Compte – Rendu de TP

GSM

(Global System for Mobiles)

Julien GUELLEC & Alexandre GERMONNEAU

GTR 202

Étude du GSM avec les :

Sagem OT 160 Sagem OT 260

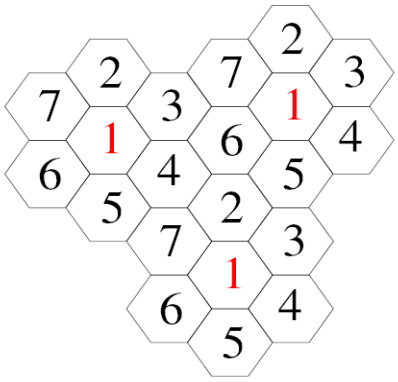
&

1. Introduction

Le GSM *(pour Global System for Mobiles)* est une technologie de téléphone cellulaire. Cette technologie est issue d'un groupe français qui commença son étude à partir de 1982. Elle permet l'accès au RTCP *(Réseau Téléphonique Commuté public)* à partir d'un terminal portatif.

Le GSM opère à 900MHz et à 1,8 GHz en Europe et à 1,9 GHz aux Etats-Unis. Les téléphones GSM comprennent une carte SIM *(Subscriber Identity Module)* qui contient les informations concernant l'utilisateur de l'appareil.

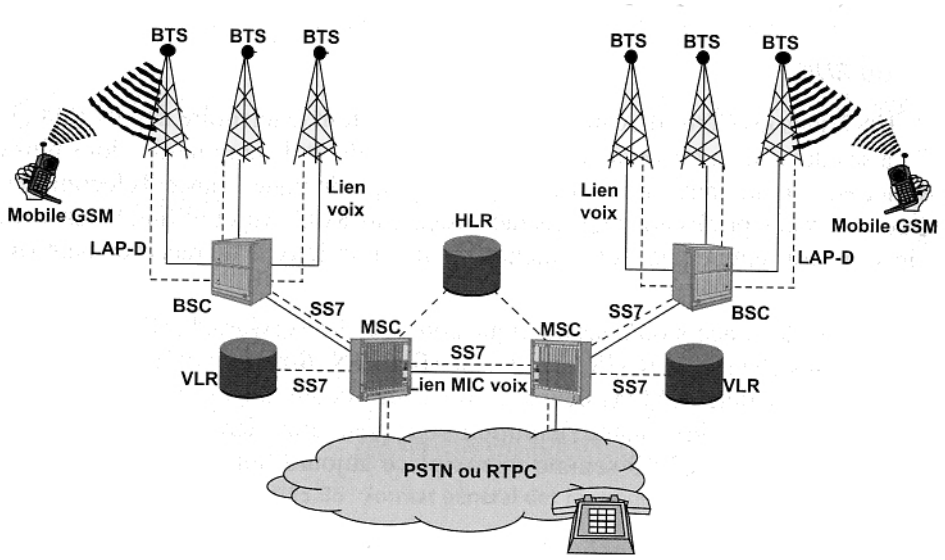
Le GSM repose sur un fonctionnement « cellulaire », c'est-à-dire sur un découpage de la zone géographique en plusieurs cellules :



Chaque cellule GSM dispose d'une Station Radio de Base *(BTS)* qui agit sur un ensemble de canaux radios, différents de ceux utilisés dans les cellules voisines pour éviter les interférences.

Ce mode de subdivision permet d'utiliser à nouveau les mêmes fréquences dans des cellules éloignées.

Cette station BTS est quand à elle reliée à une station BSC qui est en charge de l'allocation des fréquences, de la décision *(éventuelle)* d'un saut de fréquence et de son exécution *(nous verrons plus dans le détails ce dont il en retourne)*. Les stations BSC sont reliées aux MSC qui gèrent, entre autre, les identités temporaires des abonnés *(via les VLR)*, et la commutation avec le réseau RTCP.



En raison du nombre sans cesse croissant d'utilisateurs, les opérateurs sont amenés à réduire le diamètre des cellules pour augmenter la capacité du système *(et donc du nombre d'utilisateurs)*. Une conséquence de ce choix est la diminution de la distance de réutilisation des fréquences, autrement dit de la distance entre deux cellules du même canal.

Enfin, pour terminer cette approche, le standard GSM utilise la technologie d'accès à division de fréquence *(FDMA)* associé à celle d'accès à division de temps *(TDMA)*.

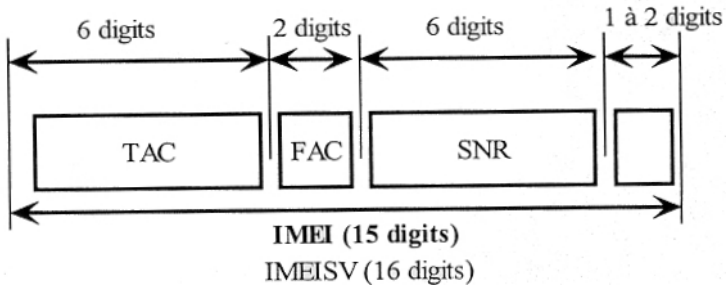
2. Étude des différents numéros d'identification

2.1. Étude de l'IMEI

◊ L'IMEI (*International Mobile Equipment Identity*), est un numéro unique spécifique à chaque mobile *(un peu comme une @MAC pour une carte réseau)*. Il peut être obtenu, sur la plupart des téléphones, par la combinaisons des touches *#06#.

En cas de vol, la déclaration du code IMEI permet d'interdire l'accès au réseau à ce mobile. Il est inscrit dans le logiciel, mais peut être reprogrammé *(à l'aide d'un logiciel adéquat)*.

L'IMEI est codé sur 15 digits (ou 16 pour l'IMEISV). Il se découpe ainsi :



- le TAC *(Type Approval Code)* : codé sur 6 digits fourni au constructeur lorsque le mobile à passé l'agrément,
- le FAC *(Final Assembly Code)* : codé sur 2 digits et identifie l'usine de fabrication,
- le SNR *(Serial Number)* : codé sur 6 digits,
- Spare : codé sur 1 ou 2 digits et représente la version logiciel du terminal.

◊ Nous relevons le code IMEI du mobile OT160 : **350833 82 004647 2**, soit :

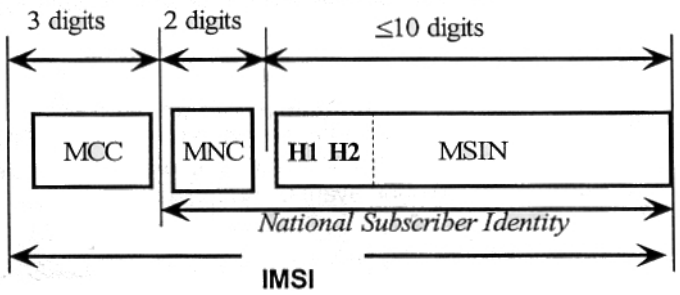
- le TAC : **350833**
- le FAC : **82**
- le SNR : **004647**
- Spare : **2**

◊ Le code identifiant l'usine ayant fabriqué l'appareil est le FAC, soit ici **82**. Ce numéro n'a absolument aucun rapport avec le numéro de téléphone associé à l'abonnement, puisque *(heureusement pour les constructeurs)*, une usine fabrique plus d'un téléphone ! Ce numéro permettra, en cas de défaut de l'appareil, de retrouver une trace de sa construction *(et de virer le technicien qui à fait la bourde !)*.

2.2. Étude de l'IMSI

◊ L'IMSI (*International Mobile Subscriber Identity*), est un numéro *(unique)* identifiant l'abonné. Il est confidentiel et transmis le moins souvent possible pour éviter qu'une personne se fasse passer pour l'abonné. L'IMSI est invariant dans le temps, il sera renouvelé que si l'utilisateur change de carte SIM *(celui-ci étant stocké dessus)*. C'est d'ailleurs « à cause » de ce numéro qu'on demande, lors de la première souscription d'un abonnement, une pièce d'identité au client.

L'IMSI est codé sur 15 digits *(mais sur 18 dans la carte SIM)* et se compose ainsi :



- le MCC *(Mobile Country Code)* : codé sur 3 digits et identifie l'indicatif du pays domicile de l'abonné,

- le MNC *(Mobile Network Code)* : indicatif identifiant l'opérateur,

- le MSIN *(Mobile Subscriber Identification Number)* qui est le numéro de l'abonné à l'intérieur du réseau GSM.

◊ Nous relevons le code IMSI de la carte SIM : **08 2 9 80102510261759**, soit :

- longueur de l'IMSI : **08** (<=> 8 octets <=> 15 digits)
- premier digit du MCC : **2 [...]**
- codage bit de parité : **9**
- reste de l'IMSI :
  - MCC : **[...] 80**
  - MNC : **10**
  - MSIN : **2510261759**

sachant que pour décoder les informations citées ci-dessus, nous devons inverser 2 à 2 les 10 derniers digits, le décryptage de l'IMSI de notre carte SIM est le suivant :

- longueur de l'IMSI : **08**
- premier digit du MCC : **2 [...]**
- codage bit de parité : **9**
- reste de l'IMSI :
  - MCC : **[...] 08** (208 <=> France)
  - MNC : **01** (<=> France Télécom)
  - MSIN : **5201627195** (<=> numéro identifiant l'abonné)

◊ Nous avons déjà expliqué que ce numéro était personnel, et unique à l'abonné. Il permet de l'identifier sur le réseau GSM et est strictement confidentiel. C'est pour cette raison qu'il est stocké sur la carte SIM, un peu comme une carte d'identité qu'un individu porte dans son porte-feuilles et qui l'identifie lui, et lui seul.

