

Chapitre 5. Réseaux Mobiles 3G, 4G et 5G

Le time-slot et le Burst	196
Le burst d'accès	197
Le burst de synchronisation	198
Le burst normal	198
Le burst de correction de fréquence	198
Le burst de bourrage	198
Format de la trame TDMA	199
Les canaux logiques GSM	200
Architecture du système GSM.....	201
Station mobile MS	203
Mobile Equipment	204
Carte SIM	206
Émetteur – récepteur BTS	207
Différents types de stations de base (BTS)	209
Les BTS rayonnantes	209
Les BTS ciblés	210
Les micros BTS	210
Les amplificateurs de signal	210
Contrôleur de station de base BSC	211
Sous-Système Réseau NSS	213
Le MSC (Mobile Services Switching Center)	214
Le HLR (Home Location Register)	215
Le VLR (Visitor Location Register)	216
L'AuC (Authentication Center)	216
Le sous-système opérationnel OSS (Operating Sub-System)	217
L'interface Um	217
L'interface Abis	217
L'interface A	217
GSM Handover	217
Exigences pour le handover GSM	218
Types de transfert GSM	218
Handover intra-BTS	218
Handover Inter-BTS Intra BSC	219
Transfert inter-BSC	219
Transfert inter-MSC	219

Le time-slot et le Burst

- ⇒ Le contenu d'un time-slot est appelé burst ;
- ⇒ Différents bursts contiennent différentes informations ;
- ⇒ Dans le GSM, il existe cinq différents types de burst;

Période de garde

- ⇒ La BTS et le MS peuvent recevoir le Burst et le décoder uniquement dans le cas où il est reçu dans le time-slot qui lui est désigné ;
- ⇒ Le timing doit donc être extrêmement précis, mais la structure permet une petite marge d'erreur en incorporant une période de garde comme le montre le diagramme de la figure (1) ;
- ⇒ Pour être précis, le time-slot est de 0,577 ms, alors que le burst ne dure que 0,546 ms ;
- ⇒ Il y a donc une différence de temps de 0,031 ms pour permettre au burst d'atteindre le time-slot approprié.
- ⇒ Les différents types de burst sont donnés comme suit :

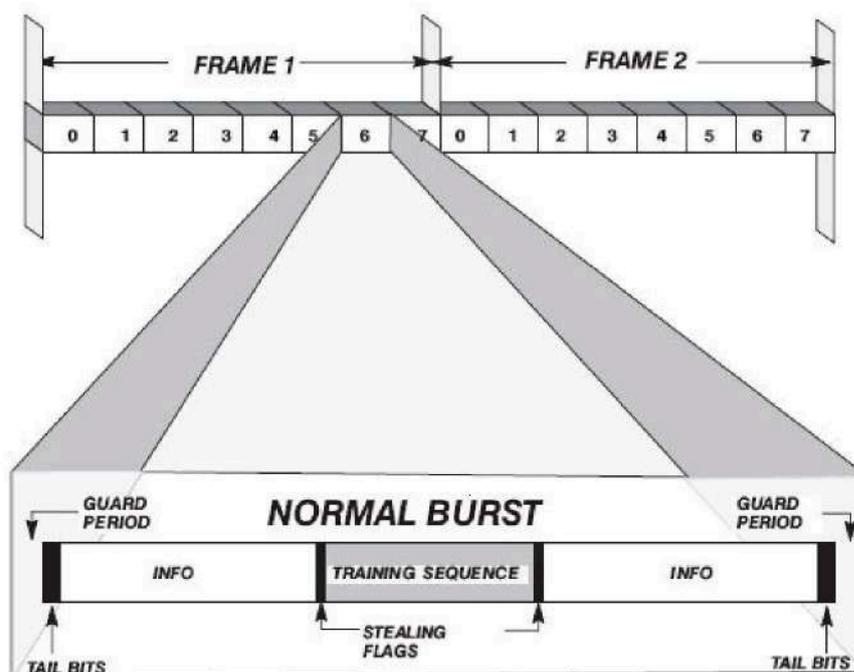


Figure.1. Format général du Burst

- 1) Les bursts d'accès qui sont envoyés par les MS lorsqu'ils veulent entrer en communication avec le réseau ;
- 2) Les bursts de synchronisation qui contiennent les informations sur la localisation et les fréquences utilisées ;
- 3) Les bursts normaux qui transportent les messages ;
- 4) Les bursts de correction de fréquence ;

- 5) Les bursts de bourrage (dummy packet) qui sont placés dans les espaces vides si aucune donnée ne doit être envoyée.

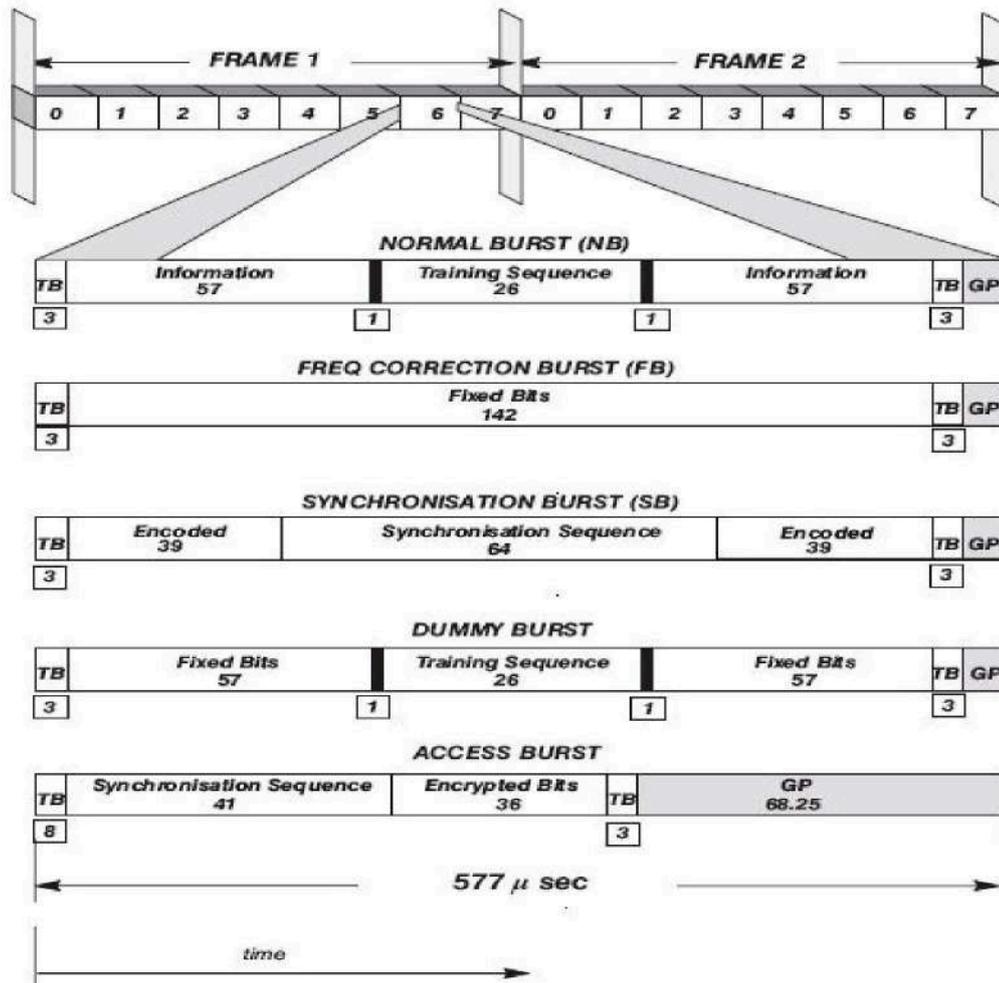


Figure.2. Structures des 5 types de burst définis par la norme GSM

Le burst d'accès

- ⇒ Ce burst est émis, sur un canal dédié, par la station mobile lorsqu'elle cherche à entrer en contact avec le réseau soit pour l'établissement d'une communication, soit pour un handover ;
- ⇒ Ce burst est le plus court des quatre types (77 bits = 41 bits de synchronisation et 36 bits d'information) ;
- ⇒ Son temps de garde est de 68.25 bits, soit 0.252 ms. Ce temps de garde permet de tenir compte de grandes cellules et d'établir ainsi une communication avec un mobile distant de 35 km ;
- ⇒ Sa Durée est de 0.577 ms = bits + période de garde = 156.25 bits.

