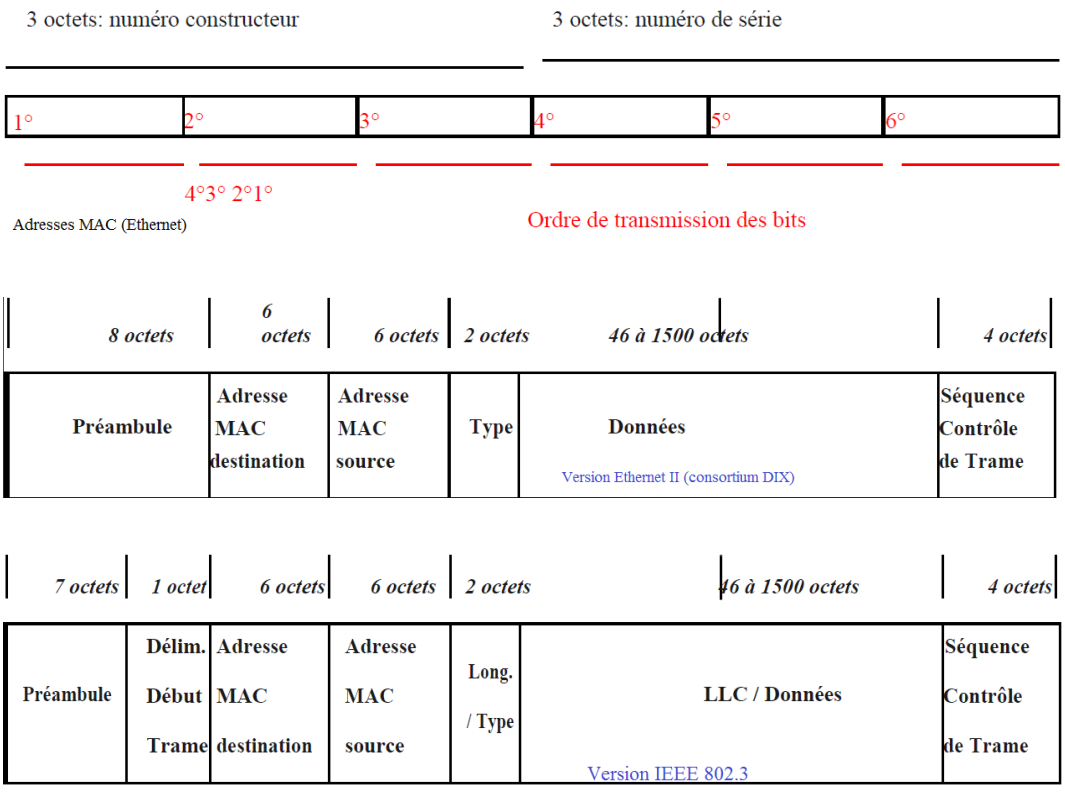
● CSMA/CA (Collision Avoidance) – Ex: WiFi Adapté au sansfil où on ne peut pas émettre/recevoir en même temps: tente d'éviter les collisions.






**a) L'accès au Réseau**

*Le format d'une trame Ethernet ;*




- Tous les LAN sont orientés et sans connexion
- Carte d'interface réseau (NIC)
- Identification d'une machine sur le support

● Adresse physique (MAC) pour tous les protocoles

● Permet d'émettre et de recevoir des trames

● format dépendant du protocole

● nous allons nous intéresser à Ethernet et/ou IEEE 802.3

● Intermédiaire pour l'adressage logique

● de type IP par les mécanismes ARP ou DHCP

Le cas Ethernet

➢ Invention en 1973 à Xerox PARC

➢ (B. Metcalfe & D. Boggs), 3 Mégabits/sec, câble coaxial

➢ Consortium DIX (DEC Intel Xerox) créé en 1979

➢ Ethernet II et IEEE 802.3 convergent en 1982

➢ 10 mégabits par seconde

➢ support coaxial, paire torsadée ou fibre optique

➢ principe d'accès CSMA/CD

➢ Carrier Sense Multiple Access with Collision Detection

➢ écoute et, si canal silencieux, tentative d'émission en écoutant. En cas de collision,

les deux émetteurs réorganisent les transmissions ultérieurement

➢ évolue en débit, principe et fonctionnalités (Full duplex,

Commutation, 10 Gigabits/s...)

Adresses MAC

➢ Identifie chaque carte d'interface sur un réseau local

➢ Nécessairement unique (pour un réseau donné)

➢ Partie dépendante du constructeur juxtaposée à numéro de série

➢ Adressage standardisé IEEE 802

➢ CSMA/CD, Token Bus, Token Ring, DQDB

➢ Également pour FDDI et ATM

➢ Longueur 6 octets, représentés en hexadécimal

➢ Classiquement sous l'une des formes

➢ 00:0B:DB:16:E7:8A ou 00-0B-DB-16-E7-8A

Adresses MAC (Ethernet)

➢ Les 6 octets sont transmis dans l'ordre, avec le bit de poids faible en premier

(LSB, Least Significant Bit first)

Les 24 premiers bits constituent l'OUI Organizationaly( Unique Identifier).

Ex: 00:00:0C (Cisco) 00:C0:4F (DELL)

Les 24 bits restant sont des numéros de série.

Préambule

Sert à synchroniser l'horloge du récepteur avec le signal entrant: 01010101 ...(x 7 octets)... 01010111

➢ Fréquence de 5 Mhz passant à la fin à 10 Mhz

➢ Fréquence codage Manchester double de fréquence NRZ.

Champ Type ou Longueur

➢ Champ Type d'Ethernet II (16 bits = 2 octets)

➢ Indique le protocole de plus haut niveau transporté

➢ 0x0800 trame IP, 0x0805 X.25, 0X0806 ARP...

➢ Champ Longueur/Type de IEEE 802.3 (16 bits)

➢ Indique le nombre d'octets dans le champ de données

RESEAUX MOBILES Partie I Réseaux et mécanismes de base

➢ Éventuellement moins de 46 octets (caractères de bourrage)

➢ Si £ 1518, c'est la taille des données en octets

➢ Si $^{3}$ 1536 (0x600), c'est utilisé comme le type des données

➢ Ethernet II est compatible avec 802.3

Zone de données

➢ Ethernet (DIX)

➢ 46 octets <= données dans une trame <= 1500 octets

➢ Cela incombe au logiciel de réseau, quitte à ajouter du bourrage

➢ IEEE 802.3

➢ 0 octets <= données dans une trame <= 1500 octets

➢ Nombre spécifié dans le champ longueur + bourrage éventuel

➢ Si longueur utilisée, on peut décrire un type LLC

➢ Il est fourni par le protocole de la couche LLC (802.2)

➢ Permet de faire du démultiplexage (DSAP/SSAP)

➢ Toute trame émise doit faire au moins 64 octets (CSMA/CD)

CSMA/CD et taille minimum de trame

➢ Le support est écouté en permanence

➢ Après 96 temps bits de silence (IFG, Inter Frame Gap), début d'émission

➢ Si collision détectée (tension moyenne double), émission d'une séquence de brouillage (jam), puis ➢ Le repli est d'une durée pseudo aléatoire multiple de 512 temps bits avec comme objectif de « désynchroniser ➢ Cette valeur est appelée le délai d'insertion ou encore slot time (temps d'aquisition du canal)

➢ En effet, une fois ce temps écoulé, toutes les machines sur le réseau savent qu'une émission a lieu actuellement

➢ L'émetteur ne peut normalement plus être interrompu

Champ de contrôle

➢ FCS (Frame Contrôle Sequence)

➢ 4 octets (32 bits) pour le Cyclic Redundancy Code

➢ CRC calculé sur les champs dest, src, type/lgr et données

➢ Calculé/inséré à l'émission et calculé/vérifié à la réception

➢ Détection de fin de trame

➢ Après toutes ces valeurs, silence sur la trame

➢ Possibilité de bits de « bavure » (bits aditionnels post FCS)

➢ Le récepteur tronque à l'octet complet le plus proche

➢ Si jamais une erreur est détectée par le récepteur en Ethernet

➢ La trame est jetée, c'est tout! Pas de demande de retransmission à ce niveau

### b) Quelques Mots sur le WIFI ;

➢ En fait un cas particulier de WLAN (Wireless LAN)

➢ Nom « commercial » pour IEEE 802.11 et ses variantes

➢ 802.11b, 802.11a, 802.11g, 802.11n...

➢ D'autres existent Bluetooh, Zigbee, WiMax...

➢ Assez semblable à Ethernet 802.3

➢ Dans les usages: interconnexion au niveau LAN

➢ Dans le format: trames avec @MAC source et destination

➢ Dans l'accès au canal: CSMA oui, mais CA et non CD...

➢ Des différences notables quand même

➢ Transmissions radioélectriques (avantages/inconvénients)

➢ Mobilité, déploiement / contraintes transmissions

### c) IEEE 802.1: modes de fonctionnement

- Mode Ad Hoc : Independant Basic Service Set (IBSS)
- Mode Infrastructure : - Utilise un ou des Acces Point (AP).
  Basic Service Set (BSS) ; 1 seul AP (Set top box).
  Extended Service Set (ESS): plusieurs AP.
  Passer de l'un à l'autre ; Roaming

#### i Transmission sans fil : couche physique

➢ Antenne radio : onde radioélectrique modulée

Différentes bandes de fréquences

➢ 802.11, 802.11b, 802.11g dans la bande 2,4 GHz

➢ 802.11a et 802.11n dans la bande 5GHz

Différentes techniques de modulation

➢FHSS (Frequency Hopping Spread Spectrum) pour 802.11

Idée: utiliser toutes les fréquences en sautant de l'une à l'autre dans un ordre pseudoaléatoire partagés entre 2 stations

➢ DSSS (Direct Sequence Spread Spectrum) pour 802.11b

➢ Idée: découper le spectre en « canaux » dont certains ne se supperposant pas peuvent être utilisés simultanément

➢ OFDM (Orthogonal Frequency Division Multiplexing) 802.11a et 802.11g; le 802.11n MIMO utilise OFDM et multiples antennes.

**i WLAN: couche liaison de données**

➢ Impossible de recevoir en même temps qu'on émet

➢ Pas de full duplex possible

➢ Pas de détection de collision possible

➢ La « portée » des ondes est limitée

➢ On tente d'éviter les collisions

➢ CSMA/CA (Carrier Sense Multiple Access Collision Avoidance)

➢ On impose un acquittement

➢ Si l'acquittemement n'est pas reçu, on doit réémettre

**i Gestion de l'accès au canal en 802.11**

➢ Deux modes de fonctionnement de la couche MAC 802.11 qui peuvent cohabiter .

➢ DCF (Distributed Coordinated Function)

➢ Pas d'entité de contrôle centralisé, de type Best Effort

➢ Le CSMA/CA (Collision Avoidance) est appliqué

➢ PCF (Point Coordinated Function)

➢ Le point d'accès gère toute l'activité de la cellule

➢ L'AP diffuse une trame de signalisation (beacon frame) contenant différents paramètres systèmes, fréquences

➢ Les stations « s'enregistrent » auprès de l'AP

➢ S'apparente à du « polling » (interrogation ou invitation à émettre)CSMA/CA (Collision Avoidance)

➢ Si une station A veut émettre vers B, elle écoute le support

➢ Si une transmission est en cours, l'émission de A est différée

➢ Si le support est libre pendant un temps DIFS (DCF InterFrame Spacing), alors A émet en amorçant un temporisateur d'acquittement

➢ B vérifie le CRC de la trame reçue et envoit un ACK à A

➢ Si A reçoit le ACK à temps, l'émission est terminée

➢ Sinon, A doit retransmettre

➢ Si le support n'est pas libre au dela du temps DIFS, alors A attend un temps calibré dit NAV (Network Allocation Vector)

➢ Après attente du NAV, les stations en compétition pour émettre attendent un temps aléatoire de type « Backoff exponentiel »

➢ Objectif: éviter les collision (Collision Avoidance)

# Partie II

IV

# 1. Réseaux sans Fil

## 1.1. Qu'est-ce qu'un réseau sans fil ?

Un réseau sans fil (en anglais wireless network) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de "mobilité".

Les réseaux sans fil sont basés sur une liaison utilisant des ondes radio-électriques (radio et infrarouges) en lieu et place des câbles habituels. Il existe plusieurs technologies se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions. Les réseaux sans fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires (creusement de tranchées pour acheminer les câbles, équipements des bâtiments en câblage, goulottes et connecteurs), ce qui a valu un développement rapide de ce type de technologies. En contrepartie se pose le problème de la réglementation relative aux transmissions radio- électriques. En effet, les transmissions radio-électriques servent pour un grand nombre d'applications (militaires, scientifiques, amateurs, ...), mais sont sensibles aux interférences, c'est la raison pour laquelle une réglementation est nécessaire dans chaque pays afin de définir les plages de fréquence et les puissances auxquelles il est possible d'émettre pour chaque catégorie d'utilisation. De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour un pirate d'écouter le réseau si les informations circulent en clair (c'est le cas par défaut). Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil.

## 1.2. Techniques de transmission dans les réseaux sans fil

il existe principalement deux méthodes pour la transmission dans les réseaux sans fil:

### 1.2.1. Transmission par les ondes infrarouges

la transmission par les ondes infrarouges nécessite que les appareils soient en face l'un des autres et aucun obstacle ne sépare l'émetteur du récepteur.(car la transmission est directionnelle).cette technique est utilisée pour créer des petits réseaux de quelques dizaines de mètres. (télécommande de : télévision, les jouets, voitures...).

### 1.2.2. Transmission par les ondes radios

La transmission par les ondes radios est utilisée pour la création des réseaux sans fil qui ont plusieurs kilos mètres. Les ondes radios ont l'avantages de ne pas êtres arrêtés par les obstacles car elles sont émises d'une manière omnidirectionnelle. Le problème de cette technique est les perturbations extérieures qui peuvent affecter la communication à cause de l'utilisation de la même fréquence .

## 1.3. Les avantages et les inconvénients des réseaux sans fil

### 1.3.1. Avantages

**a) Pour les utilisateurs :**

- Premièrement, la portabilité : un ordinateur portable ou un ordinateur de poche suffit pour se connecter.
- Deuxièmement, le choix du lieu de connexion, sous contrainte d'être toujours sous la couverture du réseau.
- Troisièmement, la flexibilité : la connexion est indépendante de la marque ou des caractéristiques techniques des appareils connectés. Seules les cartes réseaux doivent garantir une compatibilité avec la norme à laquelle elles font référence.
- Quatrièmement, la facilité : pas de câble signifie moins d'encombrement. Les appareils sur le marché tendent à se connecter automatiquement.
- Cinquièmement, la mobilité : les utilisateurs peuvent se déplacer sans couper la connexion au réseau.
- Sixièmement, les prix : ils tendent à baisser suivant l'évolution du marché. Il est difficile d'acheter un ordinateur portable sans carte réseau sans fil intégrée.

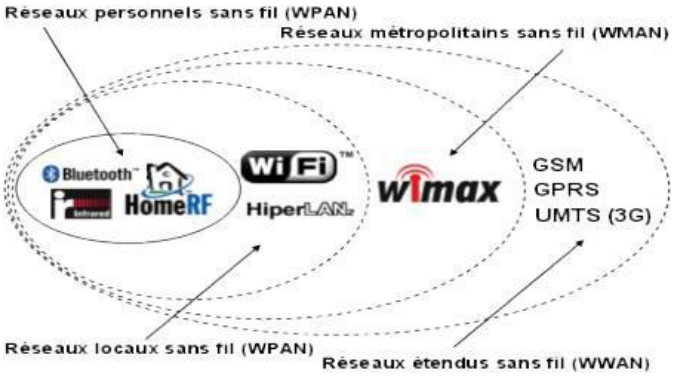
**i Pour les responsables du déploiement du réseau sans fil :**

- D'abord, moins de câble à déployer, et donc une diminution de l'investissement en câble ainsi que la charge de travail lors de l'installation.
- Ensuite, facilité et souplesse de déploiement : une machine supplémentaire peut se connecter sans pour autant réserver un espace tel qu'une prise RJ45. Qu'il y ait 10 ou 15 machines utilisateurs, la différence n'est pas aussi critique qu'avec un réseau filaire, en termes d'espace de connexion (et pas en terme d'analyse réseau).
- Enfin, le prix : Une solution sans fil peut être largement moins chère pour une entreprise. Toutefois, une sérieuse analyse est nécessaire en tenant compte des particularités des utilisateurs de l'entreprise.

