Les réseaux GSM/DCS

Les réseaux GSM : Plan

- Introduction et Historique
- Services
- Architecture
- Interface Radio
- Protocoles

GSM: Le vrai départ de la mobilité

- Avant le GSM, en Europe :
  - Des services tel que le téléphone de voiture (coût, poids)
  - Technologies analogiques nationales et mal normalisées (avec un coût élevés)

- Le GSM: une conception très visionnaire
  - Tout inventer et construire
  - Une réponse aux demandes du marché professionnel et privé de la mobilité
  - Partant d'un parc très limité, il n'y a pas eu de problème de migration (contrairement aux USA avec L'AMPS)

GSM: Une réussite Européenne

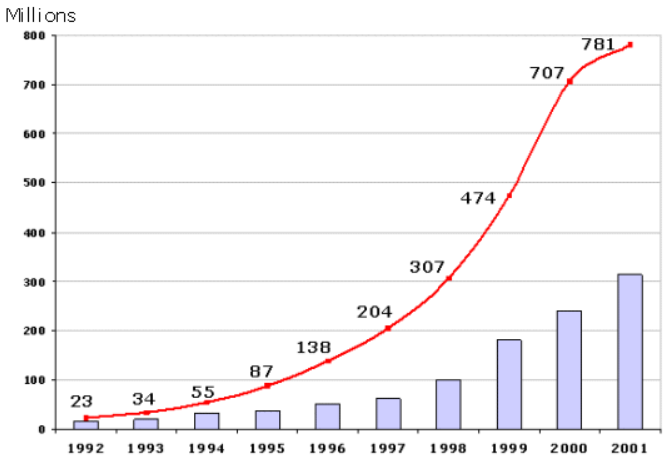
- Initiative essentiellement européenne, exploite au mieux les technologies internationales du moment
- Norme adoptée en Europe, Asie (sauf Japon), Afrique partiellement aux US et Amérique Latine
- Une vraie normalisation (européenne étendue) qui spécifie :
  - Fréquences (versions : 900 Mhz et 1800 Mhz)
  - Architecture et protocoles (fixe et radio)
  - Services génériques
  - Equipements terminaux

Objectifs

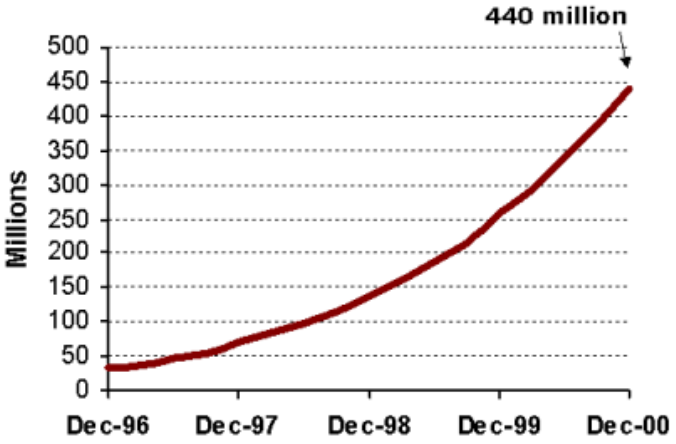
- Les objectifs affichés du projet GSM sont:
  - Système entièrement numérique
  - Bonne qualité de signal
  - Faible coût des téléphones portables
  - Possibilité de roaming (étendre le réseau à toute l'Europe)
  - Confidentialité des transmissions
  - Portabilité : possibilité de changer de téléphone en conservant ses données personnelles (grâce à la carte à puce SIM)
  - Réduction des fraudes : détection de tout usage frauduleux (téléphone, carte SIM) ! ?
  - Fonctionnalités et services avancés

Déploiement du réseau

- Evolution du nombre d'abonnés aux différents réseaux cellulaires



- Evolution du nombre d'abonnés au réseau GSM



- Les dernières statistiques peuvent être trouvées sur le site http://www.gsmworld.com

Historique du GSM

- 1979 : la WRC (World Radio Conference) réserve 2 * 25 Mhz dans la bande 900 Mhz pour les communications mobiles en Europe

- 1982 : la CEPT (Conférence Européenne des postes et Télécommunications) crée le Groupe Spéciale Mobile → GSM

- 1987 : 13 pays européens signent un accord pour l'ouverture d'un réseau de type GSM en 1991

- 1990 : première spécification. Réservation de 2*75 Mhz à 1800 Mhz pour DCS

- 1992 : GSM devient Global System for Mobile communication
  exploitation commerciale : Itenéris et SFR en France