Le burst de synchronisation

- ⇒ Pour ce type de burst, 78 bits d'informations sont véhiculés pour les stations mobiles. Ces bits contiennent les renseignements concernant les fréquences à utiliser et la localisation (le numéro de la trame TDMA, l'identité de la station de base, de la zone et de la cellule) ;
- ⇒ Il est utilisé uniquement dans le sens de la liaison descendante. Il s'agit du premier burst que la MS doit démoduler.
- ⇒ Sa Durée est de 0.577 ms = bits + période de garde = 156.25 bits.

Le burst normal

- ⇒ Ce burst consiste en une séquence d'apprentissage de 26 bits entourée de deux blocs d'informations de 58 bits ;
- ⇒ Trois bits de queue (Trail) sont ajoutés au début et à la fin de ce burst ;
- ⇒ La durée totale de burst est de 148 bits laissant une période de garde équivalente en durée à 8.25 bits ;
- ⇒ Dans ce burst, les bits chiffrés sont 57 bits de données/parole + 1 « un bit indicateur de vol » ; cela conduit à 114 bits de données utilisateur par burst. Le drapeau de vol indique le type d'informations transportées par $2 \times 57 = 114$ bits en choisissant entre les données d'utilisateur ou les données de signalisation associées au canal ;
- ⇒ Sa Durée est de 0.577 ms = bits + période de garde = 156.25 bits.

Le burst de correction de fréquence

- ⇒ Le burst de correction de fréquence est utilisée pour la synchronisation de fréquence de la MS ;
- ⇒ Il est diffusé en liaison descendante sur le BCCH (Broadcast Common Control Channel: C'est un canal point à multipoint, unidirectionnel « liaison descendante »). Les répétitions de ces burst composent le FCCH (Frequency Correction Channel: il est principalement fourni dans la trame GSM à des fins de synchronisation entre la BTS et le Mobile) ;
- ⇒ Sa Durée est de 0.577 ms = bits + période de garde = 156.25 bits.

Le burst de bourrage

- ⇒ Lorsqu'un mobile est allumé, il teste le niveau de puissance des fréquences des cellules proches pour déterminer la station de base à laquelle il doit s'asservir. Le burst de bourrage (dummy burst) est une séquence prédéfinie qui sert donc d'étalon de puissance. Ce burst est aussi utilisé pour forcer une décision de handover.

Format de la trame GSM

- ⇒ Comme le montre la figure (3), la norme GSM utilise une hiérarchie complexe de trames TDMA pour définir les canaux ;

- ⇒ Au niveau le plus bas se trouve le time-slot, également appelé période de burst, qui a une durée de $15/26$ ms (0,577 ms) → une longueur de 156.25 bits ;
- ⇒ Le time-slot comprend les champs suivants :
 - **Trail bits (Bits d'entête)** : C'est un champ qui permet la synchronisation des transmissions des unités MS situées à différentes distances de la BTS ;
 - **Bits cryptés** : les données sont cryptées en blocs par un cryptage conventionnel de 114 bits de texte en clair en 114 bits de texte chiffré ; les bits chiffrés sont ensuite placés dans deux champs de 57 bits dans le time-slot ;
 - **Stealing bit** (Bit de vol) : utilisé pour indiquer si ce bloc contient des données ou il est "volé" pour une signalisation de contrôle urgente ;
 - **Training sequence** (Séquence d'apprentissage) : utilisée pour :
 - Adapter les paramètres du récepteur aux caractéristiques de propagation du trajet actuel ;
 - Sélectionner le signal le plus fort en cas de propagation par trajets multiples ;
 - L'égalisation des trajets multiples, qui est une opération utilisée pour extraire le signal souhaité des réflexions indésirables. Cette opération est réalisée en déterminant comment la séquence d'apprentissage (connue initialement est modifiée par l'évanouissement par trajets multiples.
 - **Guard bits** (Bits de garde) : utilisés pour éviter le chevauchement avec d'autres times-slots en raison des retards des différents trajets.

Les canaux logiques GSM

- ⇒ Dans le GSM, il est nécessaire de prévoir un certain nombre de fonctions de contrôle de nature variée pour que :
 1. Le MS se rattache à une station de base favorable afin d'établir une communication ;
 2. Surveiller le déroulement de cette communication et assurer des commutations de cellules en cours de communication (Handover).
- ⇒ Ces fonctions génèrent des transferts des données suivantes :
 - Informations système ;
 - Relevés de mesures ;
 - Messages de contrôles.
- ⇒ Plusieurs canaux logiques ont été définis pour les différents types de fonction ;
- ⇒ D'une manière plus générale, il faut prévoir une multitude de fonctions de contrôle, en particulier :
 - Diffuser des informations système (Broadcast Control Channels) ;

- Prévenir les mobiles des appels rentrant et faciliter leur accès au système (cf. Common Control Channel) ;
 - Contrôler les paramètres physiques avant et pendant les phases actives de transmission (cf. FACCH, SCH et SACCH) ;
 - Fournir des supports pour la transmission de signalisation téléphonique (cf. SDCCH).
- ⇒ Ces fonctions sont résumées dans le tableau (1).