### 1.3.2. Inconvénients

- Le premier consiste à disposer d'un débit souvent plus faible qu'un réseau câblé.
- Le deuxième consiste, selon les cas, en une atténuation rapide du signal en fonction de la distance qui induit l'impossibilité pour un émetteur de détecter une collision au moment même. En effet, le medium utilisé est dit half-duplex, ce qui correspond à un medium sur lequel l'émission et la réception sont impossibles en même temps.
- Le troisième réside dans l'inévitabilité des interférences. Les transmissions radios ne sont pas isolées, et le nombre de canaux disponibles est limité, ce qui force le partage. Les interférences peuvent être de natures diverses à savoir des émetteurs travaillant à des fréquences trop proches ; des bruits parasites dus à l'environnement; des phénomènes d'atténuation, de réflexion et de chemins multiples dus à l'environnement...
- Le quatrième les limitations de la puissance du signal par des règlementations strictes en vigueur.
- Le cinquième la limitation de l'énergie par l'autonomie de batteries. En effet, les applications relatives aux réseaux sans fil ont un caractère nomade portable. Emettre ou recevoir des données consomme de l'énergie.
- L'avant dernier problème la faible sécurité : il est facile ”d'espionner” passivement un canal radio.
- Enfin, le dernier les changements provoqués par la mobilité des noeuds sur la topologie du réseau.

## 1.4. Les catégories des réseaux sans fil




On distingue habituellement plusieurs catégories de réseaux sans fil, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) :

### 1.4.1. Réseaux personnels sans fil (WPAN)

Le réseau personnel sans fil (appelé également réseau individuel sans fil ou réseau domestique sans fil et noté WPAN pour Wireless Personal Area Network) concerne les réseaux sans fil d'une faible portée (de l'ordre de quelques dizaines de mètres). Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, appareils domestiques, ...) ou un assistant personnel *(PDA) à un ordinateur sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. il existe plusieurs technologies utilisées pour les WPAN :

#### a) HomeRF

HomeRF (pour Home Radio Frequency), lancée en 1998 par le HomeRF Working Group (formé notamment par les constructeurs Compaq, HP, Intel, Siemens, Motorola et Microsoft) propose un débit théorique de 10 Mbps avec une portée d'environ 50 à 100 mètres sans amplificateur. La norme HomeRF soutenue notamment par Intel, a été abandonnée en Janvier 2003, notamment car les fondateurs de processeurs misent désormais sur les technologies Wi-Fi embarquée (via la technologie Centrino, embarquant au sein d'un même composant un microprocesseur et un adaptateur Wi-Fi).

#### i ZigBee

La technologie ZigBee (aussi connue sous le nom IEEE 802.15.4) permet d'obtenir des liaisons sans fil à très bas prix et avec une très faible consommation d'énergie, ce qui la rend particulièrement adaptée pour être directement intégrée dans de petits appareils électroniques (appareils électroménagers, hifi, jouets, ...). La technologie Zigbee, opérant sur la bande de fréquences des 2,4GHz et sur 16 canaux, permet d'obtenir des débits pouvant atteindre 250 Kb/s avec une portée maximale de 100 mètres environ.

#### ii Liaisons Infra rouge

les liaisons infrarouges permettent de créer des liaisons sans fil de quelques mètres avec des débits pouvant monter à quelques mégabits par seconde. Cette technologie est largement utilisée pour la domestique (télécommandes) mais souffre toutefois des perturbations dues aux interférences lumineuses. L'association

irDA (infrared data association) formée en 1995 regroupe plus de 150 membres. 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).

### 1.4.2. Réseaux locaux sans fil (WLAN)

Le réseau local sans fil (noté WLAN pour Wireless Local Area Network) est un réseau permettant de couvrir l'équivalent d'un réseau local d'entreprise, soit une portée d'environ une centaine de mètres. Il permet de relier entre-eux les terminaux présents dans la zone de couverture. Il existe plusieurs technologies concurrentes :

#### a) Le WIFI

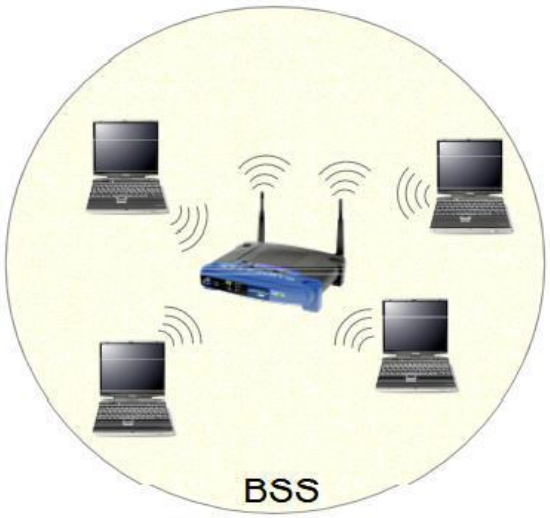
Le Wifi (ou IEEE 802.11), soutenu par l'alliance WECA (Wireless Ethernet Compatibility Alliance) offre des débits allant jusqu'à 54Mbps sur une distance de plusieurs centaines de mètres.

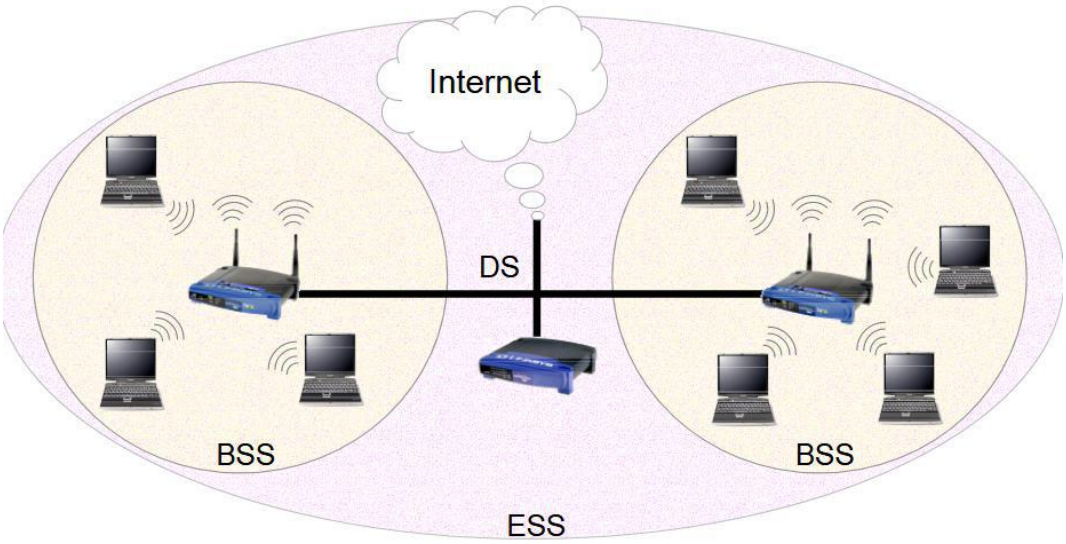
##### i Le mode infrastructure

Le mode infrastructure désigne un réseau composé d'une infrastructure permettant l'échange d'information entre les stations ; l'infrastructure est le point d'accès

Carte réseau wifi via un ou plusieurs points d'accès

Un seul point d'accès = réseau BSS (Basic Service Set) point d'accès simple qui fait lien entre le réseau filaire et le réseau sans fil






**ii Le mode Ad-hoc**

Connecter directement les ordinateurs équipés de carte réseau

**b) HIperLAN2**

hiperLAN2 (HIgh PERformance Radio LAN 2.0), norme européenne élaborée par l'ETSI (European Telecommunications Standards Institute). HiperLAN 2 permet d'obtenir un débit théorique de 54 Mbps sur une zone d'une centaine de mètres dans la gamme de fréquence comprise entre 5 150 et 5 300 Mhz.

### 1.4.3. Réseaux métropolitains sans fil (WMAN)

Le réseau métropolitain sans fil (WMAN pour Wireless Metropolitan Area Network) est connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication.Les principales technologies sont les suivantes :

- WMAX

### 1.4.4. Réseaux étendus sans fil (WWAN)

Le réseau étendu sans fil (WWAN pour Wireless Wide Area Network) est également connu sous le nom de réseau cellulaire mobile. Il s'agit des réseaux sans fil les plus répandus puisque tous les téléphones mobiles sont connectés à un réseau étendu sans fil. Les principales technologies sont les suivantes :

• GSM (Global System for Mobile Communication ou en français Groupe Spécial Mobile),

• GPRS (General Packet Radio Service),

• UMTS (Universal Mobile Telecommunication System).

## 1.5. Introduction au 802.11

L'IEEE (Institute of Electrical and Electronics Engineers) a normalisé plusieurs catégories de réseaux locaux

- Ethernet (IEEE 802.3)
- Token Bus (IEEE 802.4)
- Token Ring (IEEE 802.5)

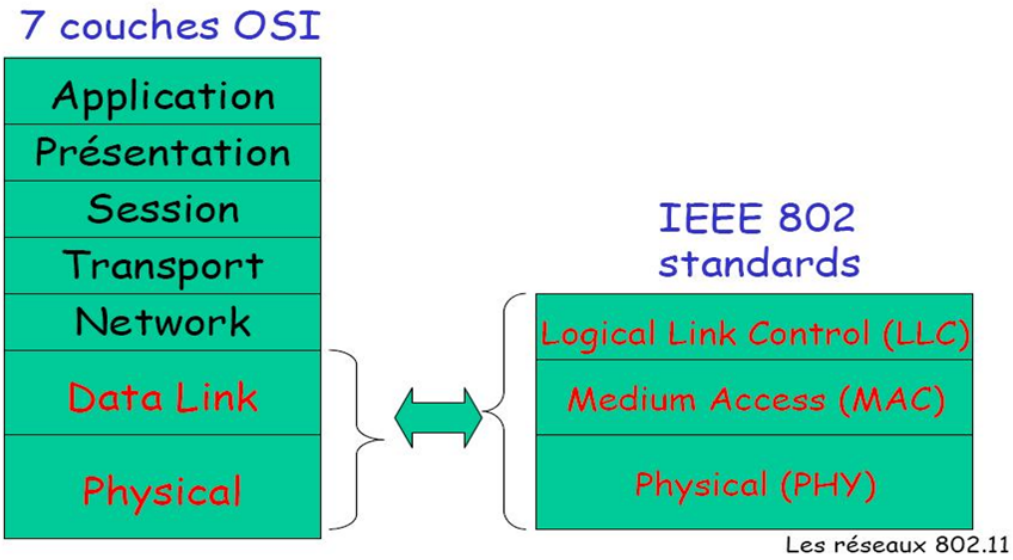
1990 : lancement du projet de création d'un réseau local sans fil ou WLAN (Wireless Local Area Network)

But : offrir une connectivité sans fil à des stations fixes ou mobiles qui demandent un déploiement rapide au sein d'une zone locale en utilisant différentes bandes de fréquences

1997 : le premier standard international pour les réseaux locaux sans fil, l'IEEE 802.11, est publié

Le groupe de travail 802.11 concentre actuellement ses efforts pour produire des standards pour des WLAN à grande vitesse

- 802.11x – Amendements
- 802.11b - Vitesse de 11 Mbits/s (bande ISM)
- 802.11a - Vitesse de 54 Mbits/s (bande UN-II)
- 802.11g - Vitesse de 54 Mbits/s (bande ISM)
- 802.11e - Qualité de service
- 802.11i - Amélioration de la sécurité
- 802.11f - Roaming



Les réseaux 802.11

## 1.6. Le Standard 802.11

Le standard d'origine définit :

La sous-couche MAC

3 couches physiques (PHY) :

- IR (Infrarouge)
- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)

Remarques :

FHSS et DSSS utilisent la bande des 2,4/2,483 Ghz de l'ISM (Industrial, Scientific and Medical): Utilisation libre dans de nombreux pays

Ajout de 2 couches physiques (amendements)

But :

- Connectivité sans fil à des stations fixes/mobiles
- Déploiement rapide
- Utilisation de différentes bandes de fréquences
  802.11b (WiFi) → 2.4-5 GHz (sans license) → Jusqu'à 11 Mb/s
  DSSS → Largement déployé
- 802.11a → 5-6 GHz → Jusqu'à 54 Mb/s
  802.11g→ 2.4-5 GHz → Jusqu'à 54 Mb/s

*Remarque*

Rappel sur les lois de la Radio

Débit plus grand = Couverture plus faible

Puissance d'émission élevée = Couverture plus grande, mais durée de vie des batteries plus faible

Fréquences radio élevées = Meilleur débit, couverture plus faible

## 1.7. Couche Physique dans Les Réseaux Sans Fil

### 1.7.1. Bandes de fréquence dans 802.11x

Pour 802.11, Wi-Fi (802.11b) et 802.11g

- Bande sans licence ISM (Instrumentation, Scientific, Medical) dans les 2,4 GHz
- Largeur de bande : 83 MHz
- Basé sur le DSSS: étalement de spectre à séquence directe
- Mécanisme de variation de débit selon la qualité de l'environnement radio

Pour Wi-Fi5 (802.11a)

- Bande sans licence UN-II dans les 5,2 GHz
- Unlicensed National Information Infrastructure : pas besoin de licence d'utilisation
- Largeur de bande : 300 MHz

| Technologie | Principaux avantages | Principales limitations | Applications |
|---|---|---|---|
| FHSS | - Technologie simple et économique<br>Permet de "contourner" les interférences (possibilité de modifier la séquence des sauts en fonction des obstacles rencontrés)<br>- Portée relativement élevée<br>- Technologie avantageuse en termes de sécurité et de fiabilité<br>- Consommation d'énergie relativement faible | - Efficacité spectrale peu élevée<br>Débits relativement faibles<br>Nécessite une synchronisation fine entre l'émetteur et le récepteur<br>- Sensible au nombre d'émetteurs émettant dans la même bande | - Convient à la transmission de signaux courts, y compris en environnement perturbé<br>- Solution retenue notamment par Bluetooth (1 600 sauts de fréquence par seconde entre 79 fréquences dans la bande ISM 2,4 GHz) |
| DSSS | -Systèmes de redondance par étalement peu sensibles aux interférences et aux erreurs de transmission<br>-Bonne efficacité spectrale<br>- Possibilité d'obtenir des débits élevés<br>- Possibilité d'améliorer les performances<br>par allongement du vecteur d'étalement<br>- Durée d'établissement relativement courte | - Technologie relativement sophistiquée<br>- Nécessite des composants rapides<br>- Consommation d'énergie relativement élevée | - Convient à la transmission de signaux relativement longs (en dessous d'un seuil de perturbations, qui est fonction du vecteur d'étalement)<br>- Solution retenue notamment pour ZigBee et Wi-Fi (802.11b) |
| OFDM | -Grande efficacité spectrale<br>- Possibilité d'obtenir des débits très élevés (si le bilan de liaison le permet)<br>- Offre une grande robustesse au regard des interférences (notamment celles qui sont dues aux multi trajets) | - Consommation d'énergie relativement élevée<br>- Nécessite d'une synchronisation très fine entre l'émetteur et le récepteur<br>- Efficacité limitée aux interférences sélectives | - Convient pour s'affranchir des interférences causées par les multitrajets<br>- Solution retenue pour Wi-Fi (802.11a dans la bande des 5 GHz et 802.11g dans la bande des 2,4 GHz) |

23

### 1.7.2. Zone de couverture

couverture de l'intérieur et de l'extérieur

- A l'intérieur des bâtiments

| Vitesses (Mbits/s) | Portée (Mètres) |
|---|---|
| 11 | 50 |
| 5 | 75 |
| 2 | 100 |
| 1 | 150 |

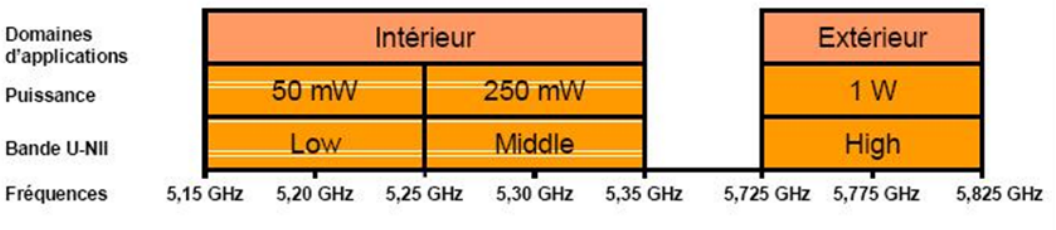
- A l'extérieur des bâtiments

| Vitesses (Mbits/s) | Portée (Mètres) |
|---|---|
| 11 | 200 |
| 5 | 300 |
| 2 | 400 |
| 1 | 500 |

## 1.8. Wi-Fi5 ou 802.11a

Bande UN-II (5GHz)

- Largeur de la bande : 200 MHz
- Basé sur OFDM
- Débits compris entre 6 et 54 Mbits/s