Ce numéro à un rapport avec le numéro de téléphone « classique » associé à l'abonnement dans la mesure où il permet d'identifier l'abonné, et donc, de retrouver son numéro d'appel.

2.3. Étude du TMSI

◊ Nous venons de voir que l'IMSI était confidentiel et qu'on évitait, autant que possible, de le transmettre sur le réseau GSM. C'est pour cela qu'est introduit le TMSI (*Temporary Mobile Subscriber Identity*) qui à pour rôle de remplacer, provisoirement, l'IMSI et donc d'identifier l'abonné. Ce numéro est renégocié régulièrement auprès de la station BTS locale.

◊ Nous relevons le code TMSI qui nous à été attribué : **01 BE B5 ED**. Nous constatons qu'il est codé sur 8 digits *(soit 10 digits de moins que l'IMSI)*. Cela n'est probablement pas un hasard, puisqu'un numéro d'appel « classique » est codé sur 10 digits, et que nous voulons, ici, garder le plus de confidentialité possible.

2.4. Les autres numéros présents dans la carte SIM

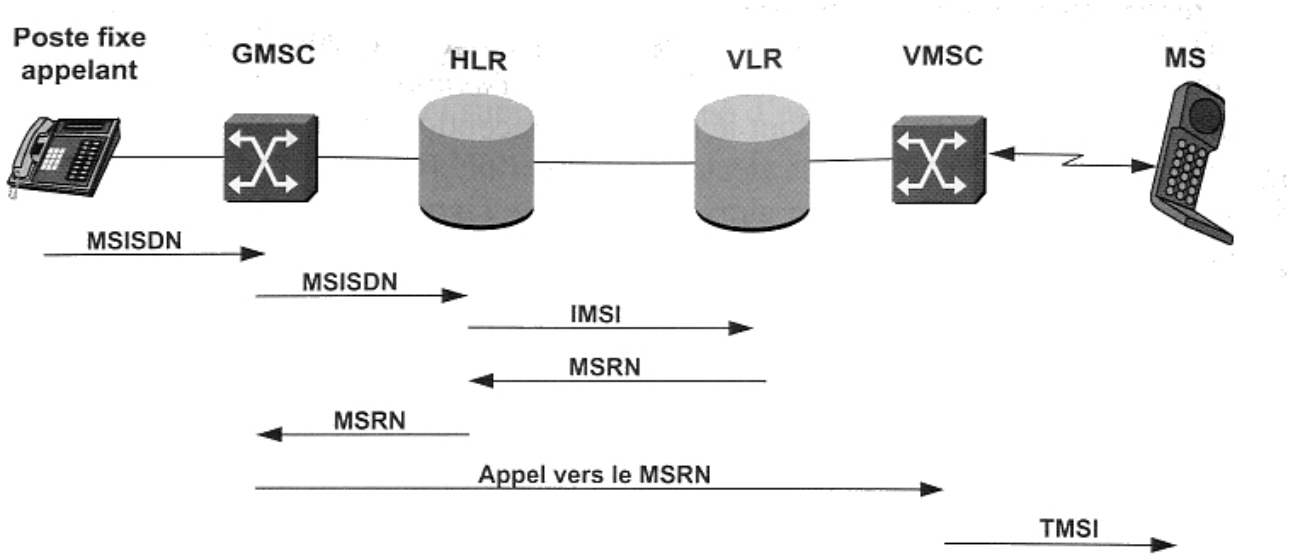
◊ Analysons les autres numéros que nous pouvons trouver sur la carte SIM :

(dans le menu SIM Info)

- KC info
- IMSI
- Lock Info
- Liste BA
- Rx préférés
- Rx interdits
- Groupe ID1
- Groupe ID2
- Administration

2.5. Conclusion

	IMEI	IMSI	TMSI
Identification du mobile auprès du réseau lors de la première mise sous tension	✗	✓	✗
Connaître le numéro de l'abonné	✗	✓	✗
Faire un appel sortant, une fois que le mobile est identifié par le réseau	✗	✗	✓
Faire un appel entrant, une fois que le mobile est identifié par le réseau	✗	✗	✓
S'assurer que le terminal n'est pas un appareil volé	✓	✗	✗
S'assurer que l'abonné a bien le droit d'utiliser le réseau	✗	✓	✗



Lorsqu'une personne, sur un poste fixe, veut joindre une autre personne sur son téléphone portable :

- il commence par composer son numéro « classique » *(<=> le MSISDN de la forme 06 87 81 03 69)*,
- L'appel est acheminé jusqu'à une passerelle *(<=> le GMSC)* qui va gérer la commutation entre le RTCP et le réseau GSM *(cf Introduction)*,
- Le GMSC interroge ensuite le HLR pour savoir où se trouve l'abonné à joindre, toujours avec le numéro MSISDN,
- Le HLR va substituer le MSISDN par l'IMSI et interroger le VLR pour avoir l'identité temporaire de l'abonné.
- Le VLR substitue l'IMSI par le MSRN *(pour plus de confidentialité)* et le retourne à l'HLR,
- ce dernier le renvoie à son tour au GMSC, qui va interroger son collègue le VMSC,
- qui va, enfin, substituer le MSRN par le TMSI et établir la liaison avec l'abonné.

3. Étude de l'interface radio (couche 1)

3.1. Rappel de cours

◊ Nous avons déjà parlé des types de multiplexages utilisés *(simultanément)* sur le réseau GSM. Ces derniers sont :

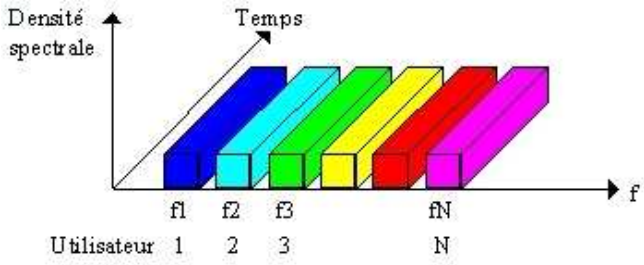
- technologie d'accès à division de fréquence : FDMA
- technologie d'accès à division de temps : TDMA

Voyons les un peu plus dans le détail :

a) Le FDMA (*Frequency Division Multiple Access*)

L'accès multiple par répartition en fréquence (ou AMRF, en anglais Frequency Division Multiple Access ou FDMA) est un mode de multiplexage destiné à la téléphonie mobile.

Il s'agit d'un découpage en bande de fréquences de manière à attribuer une partie du spectre à chaque utilisateur. De cette manière, chaque utilisateur se voit attribué une bande de fréquences distincte.

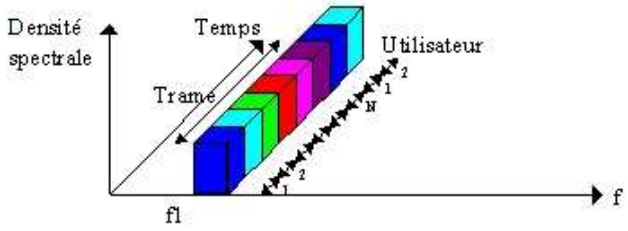


En GSM, N = 124 canaux

b) Le TDMA *(Time Division Multiple Access)*

Le TDMA est une méthode d'accès qui se base sur la répartition de ressources dans le temps. Chaque utilisateur émet ou transmet dans un intervalle de temps concret dont la périodicité est définie par la durée de la trame.

Dans ce cas, pour écouter l'utilisateur N, le récepteur n'a qu'à considérer l'intervalle de temps N associé à cet utilisateur.



En GSM, N = 8 Time Slots

=> En combinant ces 2 technologies de multiplexage, on arrive, pour le GSM, à utiliser :

124 x 8 = 992 canaux

ce qui n'est évidemment pas cohérent avec le nombre d'utilisateurs de téléphones mobiles, soit environ 42 382 800 au 2ème trimestre 2005 !!!

=> Pour pallier à ce problème, nous allons étudier, un peu plus loin, le réseau cellulaire.

c) Le Fading

◊ Le fading est la diminution momentanée de la puissance d'un signal radioélectrique à l'entrée d'un récepteur, due aux conditions de propagation des ondes.

Le fading *(ou l'évanouissement du signal)* est le résultat de la somme algébrique des ondes (directes + réfléchies) :

- Les ondes sont en phases, le signal reçu est amplifié,
- Les ondes sont en opposition de phase, le signal est atténué => évanouissement.

Pour pallier aux fadings, on émet en changeant de porteuse régulièrement, d'une façon pseudo-aléatoire. L'évanouissement va apparaître à fréquence donné, à un moment donné, en un lieu donné et en fonction des réflections multiples et trajets de l'onde, des immeubles, des voitures, etc...

En changeant de fréquence constamment on transmet les données sur une multitudes de porteuses. Les canaux *(suite de fréquences porteuses)* sont définis et chaque portable commute d'un canal à l'autre sans chevauchement de fréquences, même si elles sont proches : c'est le principe du Handover.