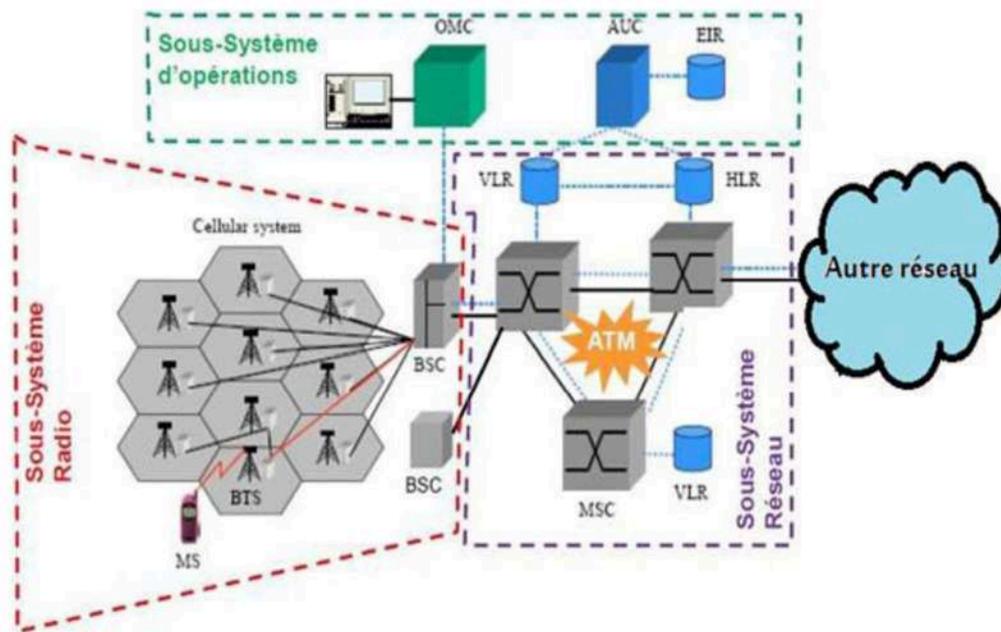
Tableau.1. Canaux logiques GSM

TYPE	NOM	FONCTION	DEBIT
Broadcast Channel: BCH	Frequency Correction Channel : FCCH	Calage sur fréquence porteuse	148 bits toutes les 50 ms
	Synchronisation Channel : SCH	Synchronisation (en temps) + Identification	148 bits toutes les 50 ms
	Broadcast Control Channel : BCCH	Information système	782 bit/s
Common Control Channel: CCCH	Paging Channel : PCH	Appel du mobile	456 bits par communication
	Random Access Channel : RACH	Accès aléatoire du mobile pour effectuer une opération sur le réseau	36 bits par message
	Access Grant Channel : AGCH	Allocation de ressources	456 bits par message d'allocation
	Cell Broadcast Channel : CBCH	Messages courts (SMS) diffusés (informations routières, météo...)	Débit variable
Dedicated Control Channel DCCH	Stand-Alone Dedicated Control Channel : SDCCH	Signalisation	782 bit/s
	Slow Associated Control Channel : SACCH	Supervision de la ligne	382bit/s pour de la parole ; 391 bit/s pour la signalisation
	Fast Associated Control Channel : FACCH	Exécution du Handover	9.2 kbit/s ou 4.6 kbit/s
Traffic Channel TCH	Traffic Channel for coded speech: TCH	Voix plein/demi débit	13 kbit/s (plein débit) 5.6 kbit/s (demi-débit)
	Traffic Channel for data	Données utilisateur	9.6kbit/s, 4.8 kbit/s ou 2.4 kbit/s

Architecture du système GSM

- ⇒ Les composants du réseau GSM sont illustrés sur la figure (4) ;
- ⇒ Le réseau GSM peut être divisé en trois sous-réseaux :

- Le réseau d'accès radio RAN (Radio Access Network) : C'est la partie radio d'un système de télécommunications mobiles. Elle met en œuvre la technologie d'accès radio ;
- Le réseau central et le réseau de gestion. Ces sous-réseaux sont appelés sous-systèmes dans la norme GSM.



➤ Figure.4. Le Réseau GSM

- ⇒ Les abréviations des termes donnés dans la figure (4) sont les suivantes :
 - MS (Mobile Station) : Station Mobile ou téléphone portable ;
 - HLR (Home Location Register) : Enregistreur de localisation géographique des abonnés ;
 - BTS (Base Transceiver Station) : Station de base ;
 - VLR (Visited Location Register) : Registre des emplacements visités ;
 - BSC (Base-Station Controller) : Contrôleur de station de base ;
 - AuC (Authentication Center) : Centre d'authentification
 - MSC (Mobile Switching Center) : Centre de commutation mobile ;
 - EIR (Equipment Identity Register) : Registre d'identité d'équipement ;
 - GMSC (Gateway MSC) : Passerelle MSC ;
 - PSTN (Public Switching Telephone Network) : Réseau téléphonique public commuté ;
 - OMC (Operation and Maintenance Center) : Centre d'exploitation et de maintenance ;
- ⇒ Les trois sous-systèmes respectifs peuvent également être appelés le sous-système Radio BSS (Base Station Subsystem), le sous-système

réseau NSS (Network and Switching Subsystem) et le sous-système d'exploitation OSS (Operation Support Sub-System) ;

⇒ Ces trois sous-systèmes sont montrés dans la figure (5).

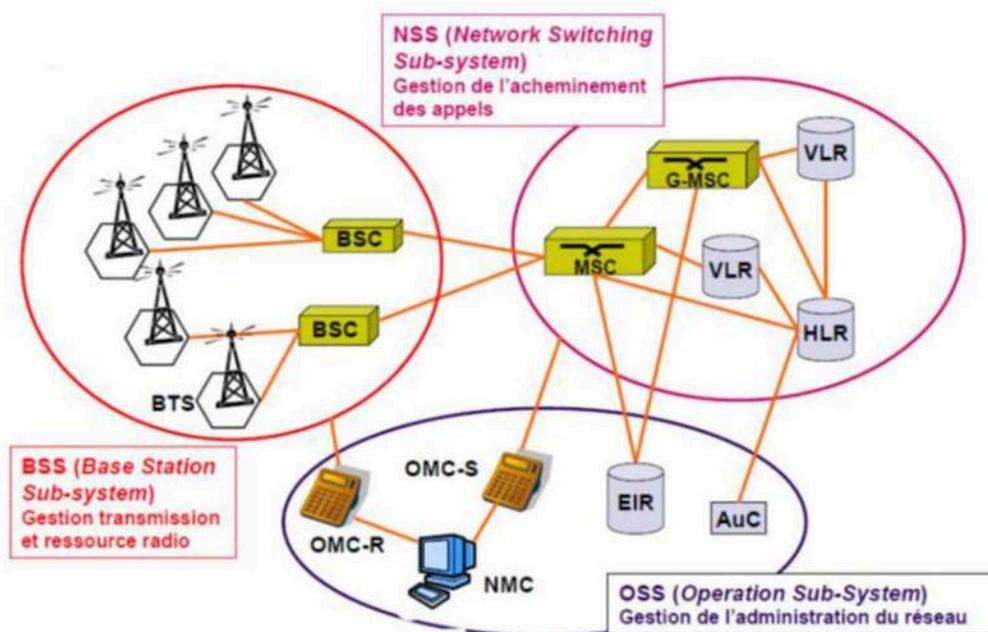


Figure.5. Les trois sous-systèmes du Réseau GSM

⇒ Ces sous-systèmes sont définis comme suit :

- **Sous-système Radio BSS** : Il assure la transmission radioélectrique et la gestion des ressources radio. Il se compose d'émetteurs-récepteurs radio (BTS) contrôlés par un BSC ;
- **Sous-système Réseau NSS** : Il gère le traitement des appels, la mobilité et l'acheminement des données de/vers les réseaux filaires. Il se compose de commutateurs radio (MCS) et d'un certain nombre de bases de données HLR et VLR ;
- **Sous-système d'exploitation OSS** : Il contrôle les droits d'accès au réseau, les droits des usagers et assure l'interface homme-machine d'exploitation. Il gère aussi le maintien en conditions opérationnelles du réseau et la remontée des alarmes.
- Les éléments de base de chaque sous-système sont définis dans ce qui suit.

Station mobile MS

- ⇒ C'est l'équipement de l'utilisateur. Il représente normalement un terminal portable qui communique, par voie hertzienne avec une station de base, appelée station d'émetteur-récepteur de base (BTS) dans le GSM ;
- ⇒ Le MS est composé du ME (Mobile Equipment – le terminal GSM) et de la carte SIM (Subscriber Identity Module) ;
- ⇒ Comme le montre la figure (6), la SIM est une petite carte douée de mémoire et de microprocesseur, qui sert à identifier l'abonné indépendamment du terminal employé ;
- ⇒ Il est donc possible de continuer à recevoir et à émettre des appels et d'utiliser tous ces services simplement grâce à l'insertion de la carte SIM dans un terminal quelconque.