## 1.9. La Norme 802.11a

La proposition IEEE contient la définition du support physique ainsi que des couches qui se trouvent au-dessus

Partie physique

Fréquence de 5 GHz dans la bande UNII

Unlicensed National Information Infrastructure : pas besoin de licence d'utilisation

Modulation OFDM: Orthogonal Frequency Division Multiplexing

52 porteuses

Excellentes performances en cas de chemins multiples

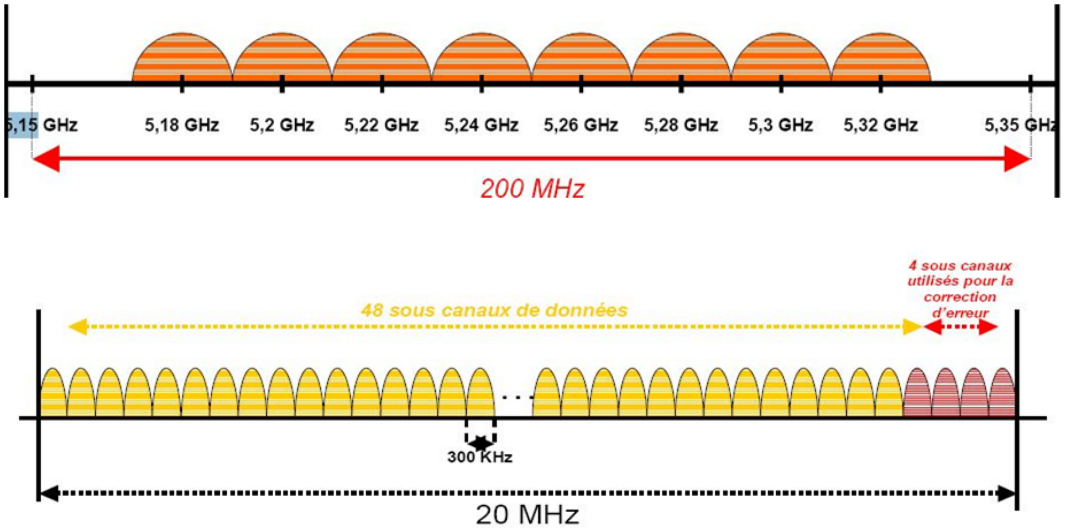
8 vitesses de 6 à 54 Mbit/s

Devrait permettre à de très nombreuses stations de travail et portables de se connecter automatiquement dans les entreprises

Couches supérieures : correspondent à celles des réseaux Ethernet

## 1.10. OFDM (Orthogonal Frequency Division Multiplex)

- 8 canaux de 20 MHz
- Co-localisation de 8 réseaux au sein du même espace 5,15




## 1.11. La norme 802.11e

Amélioration de 802.11a en introduisant De la qualité de service Des fonctionnalités de sécurité et d'authentification

But : faire transiter la parole téléphonique et les données multimédias sur des réseaux partagés

Définition de classes de service

Les terminaux choisissent la bonne priorité en fonction de la nature de l'application transportée

Gestion des priorités

Au niveau du terminal

Technique d'accès modifiée par rapport à 802.11

Les stations prioritaires ont des temporisateurs d'émission beaucoup plus courts que ceux des stations non prioritaires : avantage pour l'accès au support

Mécanismes de sécurité améliorés

Authentification mutuelle entre les terminaux et les stations de base

Trafic protégé par un chiffrement

Authentification de la source disponible

Technique de distribution des clés : elle-même sécurisée

Extensions prévues pour permettre la communication vers des terminaux qui ne sont pas en contact direct avec la station de base

Cheminements multi-sauts

## 1.12. Wifi vs. Wifi 5

- La bande ISM devient de plus en plus saturée (802.11b, 802.11g, Bluetooth, etc.)
- Co-localisation plus importante dans Wi-Fi5
- Débits plus importants pour Wi-Fi5 mais zone de couverture plus petite

## 1.13. Couche de liaison de données

Composée de 2 sous-couches

LLC : Logical Link Control

Utilise les mêmes propriétés que la couche LLC 802.2

Possible de relier un WLAN à tout autre réseau local appartenant à un standard de l'IEEE

MAC : Medium Access Control

Spécifique à l'IEEE 802.11

Assez similaire à la couche MAC 802.3 du réseau Ethernet filaire

### 1.13.1. Accès au Medium

La couche MAC définit :

2 méthodes d'accès au support:

Mécanisme de base : DCF (Distributed Coordination Function)

Mécanisme optionnel : PCF (Point Coordination Function)

Mode ad-hoc :Uniquement DCF

Mode infrastructure (avec points d'accès) ;DCF et PCF

### 1.13.2. DCF (Distributed Coordination Function)

Basé sur le protocole CSMA/CA (Carrier Sense MultipleAccess/Collision Avoidance)

CSMA :

Offre toute la bande passante si une station transmet seule

Ne transmet pas si une transmission est en cours

Ne détecte pas de collision en cours de transmission

CA :

Mécanisme d'éviter des collisions

Ethernet : CSMA/CD (Collision Detection)

CSMA/CD ne peut pas être utilisé dans les environnements sans fil

Détection de collision : une station doit être capable d'écouter et de transmettre en même temps

Systèmes radio : la transmission couvre la capacité de la station à entendre la collision

Si collision : la station continue à transmettre la trame complète (perte de performance du réseau)

### 1.13.3. CSMA

Le CSMA est basé sur :

L'écoute du support

L'utilisation d'acquittements positifs

L'algorithme de Backoff

4 type de temporisateurs IFS : SIFS, PIFS, DIFS, EIFS

Intervalles IFS = périodes d'inactivité sur le support de transmission

Intervalle de temps entre la transmission de 2 trames

Permet d'instaurer un système de priorités (plus le délais est petit, plus l'accès est prioritaire)


**a) Type de Temporisateur**

(SIFS): est le temps en microsecondes requis pour qu'une interface sans fil traite une trame reçue et réponde avec une trame de réponse.

DCF: qui contrôle l'accès au support physique. Une station doit détecter l'état du support sans fil avant de transmettre. S'il constate que le support est continuellement inactif pendant la durée de l' espace intertrame DCF (DIFS), il est alors autorisé à transmettre une trame. Si le canal est trouvé occupé pendant l'intervalle DIFS, la station doit différer sa transmission.

PCF :attend la durée PIFS plutôt que DIFS pour occuper le support sans fil. La durée du PIFS est inférieure à DIFS et supérieure à SIFS (DIFS > PIFS > SIFS). Par conséquent, AP a toujours plus de priorité pour accéder au support.

Si une trame reçue précédemment contient une erreur, une station doit différer la durée EIFS au lieu de DIFS avant de transmettre une trame;'EIFS garantit que la transmission de l'Ack peut se dérouler sans interférence de la part de ceux qui ne sont pas en mesure de décoder la trame.

### 1.13.4. CSMA (suite)

802.11 CSMA: émetteur

si le canal est libre pendant DIFS sec. alors transmission de la trame entière (pas de détection de collision)

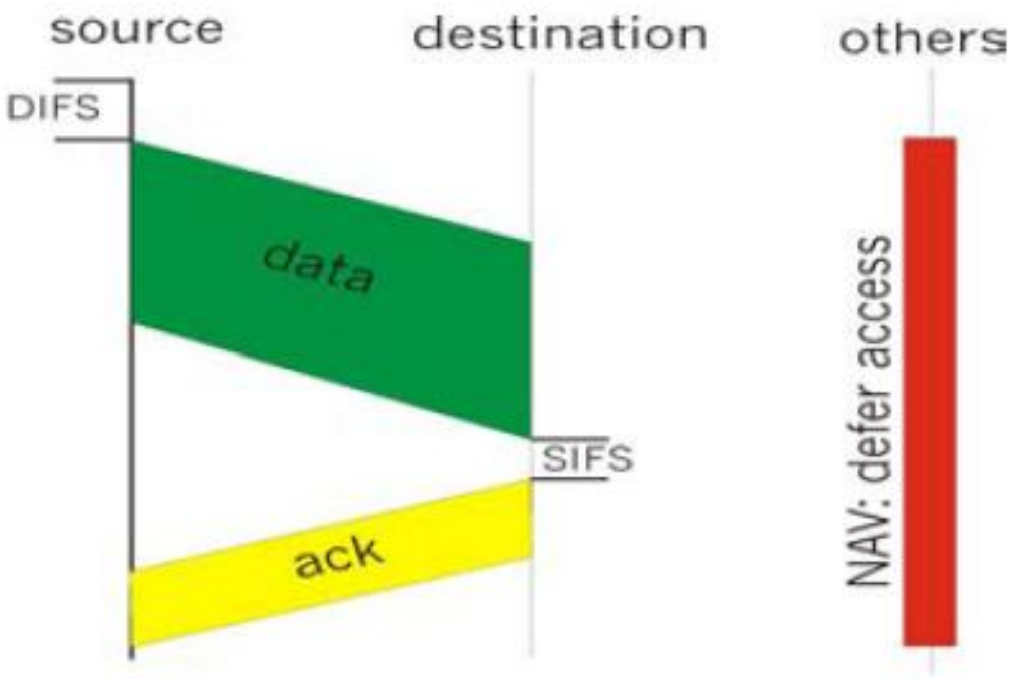
si le support est occupé

alors Binary Backoff

802.11 CSMA récepteur

si la réception est correct alors transmission d'un ACK après SIFS sec.

(ACK nécessaire : problème de la station cachée)




### 1.13.5. Algorithme du Backoff

Permet de résoudre le problème de l'accès au support lorsque plusieurs stations veulent transmettre des données en même temps

Fonctionnement :

Temps découpé en Timeslot

Fenêtre de contention : CW (CWmin ≤ CW ≤ CWmax)

Contention Window : si les participants déterminent que le canal est libre, ils attendent une période de temps aléatoire avant de commencer à transmettre. Cette durée correspond à la fenêtre de contention. Cette fenêtre temporelle double à chaque collision.

Une station écoute le support avant toute tentative de transmission

Si le support est libre après un DIFS : transmission

Sinon elle calcule un temporisateur suivant la formule : TBACKOFF = random(0, CW) x Timeslot

Chaque fois que le support est libre, TBACKOFF est décrémenté de 1.

Dès que TBACKOFF atteint la valeur 0, la trame est émise.

Il y a collision lorsque :

Deux stations ont la même valeur de temporisateur

Un ACK n'est pas reçu par l'émetteur

A chaque collision, la taille de la fenêtre de contention (CW) double

Les stations ont la même probabilité d'accéder au support car chaque station doit, après chaque retransmission, réutiliser le même algorithme

Inconvénient :

Pas de garantie de délai minimal

Complique la prise en charge d'applications temps réel telles que la voix ou la vidéo

### 1.13.6. Collision Avoidance

Problème de la station cachée:

Deux stations situées chacune à l'opposé de l'AP ou d'une autre station

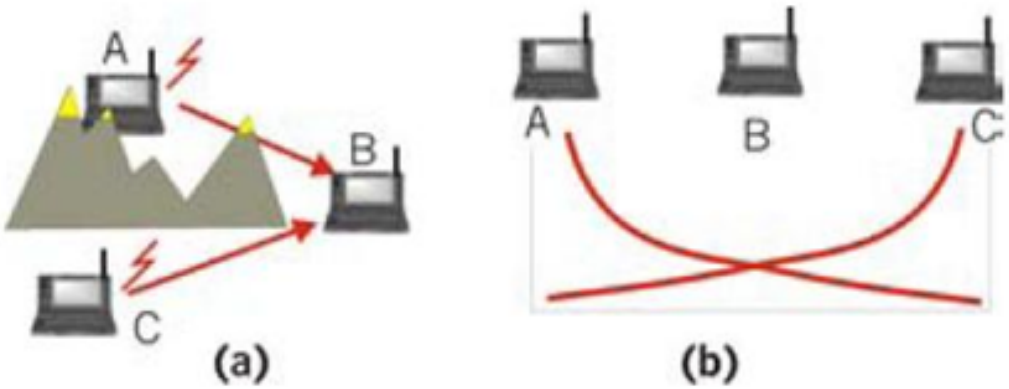
Ne peuvent pas s'entendre mutuellement pour cause de distance ou de présence d'obstacles

Effectuent des transmissions : Bande passante perdue !

Solution:

Réservation du support trames : RTS/CTS

Etat du support : NAV (network allocation vector)




### 1.13.7. Echange RTS/CTS

Mécanisme habituellement utilisé pour envoyer de grosses trames pour lesquelles une retransmission serait trop coûteuse en terme de bande passante

Les stations peuvent choisir

- D'utiliser le mécanisme RTS / CTS
- De ne l'utiliser que lorsque la trame à envoyer excède une variable RTS_Threshold
- De ne jamais l'utiliser

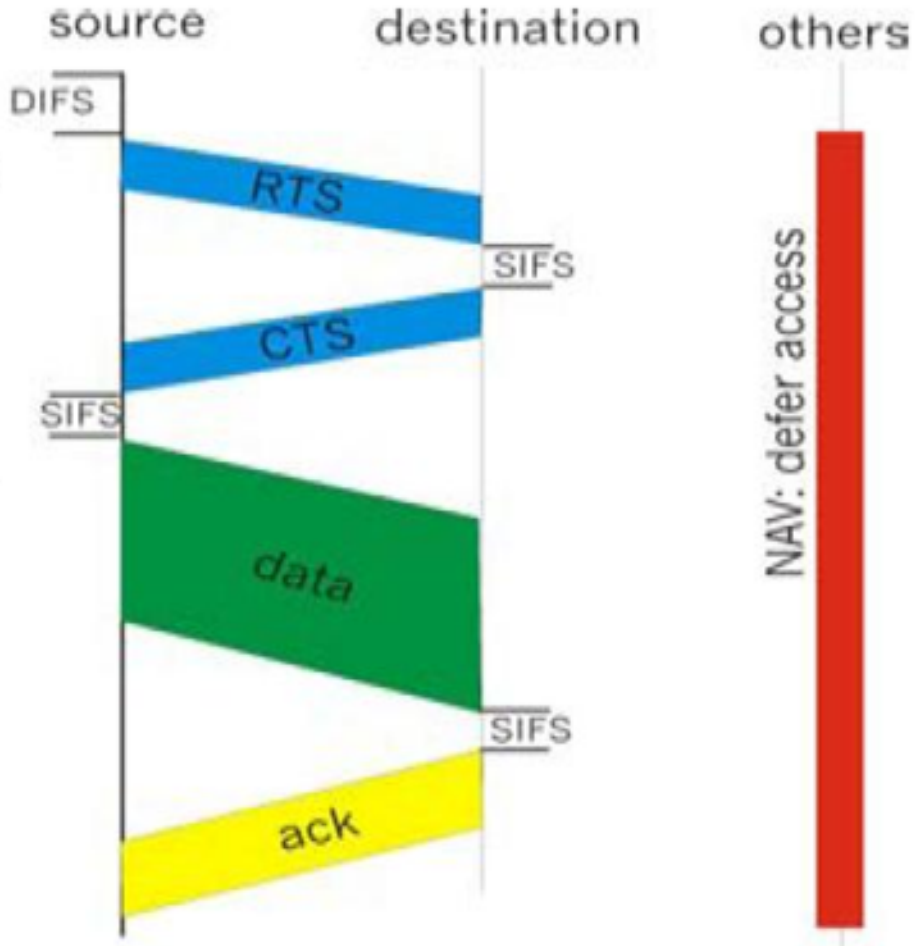
Emetteur transmet un petit paquet RTS (request to send) : indiquant l'émetteur, le récepteur et la durée de la transmission

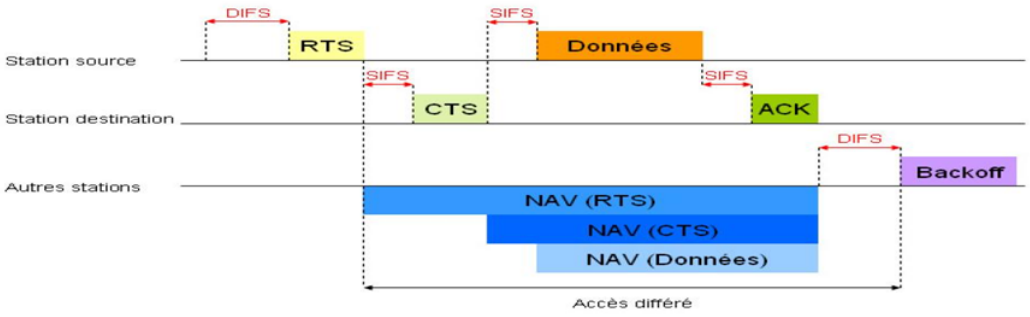
Récepteur répond avec un petit paquet CTS (clear to send) avec les mêmes infos.