3.2. Analyse spectrale

Voies descendantes :

	Fmin (MHz)	***Fmax (Mhz)***
GSM	935 + (0,2 x 1) = **932,2**	935 + (0,2 x 124) = **959,8**
DCS 1800	1805,2 + [0,2 x (512 – 512)] = **1805,2**	1805,2 + [0,2 x (885 – 512)] = **1879,8**
E-GSM	935 + [0,2 x (975-1024)] = **925,2**	935 + [0,2 x (1024-1024)] = **935**

Voies montantes :

	Fmin (MHz)	***Fmax (Mhz)***
GSM	932,2 – 45 = **887,2**	959,8 – 45 = **914,8**
DCS 1800	1805,2 – 45 = **1760,2**	1879,8 – 45 = **1834,8**
E-GSM	925,2 – 95 = **830,2**	935 – 95 = **840**

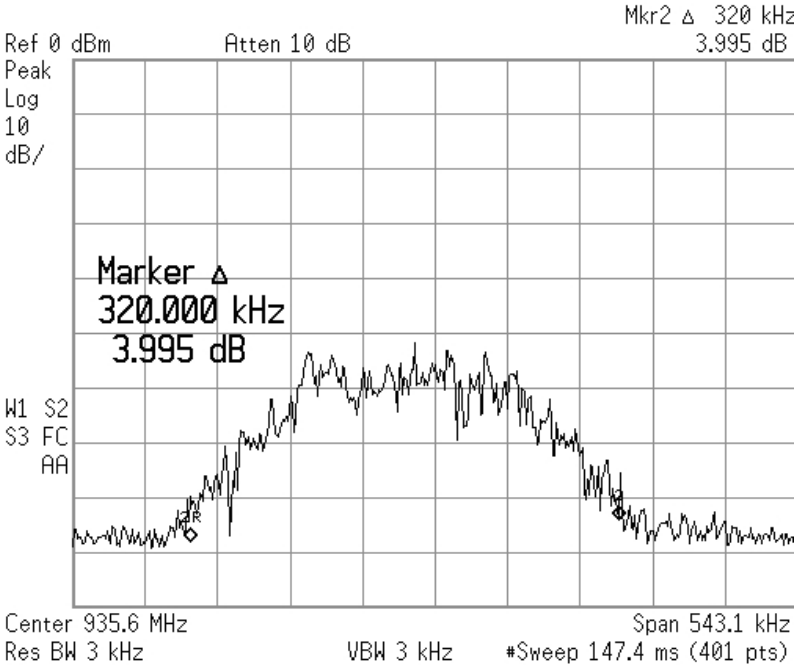
◇ On force maintenant l'OT 160 à utiliser la bande GSM uniquement :

(menu (4) > Forcing Functions > set band > 900 MHz)

◇ On règle l'analyseur de spectre pour visualiser la bande descendante du GSM :

(Fmin = 930 Mhz [...] Fmax = 960 Mhz)

◇ <u>Puis on relève le chronogramme suivant, correspondant à la voie balise</u> :



La voie balise permet au mobile de se raccorder en permanence à la station BTS la plus favorable.

Il mesure la puissance du signal reçu sur la voie balise correspondant à une fréquence particulière de l'ensemble des fréquences allouées à cette station.

Lors d'une mise sous tension, pendant l'état de veille et pendant une communication, le mobile scrute les voies balises pour connaître les stations avoisinantes susceptibles de l'accueillir en cas de Handover.

Cette voie balise étant émise en permanence, nous l'utilisons pour mesurer la largeur d'une voie de conversation, soit ici : **320 kHz**.

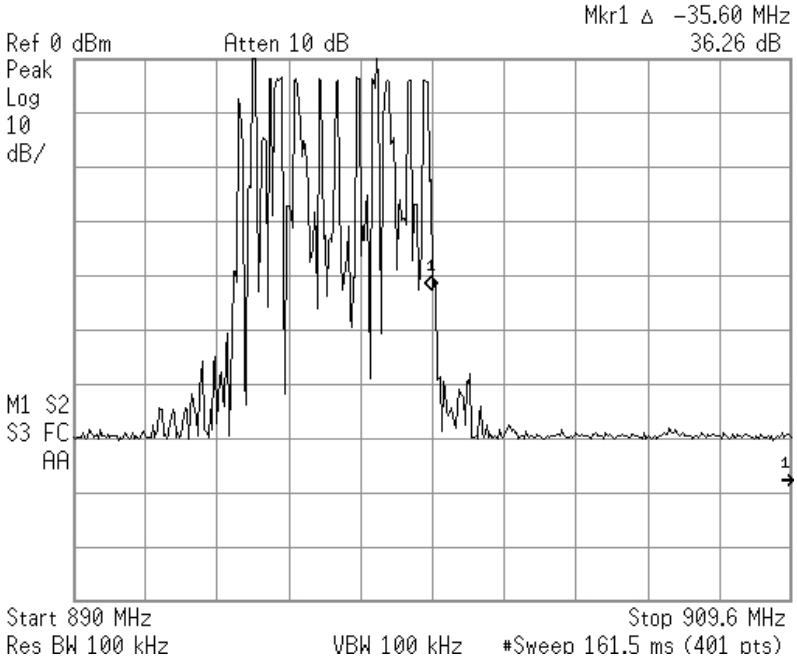
En comparant ce résultat au critère de Nyquist pratique *(B = 0,8 x R)*, on trouve :

Théorique :	0,8 x 270 = 216
Pratique :	0,8 x 320 = 256

◇ Réglons maintenant l'analyseur de spectre pour visualiser la voie montante :

(Fmin = 890 Mhz [...] Fmax = 915 Mhz)

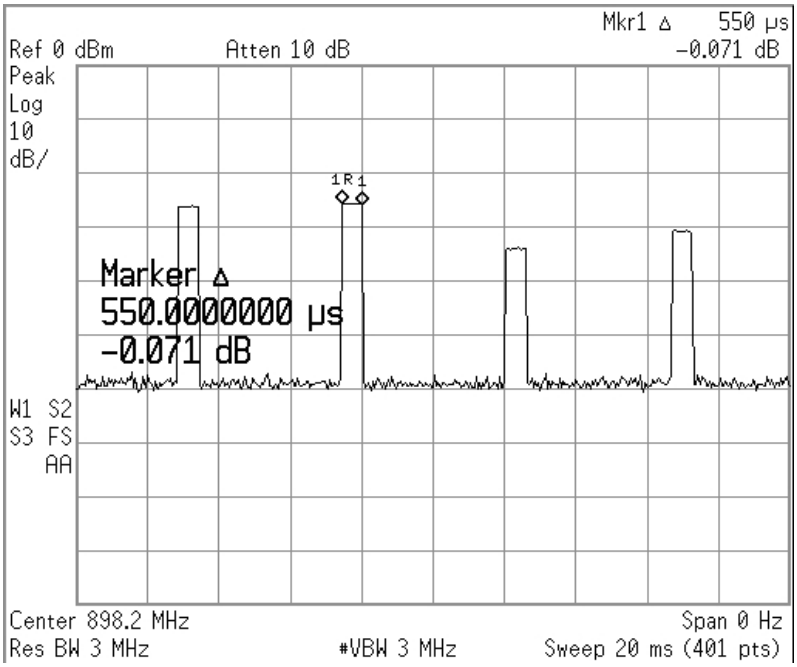
◇ On relève le chronogramme suivant :



Pour pouvoir observer ce chronogramme, nous avons émit un appel vers le numéro de la boîte vocale orange *(888)*.

Tous les « pics » que l'on aperçoit sur ce chronogramme sont en fait les différentes porteuses, utilisées par l'appareil pour porter notre signal lors de la « conversation ».

◇ Maintenant, nous paramétrons l'analyseur de spectre pour pouvoir observer, de plus près, l'une de ces porteuse. On relève le chronogramme suivant :



Nous observons plusieurs « pics » qui correspondent en fait à des bursts : c'est le moment où notre mobile parle. Le réseau GSM autorise se dernier à émettre ces bursts, pendant un intervalle de temps définis *(appelé Time Slot)* et qui dure *(pour le TDMA utilisé en GSM)* 576,92 µs. Ici nous trouvons 550 µs.

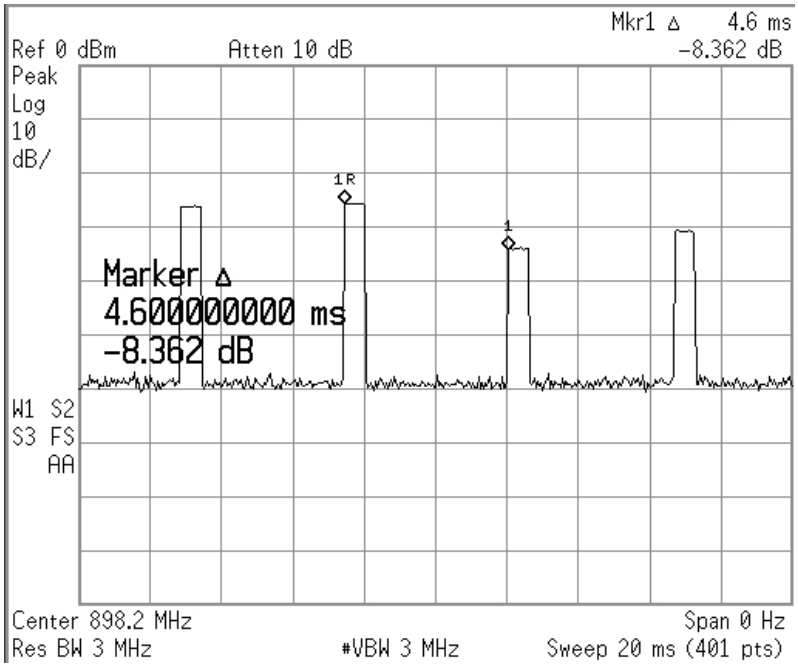
Le reste du temps *(intervalles entre les bursts)* est alloué à 7 autres utilisateurs.