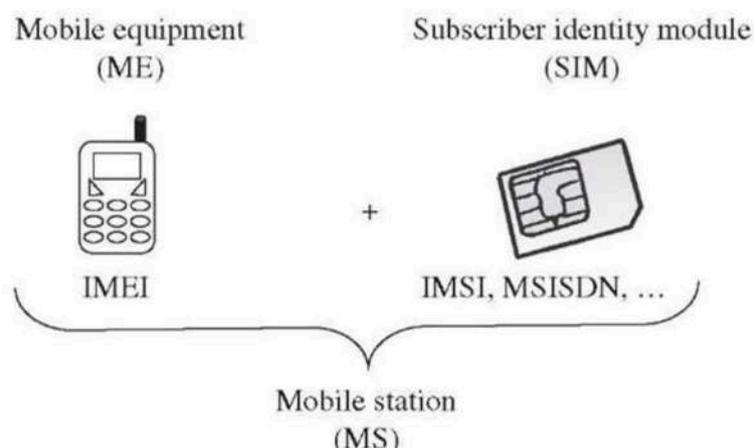


Figure.6. Mobile Station

Mobile Equipment

- ⇒ Le ME est un dispositif matériel complexe. Sa fonctionnalité comprend l'émetteur/récepteur radio plus particulièrement, la modulation et la démodulation par GMSK, le codage/décodage et la génération DTMF (dual-tone multi-frequency) ;
- ⇒ Le firmware (ou logiciel embarqué) comprend une logique de contrôle, une pile de protocoles pour le traitement/contrôle des appels et la gestion de la mobilité ;
- ⇒ L'appareil ME seul ne dispose d'aucune information d'abonné ;
- ⇒ Il ne peut pas être utilisé pour passer un appel, à l'exception des appels d'urgence ;
- ⇒ Dans l'environnement actuel, de nombreux ME disponibles sont capables de prendre en charge plusieurs bandes, c'est-à-dire 900, 1800 et 1900 MHz ;

- ⇒ Cela signifie que ces appareils peuvent être utilisés presque universellement ;
- ⇒ Le ME est identifié (exclusivement) à l'intérieur de n'importe quel réseau GSM par le code IMEI (International Mobile Equipment Identity) ;
- ⇒ L'IMEI (Voir la figure (7)) est gravé dans le module ;
- ⇒ L'IMEI est un code de 15 à 17 chiffres attribué à chaque téléphone mobile ;
- ⇒ Ce numéro est utilisé par les fournisseurs de services pour identifier de manière unique les appareils valides ;
- ⇒ L'IMEI identifie l'équipement mobile et non l'abonné ;
- ⇒ L'IMEI est intégré au matériel et ne peut pas être modifié ;
- ⇒ Il permet à un système mondial de communication mobile d'empêcher un téléphone volé par exemple de lancer des appels ;
- ⇒ L'IMEI fait également partie de la gestion des appareils mobiles ;
- ⇒ Les fournisseurs de services sans-fil conservent une liste de tous les ME volés dans une base de données (c'est-à-dire un EIR – registre d'identité d'équipement) et peuvent refuser des services à cet équipement mobile s'ils le souhaitent ;
- ⇒ L'IMEI présente la structure suivante :

IMEI = TAC / FAC / SNR / sp

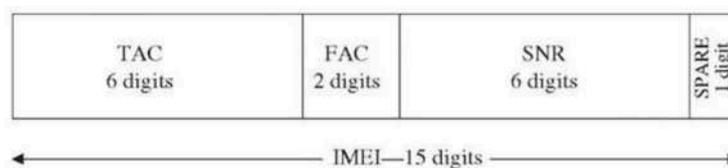


Figure.7. Structure du code IMEI

Où :

- TAC = Type Approval Code ; il désigne un modèle donné (et souvent une version donnée) d'un équipement mobile conçu pour se connecter à des réseaux de télécommunication mobile
 - FAC = Final Assembly Code, identifie le constructeur (2 chiffres) ;
 - SNR = Serial Number (6 chiffres) ;
 - sp = 1 Chiffre supplémentaire de réserve.
- ⇒ Les terminaux GSM sont divisés en cinq classes en fonction de leur puissance maximale de transmission sur le canal radio ;
 - ⇒ La puissance de la MS varie entre 0.8 Watt et 20 Watt ;
 - ⇒ Elle détermine la capacité de la MS de s'éloigner des stations émetteurs/récepteurs (BTS) du réseau tout en continuant d'utiliser le service ;

- ⇒ Une particularité de la MS consiste en la capacité de changer la puissance d'émission du signal sur le canal radio de façon dynamique sur plusieurs niveaux (18) et ceci pour pouvoir conserver à tout instant la puissance de transmission optimale, en réduisant ainsi les interférences entre canaux.

Carte SIM

- ⇒ Le module d'identité d'abonné (SIM) est une carte à puce. Le fournisseur de services sans-fil le programme avec les données d'abonnement. La carte SIM est utilisée pour stocker des données relatives au PLMN - Public Land Mobile Network (par exemple, le code pays et le réseau HPLMN), à l'abonnement (par exemple, IMSI, MSISDN), à l'itinérance (réseaux interdits, etc.) et à la sécurité (PIN, PUK, etc.). En outre, il peut également stocker des données d'abonné telles que des SMS et des numéros de téléphone ;
- ⇒ Chaque abonné dans un réseau est identifié par un numéro international unique, c'est-à-dire un numéro ISDN de station mobile (MSISDN) ;
- ⇒ Le fournisseur de services sans-fil attribue ce numéro au moment de l'abonnement ;
- ⇒ Le format du MSISDN est défini dans la recommandation ITU-T E.164. Comme le montre la figure (8), le MSISDN est de longueur variable mais limité à un maximum de 15 chiffres (à l'exclusion des préfixes) ;

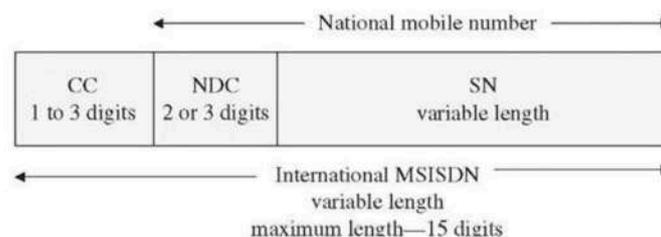


Figure.8. Format du code MSISDN

- CC ou Country Code. C'est l'indicatif du pays d'origine (exemple, +213 pour l'Algérie, +41 pour la Suisse, +33 pour la France, ...)
- NDC ou National Destination Code. C'est l'indicatif déterminant principalement l'opérateur du réseau mobile (exemple : 06 pour Mobilis, 05 pour Ooreedo, ...)
- SN ou Subscriber Number. C'est le numéro de l'abonné attribué par l'opérateur du réseau GSM ;
- ⇒ Le MSISDN est le numéro « connu du public » de l'utilisateur d'un réseau mobile GSM par opposition au numéro IMSI ;
- ⇒ C'est cet identifiant, couramment appelé numéro de téléphone (version avec préfixe international), qui est composé afin d'atteindre l'abonné. Seul

le HLR connaît la correspondance entre le MSISDN et le numéro IMSI contenu dans la carte SIM de l'abonné ;

- ⇒ La carte SIM contient l'IMSI (International Mobile Subscriber Identity), qui sert à identifier l'abonné dans n'importe quel système GSM ;
- ⇒ L'IMSI présente la structure suivante : MCC / MNC / MSIN.