Autres stations :

mettent à jour leur NAV avec les informations du RTS-CTS

Ne transmettent pas pendant la durée spécifiée par le NAV




### 1.13.8. Problème de la Station cachée

Station B cachée de la station A mais pas de la station C

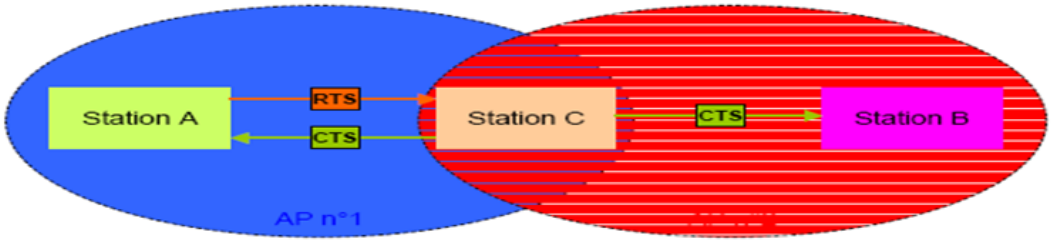
La station A transmet des données à la station C, mais la station B ne détecte pas d'activité de la station A

Dans ce cas, la station B peut transmettre librement sans interférer avec la transmission de la station A

Si A et C échangent des RTS / CTS, la station B, bien que n'écoutant pas directement la station A, est informée par l'envoi par la station C d'un CTS que le support est occupé

B n'essaie donc pas de transmettre durant la transmission entre A et C

Ce mécanisme ne permet pas d'éviter les collisions, mais une collision de RTS / CTS ne gaspille pas autant de bande passante qu'une collision de données




### 1.13.9. PCF (Point Coordination Function)

PCF permet le transfert de données isochrones

Mise en place : pendant la période CFP (Contention Free Period)

Fonctionne en alternance avec DCF

Méthode d'accès basée sur le polling

Polling : élimination de contentions

Point Coordinator (PC) : au niveau de l'AP

- Polling List
- PIFS

#### a) Fonctionnement du PCF

PC (Point Coordinator) ; si le support est libre au début de la période PCF pendant PISF sec. alors transmission d'une trame Beacon contenant CFPMaxDuration (longueur de la période PCF)

Les stations ; si réception de Beacon alors mise à jour du NAV avec CFPMaxDuration

Ne transmettent pas pendant CFP

Après SIFS sec., le PC peut transmettre les trames de données aux stations

Trame données (PC -> station)

Unicast, Broadcast, Multicast

La transmission immédiate après PIFS est possible

Trame CF Poll

Autorise les stations à transmettre

Toutes les destinations sont possibles

Transmission d'une seule trame à la fois

Trame données + CF Poll (piggyback)

Trame CF End

Annonce la fin de la période CFP

### 1.13.10. Couche de Liaison: Autres fonctions

- Accès au Réseau
- Authentification et Sécurité
- Fragmentation – Réassemblage
- Handover
- Économie d'énergie

#### a) Initialisation/Accès au Réseau

Allumer station: phase de découverte

Découvrir l'AP et/ou les autres stations

Présence détectée alors rejoindre le réseau

Service Set Id (SSID) : nom du réseau de connexion

Synchronisation

Récupération des paramètres de PHY

Négocier la connexion

Authentification & Association

#### i Ecoute passive et active

Quand un terminal veut accéder à un BSS ou à un ESS contrôlé par un ou plusieurs points d'accès

Après allumage, retour d'un mode veille ou d'un handover

Choisit un point d'accès auquel il s'associe selon un certain nombre de critères

- Puissance du signal
- Taux d'erreur des paquets
- Charge du réseau

Si la puissance d'émission du point d'accès est trop faible, la station cherche un autre point d'accès approprié

2 manières différentes : écoute passive ou active

Selon des critères tels que les performances ou la consommation d'énergie

Écoute passive

La station attend de recevoir une trame balise provenant du point d'accès

Écoute active

Une fois que la station a trouvé le point d'accès le plus approprié, il lui envoie directement une requêt d'association par l'intermédiaire d'une trame Probe Request Frame et attend que l'AP lui réponde pour s'associer

Lorsque le terminal est accepté par le point d'accès, il se règle sur son canal radio le plus approprié

Périodiquement, le terminal surveille tous les canaux du réseau pour évaluer si un AP ne possède pas de meilleures performances

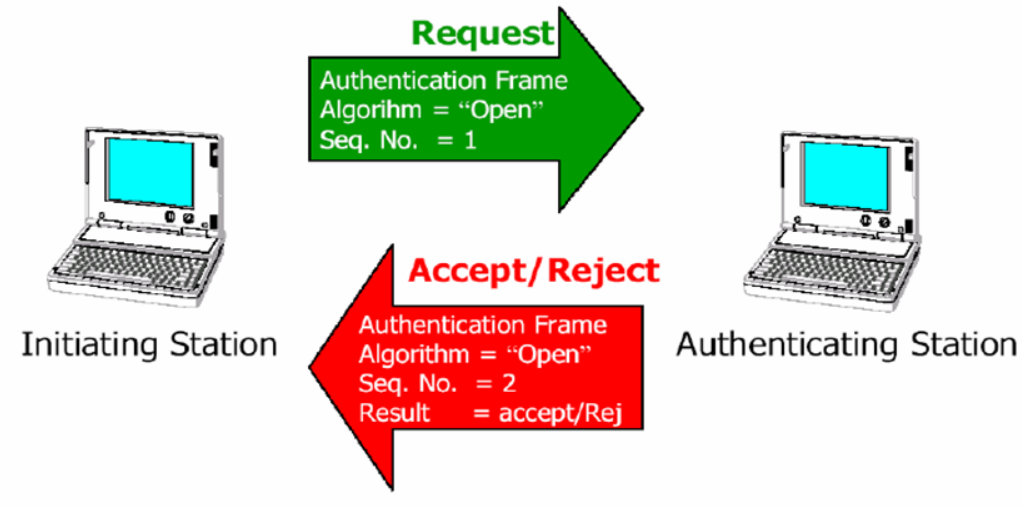
#### i Authentification

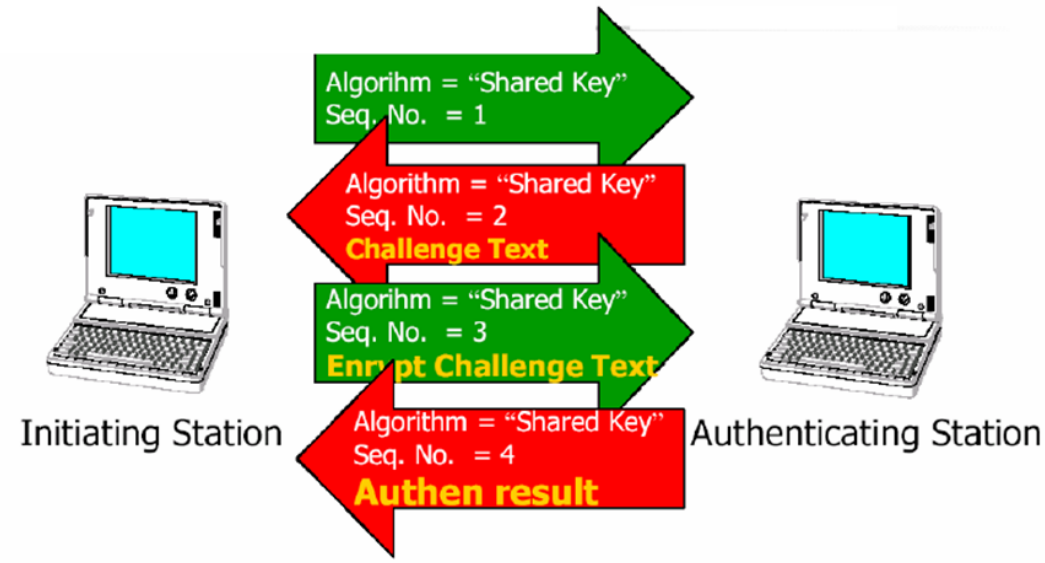
Se protéger contre les accès non autorisés

- Open system authentification
- Mode par défaut

Shared key authentification

- Plus haut degré de sécurité
- Echange de trame plus rigoureux
- Utilise le mécanisme WEP (Wired Equivalent Privacy)




### 1.13.11. Failles dans le 802.11

Tous les mécanismes de sécurité peuvent être déjoués

Solutions :

A court terme

WEP +

802.1x avec EAP (Extended Authentication Protocol)

A long terme

802.11i basée sur AES (Advanced Encryption Standard)

### 1.13.12. Fragmentation - Réassemblage

La fragmentation accroît la fiabilité de la transmission en permettant à des trames de taille importante d'être divisées en petits fragments

Réduit le besoin de retransmettre des données dans de nombreux cas

Augmente les performances globales du réseau

Fragmentation est utilisée dans les liaisons radio dans lesquelles le taux d'erreur est important

Plus la taille de la trame est grande et plus elle a de chances d'être corrompue

Lorsqu'une trame est corrompue, plus sa taille est petite, plus le débit nécessaire à sa retransmission est faible

Pour savoir si une trame doit être fragmentée, on compare sa taille à une valeur seuil, appelée Fragmentation_Threshold

Quand une trame est fragmentée, tous les fragments sont transmis de manière séquentielle

Le support n'est libéré qu'une fois tous les fragments transmis avec succès

Si un ACK n'est pas correctement reçu, la station arrête de transmettre et essaie d'accéder de nouveau au support et commence à transmettre à partir du dernier fragment non acquitté

Si les stations utilisent le mécanisme RTS / CTS, seul le premier fragment envoyé utilise les trames RTS / CTS

### 1.13.13. Handover

Passage d'une cellule à une autre sans interruption de la communication

Le standard ne définit pas de standard de roaming dans les réseaux 802.11

802.11f en cours de développement

Le standard définit quelques règles à respecter

Synchronisation

Écoute active et passive

Mécanismes d'association et de réassociation, qui permettent aux stations de choisir l'AP auquel elles veulent s'associer

Sécurité renforcée pour éviter :

Qu'un client ne prenne la place d'un autre

Qu'il n'écoute les communications d'autres utilisateurs

### 1.13.14. Économie d'énergie

Problème principal des terminaux mobiles: faible autonomie de la batterie

Mode d'économie d'énergie prévu par le standard

2 modes de travail pour le terminal

- Continuous Aware Mode

Fonctionnement par défaut

La station est tout le temps allumée et écoute constamment le support

- Power Save Polling Mode

Permet une économie d'énergie

Géré par le point d'accès

- L'AP tient à jour un enregistrement de toutes les stations qui sont en mode d'économie d'énergie
- Stocke toutes les données qui leur sont adressées
- Les stations en veille s'activent périodiquement pour recevoir une trame TIM (Traffic Information Map), envoyée par l'AP
- Si l'AP possède des données destinées à la station, celle-ci envoie une requête à l'AP : Polling Request Frame

Entre les trames TIM, les terminaux retournent en mode veille

* *

*

L'utilisation de radiofréquences pour transporter de l'information n'est guère nouvelle. Grâce aux techniques récentes d'encodage l'accès multiple au medium, l'espace, est possible ; les portées et débits atteints se rapprochent de ceux de l'Ethernet partagé.

Cette famille de techniques de construction de réseaux sans fil initiée avec le 802.11 offre une possibilité économique, performante et souple à l'architecture de réseau.

Elle remet aussi sur le tapis des problèmes un peu oubliés, et leur donne ainsi une chance de trouver une solution correcte :

sécurité des personnes dans un environnement de plus en plus saturé en rayonnements électro-magnétiques (fours à micro-ondes, téléphones DECT, téléphones mobiles, radars...) ;

cohabitation de diverses techniques utilisant des radiofréquences : 802.11b, 802.11a, 802.11g.

sécurité des réseaux : problème de contrôle d'accès au medium, problème de répéteurs pirates, périmètre de sécurité face à la mobilité ,...

# 2. Réseaux Cellulaires

## 2.1. Introduction

La téléphonie cellulaire n'est rien d'autre qu'un système de communication sans support matériel ayant pour but d'assurer la communication entre les abonnés mobiles pare la présence des stations radios formant ainsi des cellules.

La téléphonie révolutionna nos moyens de communiquer permettant enfin de dialoguer à longue distance. Malgré des débuts difficiles, la téléphonie était devenue au même titre que l'eau courante ou l'électricité un service de base.

Avec les progrès de l'informatique et des codages numériques, une nouvelle génération se profile ; la télécommunication mobile devenant ainsi un service de masse.

*Définition*

Par définition, un réseau cellulaire est un système de télécommunication qui doit répondre aux contraintes de la mobilité de l'abonné dans le réseau, par l'étendue du réseau et par les ondes radio qui lui sont allouées.

Un système de réseau cellulaire couvre l'ensemble d'infrastructures spécialement destinées aux équipements d'acheminement de communication vers les mobiles et où les ondes radio, dans le cas d'un réseau cellulaire servent de lien entre le terminal de l'abonné et l'infrastructure de l'opérateur.

## 2.2. Radiotéléphonie Cellulaire

Un système de radiotéléphonie mobile autrefois analogique et maintenant numérique assurant la totalité des services proposés par le réseau fixe, plus celui de la mobilité : possibilité de maintenir une communication en cours de déplacement (hand over) et la possibilité d'appeler et d'être appelé lorsque l'on se trouve à l'étranger (Roaming international).

## 2.3. Concepts Cellulaires

L'introduction de concept cellulaire amène le grand progrès et la nouvelle technique pour remédier aux inconvénients laissés par la téléphonie classique. La téléphonie cellulaire rassemble tous les postes radio à deux canaux, l'un pour l'émission et l'autre pour la réception en évitant les interférences probables.

Le concept cellulaire permet aussi d'atteindre des capacités importantes illimitées au moyen d'un grand nombre des stations radio dont chacune couvre une surface géographique appelée «cellule».

Ce concept consiste à diviser un territoire en cellules dont chacune est couverte par une station radio ou station de base (BTS) du réseau. Et ainsi la réutilisation d'une même fréquence que celle des cellules différentes, c'est-à-dire qui sont adjacentes ou sécantes afin d'éviter les phénomènes d'interférences sur le signal utile reçu par le terminal mobile pour la station de base.

### 2.3.1. Notion de la Cellule

L'opérateur qui choisit le secteur de télécommunication mobile doit définir la zone géographique à couvrir par son réseau. Chaque zone couverte par un émetteur est appelée cellule. Une cellule peut avoir un ou plusieurs secteurs. La taille d'une cellule est variable, elle dépend de la fréquence d'émission.C'est pourquoi un réseau de téléphonie mobile à très haute fréquence comporte beaucoup de cellules pour une meilleure couverture de l'espace à desservir.Deux cellules mitoyennes ne peuvent utiliser deux fréquences similaires à cause des

interférences. L'opérateur gère la bande passante qui lui a été allouée par l'Etat pour acheminer une conversation, la position du mobile étant signalée par le relais de passage desservant la cellule traversée. Plus la taille d'une cellule est petite, plus la quantité d'appels passés sur le réseau pour une surface donnée est grande. L'opérateur utilise des microcellules de quelques centaines de mètres de rayon pour écouler un trafic important par unité de surface dans les zones urbaines, souvent ces zones ont une couverture assurée par des antennes sectorielles de gains élevées (11 dB), que les antennes omnidirectionnelles (9 dB), tandis que dans les zones rurales peu peuplées, les cellules sont de grandes tailles (en allant jusqu'à 30 km de diamètre) et elles sont alors appelées « macrocellules ».C'est pourquoi l'utilisation d'un téléphone portable (portatif) n'est donc possible que sur la totalité de la surface d'une cellule rurale. La figure ci-dessous nous présente la division cellulaire et sa forme hexagonale.

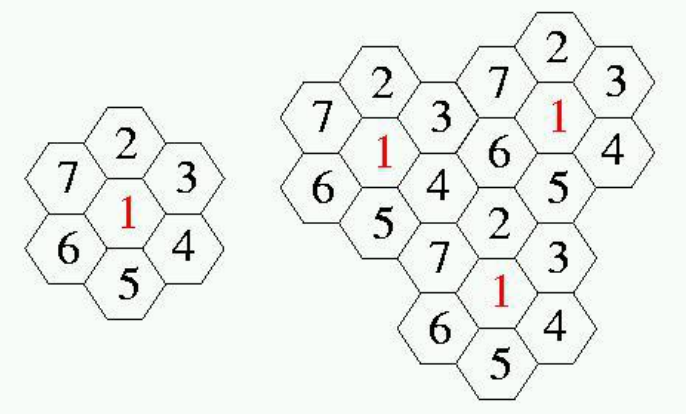
Un réseau comporte plusieurs cellules de même dimension ou des dimensions différentes selon :

- La ou les licences achetées par l'opérateur.
- le nombre d'utilisateurs potentiels dans sa zone.
- la configuration du terrain (relief géographique, présence d'immeubles).
- la nature et la densité des constructions (maisons, buildings, immeubles en béton,...).
- la localisation (rurale, suburbaine, ou urbaine).