C'est le principe du TDMA qui découpe la bande passante pour la distribuer à plusieurs utilisateurs.

Nous savons également que la trame TDMA *(celle qui regroupe les 8 utilisateurs),* dure :

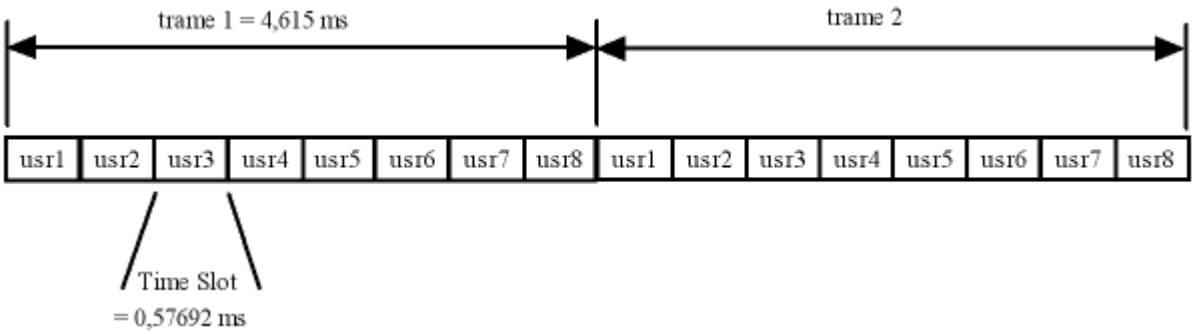
0,57692 x 8 = **4,61536 ms**

Ce que nous nous empressons de vérifier :



On trouve ici, entre les 2 markers, un intervalle de temps de 4,6 ms, ce qui correspond à la valeur théorique.

=> Notre téléphone « parle » tout les 4,6 ms



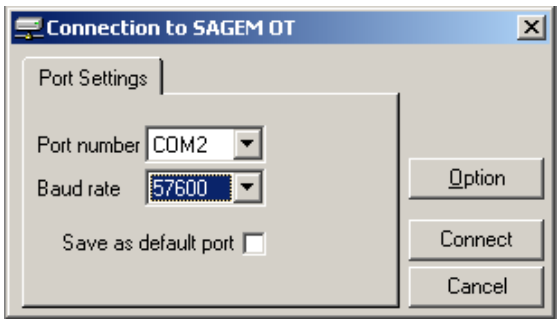
Ce schéma résume ce que nous venons d'aborder :

- 1 trame est composée de 8 Time Slots et dure 4,615 ms => elle permet à 8 utilisateurs de se partager le temps sur 1 même fréquence,

- chaque Time Slot dure 0,57692 ms, et permet l'émission de bursts.

3.3. Fréquences / canaux

◊ Nous connectons maintenant l'OT 160 au port série de l'ordinateur. Puis nous lançons OT Drive, le logiciel de gestion du mobile, qui va nous servir dans la suite du TP. Une fois OT Drive lancé, nous réalisons la connexion avec l'appareil :



On sait que la répartitions des 124 canaux GSM est déterminée de la manière suivante :
(source : http://www.art-telecom.fr)

valeur de n	fréquences centrale du canal (MHz)		
	bande basse	bande haute	
1 n 124	890 + 0,2n	935 + 0,2n	sous-bande A (900)
n = 0	890 + 0,2n	935 + 0,2n	sous-bande B (900)
975 n 1023	890 + 0,2(n-1024)	935 + 0,2(n-1024)	sous-bande B (900)
512 *n* 885	1710,2 + 0,2(*n*-512)	1805,2 + 0,2(*n*-512)	GSM 1800

◊ Avec la fonction *scanning*, on relève maintenant les 10 plus forts canaux suivants, et l'on en déduit les fréquences associées, avec les formules du tableau ci-dessus :

CANAL	3	107	113	10	78	93	90	109	117	102
BSIC (NCC – BCC)	2 – 7	0 – 1	0 – 6	1 – 0	0 – 1	0 – 3	0 – 7	0 – 4	0 – 2	0 -5
Rx_Level (dBm)	-50	-66	-70	-74	-74	-76	-78	-79	-79	-81
Fréquence basse (MHz)	890,6	911,4	912,6	892	905,6	908,6	908	911,8	913,4	910,4
Fréquence haute (Mhz)	935,6	956,4	957,6	937	950,6	953,6	953	956,8	958,4	955,4
Puissance$_{reçue}$ (W)	10^{-8}	$2{,}5\times10^{-10}$	10^{-10}	4×10^{-11}	4×10^{-11}	$2{,}5\times10^{-11}$	$1{,}6\times10^{-11}$	$1{,}2\times10^{-11}$	$1{,}2\times10^{-11}$	8×10^{-12}

Et les conversations dBm => Watt de la manière suivante :

$$P(Watts) = 10^{-3} * 10^{\frac{PdBm}{10}}$$

◊ Nous relevons les canaux des voies balises présentent à portée du mobile (Orange) :
(dans le menu Network)

	BCCH	**BSIC**	**Rx_Lvl**
Serving cell	0003	2 - 7	-50
Neighbouring cell 1	0010	1 - 0	-74
Neighbouring cell 2	0002	* * *	-73
Neighbouring cell 3	0005	3 - 7	-74
Neighbouring cell 4	0011	1 - 1	-83
Neighbouring cell 5	0007	1 - 7	-85
Neighbouring cell 6	0009	* * *	-91

Le canal BCCH *(Broadcadt Control Channel)* que nous relevons ici, est un canal caractéristique de la cellule à laquelle il appartient *(différent d'une cellule à une autre)*. Il permet la diffusion de données la caractérisant.

Le BSIC *(Base Station Identify Code)* est composé du :

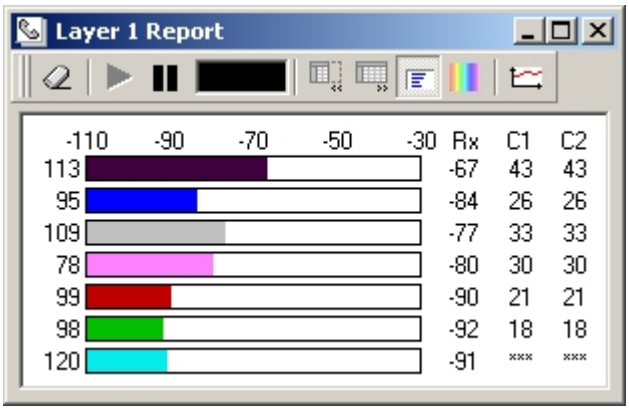
- NCC *(Network Color Code)* : permet de différencier 2 opérateurs GSM. Il est codé sur 3 bits = 2^3=8 valeurs possibles
- BCC (BTS Color Code) : numéro attribué à la BTS pour la différencier d'une autre utilisant le même canal.

Ensembles (NCC + BCC) forment le BSIC qui permet de différencier 2 BTS utilisant le même canal.

Le Rx_Level est, quand à lui, la mesure sur ½ seconde du champs reçu par le mobile. Il est exprimé ici en dBm.

◇ Nous recommençons la manip avec une carte SIM de l'opérateur SFR :
(dans le menu Network)

	BCCH	BSIC	Rx_Lvl
Serving cell	0113	0 - 6	-66
Neighbouring cell 1	0095	0 - 3	-84
Neighbouring cell 2	0109	0 - 4	-78
Neighbouring cell 3	0078	0 - 1	-79
Neighbouring cell 4	0099	0 - 6	-86
Neighbouring cell 5	0118	* * *	-92
Neighbouring cell 6	0098	0 - 2	-92



- On remarque que le mobile est cette fois « accroché » à la cellule diffusant le canal 0113 et que les numéros des canaux des cellules voisines sont plus élevés. Cela provient du fait que, ces derniers ont été attribués de la façon suivante :

Pour le GSM à 900 Mhz *(c'est-à-dire entre Orange et SFR, Bouygues utilisant des fréquences plus hautes)* les 124 canaux disponibles sont répartis ainsi :

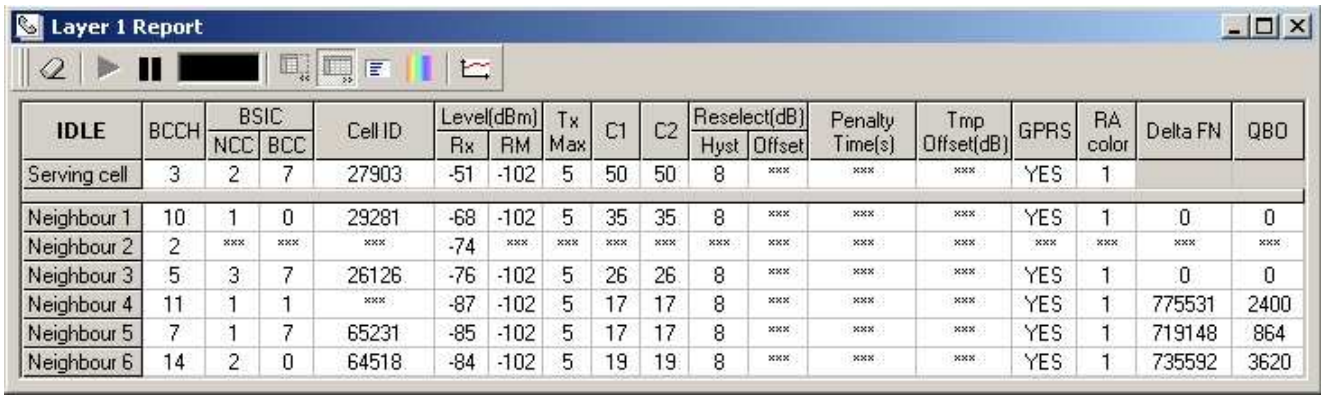
- Orange (zones très denses) : 62 canaux => 1 [...] 62
- SFR (zones très denses) : 62 canaux => 63 [...] 124

- De plus : le NCC de la cellule serveuse SFR (« 0 ») est différent de celui de la cellule serveuse Orange (« 2 »), ce qui indique bien que nous ne sommes plus sur le même réseau opérateur que tout à l'heure.