Où:

- MCC= Mobile Country Code (2 ou 3 chiffres) ;
 - MNC= Mobile Network Code (2 chiffres) ;
 - MSIN= Mobile Station Identification Number (maximum 10 chiffres).
- ⇒ La carte SIM peut également stocker des données spécifiques au réseau. Par exemple, des listes de fréquences porteuses utilisées par le réseau pour diffuser périodiquement des informations système ;
 - ⇒ La carte SIM représente la base de données de l'utilisateur. En effet, elle comporte toutes les données relatives à l'abonnement et à l'identité de l'utilisateur (les données personnelles de l'utilisateur) ;

Émetteur – récepteur BTS

- ⇒ La BTS contient les émetteurs-récepteurs radio et les antennes qui fournissent une interface radio vers et depuis la station mobile ;



Figure.9. Station BTS

- ⇒ Elle définit la cellule et gère les protocoles au niveau de la liaison radio avec le MS ;
- ⇒ Chaque BTS peut avoir jusqu'à 16 émetteurs-récepteurs, chacun d'eux se voit attribuer un canal RF différent ;
- ⇒ Le nombre d'émetteurs-récepteurs dépend des exigences de traitement du trafic dans une cellule particulière ;
- ⇒ Un certain nombre de BTS sont déployées dans un réseau pour obtenir la couverture souhaitée ;

- ⇒ Une BTS est généralement installée au centre d'une cellule. La taille d'une cellule est déterminée par la puissance d'émission d'une BTS ;
- ⇒ Les tâches principales d'une BTS sont les suivantes :
 - Codage et décodage des canaux : parole, données, signalisation ;
 - Chiffrement ;
 - Modulation et démodulation GMSK ;
 - Saut de fréquence ;
 - Synchronisations temporelle et fréquentielle ;
 - Contrôle de puissance ;
 - Mesures et gestion du lien radio ;
 - Exploitation et entretien ;
 - La BTS gère également l'interface et le dialogue avec le BSC ;
 - Elle mesure les interférences sur les canaux non alloués à des communications (idle channels).
 - Elle calcule le Timing Advance (Dans la norme GSM, la valeur du « Timing Advance » correspond au temps nécessaire à un signal pour atteindre la station de base à partir d'un téléphone mobile) pour la synchronisation temporelle, selon la distance qui sépare la BTS du mobile ;
 - Elle réalise la détection des demandes d'accès des mobiles reçus sur le canal de contrôle commun (RACH) ;
 - Elle réalise la détection des messages de handover access (HO ACCESS) ;
 - Elle réalise la gestion de la Diversité d'Antennes, autrement dit l'utilisation de deux antennes de réception afin d'améliorer la qualité du signal reçu ; les deux antennes reçoivent le même signal indépendamment l'une de l'autre et sont atteintes différemment par le fading : la probabilité qu'elles soient atteintes en même temps par un fading important est presque nulle ;
 - Elle réalise le Contrôle Dynamique de la Puissance (DPC) de la MS et des BTS: le BSC détermine la puissance optimale avec laquelle le MS et la BTS effectuent la transmission sur le canal radio ;
 - Elle réalise la gestion des algorithmes de chiffrement : l'information de l'utilisateur est cryptographiée afin de garantir à l'abonné une certaine réserve sur le canal du trafic. Le processus de cryptographie des données doit être mis en œuvre par la BTS sur les informations transmises sur le canal radio ; l'algorithme de cryptographie qui doit être utilisé est transmis à la BTS par le BSC sur la base des indications reçues par le MSC et la clef cryptographique est unique pour chaque utilisateur.
- ⇒ La BTS utilise :

- Un Duplexeur qui permet d'acheminer les canaux montants et descendants sur une même antenne ;
- Un Multiplexeur qui permet de concentrer plusieurs canaux sur une même antenne en les couplant deux à deux.

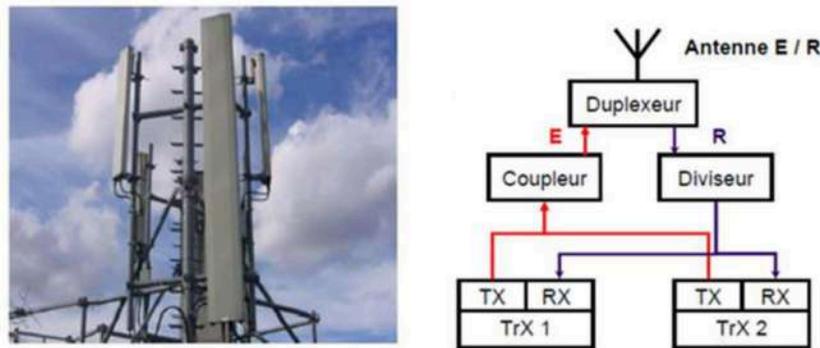


Figure.10. Duplexeur utilisé par une BTS

Différents types de stations de base (BTS)

- ⇒ Il existe différents types de BTS proposés pour répondre aux différents besoins du réseau. Ces dernières seront données dans ce qui suit.

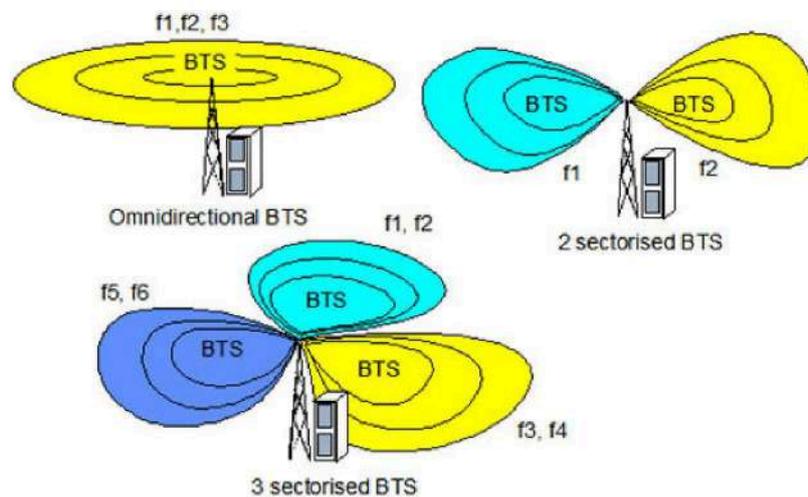


Figure.11. Différents types de BTS

Les BTS rayonnantes

- ⇒ Elles sont idéales pour couvrir les sites où la densité d'abonnés est faible ;
- ⇒ Elles sont situées sur des points stratégiques (sommets, pylônes...)
- ⇒ Ces stations émettent dans toutes les directions ;
- ⇒ Elles couvrent des macro cellules (Il s'agit d'une cellule de quelques dizaines de kilomètres de rayon) ;

- ⇒ Ces BTS ne peuvent pas être utilisées dans les zones de forte densité car elles émettent et occupent la bande passante du réseau sur une grande distance (jusqu'à 20 Kms).

Les BTS ciblés

- ⇒ Elles sont le plus souvent placées dans des zones à plus forte densité d'abonnés ;
- ⇒ On les retrouve en ville par exemple ;
- ⇒ Elles permettent d'émettre suivant un angle très précis ;
- ⇒ On peut grâce à cela réutiliser facilement le même canal dans une autre cellule à proximité.

Les micros BTS

- ⇒ Elles couvrent des zones très étroites et sont très utilisées dans les sites où la densité d'abonnés est très importante (microcellules) ;
- ⇒ Elles peuvent être installées dans les périmètres autour des centres villes. Une bonne étude d'implantation permet avec ce type de BTS de créer une couverture à deux niveaux : sur un premier niveau, les micro-BTS couvrent les 3 premiers mètres grâce à des émetteurs très ciblés. Un second niveau (étage plus élevé des immeubles) sera couvert par des BTS ciblés.