Alors, le réseau radio mobile sera divisé en petites zones de couverture radio, en forme de nid d'abeilles, au centre desquelles sont implantés les émetteurs-récepteurs.

Ces zones sont appelées cellules. D'où l'on pourrait dire aussi qu'une cellule comprend l'étendue de la zone couverte par l'ensemble des secteurs dépendant d'un même site. Ce dernier correspond à la zone couverte par une antenne. Elle est caractérisée par :

- La puissance d'émission normale de sa BTS (dans cette zone le niveau de champ électrique doit être supérieur à un seuil déterminé).
- Sa fréquence de porteuse utilisée pour l'émission radio électrique.
- Le réseau auquel elle est interconnectée.




## 2.4. Déploiement des Réseaux Cellulaires

L'idée de base qui soutient la conception du réseau cellulaire est le respect des contraintes évoquées au point I. 2. Mais un autre facteur additionnel important est la prise en compte de la taille et de la forme des cellules du réseau radiomobile.Diverses tailles et types de cellules sont à déployer en fonction de l'environnement considéré et de la technologie. Un opérateur devra donc tenir compte des contraintes du relief topographique et des contraintes urbanistiques pour dimensionner les cellules de son réseau. Pour cela, on distingue :

- La macro cellule omnidirectionnelle : Elle est composée d'une frame et donc d'un seul secteur. Elle possède au minimum un TRX. Ce type classique de cellule est plus utilisé dans les zones rurales (à faible densité d'abonnés).
- La macro cellule bisectorisée : Elle est composée de deux frames (une par secteur) et de deux secteurs. Elle possède au minimum un TRX chacun. Ce type de cellule conviendrait mieux à un environnement médian (ruro-urbain). Malheureusement ce type de cellule est de plus en plus délaissé au profit des cellules trisectorisées.
- La macro cellule trisectorisée : Elle est composée de trois frames (une par secteur) et de trois secteurs possédant chacun au minimum un TRX. C'est le type de cellule la plus utilisée, notamment en zones urbaines à forte densité de trafic.Les microcellules sont des cellules de petite dimension destinées aux zones à fortes densité de trafic (par exemple une rue passante), tandis que les pico cellules sont pourtant des cellules de taille encore plus inférieures, prévues pour des endroits tels que les gares, les galeries marchandes,...

## 2.5. Caractéristiques des Réseaux Cellulaires

Un réseau cellulaire est caractérisé par :

### 2.5.1. Hand Over

La présence d'un grand nombre des cellules liées à la mobilité de l'utilisateur implique l'une des fonctionnalités la plus révolutionnaire du réseau cellulaire.

Le Hand Over est donc la capacité pour un terminal de changer de cellule de manière tout à fait transparente sans coupure de communication.

C'est une prise en charge par la cellule ayant le niveau de puissance élevée suivant certains critères préalablement définis. Cette opération s'effectue en une durée maximale de 200 ms.

### 2.5.2. Roaming

Du fait que le réseau cellulaire est plus normalisé, ce qui permet à un abonné de téléphoner même s'il est en dehors de son pays (dans un pays étranger par exemple) sans changer son terminal, ni son abonnement et cela peut se faire avec accords entre les opérateurs de tous ces pays pour fournir les services voulus.

### 2.5.3. Sectorisation

On appelle site, le lieu physique où sont installées une ou plusieurs stations de base avec leur alimentation en énergie, et les liaisons avec le BSC. Le coût de l'exploitation d'un réseau est essentiellement lié au nombre des sites installés.

Pour minimiser le nombre des sites, pour un nombre de cellule donnée, les opérateurs utilisent la sectorisation (le fait de couvrir une cellule par une antenne). Au lieu d'une antenne omnidirectionnelle, on place un ensemble d'antennes dont le diagramme de rayonnement couvre un secteur angulaire restreint.

### 2.5.4. Assignation des fréquences

L'attribution des fréquences en téléphonie cellulaire n'est possible que lorsque l'abonné lance un appel de communication. Les paires de fréquences sont gérées par le système c'est ce qui fait que l'abonné ne dispose pas de fréquence en permanence. Après la communication, la paire de fréquence redevient disponible pour d'autres personnes.

### 2.5.5. Réutilisation des fréquences

Elle permet d'utiliser une fréquence plusieurs fois à l'intérieur d'une même ville dans les cellules non adjacentes, c'est-à-dire qui ne se touchent pas. Ce principe permet d'éviter la saturation dans les cellules quand le nombre d'abonné augmente pour éviter les effets d'interférence entre les canaux. Il est recommandé de réutiliser les fréquences dans des cellules distantes d'au moins 6 fois leurs rayons.

## 2.6. Constitution d'un Réseau Cellulaire

D'une manière générale, un réseau cellulaire est composé de :

- La cellule.
- Le central téléphonique.
- Les supports de transmission.
- Les postes d'abonnés.

### 2.6.1. Cellule

On appelle cellule, une surface géographique de service du réseau couverte par des antennes (couverture) sur laquelle il y a la disponibilité d'un canal de transmission donnée (voie balise), constitué d'une voie radio électrique caractérisée par une fréquence donnée ou un couple de fréquences données selon les services assurées.

Les cellules sont disposées de façon adjacentes les unes contre les autres et peuvent couvrir un rayon variant de 5 à 20 Km, c'est-à-dire qu'elles peuvent desservir les abonnés situés dans un cercle de 10 à 40 Km de diamètre. La cellule joue le rôle d'interface entre le mobile et le central cellulaire, elle assure donc les fonctions suivantes :

- Affectation des canaux de communication aux mobiles,
- Emission permanente de la signalisation,
- Supervision de la communication.

### 2.6.2. Central téléphonique

Le central téléphonique est le cerveau moteur du système. Il permet la connexion entre les abonnés, il coordonne toutes les opérations et les sélections automatiques ou temporaires d'une ou plusieurs liaisons entre deux points. Il définit chaque appel par son ordinateur et le valide avant de le connecter au correspondant de l'abonné.

Le central assure les fonctions suivantes :

- La commutation des communications entre l'abonné demandeur et demandé.
- le traitement des appels et l'identification des abonnés.
- l'interconnexion avec différents réseaux.
- la collecte des données favorables.
- la signalisation.
- la maintenance et l'exploitation du réseau.

### 2.6.3. Supports de transmission

Les supports de transmission ont pour rôle de faire véhiculer les informations téléphoniques entre deux points quelconques distants, et leur bande passante varie en fonction de leur nature.

Les supports de transmission se classent en plusieurs catégories suivant la nature des signaux à transmettre et des systèmes mis en oeuvres. Mais pour le cas du réseau cellulaire, il y a :

- Le câble coaxial.
- la fibre optique.
- le faisceau hertzien (c'est le support le plus utilisé en téléphonie cellulaire grâce au rayonnement des ondes électromagnétiques).

Les supports de transmission assurent la liaison entre les mobiles, sites cellulaires et le central cellulaire. La liaison entre le mobile et le site cellulaire se fait par rayonnement électromagnétique en modulation de fréquence sans oublier que la transmission entre le site cellulaire et le central téléphonique peut se faire soit par câble, soit par fibre optique ou soit par faisceau hertzien.

## 2.7. Fonctionnement d'un Réseau Cellulaire

La procédure générale pour l'établissement d'une communication cellulaire, se fait de la manière suivante :

L'abonné par son canal de signalisation demande l'attribution d'une fréquence ; cet abonné forme le numéro de son correspondant qui sera enfin envoyé à l'ordinateur central en temps réel, et cet ordinateur analyse les autorisations de deux correspondants se trouvant dans sa base de données.

Si elles sont conformes, l'ordinateur lance une recherche du correspondant dans toutes les cellules ; si cet abonné se trouve dans un réseau câble, il établit une liaison avec le central PSTN (Public Switched Telephon Network) ; si l'abonné est du type cellulaire, la cellule en charge l'identifie et répond à l'ordinateur central ordonnant une connexion en passant par le commutateur central.

Après cette identification, la communication peut se réaliser et cela dans un délai de 20 ms sans être audible à l'oreille.

## 2.8. Avantages & Inconvénient d'un Réseau Céllulaire

### 2.8.1. Avantages

Le réseau cellulaire présente les avantages suivants :

- La suppression des câbles entraine la mobilité de l'abonné,
- le contrôle rapide et automatique du réseau grâce aux ordinateurs et leurs bases de données,
- l'adaptation rapide et facile aux réseaux à forte ou à faible densité de trafic en restant dans les mêmes proportions de l'investissement par abonné.

### 2.8.2. Inconvénients

Un réseau cellulaire présente aussi les inconvénients tels que nous les citons :

- La maintenance coûteuse,
- la disponibilité des fréquences limitées.

## 2.9. Évolutions des Normes Cellulaires

On distingue trois types des systèmes radio mobiles suivant la date de leur développement et leurs caractéristiques techniques :

- Les systèmes de première génération (tels que AMPS, TACS, NMT, RC 2000,...) étaient des systèmes analogiques. Ces réseaux étaient en général nationaux et ne permettaient pas l'itinérance internationale.

- Les systèmes de deuxième génération (tels que GSM, GPRS désigné souvent par GSM 2,5 G, EDGE ...), utilisent la transmission numérique et permettent l'itinérance internationale, mais ils sont limités en débit à quelques dizaines de Kbits/s et ils sont majoritairement utilisés pour les communications vocales.
- Les systèmes de troisième génération qui furent prévus à partir de 2001, offriront des services de données à haut débit (jusqu'à 2 Mbits/s). Le système de troisième génération le plus répandu à l'heure actuelle est l'UMTS (Universal Mobile Telecommunication System).

| Géné-ration | Services principaux | Nom de la technologie en Europe | Type d'accès sur la voie radio | Période de vie |
|---|---|---|---|---|
| 1 | Téléphonie | R2000, NMT,.. | Analogique FDMA | 1980-1995 |
| 2 | Téléphonie, SMS | GSM | TDMA | 1995- |
| 2.5 | Téléphonie, SMS<br>Accès IP à 100 kbit/s | extension GPRS-EDGE | + accès paquet et nouvelle modulation | 2000- |
| 3 | Téléphonie, SMS<br>Accès IP 1 Mbit/s | UMTS | CDMA | 2002- |
| 3.9 | Téléphonie, SMS<br>Accès IP à 10 Mbit/s | extension HSDPA | CDMA<br>+ accès paquet et nouvelle modulation | 2008- |
| 4 | Accès IP à 100 Mbit/s avec faible latence | LTE, LTE-advanced | OFDMA | 2010- |

* *

*

Dans ce chapitre, nous venons de voir les généralités sur les réseaux cellulaires. Nous avons définis ses différents principes et concepts, sa constitution, ses caractéristiques et son fonctionnement.

# 3. GSM (Global System for Mobile Communications)

la norme GSM remonte au début des années 80. A l'origine, la prise de conscience par les opérateurs que le marché du radiotéléphone en Europe était morcelé du fait de la multiplicité des systèmes analogiques alors en place et des bandes de fréquence correspondantes. La conséquence était l'impossibilité pour l'usager d'utiliser son terminal ailleurs que dans son réseau d'origine. De ce constat est né le concept de système de radiotéléphonie européen permettant d'abolir les frontières du réseau et de constituer un véritable marché européen pour les équipements d'infrastructure et de terminaux.

En 1982, le CEPT (Conférence Européenne des Postes et Télécommunications) décide alors de constituer le Groupe Spécial Mobile qui regrouper (ITU,ETSI,3GPP et autres) avec pour mission :

- développer un standard paneuropéen pour les communications mobiles. L'acronyme GSM correspond à Global System for Mobile Communications.
- le réseau radiomobile GSM représente le premier système standardisé qui utilise une technique de transmission numérique pour le canal radio: Ce point représente une caractéristique particulière du réseau, parce que tous les systèmes radio cellulaires précédents utilisaient des techniques de transmission analogiques.
- Une autre caractéristique essentielle du système est le roaming (itinérance), c'est à dire la possibilité offerte à l'utilisateur mobile d'accéder aux services GSM même dans le cas où il se trouve à l'extérieur de la zone de couverture de son réseau de souscription, en tant qu'utilisateur visiteur.

- de nombreux pays européens et non-européens l'ont adopté. Le GSM constitue pour l'utilisateur européen le premier point de la future Europe des télécommunications. Aujourd'hui, il existe plus de 690 opérateurs GSM répartis dans 213 pays.

## 3.1. Architecture GSM

L'appellation GSM (Global System for Mobile Communications) regroupe deux types de

réseaux cellulaires numériques de télécommunications pour abonnés mobiles :

- Le réseau GSM900 : il utilise des fréquences porteuses dans la gamme des 900 MHz et il a été le premier type de réseau mobile cellulaire numérique européen.
- Le réseau DCS1800 (Digital Cellular Telecommunications System) qui utilise des fréquences porteuses dans la gamme des 1800 MHz.

Les réseaux GSM/DCS permettent d'offrir au public des services de télécommunication avec une couverture continue sur un vaste territoire.

Cette disponibilité du service est obtenue par la localisation automatique de la station mobile et par des accords d'itinérance (roaming) entre opérateurs.

Ces fonctions sont celles requises dans tout réseau mobile comme la numérotation,l'acheminement vers un usager mobile, le transfert de cellules, etc. Ces fonctions sont regroupées en entités fonctionnelles. Le système GSM est constitué des entités suivantes :

- La station mobile (MS) : La station mobile est l'équipement physique utilisé par l'usager du réseau GSM pour accéder aux services de télécommunication offerts.
- Le sous-système radio (BSS, Base Station Subsystem) : il assure la couverture de zones géographiques données appelées cellules et qui contiennent les matériels et logiciels nécessaires pour communiquer avec les stations mobiles.
- Le sous-système d'acheminement appelé couramment sous-système réseau (NSS, Network Sub-System) : il comprend l'ensemble des fonctions nécessaires à l'établissement des appels et à la mobilité.
- Le sous-système d'exploitation et de maintenance (OMC, Operations and Maintenance Centre) : il permet à l'exploitant d'administrer son réseau GSM.

Le BSS comprend :

- Les BTS (Base Transceiver Station), émetteurs-récepteurs ayant un minimum "d'intelligence",
- le BSC (Base Station Controller) qui contrôle un ensemble de BTS.

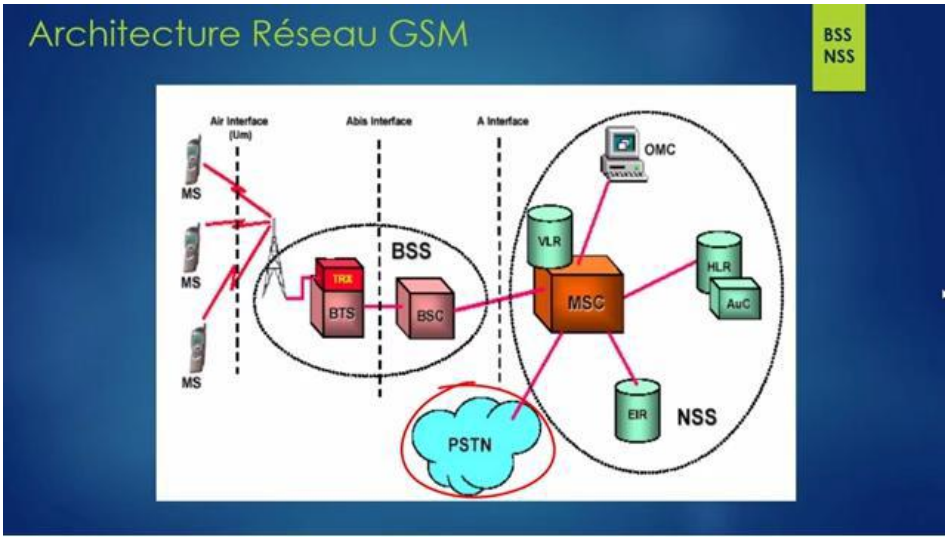
Le NSS comprend des bases de données et des commutateurs :

- Les MSC (Mobile Switching Center), commutateurs mobiles associés en général aux bases de données VLR (Visitor Location Register) fichier des abonnés visiteurs,
- le HLR (Home Location Register) : base de données de localisation et de caractérisation des abonnés.
- l'AUC (Authentication Centre) : base de données qui génère des paramètres sur demande du HLR pour protéger le réseau des utilisateurs frauduleux.
- L'EIR (Equipment Identity Register) qui vérifie l'identification de l'équipement mobile.