- 1994 : licence DCS 1800 à Bouygues

Historique du GSM

- 1995 spécification phase 2 : Europe, Asie, Moyen-Orient, Afrique : 69

… … …

- 2000 :
  - 30 millions d'abonnées en France
  - 400 millions dans le monde
  - Couverture quasi mondiale
  - Etendu à la bande de fréquences de 1900 Mhz

Structure de la normalisation

- Structure de la normalisation :
  - European Telecomminication Standards (ETSI)
- Structuré en comités techniques : Special Mobile Group (SMG)

  - SMG1 définition de service
  - SMG2 interface radio
  - SMG3 réseau fixe
  - SMG4 services de données
  - SMG5 Universal Mobile Telecommunication System
  - SMG6 administration des réseaux
  - SMG7 et 8 tests pour la station mobile et sous-system radio
  - SMG9 Carte SIM

GSM : Caractéristiques

- Système numérique
- N'accepte pas le dual-mode avec un système analogique
- Beaucoup d'interfaces spécifiées (1 seule pour CDMA et TDMA américains)
- Roaming international
- Interconnexion efficace avec ISDN
- Qualité du signal ≥ systèmes existants
- Capacité du trafic ≥ systèmes existants
- Coût d'abonnement ≤ systèmes existants
- Services "non voix"

- 2 phases de spécification
  - phase 1 : système (5000 pages)
  - phase 2 : services supplémentaires

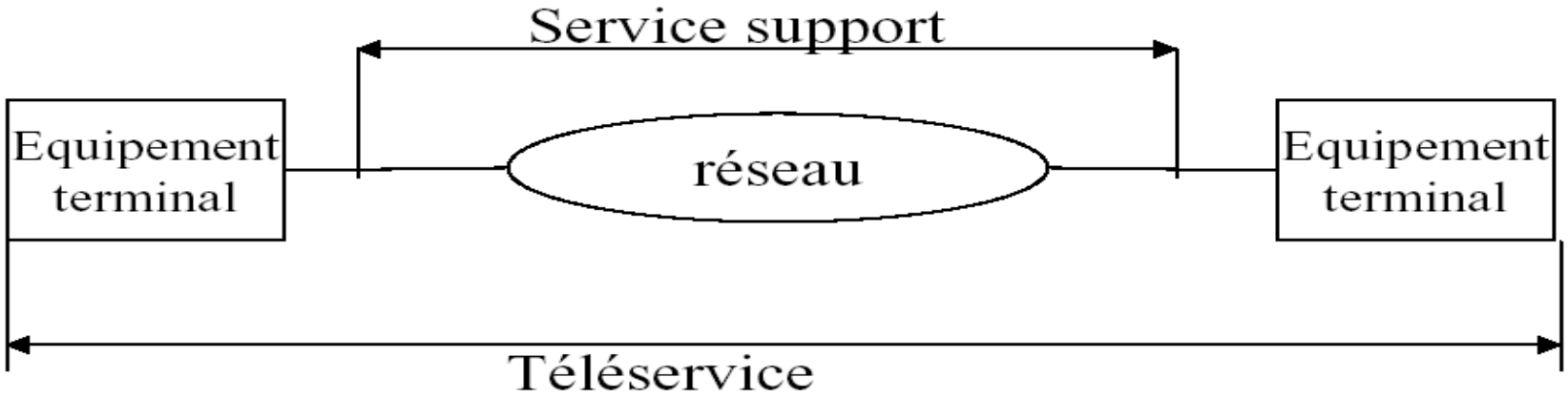
- Innovations reprises par les autres systèmes
  - Localisation
  - Handoff assisté par la station mobile

Les réseaux GSM : Plan

- Introduction et Historique
- Services
- Architecture
- Interface Radio
- Protocoles

Classification des services

- service support (bearer services)
  - offre d 'une capacité de transmission entre interface utilisateur (caractéristiques techniques de débit, de taux d'erreur, de mode de transmission sync/assync
- téléservices
  - offre de communication incluant les terminaux
- services supplémentaires
  - toutes facilités d 'utilisation en complément



Téléservices

Classe	Dénomination	Abréviation
Transmission de la voix	Téléphonie	
	Appels d'urgence	
Messages courts	Massages courts vers un mobile en point à point	SM MT/PP
	Massages courts venant d'un mobile en point à point	SM MO/PP
	Messages courts en diffusion vers mobiles	
Fax	Transmission alternée voix/fax groupe 3 (T ou NT)	
	Transmission automatique fax groupe 3 (T ou NT)	