Les amplificateurs de signal

- ⇒ Les amplificateurs captent le signal émis par les BTS, l'amplifient et le réémettent d'un autre site ;

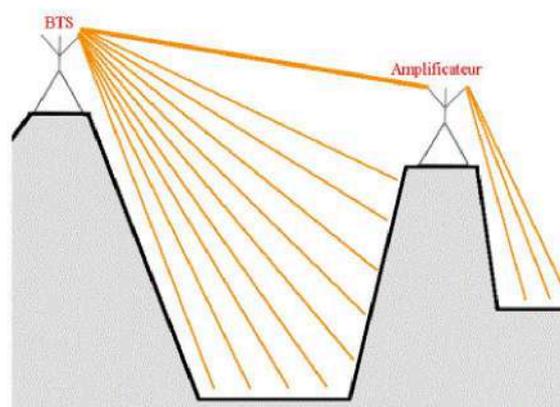


Figure.12. BTS Amplificateur

- ⇒ Ces amplificateurs ne nécessitent aucune connexion vers les BSC ;
- ⇒ Ils peuvent donc être placés sans contraintes physiques (sommet isolé de tous réseaux électriques et télécoms) ;

- ⇒ Ils sont idéals pour couvrir les zones à faible densité ou à relief difficile ;
Ils sont néanmoins très gourmands en ressource réseau, car la BTS mère doit gérer tout le trafic des réémetteurs ;

Contrôleur de station de base BSC

- ⇒ Comme son nom l'indique, le BSC surveille et contrôle une ou plusieurs stations de base BTS ;

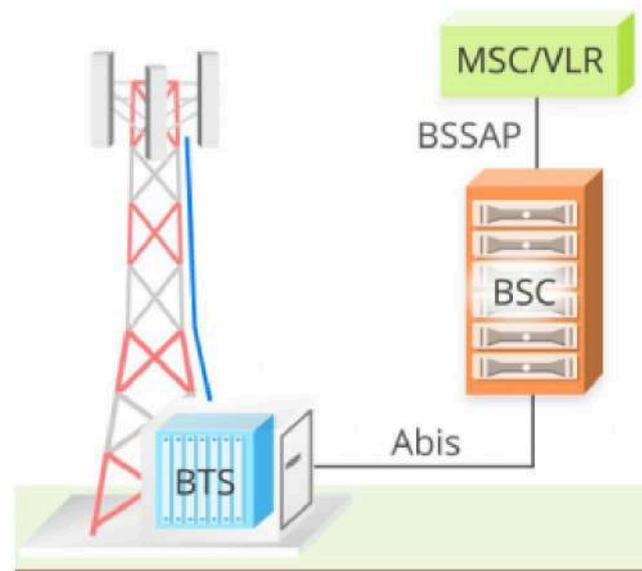
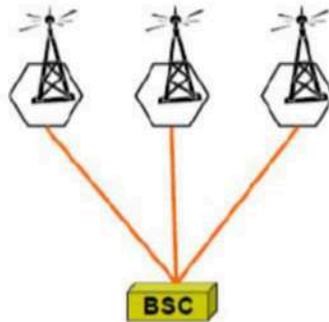


Figure.13. Le BSC

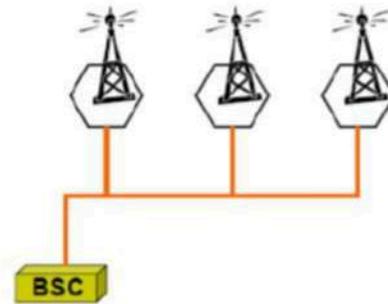
- ⇒ Le nombre de BTS contrôlées par un BSC varie en fonction de la technologie adoptée ;
- ⇒ Le BSC fournit un certain nombre de fonctions liées à la gestion des ressources radio RRM (Radio Ressources Management) et à la gestion de la mobilité MM (Mobility Management) ;
- ⇒ Le BSC se connecte au BTS en utilisant l'interface Abis, dont une description sera donnée plus loin ;
- ⇒ Les tâches principales d'un BSC comprennent :
 - Gestion des fréquences ;
 - Synchronisation temporelle et fréquentielle ;
 - Mesures des retards ;
 - Transferts ;
 - Gestion de la puissance ;
 - Fonctionnement et entretien ;
- ⇒ Le même fournisseur fournit généralement la BTS et le BSC. En effet, l'implémentation BTS est spécifique au fournisseur. Aucune norme n'est disponible pour la conception interne d'un BSC.

• **Configurations**



1. En étoile

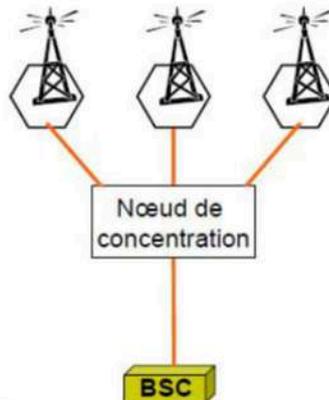
- + : connexions indépendantes
- : coûts élevés, capacité des liens est sous-exploitée



2. Chaînée

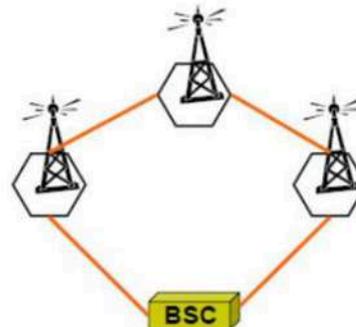
- + : réduction des coûts, optimisation de la capacité des liens
- : en cas de problèmes, perte de connexion avec toutes les BTS

• **Configurations**



3. Hybride

- + : réduction des coûts



4. En boucle

- + : meilleure sécurisation du réseau, possibilité de re-routage en cas de problèmes

Figure.14. Configuration des BTSs avec le BSC

- Les stations de base et le BSC sont reliés par des lignes fixes ou des liaisons radio point à point, cette partie de l'infrastructure du système est appelée Mobile Backhaul ;
 - Les BTS, les BSC et le Backhaul forment ensemble le réseau d'accès radio, RAN ;
- ⇒ La répartition des tâches entre les nœuds est donnée dans le Tableau (2).

Tableau.2. Fonctionnalités de la BTS et du BSC

Fonction de base	BTS	BSC
Gestion des canaux radio		X
Mappage des couches supérieures aux canaux radio		X
Codage de canal et adaptation du débit	X	
Authentification		X
Cryptage	X	X
Saut de fréquence	X	
Mesure du signal de liaison montante	X	
Mesure du trafic		X
Pagination	X	X
Gestion des Handovers		X
Mise à jour de l'emplacement		X

Sous-Système Réseau NSS

- ⇒ Les éléments du NSS prennent en charge toutes les fonctions de contrôle et d'analyse d'informations contenues dans des bases de données nécessaires à l'établissement de connexions utilisant une ou plusieurs des fonctions de chiffrement, d'authentification ou de roaming ;

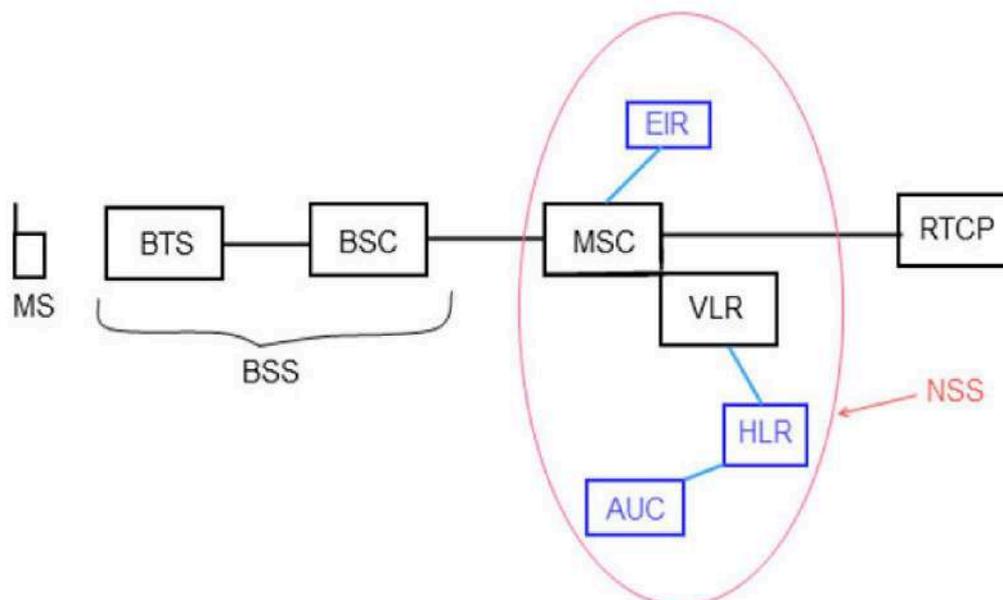


Figure.15. Sous-système NSS

- ⇒ Le NSS assure principalement les fonctions de commutation et de routage. C'est donc lui qui permet l'accès au réseau public RTCP