L'OMC peut être scindé en deux parties :

- L'OMC-R (Operations and Maintenance Centre Radio), qui a pour fonction de gérer les éléments du BSS

- l'OMC-S (OMC Switching), qui a pour fonction de gérer les éléments du NSS.




## 3.2. Interfaces GSM :

Le système GSM normalise un ensemble d'interfaces entre les entités afin de permettre l'interfonctionnement entre équipements de fournisseurs différents .

- Le BSC et le MSC disposent de l'interface A basée sur l'utilisation d'une ou plusieurs liaisons numériques à 2Mbit/s qui supportent le trafic ainsi que la signalisation nécessaire.

L'interface A est définie à la sortie du MSC et le débit du canal de parole y est égal à 64 kbit/s. Or, le débit correspondant sur l'interface radio est égal au plus à 16 kbit/s il permet que ces fonctions soient géographiquement situées près du MSC ou du BSC .

- Le BSC et la BTS partagent une interface Abis qui utilise au niveau physique des liens à 2 Mbit/s Cette interface devait à l'origine faire l'objet d'une spécification technique très stricte, afin de permettre l'interfonctionnement entre des BTS et des BSC de différents fournisseurs.
- La station mobile (MS) communique avec la BTS par le biais de l'interface radio Um Qui lui permet d'établir une connexion de niveau 2 avec la BTS pour fiabiliser le dialogue sur le canal dédié. Le sens montant désigne les activités radio de la station mobile vers le réseau; le sens descendant désigne les activités radio du réseau vers la station mobile.

Lorsqu'un MSC nécessite des informations concernant une station mobile localisée dans sa zone de couverture radio, il interroge le VLR qui lui est dédié, par le biais de l'interface B.

Lorsqu'un mobile démarre une procédure de mise à jour de sa localisation avec un MSC, le MSC en informe son VLR toujours à travers l'interface B qui sauvegarde les informations appropriées.

Le GMSC et le HLR disposent de l'interface C permettant au GMSC d'interroger le HLR contenant les caractéristiques d'abonnement d'un abonné mobile, afin d'établir un appel vers sa station mobile.

- L'interface D est utilisée entre VLR et HLR pour échanger les données relatives à la localisation d'un mobile ainsi que pour la gestion des caractéristiques de l'abonné. Lorsqu'un mobile met à jour sa localisation auprès d'un nouveau MSC/VLR, le nouveau VLR envoie au HLR les données relatives à la dernière localisation du mobile; le HLR lui retourne toutes les informations afin de fournir le service à la station mobile. Le HLR demande ensuite au VLR ayant géré la précédente localisation d'effacer les informations de localisation qu'il possédait concernant ce mobile.

Lorsqu'une station mobile se déplace d'un MSC vers un autre pendant une communication,une procédure de transfert intercellulaire (handover) inter-MSC doit être exécutée afin de garantir la continuité de la communication.

- A cette fin, les MSCs doivent échanger des données afin d'initier puis de réaliser l'opération. L'interface F utilisée entre MSCs et supportée par le protocole MAP est utilisée à cet effet.

L'interface F est utilisée entre MSC et EIR afin d'échanger des données pour que l'EIR puisse vérifier l'état de l'identité de l'équipement mobile.

Lorsqu'un abonné mobile se déplace d'une zone contrôlée par un MSC/ VLR à une autre sous la responsabilité d'un autre MSC/VLR, une procédure de mise à jour de localisation a lieu. Cette procédure peut comprendre l'échange de signalisation entre VLRs sur l'interface G afin que le nouveau VLR puisse obtenir de l'ancien VLR, l'IMSI et les triplets d'authentification concernant la station mobile.

## 3.3. Identités dans un réseau GSM

### 3.3.1. IMSI

Lorsqu 'un abonné souscrit à un abonnement mobile auprès d 'un opérateur, un identifiant unique appelé IMSI (International Mobile Subscriber Identity) lui est affecté. Ce numéro d'IMSI a été préalablement stocké sur la carte SIM (Subcriber Identity Module). Un téléphone mobile ne peut être utilisé que si une carte SIM valide a été insérée dans l 'équipement mobile car c 'est la seule façon de facturer correctement un abonné mobile.Le numéro d 'IMSI n 'est pas connu de l 'abonné mobile et n 'est utilisé que par le réseau GSM. L'IMSI est constitué de trois sous-champs :

• MCC (Mobile Country Code) : Il s'agit du code du pays du réseau GSM (603 pour l'Algerie). Le 1er Chiffre du champ MCC identifie le continent. Europe: 2; Etats-Unis: 3;Asie: 4; Australie: 5; Afrique: 6; Amérique du Sud: 7.

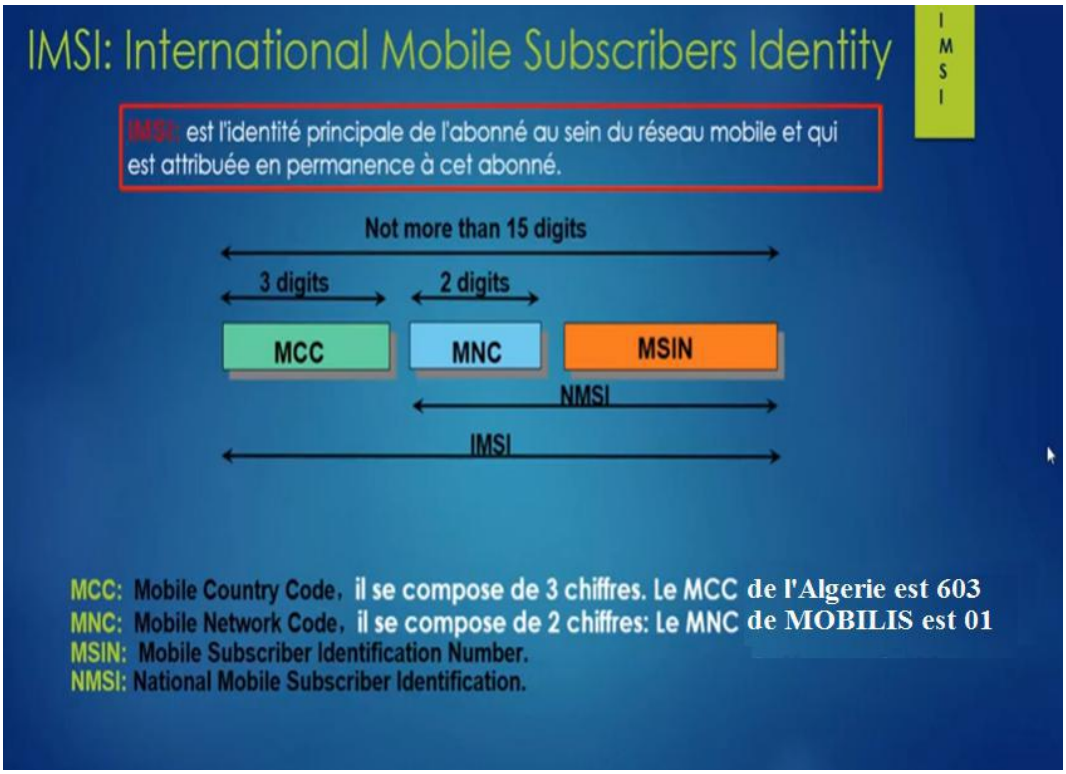
L'allocation des valeurs des codes de pays pour réseaux GSM est régie par l'ITU-T.

• MNC (Mobile Network Code) : Il s'agit du code du réseau mobile. Il est codé sur 2 chiffres et identifie de manière unique le réseau GSM à l'intérieur d'un pays. Le code réseau Mobilis Algerie est 01. Le code réseau ooredoo est 03. Enfin, le code réseau Djezzy 02.

• MSIN (Mobile Subscriber Identification Number) : il s'agit du numéro d'identification du mobile. Il identifie l'abonné mobile à l'intérieur du réseau mobile.

Les deux champs MCC et MNC permettent de déterminer de façon unique dans le monde le réseau mobile de l'abonné.

Les deux premiers chiffres du champ MSIN donnent l'indicatif du HLR de l'abonné au sein de son réseau mobile. Les MSC/VLR sont capables, à partir d'un IMSI quelconque, d'adresser le HLR de l'abonné correspondant



### 3.3.2. MSISDN :

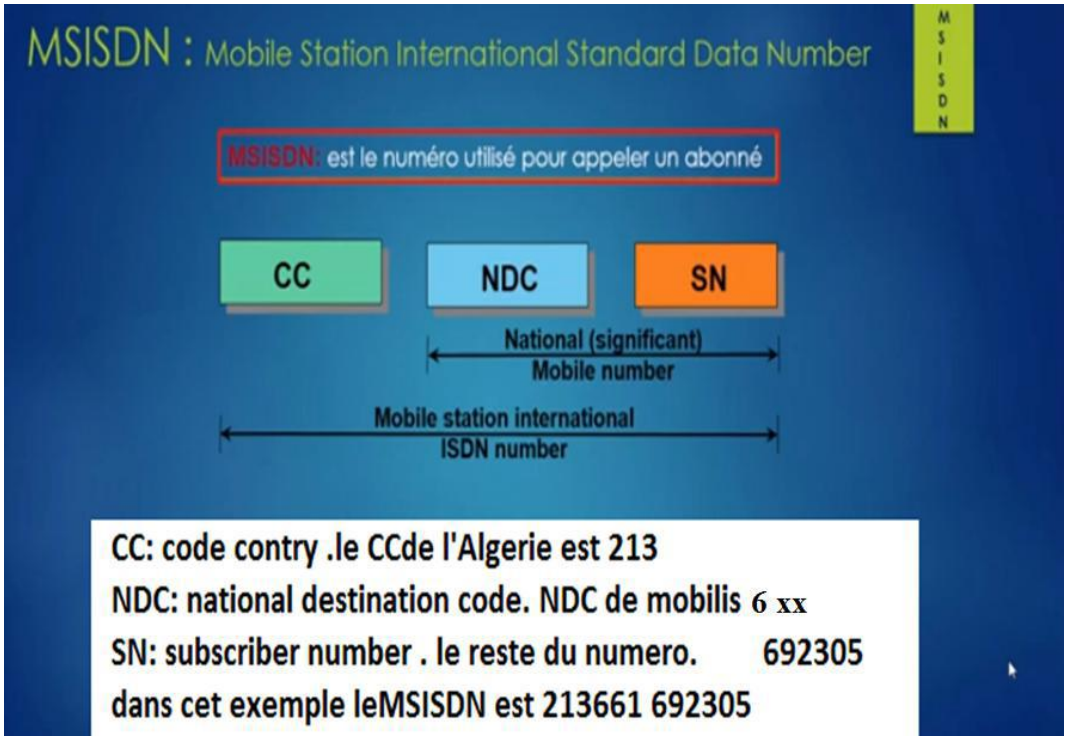
Le numéro de téléphone associé à la station mobile est le MSISDN (Mobile Station ISDN Number).

Le MSISDN consiste en trois sous-champs :

• CC (Country Code) : Il s'agit du code du pays dans lequel l'abonné mobile a souscrit un abonnement (e.g., Code CC Algerie = 213)

• NDC (National Destination Code) : Il s'agit du numéro national du réseau GSM dans lequel un client a souscrit un abonnement. (Mobilis Algerie = 6xx, Ooredoo = 5xx).

• SN (Subscriber Number) : En ALgerie le numéro MSISDN a la forme 213 6 AB PQ MCDU. 6 regroupe tous les abonnées mobiles. AB est l'indicatif Mobile GSM. PQ est le numéro de HLR logique dans le réseau GSM (à l'intérieur d'un même HLR physique, peuvent exister plusieurs HLR logiques identifiés par des valeurs PQ différentes). MCDU est le numéro de l'abonné dans le HLR.

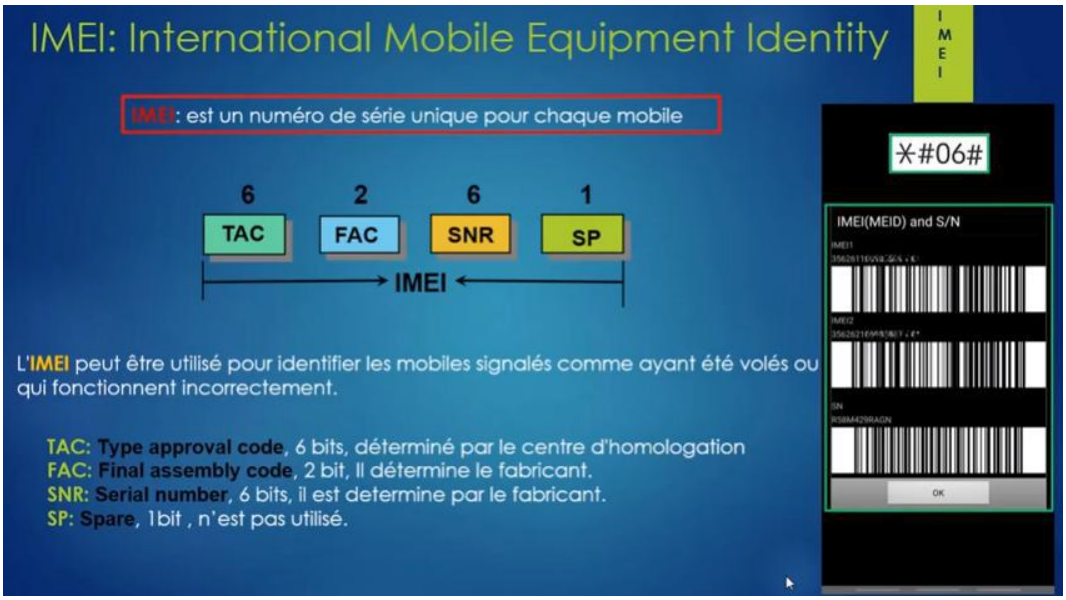



### 3.3.3. IMEI

L 'IMEI (International Mobile Equipment Identity) identifie de façon unique un terminal mobile au niveau international. Il s 'agit d 'un numéro de série. Ce numéro est alloué par le constructeur du terminal mobile. L'IMEI est utilisé de manière optionnelle par les opérateurs GSM pour lutter contre les vols de terminaux ou pour interdire l'accès au réseau à des terminaux qui auraient un comportement perturbant ou non conforme aux spécifications. A cet effet, l'opérateur dispose de la base de données EIR (Equipment Identity Register). Lorsque la station mobile, suite à sa mise sous tension, s'enregistre au réseau, le réseau a la possibilité de demander son IMEI au terminal et peut par conséquent refuser l'accès à un mobile identifié dans l'EIR comme suspect ou volé.

L'IMEI est composé des éléments suivants :

- TAC (Type Approval Code) : Il s'agit d'un numéro indiquant la version de validation du matériel.
- FAC (Final Assembly Code) : Il s'agit du numéro qui identifie l'usine où a été assemblé le poste.
- SNR (Serial Number) : Il s'agit du numéro de série de l'appareil dans le TAC et le FAC.
- Spare (en réserve) : Ce chiffre doit être codé à "0" lorsqu'il est transmis par le mobile.




### 3.3.4. TMSI

e manière à conserver la confidentialité de l'identité de l'IMSI, le VLR alloue un numéro temporaire unique à chaque mobile se localisant dans sa zone de couverture ; ce numéro est appelé TMSI (Temporary Mobile Subscriber Identity). Le VLR est capable de corréler l'IMSI d'un mobile et son identité temporaire courante (TMSI).

A l 'intérieur d 'une zone gérée par un VLR, un abonné dispose donc d'un TMSI, attribuée au mobile de façon locale, c 'est à dire pour la zone gérée par le VLR courant du mobile. Le TMSI est utilisé pour identifier le mobile lors des interactions station mobile __ réseau.

Le TMSI n 'est connu que sur la partie MS __ MSC/VLR. Le HLR n 'en n'a jamais

connaissance. A chaque changement de VLR, un nouveau TMSI est attribué.

L 'utilisation du TMSI est optionnelle. On peut avoir recours à l 'IMSI uniquement.

La structure et le codage du TMSI sont laissés à la discrétion d'accords entre l'opérateur

GSM et les fabricants des postes mobiles utilisés par les abonnés du réseau de l'opérateur.

Le TMSI est codé sur 4 octets.

Lorsqu'un mobile reçoit une identité temporaire (TMSI) d'un VLR (suite à une procédure

d'authentification), il stocke cette identité sur sa carte SIM.