Services supplémentaires

- Identification de numéro (appelant/appelé)
- Renvoi d'appel
- Double appel
- Appel en conférence
- Groupe fermé d'usagers (virtuel privé)
- Facturation (coût de la communication)
- Restriction d'appel (pour les envois et réception)
- Blocage des appels sortants/entrants
- Indication de ligne transférée
- Indication de coût

Fonctions de sécurité

- Aspects confidentialité et sécurité
  - des communications, des données,
  - Algorithme de chiffrement (activé par l'opérateur)
- Transmission de l'identité du mobile
  - localisation, réception en claire pour que le mobile la décode (Suivre à la trace...)
  - Temporary Mobile Subscriber Identity
  - Changer après 1+ utilisation
- Clé d'accès au réseau sur la carte SIM

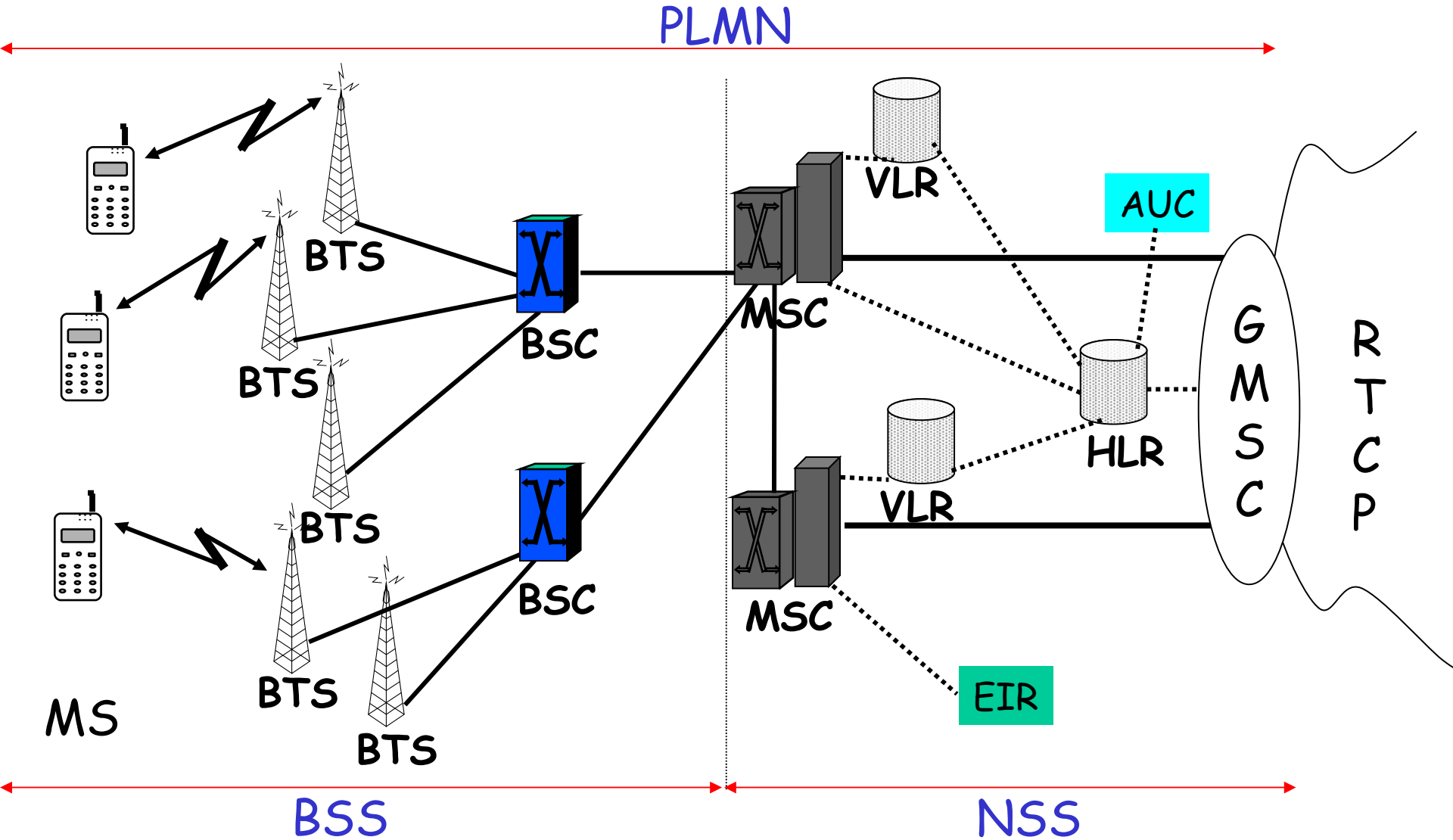
Les réseaux GSM : Plan

- Introduction et Historique
- Services
- Architecture
- Interface Radio
- Protocoles