(Le réseau téléphonique commuté – RTC) ou réseau téléphonique commuté public) ou RNIS. En plus des fonctions indispensables de commutation, on y retrouve les fonctions de gestion de la mobilité, de la sécurité et de la confidentialité qui sont implantées dans la norme GSM ;

- ⇒ Le NSS comprend un centre de commutation mobile (MSC), un HLR, un VLR et un certain nombre de nœuds de réseau logiques, notamment le Gateway MSC (GMSC), le registre d'identité d'équipement (EIR), le centre d'authentification (ASC). Ces éléments seront discutés dans les sections suivantes.

Le MSC (Mobile Services Switching Center)

- ⇒ Le MSC est l'élément central du NSS ;
- ⇒ Il gère, grâce aux informations reçues par le HLR et le VLR, la mise en route et la gestion du codage de tous les appels directs et en provenance de différents types de réseau tels que PSTN, ISDN, PLMN et PDN ;
- ⇒ Il développe aussi la fonctionnalité du gateway (*Passerelle GSM qui permet l'acheminement des appels d'un appareil fixe vers un équipement mobile*) face aux autres composants du système et de la gestion des processus de handover, et il assure la commutation des appels en cours entre des BSC différents ou vers un autre MSC.
- ⇒ A l'intérieur de la surface de service, on peut retrouver plusieurs MSC et chacun d'entre eux est responsable de la gestion du trafic d'un ou de plusieurs BSS et à partir du moment où les usagers se déplacent sur toute la surface de couverture, les MSC doivent être capables de gérer un nombre d'utilisateurs variables en assurant à chacun un niveau de service constant.
- ⇒ D'autres fonctions fondamentales du MSC sont décrites ci-après :
 - L'authentification de l'auteur de l'appel : l'identification de la MS à l'origine de l'appel est nécessaire pour déterminer si l'utilisateur est en droit de bénéficier du service ;
 - La discrétion quant à l'identité de l'utilisateur, pour pouvoir garantir la réserve sur son identité sur le canal radio, même si toutes les informations sont cryptographiées, le système se garde toujours de transmettre l'IMSI attribué lors de la signature du contrat par l'utilisateur; Il attribue le TMSI (Temporary Mobile Subscriber Identity) à l'utilisateur, au moment de l'appel car il ne présente qu'une utilité temporaire : le MSC a aussi pour mission de mettre en relation le TMSI et le IMSI et lorsque le mobile se déplace sur l'aire de location contrôlée par un autre MSC, il doit lui attribuer un nouveau TMSI.
 - Le processus de handover.

Le HLR (Home Location Register)

- ⇒ Lorsqu'un utilisateur souscrit à un nouvel abonnement au réseau GSM, toutes les informations qui concernent son identification sont mémorisées sur le HLR. Ce dernier a pour mission de communiquer au VLR quelques données relatives aux abonnés, à partir du moment où ces derniers se déplacent d'une Location Area (LA) à une autre. A l'intérieur du HLR les abonnés sont identifiés par le MSISDN ;



Figure.16. HLR HUAWEI

- ⇒ Le HLR est une base de données qui peut être soit unique pour tout le réseau soit distribuée dans le système ;
- ⇒ Dans le cas où il existe plusieurs HLR, chacun d'eux se voit attribuer un ensemble de MSISDN ;
- ⇒ Le HLR, comme toutes les autres bases des données, est inséré dans des stations de travail dont les services (mémoire, processeurs, capacité des disques) peuvent être mis à jour au fur et à mesure de l'augmentation du nombre d'abonnés. Il contient toutes les données relatives aux abonnés et leurs informations détaillées :
- ✓ **Les informations de type permanent :**
 - L'IMSI, le MSISDN ;
 - Tous les services auxquels l'abonné a souscrit et auxquels il est capable d'accéder (voix, service de données, SMS, éventuels verrouillages des appels internationaux, et d'autres services complémentaires).
 - ✓ **Les informations de type dynamique :**
 - La position courante de la station mobile MS, autrement dit l'adresse de VLR sur lequel elle a été enregistrée ;
 - Eventuellement la situation d'un certain nombre de services auxiliaires.
- ⇒ Si l'on veut résumer, les fonctions exercées par le HLR sont :
- La sécurité : dialogue avec l'AUC et le VLR.
 - L'enregistrement de la position : dialogue avec le MSC.

- La gestion des données relatives à l'abonné : dialogue avec l'OMC et le VLR.

Le VLR (Visitor Location Register)

- ⇒ Le VLR est une base de données qui mémorise de façon temporaire les données concernant tous les abonnés qui appartiennent à la surface géographique qu'elle contrôle. Ces données sont réclamées à l'HLR auquel l'abonné appartient. Généralement pour simplifier les données réclamées et ainsi la structure du système, les constructeurs installent le VLR et le MSC côte à côte, de telle sorte que la surface géographique contrôlée par le MSC et celle contrôlée par le VLR correspondent.
- ⇒ Plus précisément, le VLR contient les informations suivantes :
 - Le TMSI, employé comme garant de la sécurité du IMSI, et il est attribué à chaque changement de LA ;
 - L'état du MS (en veille, occupé, éteint) ;
 - L'état des services complémentaires comme **Call Waiting** (L'appel en attente est un service téléphonique dans lequel un abonné peut accepter un deuxième appel téléphonique entrant en mettant en attente un appel en cours et peut également basculer entre les appels), **Call Divert** (Le renvoi d'appel est une fonctionnalité téléphonique permettant de rediriger un appel téléphonique vers une autre destination, qui peut être, par exemple, un mobile ou un autre numéro de téléphone), **Call Barring** (L'interdiction d'appels est un service qui aide à éviter les appels indésirables entrants ou sortants vers et depuis un smartphone), etc.
 - Les types de services auxquels l'abonné a souscrit et auxquels il a droit d'accès (voix, service de données, SMS, d'autres services auxiliaires) ;
 - La Location Area Identity (LAI) qui comprend le MS faisant partie du groupe contrôlé par le MSC/VLR.

L'AuC (Authentication Center)

- ⇒ Le centre d'authentification (AUC) est une fonction d'un réseau GSM utilisée pour l'authentification d'un abonné mobile qui souhaite se connecter au réseau. L'authentification se fait par identification et vérification de la validité de la SIM.
- ⇒ Une fois l'abonné authentifié, l'AUC se charge de la génération des paramètres utilisés pour la confidentialité et le chiffrement de la liaison radio. Pour garantir la confidentialité de l'abonné mobile, une identité temporaire d'abonné mobile (TMSI) est attribuée pour la durée pendant laquelle l'abonné est sous le contrôle du MSC spécifique associé à l'AUC ;
- ⇒ L'authentification dans les cas suivants :
 - Chaque fois que le MS reçoit ou émet un appel ;

- A chaque mise à jour de la position du MS (location updating).
- A chaque demande de mise en activité, de cessation d'activité ou de l'utilisation des services supplémentaires.