- On remarque aussi que les niveaux de réception *(Rx_Level)* du réseau SFR sont un petit moins bon que ceux relevés tout à l'heure avec le réseau Orange.

3.4. Structure cellulaire du réseau GSM

◇ Avec la fonction Layer 1 Report, on relève les caractéristiques suivantes :



IDLE	BCCH	BSIC NCC	BSIC BCC	Cell ID	Level(dBm) Rx	Level(dBm) RM	Tx Max	C1	C2	Reselect(dB) Hyst	Reselect(dB) Offset	Penalty Time(s)	Tmp Offset(dB)	GPRS	RA color	Delta FN	QBO
Serving cell	3	2	7	27903	-51	-102	5	50	50	8	***	***	***	YES	1		
Neighbour 1	10	1	0	29281	-68	-102	5	35	35	8	***	***	***	YES	1	0	0
Neighbour 2	2	***	***	***	-74	***	***	***	***	***	***	***	***	***	***	***	***
Neighbour 3	5	3	7	26126	-76	-102	5	26	26	8	***	***	***	YES	1	0	0
Neighbour 4	11	1	1	***	-87	-102	5	17	17	8	***	***	***	YES	1	775531	2400
Neighbour 5	7	1	7	65231	-85	-102	5	17	17	8	***	***	***	YES	1	719148	864
Neighbour 6	14	2	0	64518	-84	-102	5	19	19	8	***	***	***	YES	1	735592	3620

En plus du BCCH, BSIC (NCC + BCC) et du Rx_Level, nous trouvons d'autre informations telles que :

- **Cell ID** : représente le numéro d'identité de la cellule dans la zone de localisation

- **C1 :** Critère d'affaiblissement. Ce critère a pour objet de s'assurer qu'une communication entre le mobile et la BTS serait possible dans les 2 sens *(montants et descendants).*

- **C2 :** Critère de re-sélection de cellules. C2 = C1 + différents paramètres de contrainte. Pour la re-sélection de cellule, le mobile utilise le critère C2. il peut comporter une composante temporelle *(Penalty time, Temporary Offset, et Cell Reselect Offset)* afin de défavoriser une cellule pendant un temps donné. La re-sélection de cellule en mode veille est toujours à l'initiative du mobile.

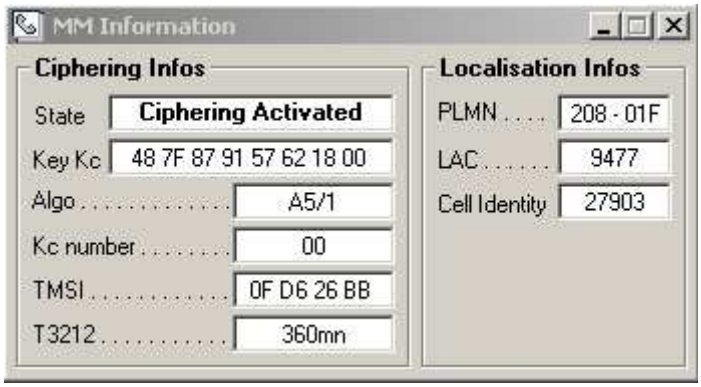
- [...] encore beaucoup d'autres paramètres, comme par exemple si la cellule supporte le GPRS etc...

◊ En comparant les résultats que nous venons de relever avec OTDrive, et les résultats obtenus, tout à l'heure, directement à partir du mobile *(page 12)*, nous nous apercevons que :

- la cellule serveuse *(BCCH = 3)*, est toujours la même,
- elle possède toujours le meilleur niveau de champs Rx_Level.
- les cellules voisines varient légèrement : par exemple, nous nous apercevons que la numéro 9 à disparue, laissant sa place à la numéro 14,
- et enfin que les niveaux de réceptions ne sont plus exactement les mêmes

globalement, la réception des caractéristiques des cellules se fait de la même manière *(le mobile n'ayant pas beaucoup bougé !!)*, et les niveaux varient légèrement. La cellule avec le canal BCCH 10 pourrait servir de cellule serveuse... Nous en ferons l'expérience par la suite.

◊ <u>Utilisons maintenant la fonction MM Information de OTDrive</u> :



on s'intéresse à la fenêtre de droite, dans laquelle on trouve :

PLMN *(Public Land Mobile Network),*

LAC *(Location Area Code),*

CI *(Cell Identity).*

Le PLMN permet d'identifier le réseau GSM d'un opérateur dans un pays :

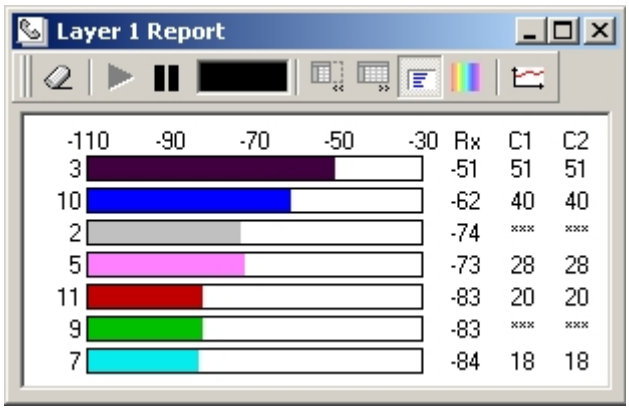
- 208 <=> France
- 01F <=> Orange France *(Itineris)*

Le LAC est la zone de localisation au sein du PLMN :

- les cellules sont regroupées par zones géographiques et à chaque zone est attribuée un LAC. Ces zones peuvent être plus ou moins grandes selon la densité de la surface couverte, en moyenne quelques dizaines de kilomètres.
- A l'intérieur de ces LAC, chaque cellule possède un numéro d'identifiant unique: le CI. C'est la différence fondamentale qu'il existe entre le LAC et le CI.

◇ Nous allons maintenant forcer le mobile à s'accrocher sur la fréquence d'une cellule voisine. Nous utiliserons pour cela la fonction « forcing BCCH » de OTDrive.

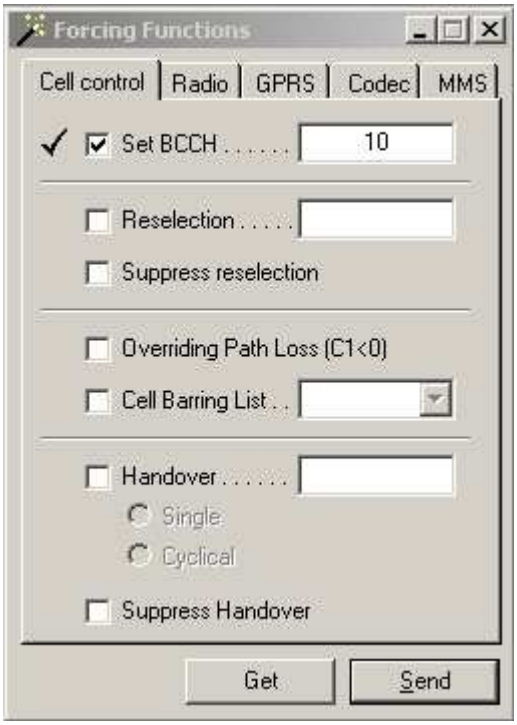
Tout d'abord, nous devons déterminer quelle cellule voisine serait le plus susceptible d'être utilisée comme cellule serveuse. Nous jetons un coup d'oeil aux Rx_Levels du moment :



clairement, les résultats que nous avons annoncés précédemment sont confirmés, et nous pouvons utiliser la cellule BCCH = 10 comme cellule serveuse :

c'est celle qui est la mieux reçue, à ce moment et à cet endroit, par le mobile.