Architecture Générale

- PLMN (Public Land Mobile Network)
  - Réseau mobile public terrestre relié au RTCP
  - Réseau GSM opéré par un opérateur particulier sur un territoire (ex : PLMN SFR, Orange, ..)
  - Se décompose en 3 sous-systèmes:
    - radio (BSS Base Station Subsystem)
    - réseau (NSS Network SubSystem)
    - gestion et de maintenance (OSS Operation Support Subsystem)
- RTCP = RTC = PSTN
  - Réseaux téléphonique commuté

Architecture générale



Glossaire

- MS : Mobile Station
- BTS : Base Transceiver Station
- BSC : Base Station Controller
- MSC : Mobile-services Switching Center
- HLR : Home Location Register
- VLR : Visitor Location Register
- GMSC : Gateway MSC
- EIR : Equipment Identity Register
- AUC : Authentification Center

Découpage géographico-administratif

- Cellule (Cell)
  - aire géographique couverte par une antenne radio
- Zone de localisation (Location Area)
  - ensemble de cellules dans lequel l'abonné est localisé
- Zone de commutation (Communication Area)
  - ensemble de zones de localisation qui dépendent d'un même centre de commutation
- Réseau terrestre mobile (Public Land Mobile Network PLMN)
  - ensemble des zones de commutation sous la responsabilité d'un opérateur

- une BTS par cellule
- 1 à n BSC par zone de localisation et 1 à p zones de localisation par BSC
- un MSC par zone de commutation

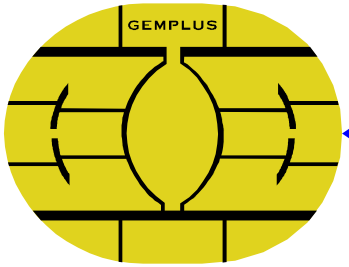
Les identités dans le GSM

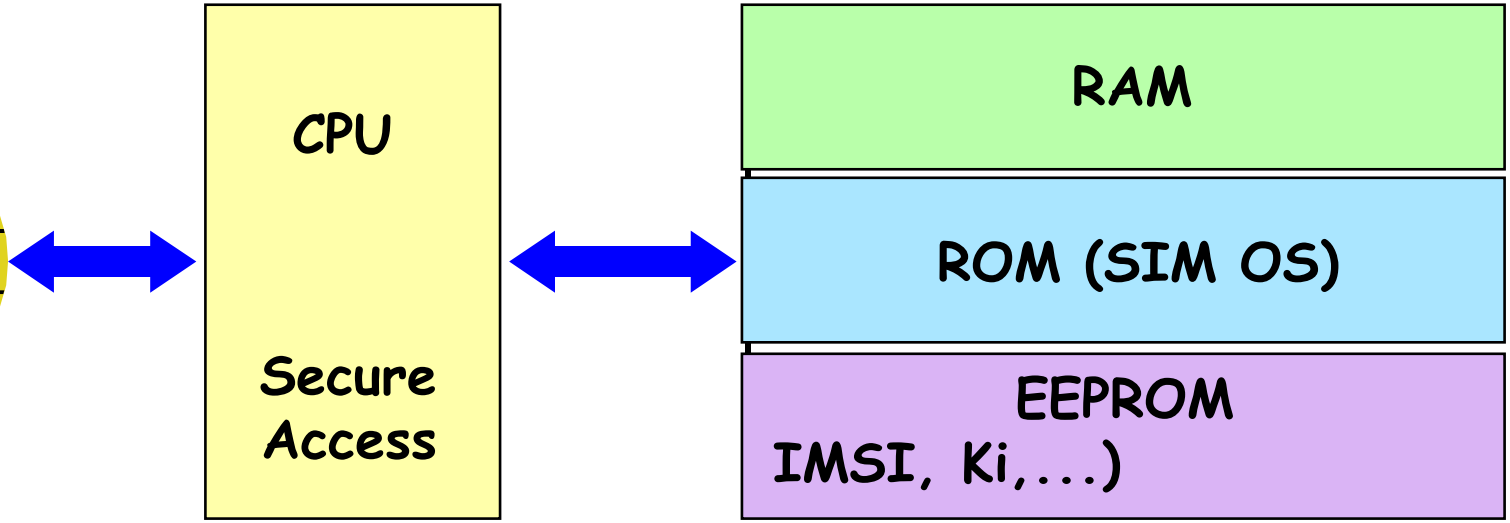
- IMSI (International Mobile Subscriber Identity)
  - Identité invariante de l'abonné (15 chiffres), stocké dans la carte SIM et dans le HLR
  - Elle doit rester secrète autant que possible → recours au TMSI
- TMSI (Temporary Mobile Subscriber Identity)
  - Identité temporaire propre à un VLR
  - Utilisée pour identifier le mobile lors des interactions Mobile/Réseau
- MSISDN (Mobile Station International ISDN Number)
  - Numéro de l'abonné (ex 336 98 76 54 32)
  - Seul identifiant de l'abonné connu dans le monde téléphonique
- MSRN (Mobile Station Roaming Number)
  - Numéro attribué lors d'un établissement d'un appel
  - Permet l'acheminement des appels par les commutateurs MSC et GMSC (contient des informations de localisation : MSC courant)
  - Compréhensible par le réseau fixe (même structure que MSISDN : pays, PLMN, numéro abonné)
- IMEI (International Mobile station Equipment Identity)
  - Identificateur du terminal (15 chiffres)