Le sous-système opérationnel OSS (Operating Sub-System)

- ⇒ Il assure la gestion et la supervision du réseau. C'est la fonction dont l'implémentation est laissée avec le plus de liberté dans la norme GSM. La supervision du réseau intervient à de nombreux niveaux :
 - Détection de pannes.
 - Mise en service de sites.
 - Modification de paramétrage.
 - Réalisation de statistiques.
- ⇒ Dans les OMC (Operation and Maintenance Center), on distingue l'OMC/R (Radio) qui est relié à toutes les entités du BSS, à travers les BSC, l'OMC/S (System) qui est relié au sous-système NSS à travers les MSC. Enfin l'OMC/M (Maintenance) contrôle l'OMC/R et l'OMC/S.

L'interface Um

- ⇒ C'est l'interface entre la station mobile (MS) et la station émettrice-réceptrice de base (BTS). On l'appelle Um car c'est l'analogie mobile de l'interface U du RNIS ;
- ⇒ On la nomme couramment "interface radio" ou "interface air".

L'interface Abis

- ⇒ C'est l'interface entre les deux composants du sous-système BSS : la BTS et le BSC.

L'interface A

- ⇒ C'est l'interface entre les deux sous-systèmes BSS et le NSS.

GSM Handover

- ⇒ Le handover ou le handoff est l'une des fonctions clés d'un système de téléphonie mobile ;
- ⇒ Lorsque le mobile se déplace d'une cellule à une autre, il doit être capable de conserver la connexion ;
- ⇒ Le processus par lequel cela se produit est connu sous le nom handover ou handoff ;
- ⇒ Le terme « handover » est plus largement utilisé en Europe, tandis que le terme « handoff » a tendance à être davantage utilisé en Amérique du Nord ;
- ⇒ Dans tous les cas, le handover ou le handoff représentent le même processus.

Exigences pour le handover GSM

- ⇒ Le processus handover au sein de tout système cellulaire est d'une grande importance car c'est l'une des techniques qui fait des télécommunications cellulaires une technologie durable ;
- ⇒ Il s'agit d'un processus critique et, s'il est effectué de manière incorrecte, le transfert peut entraîner une dégradation significative de la qualité de l'appel ou, pire encore, il peut entraîner la perte d'un appel si le transfert est effectué trop tard ;
- ⇒ Les appels interrompus sont particulièrement gênants pour les utilisateurs et si le nombre d'appels interrompus augmente, l'insatisfaction des clients augmente et ils sont susceptibles de changer de réseau ;
- ⇒ Par conséquent, le handover GSM était un domaine auquel une attention particulière a été accordée lors de l'élaboration de la norme ;
- ⇒ S'assurer que tous les éléments du réseau sont en mesure de fournir un transfert rapide et efficace est essentiel au bon fonctionnement du réseau dans son ensemble.

Types de transfert GSM

- ⇒ Il existe de nombreuses façons dont un handover peut fonctionner, et la méthode adoptée dépend de la position du mobile par rapport aux divers éléments au sein du réseau de communications mobiles ;
- ⇒ Dans le système GSM, il existe quatre types de handover. Ces derniers sont donnés dans ce qui suit.

Handover intra-BTS

- ⇒ Cette forme de handover GSM se produit s'il est nécessaire de modifier la fréquence ou le time-slot utilisé par un mobile en raison d'interférences ou pour d'autres raisons ;
- ⇒ Dans cette forme de handover GSM, le mobile reste attaché au même émetteur-récepteur BTS, mais change de canal ou de time-slot.

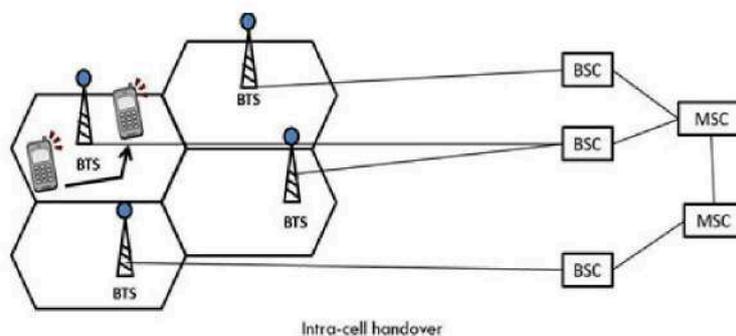


Figure.17. Handover intra BTS

Handover Inter-BTS Intra BSC

- ⇒ Cette forme de handover GSM se produit lorsque le mobile sort de la zone de couverture d'une BTS vers une autre contrôlée par le même BSC. Dans ce cas, le BSC est capable d'effectuer le transfert et il attribue un nouveau canal et un nouveau time-slot au mobile, avant de libérer la communication avec l'ancienne BTS.

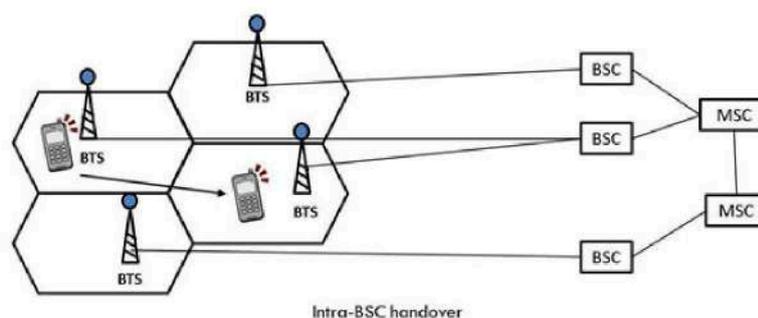


Figure.18. Handover intra BSC

Handover inter-BSC

- ⇒ Lorsque le mobile sort de la zone de cellules contrôlées par un BSC, une forme plus complexe de handover doit être effectuée, passant non seulement d'une BTS à une autre, mais également d'un BSC à un autre. Pour cela, le handover est contrôlé par le MSC.

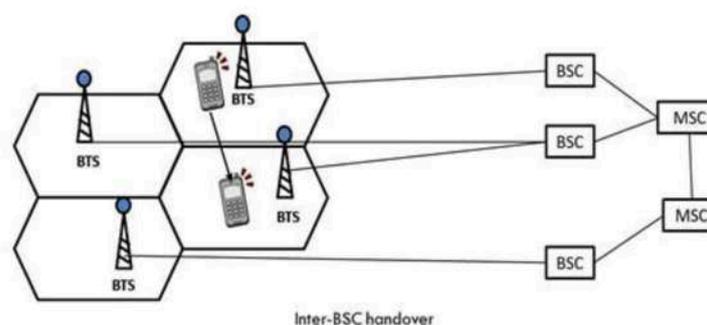


Figure.19. Handover inter BSC

Handover inter-MSC

- ⇒ Cette forme de handover se produit lors du changement entre les réseaux ;
- ⇒ Les deux MSC impliqués négocient pour contrôler le handover ;
- ⇒ Même si ces différents types de transfert concernaient différentes zones du réseau mobile, ils devaient tous être effectués rapidement et efficacement afin que la qualité des appels ne soit pas dégradée et que les appels ne soient pas interrompus.

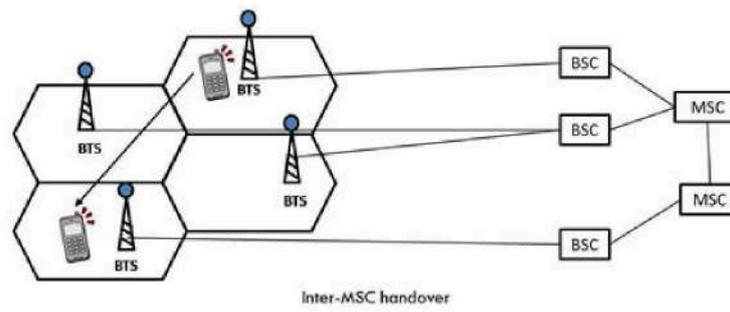


Figure.20. Handover inter MSC