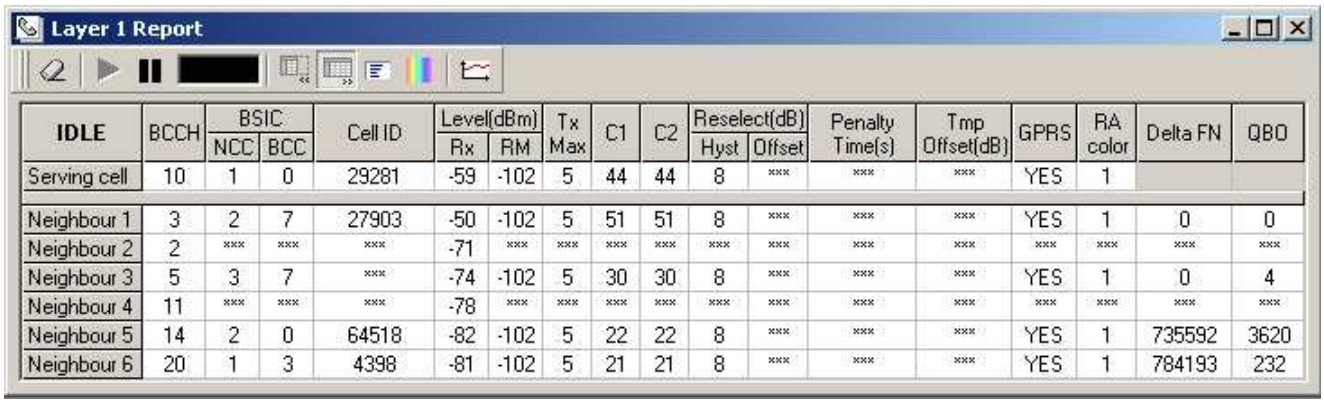
Nous forçons donc le mobile sur cette cellule =>



La procédure est assez simple :

- on indique le numéro de BCCH
- on clique sur « Send »

Le résultat est quasi immédiat, et l'affichage que nous avions dans la fenêtre « Layer 1 Report » à la *page 13 (où le BCCH de la cellule serveuse était le numéro 3)* change de la manière suivante :

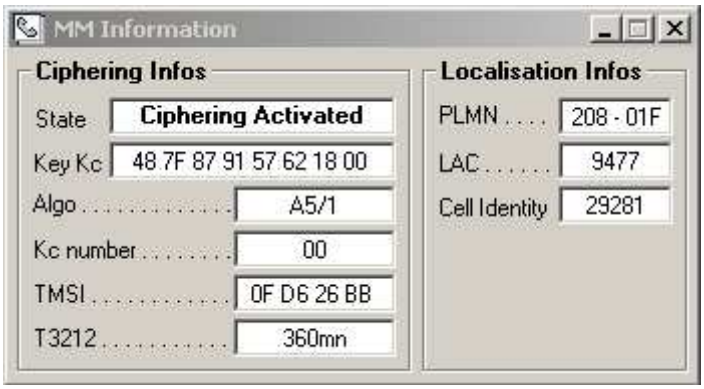


IDLE	BCCH	BSIC		Cell ID	Level(dBm)		Tx Max	C1	C2	Reselect(dB)		Penalty Time(s)	Tmp Offset(dB)	GPRS	RA color	Delta FN	QBO
		NCC	BCC		Rx	RM				Hyst	Offset						
Serving cell	10	1	0	29281	-59	-102	5	44	44	8	***	***	***	YES	1		
Neighbour 1	3	2	7	27903	-50	-102	5	51	51	8	***	***	***	YES	1	0	0
Neighbour 2	2	***	***	***	-71	***	***	***	***	***	***	***	***	***	***	***	***
Neighbour 3	5	3	7	***	-74	-102	5	30	30	8	***	***	***	YES	1	0	4
Neighbour 4	11	***	***	***	-78	***	***	***	***	***	***	***	***	***	***	***	***
Neighbour 5	14	2	0	64518	-82	-102	5	22	22	8	***	***	***	YES	1	735592	3620
Neighbour 6	20	1	3	4398	-81	-102	5	21	21	8	***	***	***	YES	1	784193	232

◊ Nous venons donc de forcer le mobile à utiliser la cellule avec le canal BCCH 10. Voyons à présent comment ont évolué le LAC et le CI…

Nous avons déjà décrits à quoi correspondaient le LAC & le CI. Logiquement, après la manipulation que nous venons de faire, nous devrions récupérer le même LAC *(le mobile n'a pas changé de zone géographique)*, mais le CI doit être différent dans la mesure où le mobile est accroché sur une autre cellule, et que, par conséquent, le numéro d'identification de celle-ci ne peut être le même…

Vérifions ceci à l'aide de la fonction « MM Information » :



dans la fenêtre de droite, nous constatons que :

- le PLMN est le même *(on est toujours sur le réseau Orange France)*
- le LAC est le même
- le CI est bien différent

=> ce qui confirme nos résultats.

En changeant la cellule serveur, nous avons, bien évidemment, changé de BSIC.

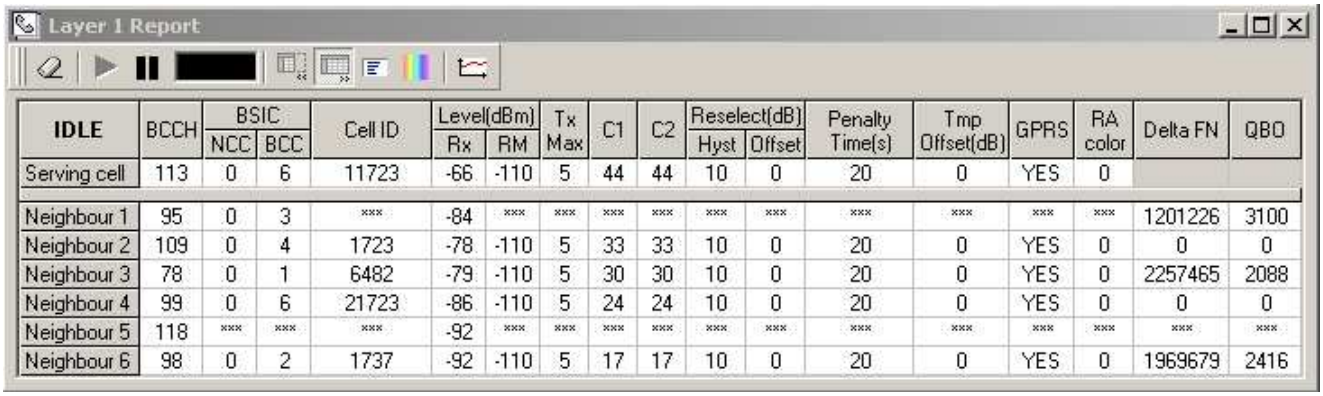
Ce dernier change obligatoirement, au moins pour le BCC *(rappelons que c'est le numéro attribué à la BTS pour la différencier d'une autre qui utiliserait le même canal)*.

◊ Changeons maintenant notre carte SIM Orange pour une carte SIM SFR. Les résultats obtenus concernant les caractéristiques des différentes cellules figurent en haut de la page 13.

Les fréquences associées à cet opérateur ne sont pas les mêmes que pour Orange : nous avons déjà vu que les 124 canaux GSM disponibles étaient équitablement répartis entre les 2 opérateurs *(62 – 62)*.

Cette nécessité *(en dehors des enjeux commerciaux)* provient du fait que Orange et SFR veulent, tous les 2, pouvoirs couvrir la France entière, sans se perturber l'un l'autre !

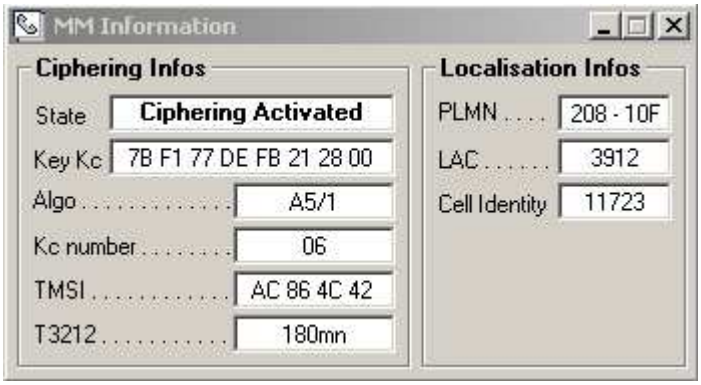
Dans le cas de SFR, nous avons vu que les canaux qui lui étaient attribués étaient compris entre 63 et 124. Nous pouvons confirmer les résultats obtenus à la page 13 en ouvrant la fenêtre « Layer 1 Report » :



IDLE	BCCH	BSIC		Cell ID	Level(dBm)		Tx Max	C1	C2	Reselect(dB)		Penalty Time(s)	Tmp Offset(dB)	GPRS	RA color	Delta FN	QBO
		NCC	BCC		Rx	RM				Hyst	Offset						
Serving cell	113	0	6	11723	-66	-110	5	44	44	10	0	20	0	YES	0		
Neighbour 1	95	0	3	***	-84	***	***	***	***	***	***	***	***	***	***	1201226	3100
Neighbour 2	109	0	4	1723	-78	-110	5	33	33	10	0	20	0	YES	0	0	0
Neighbour 3	78	0	1	6482	-79	-110	5	30	30	10	0	20	0	YES	0	2257465	2088
Neighbour 4	99	0	6	21723	-86	-110	5	24	24	10	0	20	0	YES	0	0	0
Neighbour 5	118	***	***	***	-92	***	***	***	***	***	***	***	***	***	***	***	***
Neighbour 6	98	0	2	1737	-92	-110	5	17	17	10	0	20	0	YES	0	1969679	2416

On remarquera au passage que le NCC du BSIC à changé (« 2 » pour Orange « 0 » pour SFR).