Identifiants de localisation

- LAI (Localisation Area Identification)
  - utilisée pour localiser les abonnés
  - structure : Code du pays (208 pour la France) + Code du réseau dans le pays (10 pour SFR) + Code de la zone de localisation dans le réseau
- CGI (Cell Global Identification)
  - identification globale de cellule
  - structure : LAI + Identification de cellule
- BSIC (Base Station Identity Code)
  - code couleur permettant au MS de distinguer deux BTS utilisant la même fréquence de voie balise localement
  - Le couple (fréquence, BSIC) permet de déterminer une cellule
  - Possibilité d'avoir des couples identiques dans le même PLMN sur des zones éloignées
  - structure : Code couleur du PLMN + Code couleur de la BTS
- + HLR Number, VLR Number, MSC Number

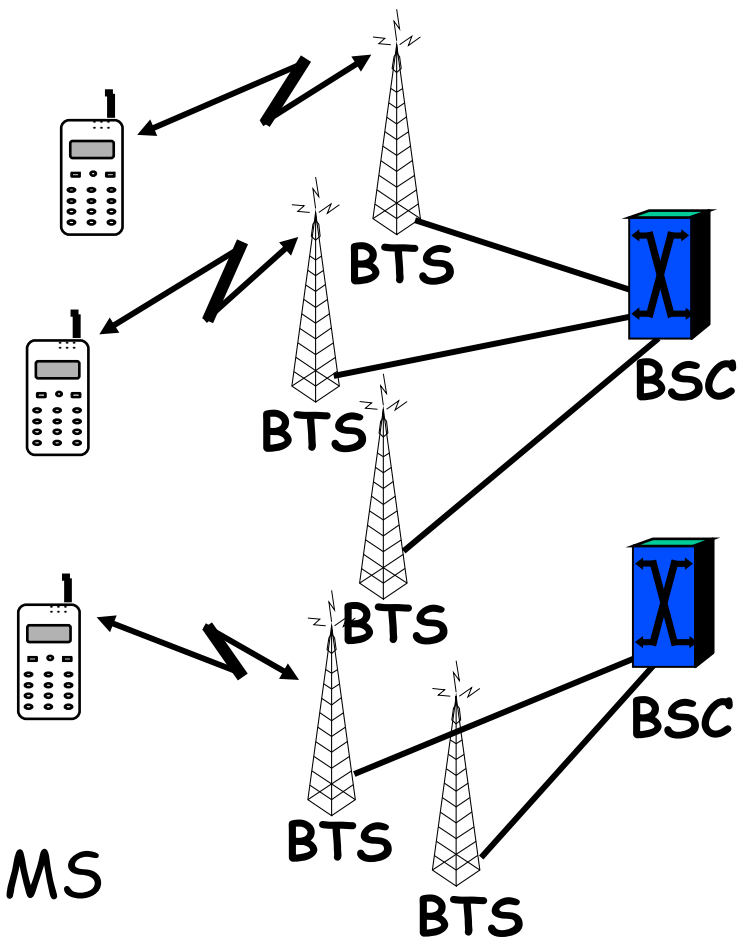
La carte SIM (Subscriber Identity Module)