### 3.3.5. MSRN

Un numéro de roaming (numéro de réacheminement) est utilisé pour router les appels vers un mobile. Le MSRN (numéro de réacheminement) est un numéro PSTN (E164) attribué temporairement à la MS et qui permet d'acheminer l'appel vers le MSC dans l'aire duquel se trouve la MS ; tout se passe comme si la MS était un abonné du MSC. A la demande d'un GMSC au HLR concerné, un MSRN (Mobile Station Roaming Number) est alloué temporairement par le VLR qui possède les dernières informations de localisation de ce mobile.

Un numéro de réacheminement (MSRN) doit avoir la même structure que les MSISDN

relatifs à une zone de localisation donnée, dans un réseau GSM et dans un pays donné.

### 3.3.6. LAI

Un réseau GSM est divisé en aires de service. Chaque MSC/VLR dans un réseau GSM

contrôle une aire de service, composée d'un ensemble de zones de localisation (LAs,

Location Areas), chaque LA représentant un ensemble de cellules

Une zone de localisation est identifiée par l'adresse LAI (Location Area Identification)

composée des champs suivants :

- MCC : Il s'agit du code du pays du réseau GSM (603 pour l'Algerie), champ également

présent dans l'IMSI.

- MNC : Il s'agit du code du réseau mobile, champ également présent dans l'IMSI.
- LAC (Location Area Code) : il s'agit du code de la zone de localisation librement affecté par l'opérateur.

A la mise sous tension et ensuite lorsqu'il se déplace, la MS se met à l'écoute du canal

BCCH de la cellule la plus puissante ; le BCCH (Broadcast Control Channel) diffuse l'identité de la LA. Le MS compare l'identité de la LA avec celle qui est mémorisée sur sa carte SIM.

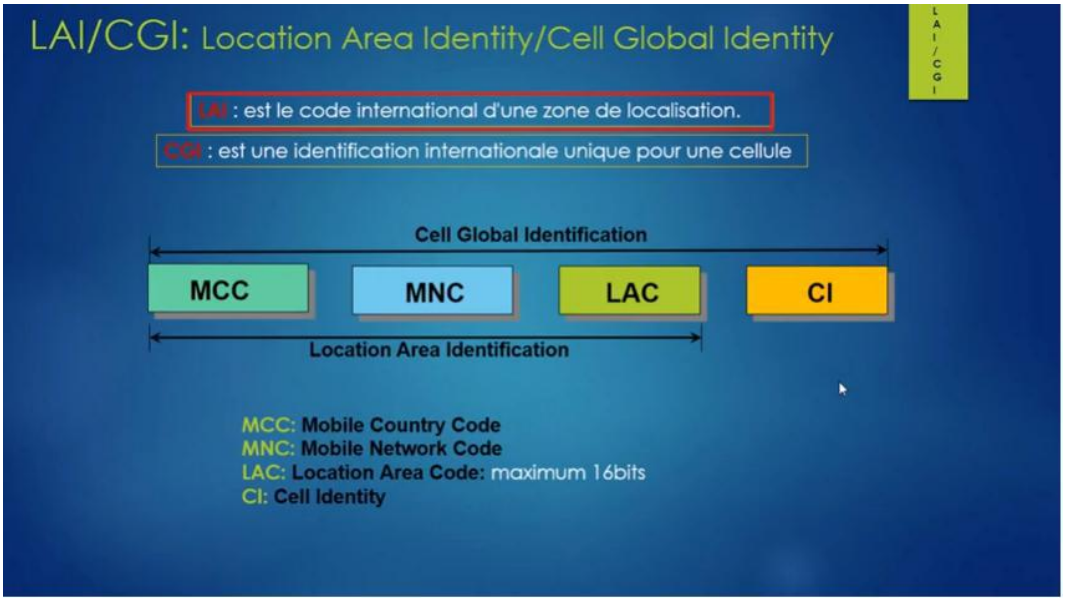
Si les identités sont identiques, la MS est correctement localisée et il ne se passe rien. Dans le cas contraire, la MS initie une procédure de mise à jour de localisation en signalant au réseau (VLR) l'identité de la nouvelle LA et son identité IMSI (ou TMSI).

Après localisation, la MS se met à l'écoute du canal de recherche PCH (Paging Channel)

afin de pouvoir recevoir d'éventuels appels. En effet, lors d'un appel entrant, le VLR ne

connaît que la LA courante du mobile. C'est la raison pour laquelle un avis de recherche

(Paging) est émis sur cette LA.




### 3.3.7. CGI :

La cellule au sein d'une zone de localisation est identifiée en rajoutant un numéro de cellule (CI, Cell Identity) à l'identification de la zone de localisation .

L'identification globale de la cellule (CGI, Cell Global Identification) qui est unique, est donc la concaténation LAI+CI.

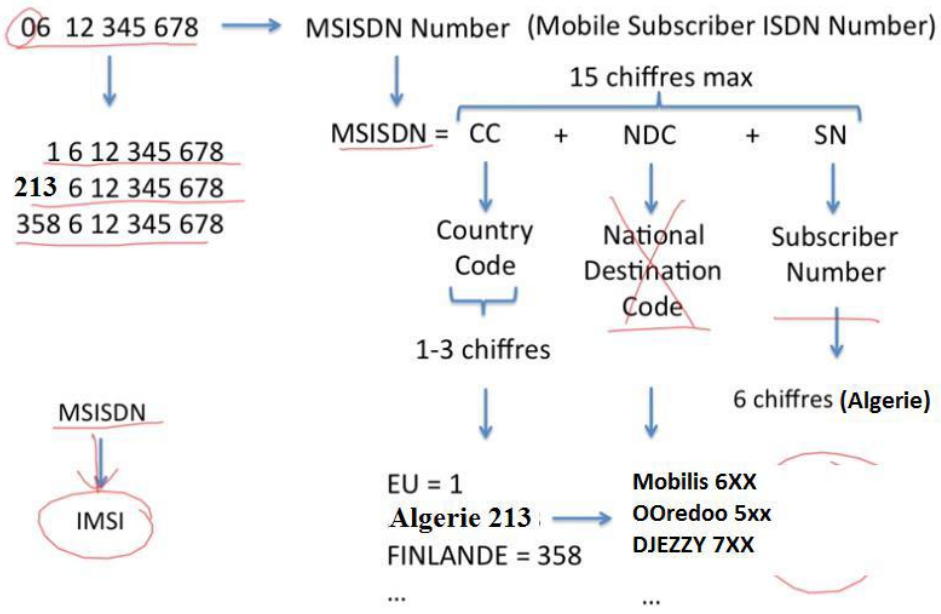
### 3.3.8. Identités pour l'authentification et le chiffrement

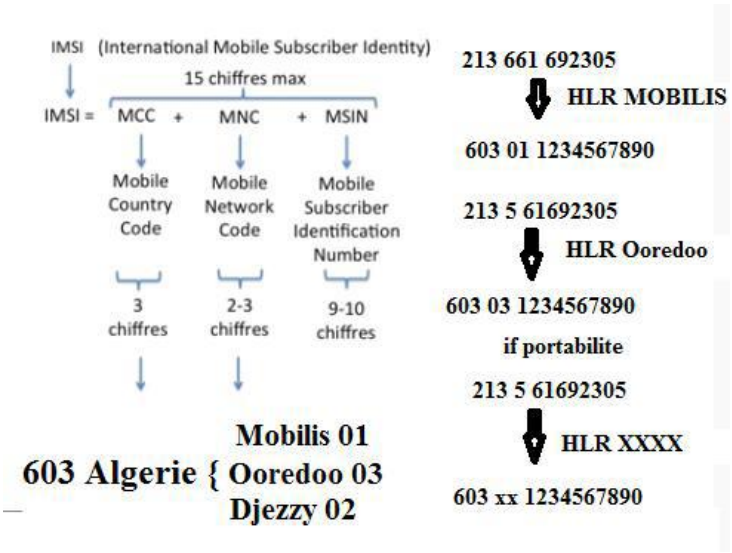
La sécurité GSM est adressée sur deux plans : authentification et chiffrement.

L'authentification empêche l'accès frauduleux par une station mobile clonée. Le chiffrement empêche l'écoute par un usager non autorisé.

Après que l'usager se soit identifié au réseau, il doit être authentifié. Pour ce faire, une clé d'authentification individuelle Ki et un algorithme d'authentification A3 sont utilisés. L'AuC et la carte SIM contiennent Ki et A3.

3.3.9. Organisation des informations de l'abonné mobile




Les données de l'abonné sont stockées dans trois entités :

• L'entité HLR qui contient toutes les informations permanentes de souscription et certaines informations temporaires des usagers enregistrés sur ce HLR.

• L'entité VLR qui contient toutes les informations nécessaires pour le traitement d'appel et autres procédures pour les abonnés mobiles actuellement dans l'aire de localisation contrôlée par ce VLR.

• La carte SIM qui contient des informations permanentes liées aux services souscrits par l'abonné ainsi que des informations temporaires modifiées par le réseau au cours de la vie de la carte SIM.

L'IMSI est une information permanente. Elle est stockée dans le HLR, le VLR, et la carte

SIM.

Le MSISDN est une information permanente présente dans les entités HLR et VLR.

Le TMSI est une information temporaire qui n'est stockée que dans le VLR et la carte SIM.

Le MSRN est une information temporaire générée et stockée dans le VLR.

Le LAI est une information temporaire présente sur le VLR et la carte SIM.

Le numéro de MSC/VLR est une information temporaire qui permet au HLR de connaître la localisation courante de la station mobile. Cette information est stockée dans le HLR.

La clé Ki est une information permanente stockée dans l'AuC et la carte SIM, l'AuC étant intégrée dans le HLR.

Le triplet (RAND, SRES, Kc) qui correspond à une information temporaire est calculé par l'AuC, et stocké dans le HLR et le VLR.

### 3.3.10. Les Canaux GSM

On distingue deux grandes catégories de canaux : les canaux physiques et les canaux logiques.

#### a) Canaux Logiques

Sur une paire de fréquences, un slot particulier parmi huit est alloué à une communication avec un mobile donné. Cette paire de slots forme un canal physique (duplex) qui correspond dans ce cas à un circuit téléphonique. Il forme alors la base de deux canaux logiques ; d'abord le TCH, Traffic Channel, qui porte la voie numérisée, mais aussi un petit canal de contrôle, le SACCH, Slow Associated Control Channel, qui permet principalement le contrôle des paramètres physiques de la liaison.

D'une manière générale, il faut prévoir sur une interface radio une multitude de fonctions de contrôle qui sont de nature et de niveau variés. Il faut, en particulier :

- diffuser des informations systèmes,
- prévenir les mobiles des appels entrants et faciliter leur accès au système,
- contrôler les paramètres physiques avant et pendant les phases actives de transmission,
- fournir des supports pour la transmission de la signalisation téléphonique.

On distingue aussi deux grandes classes de canaux logiques: les canaux dédiés et les canaux non dédiés.

#### i Les canaux dédiés

Un canal logique dédié fournit une ressource réservée à un seul mobile. Ce dernier se verra réserver dans une structure de multitrame, une paire de time slots (un en émission, un en réception) dans laquelle il est le seul à transmettre et à recevoir. Dans la même cellule, aucun autre mobile ne peut transmettre ni recevoir dans un même slot à la même fréquence. Les canaux dédiés sont duplex.

On distingue :

• Les canaux TCH et SDCCH

Ils transportent des informations utilisateur (voix, données) ou en provenance des couches hautes (applicatives) du système. Suivant le type d'information transportée, il s'agit des canaux de trafic TCH, Traffic Channel, ou des canaux de signalisation SDCCH, Stand-Alone Dedicated Control Channel. Les premiers permettent de transmettre la parole ou les données. Les canaux de signalisation SDCCH ont un débit plus faible que celui des canaux TCH. Ils peuvent être vus comme des TCH de taille réduite, dédiés à la signalisation.

Les canaux SDCCH sont requis pour mener à bien les procédures suivantes:

• Mise à jour de localisation : le mobile informe le système dans quelle zone de localisation il se trouve.

• Procédure IMSI Attach, qui permet au mobile de se faire connaître auprès du réseau et d'accéder aux services souscrits.

• Procédures IMSI Detach, qui Permet au mobile ou au réseau de s'informer l'un ou l'autre lorsque les services gérés par le MSC ne sont plus accessibles.

• Initiation d'appel. • SMS, Short Message Service.

• SACCH

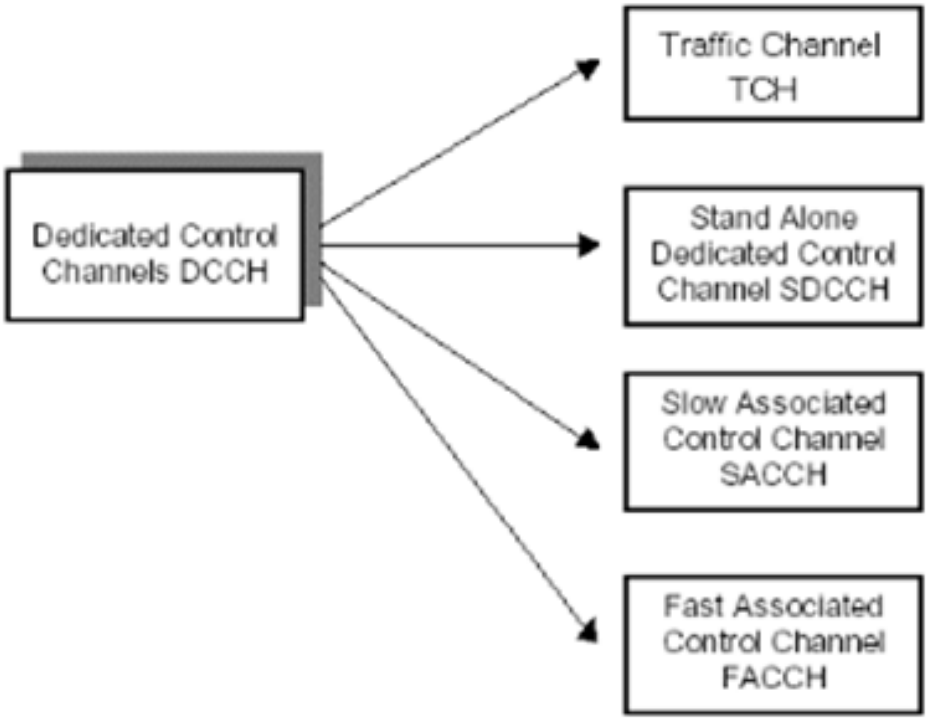
Une liaison radio est fluctuante. Il n'est pas possible de dédier un canal à un mobile sans le contrôler en permanence. Il faut constamment ajuster des paramètres pour conserver une qualité de service acceptable. Enfin, le réseau doit vérifier que le mobile est toujours actif sur le canal. Les canaux dédiés TCH et SDCCH possèdent chacun un canal de contrôle associé à faible débit appelé SACCH, Slow Associated Control Channel. Le canal SACCH supporte les informations suivantes :

- Compensation du délai de propagation aller-retour (round trip delay) par le écanisme d'avance en temps,
- Contrôle de la puissance d'émission du terminal mobile,
- Contrôle de la qualité du lien radio,
- Rapatriement des mesures effectuées sur les stations voisines.

• FACCH

Le canal SACCH est alloué conjointement à un canal dédié (TCH ou SDCCH) et permet d'écouler différents types de contrôle ou de signalisation. Cependant son débit est très faible (380 bit/s) et il introduit des délais assez importants de l'ordre d'une demi-seconde. Lorsque le canal alloué est un TCH, on suspend dans ce cas d'urgence, la transmission des informations usagers, et on récupère la capacité ainsi libérée afin d'écouler la signalisation. On obtient donc un nouveau canal de signalisation appelé FACCH, Fast Associated Control Channel.

Lorsque le canal dédié alloué est un SDCCH, ce dernier peut écouler tous les types de signalisation, en particulier la signalisation rapide nécessaire au déroulement d'un handover ; il n'y a pas dans ce cas de nécessité d'introduire le FACCH.




**Les canaux logiques dédiés**

**i Les Canaux non Dédies**

Un canal logique non dédié est simplex et partagé par un ensemble de mobiles. Dans le sens descendant, cela signifie que les données sont diffusées et tous les mobiles de la cellule sont à l'écoute du canal, si, bien sûr, la cellule est suffisamment chargée. Ces données peuvent concerner le système dans son ensemble ou des mobiles qui doivent être réveillés (appel entrant) et qui ne disposent pas encore de canaux dédiés. Dans le sens montant, la fonction remplie par un canal non dédié est la fonction d'accès multiple.

On distingue deux classes de canaux non dédiés :

- Les canaux de contrôle diffusés BCCH, Broadcast Control Channel ;
- Les canaux de contrôle commun CCCH, Common Control Channel.