Le LAC et le CI ont également changés, cette fois tous les 2 :

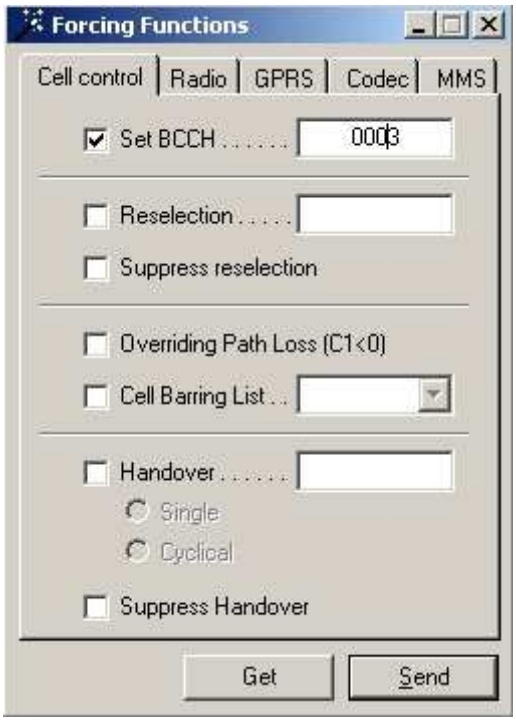


- le CI, pour des raisons évidentes *(non seulement nous ne sommes plus sur la même cellule, mais en plus chez un autre opérateur !),*
- et le LAC, pour cette dernière raison : nous sommes cette fois sur le réseau SFR, et il n'y a aucune raison que cet opérateur ait attribué les mêmes aux mêmes endroits !

Le PLMN n'est également plus le même :

- nous sommes toujours en France *(si,si!)* : 208
- nous sommes sur SFR : 10F

◊ <u>Contrarions maintenant le mobile à se brancher sur une cellule de chez Orange…</u> Pour ce faire, nous choisissons d'utiliser la cellule serveuse que nous avions tout à l'heure par défaut chez Orange, celle diffusant le canal BCCH 3.



Le mobile s'accroche bien sur le canal de la cellule concurrente et l'affichage du logo opérateur SFR sur l'écran de celui-ci disparaît.

Il n'est pas possible d'établir de communication *(le mobile refuse de numéroter)*, et lorsqu'on essaye de joindre l'abonné à partir d'un autre mobile, on tombe directement sur la messagerie.

=> l'abonné n'est pas présent dans la VLR, et pour l'opérateur le mobile est considéré comme éteint.

Enfin, nous avons remarqué que le mobile, tout seul, cherchait à se remettre sur une cellule SFR.

4. Étude du protocole (couche 2 & 3) lors d'une connexion au réseau

◊ Classification des canaux :

BCH (Broadcast Channels) Canal descendant sur lequel sont diffusés des messages courts spécifiques, utilisant la voie balise	**FCCH** (Frequency Correction Channel)	Canal permettant à un mobile de se caler sur la fréquence nominale d'une BTS.
	SCH (Synchronisation Channel)	Canal de synchronisation dont les burst, diffusés par la BTS ont une séquence d'apprentissage. Il permet au mobile de se synchroniser sur la BTS.
	BCCH (Broadcast Control Channel)	Canal sur lequel sont diffusées régulièrement des informations de la cellule vers le mobile en veille. Il diffuse des infos sur les règles d'accès à la cellule courante et aux cellules voisines.
CCCH (Common Control Channels) canaux partagés par tous les usagers, dans les 2 sens.	**PCH** (Paging Channel)	Canal logique supportant l'ensemble des appels en diffusion. lorsque le réseau désire communiquer avec un mobile, elle diffuse l'identité du mobile sur un ensemble de cellules d'une zone de localisation via le PCH.
DCCH (Dedicated Control Channels) canaux dédiés de contrôle	**SDCCH** (Stand Alone Dedicated Control Channel)	Canal de signalisation dédié (assignation d'un canal TCH, mise à jour de localisation etc..)
	SACCH (Slow Associated Control Channel)	Supervision de la liaison. Canal de contrôle lent faible débit (380 bit/s), associé à tout canal dédié (TCH ou SDCCH) permettant d'en effectuée la supervision
	FACCH (Fast Associated Control Channel)	Utilisé particulièrement pour le Hand-over, il utilise les ressources du TCH pour transmettre ses infos de signalisation lors d'une communication.
TCH (Traffic Channel) canaux dédiés acheminant le trafic utilisateur	**TCH/FS &HS** (trafic Channel for Coded Speech)	Voix plein et ½ débit (13kbps & 5,6kbps)
	TCH/D (Trafic Channel dor Data)	Modem GSM

◊ A l'aide d'OTDrive, nous lançons maintenant une capture de trame de niveau 2&3 *(menu Trace)* et nous observons les échanges qui se produisent lorsque le mobile est en veille :

1882354		RR PAGING REQUEST TYPE 1	
1882354	PCH	RR PAGING REQUEST TYPE 1	
1882212		RR SYSTEM INFORMATION TYPE 3	
1882212	BCCH	RR SYSTEM INFORMATION TYPE 3	109
1882154		RR SYSTEM INFORMATION TYPE 3	
1882154	BCCH	RR SYSTEM INFORMATION TYPE 3	98
1882099		RR PAGING REQUEST TYPE 1	
1882099	PCH	RR PAGING REQUEST TYPE 1	
1882008		RR SYSTEM INFORMATION TYPE 3	
1882008	BCCH	RR SYSTEM INFORMATION TYPE 3	78
1881906		RR SYSTEM INFORMATION TYPE 13	
1881906	BCCH	RR SYSTEM INFORMATION TYPE 13	113
1881844		RR PAGING REQUEST TYPE 1	
1881844	PCH	RR PAGING REQUEST TYPE 1	
1881589		RR PAGING REQUEST TYPE 1	
1881589	PCH	RR PAGING REQUEST TYPE 1	
1881334		RR PAGING REQUEST TYPE 2	
1881334	PCH	RR PAGING REQUEST TYPE 2	
1881079		RR PAGING REQUEST TYPE 3	

Nous observons tout d'abord que, en veille, le mobile ne fait que recevoir des informations. Celles-ci sont les suivantes :

- PCH : le mobile « écoute » la voie balise *(935 Mhz)* et reçoit de la BTS des informations sur la cellule, demande d'identification, etc...

- BCCH : on retrouve également le numéro de BCCH de la cellule sur laquelle le portable est accroché : « 113 » mais également des informations sur les cellules voisines *(notamment leur BCCH : 78, 98 & 109)*...

=> même en veille, le mobile continue à recevoir des informations sur l'état actuel de la cellule dans laquelle il se trouve. Cela lui permet, même s'il n'est pas utilisé et en mouvement, *(dans un poche en voiture par exemple)*, de changer de cellule lorsque le signal devient trop faible, ou lorsqu'il entre dans une cellule différente.

◊ Observons maintenant une capture de trame lorsque le mobile établit, puis coupe une connection :

1894580	SDCCH-RR	↘	NO INFORMATION FIELD
1894560	SACCH-UI	↗	RR MEASUREMENT REPORT
1894560		↗	RR MEASUREMENT REPORT
1894545		↘	RR SYSTEM INFORMATION TYPE 5ter
1894545	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 5ter
1894529	SDCCH-I	↗	RR CIPHERING MODE COMPLETE
1894479		↗	CC SETUP
1894479		↗	RR CIPHERING MODE COMPLETE
1894478	SDCCH-RR	↗	NO INFORMATION FIELD
1894478		↘	RR CIPHERING MODE COMMAND
1894478	SDCCH-I	↘	RR CIPHERING MODE COMMAND
1894458	SACCH-UI	↗	RR MEASUREMENT REPORT
1894458		↗	RR MEASUREMENT REPORT
1894443		↘	RR SYSTEM INFORMATION TYPE 6
1894443	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 6
1894427	SDCCH-RR	↘	NO INFORMATION FIELD
1894356	SACCH-UI	↗	RR MEASUREMENT REPORT
1894356		↗	RR MEASUREMENT REPORT
1894345	SDCCH-I	↗	MM AUTHENTIFICATION RESPONSE
1894345		↗	MM AUTHENTIFICATION RESPONSE
1894341		↘	RR SYSTEM INFORMATION TYPE 5
1894341	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 5
1894274	SDCCH-RR	↗	NO INFORMATION FIELD
1894274		↘	MM AUTHENTIFICATION REQUEST
1894274	SDCCH-I	↘	MM AUTHENTIFICATION REQUEST
1894239		↘	RR SYSTEM INFORMATION TYPE 6
1894239	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 6
1894225	SDCCH-I	↗	RR CLASSMARK_CHANGE
1894224		↗	RR CLASSMARK_CHANGE
1894223	SDCCH-UA	↘	MM CM SERVICE REQUEST
1894178	SDCCH-SABM	↗	MM CM SERVICE REQUEST

Cette fois nous observons des échanges dans les 2 sens de communication montant et descendant.