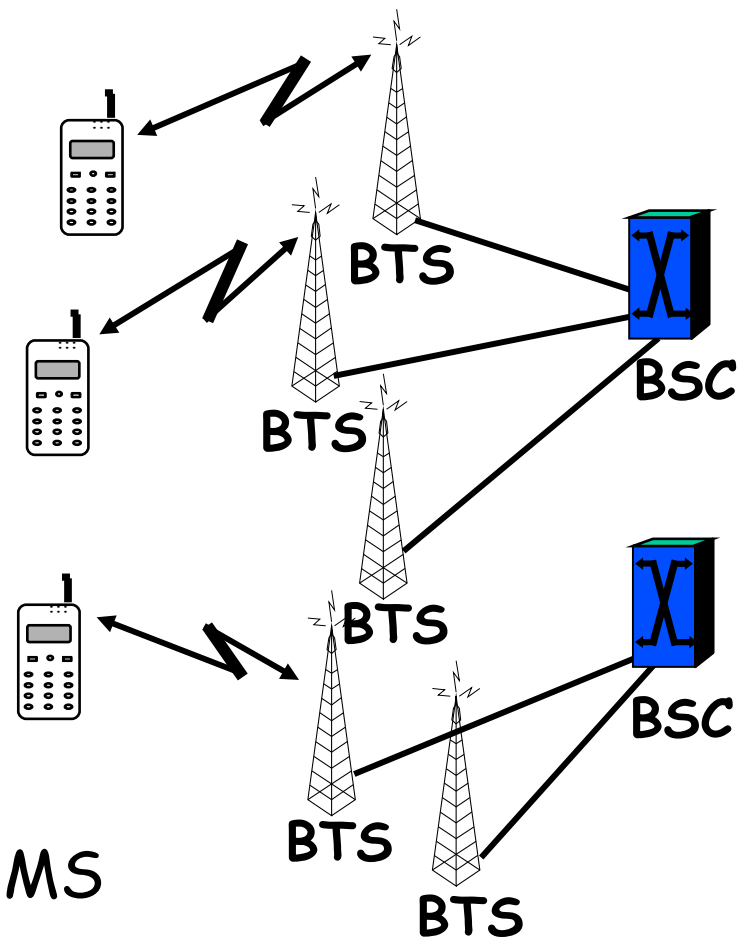
- Accès aux service GSM → carte SIM
- Sortie d'usine, la carte SIM contient :
  - Contient différentes clés de protection
  - Contient l'algorithme d'authentification
- Pour la personnaliser attribution :
  - Clé d'authentification Ki
  - IMSI

Le sous-système radio (BSS)



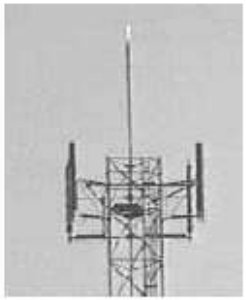
- MS : terminal mobile
  - De plus en plus performants et légers
  - Abonnement séparé du terminal
    - Blocage par certain opérateurs
  - Carte à puce SIM (Subscriber Identity Module)
    - Caractéristiques de l'abonnement, identités IMSI et le TMSI, et les algorithmes de chiffrement
  - Identité propre au terminal : IMEI
  - Puissance maximale d'émission de 0.8 à 8 W

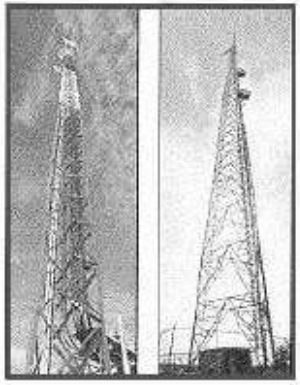
Le sous-système radio (BSS)



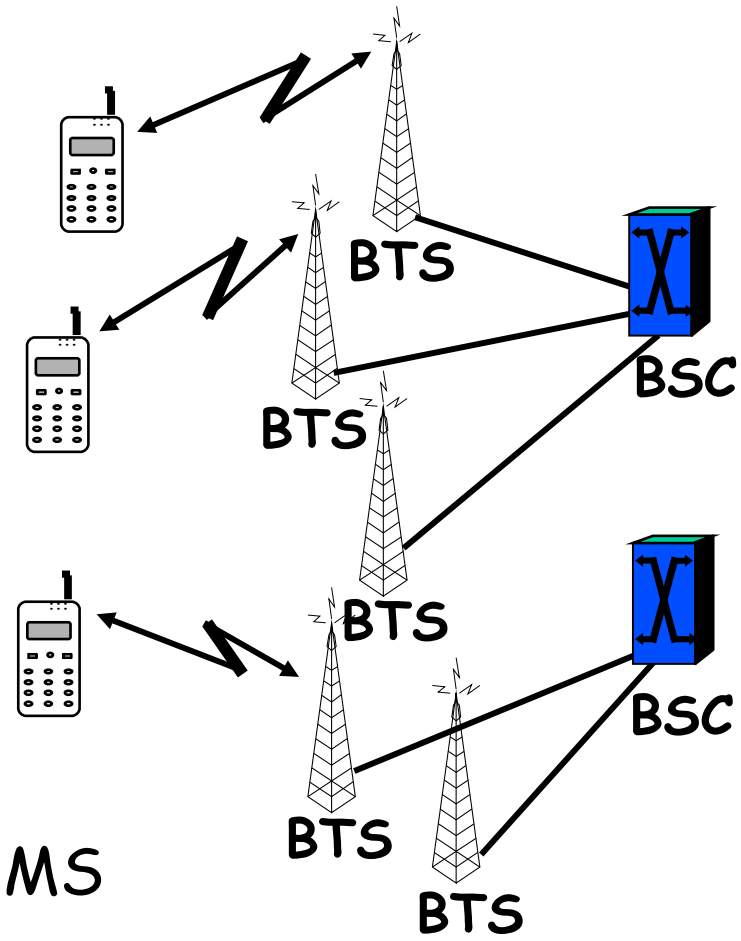
- BTS : station de base
  - Emetteurs-récepteur
  - Chargée de la transmission radio : modulation, démodulation, égalisation,codage correcteur d'erreur
  - Gère toute la couche physique : multiplexage TDMA, chiffrement, saut de fréquence…
  - Réalise l'ensemble des mesures radio nécessaires pour vérifier qu'une communication se déroule normalement
  - gère la couche liaison de données pour l'échange de signalisation entre les mobiles et l'infrastructure
  - Plusieurs puissances possibles
  - capacité maximale : 16 porteuses (~100 communications simultanées