• Les canaux de contrôles diffusés BCCH (Broadcast Control Channel)

Les canaux logiques en diffusion permettent à chaque mobile de s'accrocher au système local en acquérant les paramètres analogiques et logiques nécessaires. Il s'agit des canaux suivants :

Le canal FCCH, Frequency Control Channel, pour le calage en fréquence ;

Le canal SCH, Synchronisation Channel, pour la synchronisation en temps ;

Le canal BCCH, Broadcast Control Channel, pour la diffusion des informations locales du système.

Le canal CBCH, Cell Broadcast Channel, pour la diffusion des informations spécifiques (informations routières, météo, etc.).

• Les canaux de contrôles communs CCH (Common Control Channel)

Ils sont impliqués dans toutes les procédures d'accès du mobile au réseau. On distingue :

Le canal d'accès aléatoire RACH, Random Access Channel, mobile, vers réseau) est utilisé par le mobile en mode ALOHA pour accéder au réseau lorsqu'il veut s'enregistrer dans une cellule ou passer un appel. Le protocole d'accès dit ALOHA consiste à émettre un appel sur le canal d'accès sans précaution particulière. Si un autre mobile utilise le même canal au même moment, il y a risque de collision et de perte des messages émis. Au bout d'un temps aléatoire, il y a alors réémission, en principe de manière non simultanée, donc sans collision. Ce type de protocole est peu performant en cas de forte charge. C'est un point faible du GSM. toutefois ce canal nous permettra de nous renseigné sur le service sollicité par un mobile.

le canal d'allocation de ressources AGCH, Access Grant Channel, réseau vers mobile est utilisé pour allouer des ressources dédiées (canal de signalisation SDCCH ou canal de trafic TCH) au mobile qui les a demandées via un canal d'accès aléatoire RACH ;

Le canal de messagerie PCH, Paging Channel, réseau vers mobile] est utilisé pour rechercher et avertir un mobile lors d'un appel en provenance du réseau. Il est à noter qu'un mobile n'a jamais l'usage d'un AGCH et d'un PCH en même temps.

• Le canal BCCH

Le canal BCCH, Broadcast Control Channel, permet la diffusion des données caractéristiques de la cellule. C'est par ce canal que le mobile peut identifier la cellule sur laquelle il se trouve. Il comprend les informations système diffusées au mobile. Ces informations sont diffusées plus ou moins fréquemment suivant la rapidité d'acquisition par le mobile.

Le BCCH contient des informations déterminant les règles d'accès à la cellule :

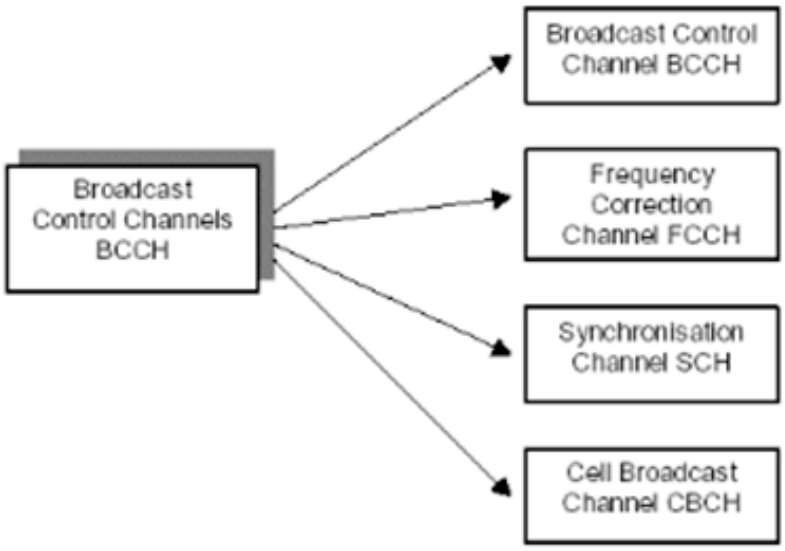
• Les paramètres de sélection de la cellule permettent à un mobile de déterminer s'il peut se mettre en veille sur la cellule après une mise sous tension ou après y être entré ;

• Le numéro de zone de localisation permettant au mobile de savoir si une inscription est nécessaire (deux diffusions par seconde).

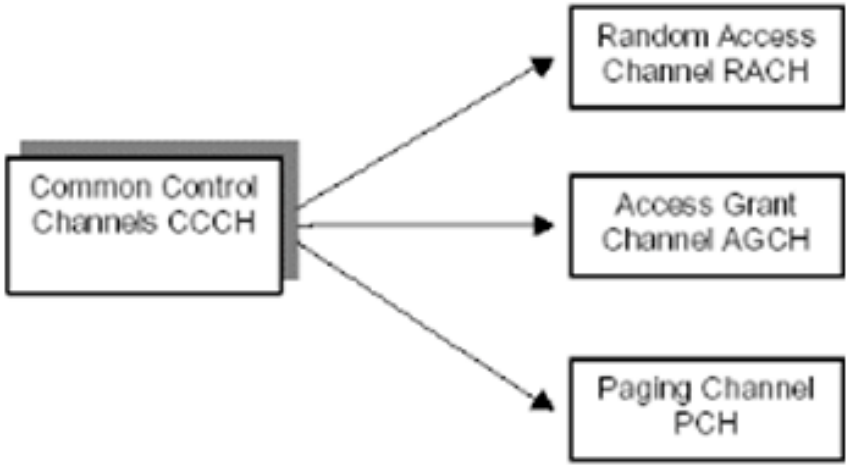
Chaque cellule diffuse également son identité complète CI, Cell Identity, au sein de la zone de localisation.

En bref, l'interface radio d'un réseau GSM constitue la porte d'accès aux services fournis par l'opérateur. L'établissement d'une requête d'un mobile vers le réseau se fait sur le lien montant, utilisant la bande fréquentielle basse attribuée par la norme à cet effet. Après traitement de la demande, le système répond au mobile sur un canal physique de la fréquence descendante équivalente (duplexage). L'ensemble des messages échangés entre le mobile et le réseau se fait au moyen de canaux logiques multiplexés dans le temps et le mobile en particulier occupe son spectre fréquentiel lorsqu'il est en veille sur le canal RACH.

Une fois que le mobile est en mode veille, il peut initier ou recevoir une communication, en suivant la procédure d'allocation des ressources radio . Cette dernière aboutit à l'octroi d'un canal physique (TS) qui, ordinairement, correspond à une fréquence et un espace temporel fixes. Or, à mesure que le réseau s'agrandit, la planification des fréquences opérationnelles sur les cellules devient d'autant plus ardue que le réseau en lui même est victime d'importantes interférences. L'implémentation du saut de fréquence pour les opérateurs de téléphonie, constitue une échappatoire certaine à ces désagréments




Les canaux de contrôle diffusés BCCH




Les canaux de contrôle communs

**i Les Canaux Physiques**

Chaque utilisateur utilise un slot par trame TDMA. Les slots sont numérotés de 0 à 7. Un « canal physique » est donc constitué par la répétition périodique d'un slot dans la trame TDMA sur une fréquence particulière.

Métriques temporelles des canaux physiques:

Trame radio: Intervalle de temps de longueur 8 slots, soit 4,615 ms.

Slot: Intervalle de temps de longueur 577 µs.

FN: Compteur de trames qui sert de référence temporelle dans une cellule, repère pour le mobile, chiffrement, séquence de saut de fréquences...

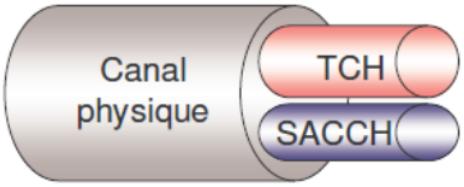
Chaque BTS transmet régulièrement sur le canal SCH (Synchronization channel) :

** RFN Reduced Frame Number

L'information de chaque MS est envoyée en Burst dans la même timeslot de la trame successive:

- Normal Burst (NB).
- Acces Burst (AB).
- Frequency Correction Burst.
- Synchronization Burst.
- Dummy Burst.

- **Un canal physique est caractérisé par :**
  - une paire de fréquences
  - un slot particulier par fréquence choisi parmi huit.




- un canal physique convoie un ou plusieurs canaux logiques.

| Type BURST | Direction | Canaux |
|---|---|---|
| Normal Burst | Uplink and Downlink | TCH, SDCCH, FACCH, SACH |
| | Downlink | PCH, AGCH, **CBCH**, BCCH |
| Acces Burst | Uplink | RACH |
| Frequency Correction Burst | Downlink | FCCH |
| Synchronisation Burst | Downlink | FCCH |
| Dummy Burst | Downlink | BCCH |

# 4. Mobilité IP

## 4.1. Mobilité IP V4

La mobilité IP (mobile IP ou IP mobility en anglais) est un protocole standard de communications de l'IETF (Internet Engineering Task Force). Il a été conçu pour permettre aux utilisateurs de se déplacer depuis un réseau IP vers un autre réseau IP tout en maintenant les connexions actives et la même adresse IP. La mobilité IP pour IPv4 est décrite dans la RFC 59441, avec des extensions décrites dans la RFC 47212. La mobilité IPv6, l'implémentation de la mobilité IP pour IPv6, est définie dans la RFC 37753.

### 4.1.1. Applications

Dans de nombreuses applications (par exemple les réseaux privés virtuels ou la voix sur IP), les changements brutaux de la connexion au réseau et en particulier de l'adresse IP peuvent causer des problèmes. Le protocole de mobilité IP a été conçu pour permettre un nomadisme transparent et une connexion continue à Internet.

On rencontre le plus souvent la mobilité IP dans les environnements câblés et sans fil où les utilisateurs ont besoin de se déplacer avec leurs équipements portables de réseau local en réseau local. On peut citer les déplacements entre réseaux sans fil qui se recouvrent, c'est-à-dire dans les cas de IP par diffusion vidéo numérique, Wi-Fi, WiMAX et technologie large bande mobile.

La mobilité IP n'est pas nécessaire avec les systèmes cellulaires comme la téléphonie mobile 3G pour offrir la transparence quand les utilisateurs d'Internet se déplacent d'une antenne cellulaire à l'autre. En effet, ces systèmes fournissent leur propre système de basculement au niveau de la couche de liaison ainsi que leurs propres mécanismes de prise en charge du nomadisme. Néanmoins, on l'utilise fréquemment dans les systèmes 3G pour éviter les heurts lorsque l'on change de point d'accès à l'Internet (packet data serving node ou PDSN).

### 4.1.2. Principe de fonctionnement

Un nœud itinérant a deux adresses : une adresse personnelle qui ne change pas et une adresse aux bons soins de (care-of address ou CoA en anglais), qui appartient au réseau hôte visité. 2 machines interviennent dans le mécanisme de la Mobilité IP :

Un agent personnel (home agent) enregistre les informations sur les nœuds nomades. L'adresse personnelle permanente se trouve dans le réseau de l'agent personnel.

Un agent étranger (foreign agent) enregistre les informations sur les nœuds itinérants visitant son réseau. Les agents étrangers annoncent les adresses aux bons soins de permettant de joindre les nœuds en déplacement. S'il n'y a pas d'agent étranger dans le réseau hôte, c'est le nœud itinérant lui-même qui se charge de tout.

Un ordinateur qui désire communiquer avec le nœud itinérant utilise son adresse permanente pour le joindre. Comme l'adresse personnelle appartient au réseau du home agent, les mécanismes normaux du routage IP font parvenir cette adresse à cet agent. Au lieu de remettre les paquets qui sont destinés au nœud itinérant sur le réseau local, l'agent personnel redirige ces paquets vers l'emplacement réel du poste itinérant au moyen d'un tunnel IP. Pour cela, il encapsule le datagramme en ajoutant un nouvel en-tête IP qui utilise l'adresse temporaire du nœud itinérant.

Lorsque le nœud itinérant est à l'origine de la transmission de données, il envoie les paquets directement à son destinataire, sans passer par son agent personnel. Pour cela, il utilise son adresse permanente personnelle comme adresse source dans le paquet IP. Ce mécanisme est connu sous le nom de routage triangulaire. Si c'est nécessaire, l'agent étranger peut utiliser un tunnel inverse (reverse tunneling en anglais) en plaçant les paquets

du nœud itinérant dans un tunnel à destination de l'agent personnel, qui les réémet alors au destinataire. Ce détour est nécessaire dans les réseaux où les passerelles vérifient que l'adresse IP source du nœud itinérant appartient bien à leur réseau.

## 4.2. Mobilité IPV6

IPv6 offre la possibilité d'ajouter de nouveaux comportements aux machines de l'Internet. L'utilisation des extensions d'en–tête d'IPv6 permet le support de la mobilité pour le modèle de l'IETF . Mobile IPv6, contrairement à son homologue Mobile IPv4, fait parti intégrante du protocole IPv6. Cette nouvelle version du protocole Internet définit un certain nombre de fonctionnalités.Le problème actuellement est qu'un correspondant envoie toujours un paquet à destination du noeud mobile vers l'agent mère de ce noeud, et ce dernier le renvoie vers l'agent relais. Cette extension permet de pallier à ce problème grâce à un système de correspondance d'adresses. Le correspondant reçoit de l'agent mère un message de mise à jour de correspondance. Celui–ci contient l'adresse mobile du noeud mobile. Celle–ci est alors stockée chez le correspondant, qui crée ensuite un tunnel directement entre lui et l'adresse mobile, évitant ainsi de passer par l'agent mère.On optimise ainsi les routes. on voit que la mobilité IPv6 a comme objectifs: Offrir une communication la plus directe possible entre le mobile et ses correspondants. Réduire le nombre d'acteurs (plus de Foreign Agent) Une adresse IPv6 globale et unique est assignée pour cela à chaque noeud mobile : Home Address. Cette adresse identifie le mobile auprès de ses correspondants Un mobile doit être capable de communiquer directement avec des noeuds non mobiles (supportant la mobilité IPv6) Pas de rupture des communications pendant les déplacements d'un mobile pour cela on utilisera le fast handover IPv6.

# Références Bibliographiques

V

## 1. Abréviation

1. BSC : Base Station Controller
2. BSIC : Base Station Identification Code
3. BSS : Base Station Subsystem
4. BTS : Base Transceiver Station
5. EDGE : Enhanced Data Rates for GSM Evolution
6. EIR : Equipment Identity Register
7. ETSI : European Telecom Standard Institute
8. FDD : Frequency Division Duplex
9. FDMA : Frequency Division Multiple Access
10. HLR : Home Location Register
11. HSDPA : High Speed Downlink Packet Access
12. HSPA+ : High Speed Packet Access +
13. IMEI : International Mobile Equipment Identity
14. IMSI : International Mobile Subscriber Identity
15. LAC : Location Area Code
16. LTE : Long Term Evolution (évolution des normes UMTS)
17. MCC : Mobile Country Code
18. MNC : Mobile Network Code
19. ME : Mobile Equipment
20. MS : Mobile Station
21. MSC : Mobile Switching Center
22. MSIN : Mobile Subscriber Identification Number
23. MSISDN : Mobile Station ISDN Number
24. MSRN : Mobile Station Roaming Number
25. NSS : Network Switching Subsystem

26. OFDMA : Orthogonal Frequency Division Multiple Access (Accès multiple par répartition en fréquences orthogonales)

27. OMC : Operation and Maintenance Center

28. OSS : Operation and Support System

29. PLMN : Public Land Mobile Network (réseau mobile terrestre public)

30. PSTN : Public Switch Telephone Network (réseau téléphonique commuté)

31. SIM : Subscriber Identity Module

32. SMS : Short Message Service

33. TDMA : Time division multiple access (Accès multiple à répartition dans le temps)

34. TMSI : Temporary Mobile suscriber Identity

35. UE : User Equipment (terminal mobile : téléphone ou smartphone)

36. UIT : Union Internationale des Télécommunications

37. UL : UpLink (liaison montante : vers la station de base)

38. UMTS : Universal Mobile Telecommunications System

39. VLR : Visitor Location Register (base de données d'abonnés)

# 2. Bibliographie

1. Guy Pujolle, "Les Réseaux", Eyrolles

2. Andrew Tanenbaum, "Computer Networks", Prentice Hall

3. Z 70-001, Norme expérimentale, Systèmes de traitement de l'information, Modèle le référence de base pour l'interconnexion de systèmes ouverts, AFNOR, 1982.

4. Réseaux de mobiles et réseaux sans fil Al Agha, Pujolle, Vivier (Eyrolles).

5. Principles of Wireless Networks K. Pahlavan, P. Krishnamurthy (Prentice Hall).

6. Wi-Fi par la pratique Davor Males et Guy Pujolle (Eyrolles).

7. Cours C.Pham Université de Pau et des Pays de l'Adour.

8. Cours F. Dupond de l'université Claude Bernard, Lyon 1.

9. ART – Autorité de Régulation des Télécommunications http://www.art-telecom.fr/

10. + nombreux sites.