Les types de messages reçus sont les suivants :

- SDCCH
- SACCH

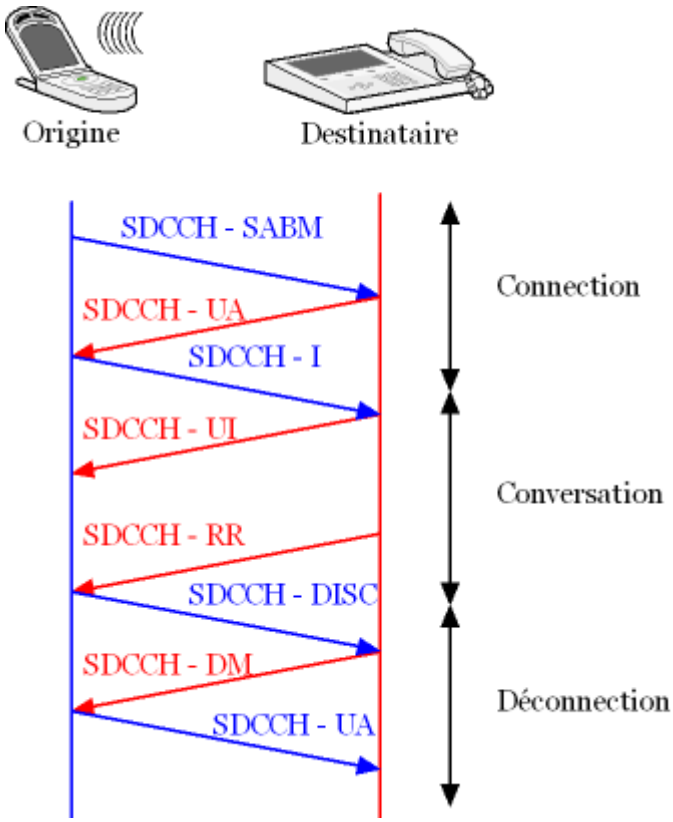
Les messages SDCCH :

- SDCCH-SABM *(Asynchronous Balanced Mode)* : sert à établir et à couper la connexion
- SDCCH-UA *(Unnumbered Acknoledge)* : sert d'acquittement non numéroté
- SDCCH-I *(Information)* : transporte les messages de niveau 3
- *SDCCH-RR* (Receiver Ready) : sert d'acquittement
- SDCCH-UI *(Unnumbered Information)* : information non numérotée

Les messages SACCH :

- il est chargé de contrôler, en permanence, le fonctionnement du SDCCH auquel il est associé.

◊ Diagramme d'échanges des messages de type DCCH :



5. Étude des échanges lors d'un handover

◊ Le processus du handover permet de basculer une communication en cours d'un canal physique à un autre sans que la QoS ne soit dégradée *(<=> communication coupée ou détériorée)*. Il est donc absolument indispensable d'avoir un minimum d'interruption *(car elle existe tout de même)* soit, en moyenne, <100ms.

Le handover peut se produire dans différents cas :

Intercellulaire	**Intracellulaire**
se produit lorsque qu'une cellule voisine offre une meilleure qualité *(un meilleur Rx_Level)*	se produit lorsque les mesures montrent que la qualité du signal reçu *(Rx_Level)* est faible avec un niveau de champ élevé dans la cellule active.
se produit lorsqu'une cellule voisine permet la communication avec un niveau de puissance signal plus faible	
se produit lorsque le réseau veut transférer la charge du trafic sur des cellules adjacentes	

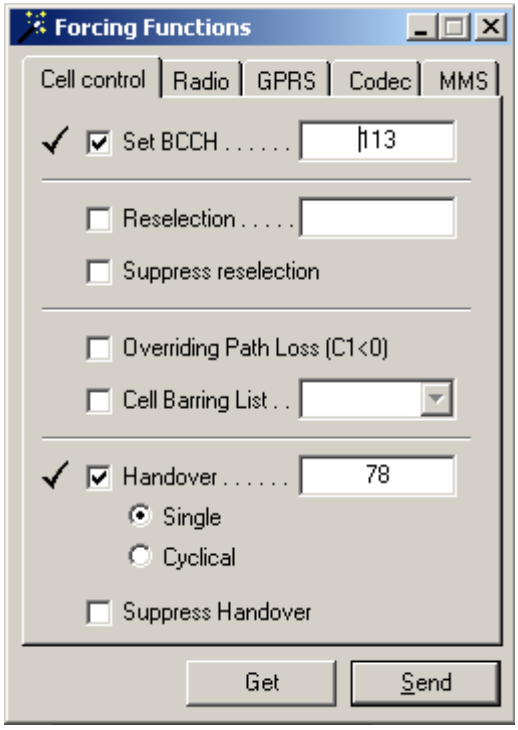
◊ Le mobile étant toujours branché au port COM du PC, nous relevons les informations suivantes :

Layer 1 Report - IDLE

IDLE	BCCH	BSIC		Cell ID	Level(dBm)		Tx Max	C1	C2	Reselect(dB)		Penalty Time(s)	Tmp Offset(dB)	GPRS	RA color	Delta FN	QBO
		NCC	BCC		Rx	RM				Hyst	Offset						
Serving cell	113	0	6	11723	-69	-110	5	41	41	10	0	20	0	YES	0		
Neighbour 1	78	0	1	6482	-83	-110	5	25	25	10	0	20	0	YES	0	2257465	2061
Neighbour 2	77	***	***	1759	-88	-110	5	25	25	10	0	20	0	YES	0	***	***
Neighbour 3	99	0	6	21723	-94	-110	5	14	14	10	0	20	0	YES	0	0	0
Neighbour 4	95	***	***	21735	-89	-110	5	19	19	10	0	20	0	YES	0	***	***
Neighbour 5	98	0	2	***	-93	-110	5	16	16	10	0	20	0	YES	0	1969679	2412
Neighbour 6	109	0	4	***	-85	-110	5	26	26	10	0	20	0	YES	0	0	0

Nous allons cette fois établir une communication à partir du portable, et le forcer, en cours de communication, à faire un handover.

Comme le montre la capture ci contre, nous sommes actuellement sur la cellule serveuse, celle qui à le BCCH 113, et nous basculons, en cours de communication, sur la cellule 78 en cliquant sur « Send ».



La fenêtre « Layer 1 report » évolue et deviens :

Layer 1 report - DEDICATED

DEDICAT.	BCCH	BSIC		TA	PL	Rx Lev(dBm)		Rx Qual		BCCH RX(dBm)
		NCC	BCC			Full	Sub	Full	Sub	
Serving cell	78	0	1	3	5	-80	-79	5	5	-77
	BCCH	NCC	BCC	RX Lev(dBm)		Delta FN		QBO		
Neighbour 1	113	0	6	-71		458184		2936		
Neighbour 2	90	0	7	-70		1681895		1126		
Neighbour 3	93	0	3	-73		153832		42		
Neighbour 4	117	0	2	-77		1681895		1126		
Neighbour 5	102	0	5	-81		1		4998		
Neighbour 6	109	0	4	-82		458184		2934		

ce qui prouve bien que le handover à été effectué.

NB : le mobile reviens, de lui même, assez rapidement sur la cellule serveuse précédente car il s'aperçoit qu'elle offre une meilleure qualité que celle que nous avons choisie.

◊ Analysons les trames qui sont passées pendant ce handover :

842165	SACCH-UI	↗	RR MEASUREMENT REPORT
842165		↗	RR MEASUREMENT REPORT
842153		↘	RR SYSTEM INFORMATION TYPE 6
842153	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 6
842061	SACCH-UI	↗	RR MEASUREMENT REPORT
842061		↗	RR MEASUREMENT REPORT
841957	SACCH-UI	↗	RR MEASUREMENT REPORT
841957		↗	RR MEASUREMENT REPORT
841945		↘	RR SYSTEM INFORMATION TYPE 6
841945	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 6
841853	SACCH-UI	↗	RR MEASUREMENT REPORT
841853		↗	RR MEASUREMENT REPORT
841841		↘	RR SYSTEM INFORMATION TYPE 5ter
841841	SACCH-UI	↘	RR SYSTEM INFORMATION TYPE 5ter
841823	FACCH_F-RR	↘	NO INFORMATION FIELD
841797	FACCH_F-I	↗	RR HANDOVER COMPLETE
841797	FACCH_F-UA	↘	NO INFORMATION FIELD
841793		↘	RR PHYSICAL INFORMATION
841793	FACCH_F-UI	↘	RR PHYSICAL INFORMATION
841772	FACCH_F-SA	↗	NO INFORMATION FIELD
841772		↗	RR HANDOVER COMPLETE
841771		↘	RR PHYSICAL INFORMATION
841771	FACCH_F-UI	↘	RR PHYSICAL INFORMATION
2333668	FACCH_F-RR	↗	NO INFORMATION FIELD
2333668		↘	RR HANDOVER COMMAND
2333668	FACCH_F-I	↘	RR HANDOVER COMMAND-L3 SEG END
2333642	FACCH_F-RR	↗	NO INFORMATION FIELD
2333642	FACCH_F-I	↘	RR HANDOVER COMMAND-L3 SEG BEGIN

<= FIN du handover

<= DEBUT du handover

Ce sont les canaux FACCH qui sont utilisés pour réaliser un handover. Ils sont de différents types *(Information, Acquittement, …)*. Ces canaux remplacent tout ou en partie le canal de trafic *(TCH, cf tableau page 18)* lorsqu'une information de signalement urgente doit être transmise *(par exemple un handover)*.