Exemples de BTS





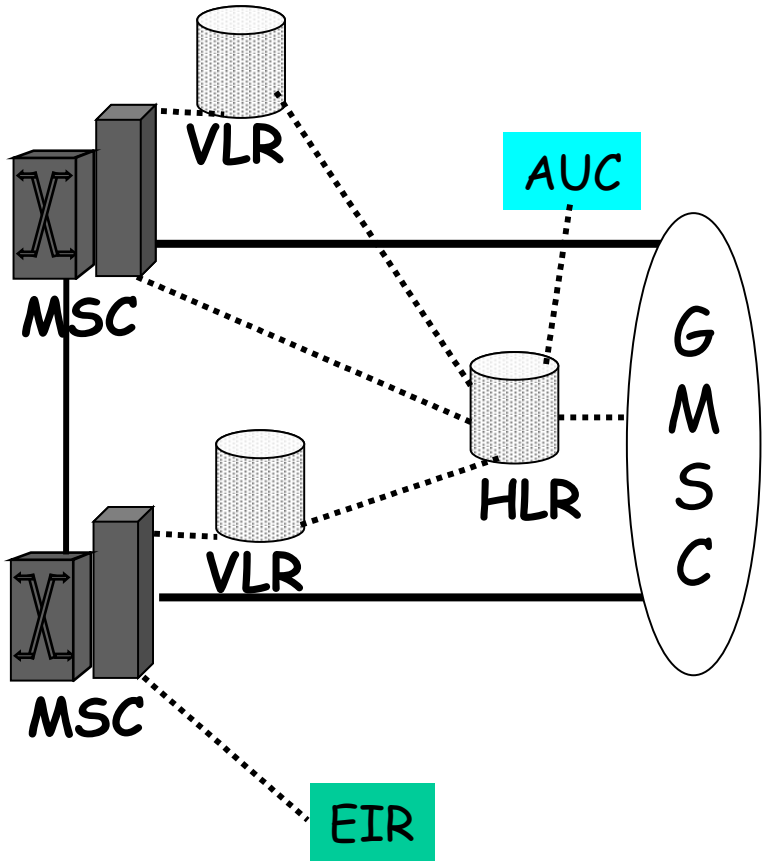
Le sous-système radio (BSS)



- BSC : Contrôleur de BTS
  - le BSC contrôle plusieurs BTS
  - organe 'intelligent' du BSS
  - Gère :
    - l'allocation des fréquences, le contrôle de puissance,
    - le contrôle d'admission,
    - le handover : décision et exécution
    - les mesures reçues par les BTS
  - liaison BTS-BSC similaire au RNIS
  - Paris intra-muros 150 BTS et 12 BSC

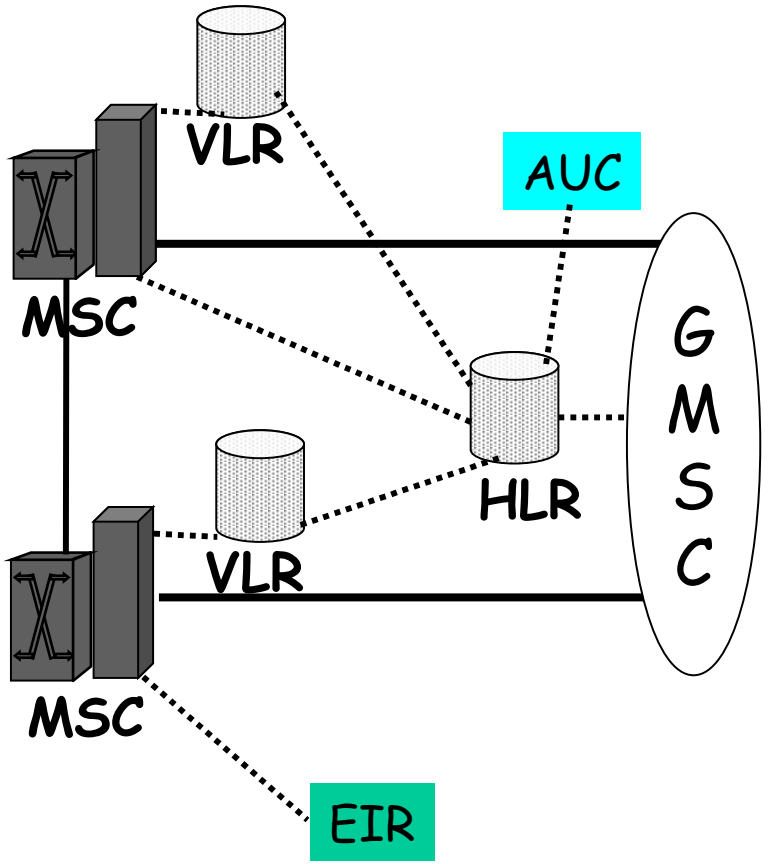
Le sous-système réseau (NSS)

- MSC : commutateur du service mobiles
- gère les communications des mobiles sous sa couverture :
  - gère l'établissement des communications entre un mobile et un autre MSC
  - transmission des messages courts
  - exécution du handover si hors BSC
  - dialogue avec le VLR pour gérer la mobilité des usagers (vérification, transfert d'information de localisation …)
- sert de passerelle active lors d'appels d'abonné fixe vers un mobile GMSC (Gateway MSC)



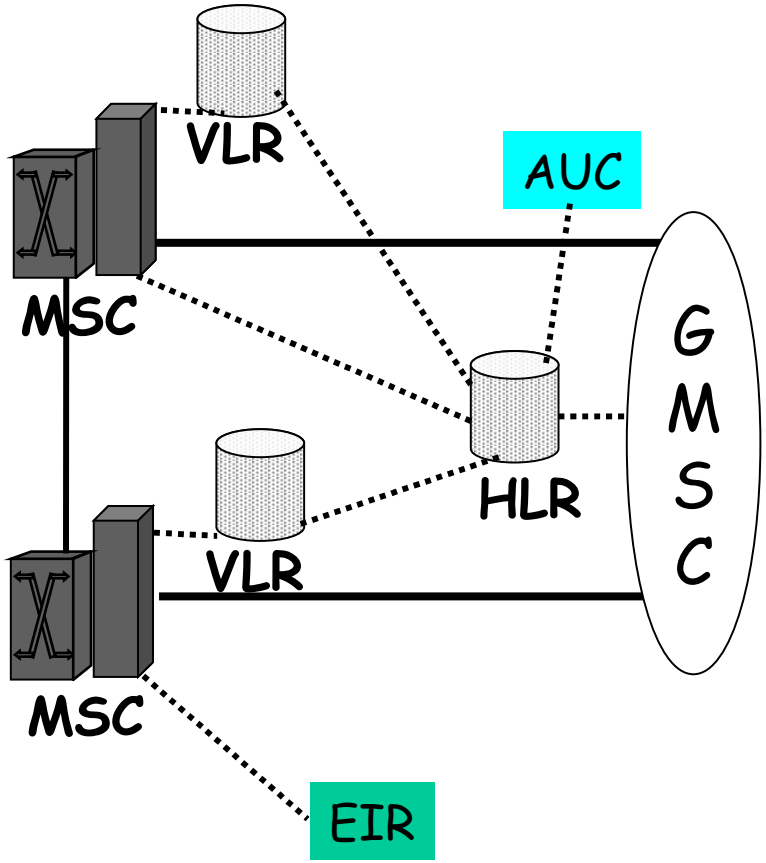
Le sous-système réseau (NSS)

- HLR : BD de localisation nominale
- gère les abonnés d'un PLMN donné
- mémorise le profile de l'abonné :
  - MSISDN : numéro de téléphone
  - IMSI : identité nationale de l'abonné
  - Informations chiffrement
  - Localisation courante
  - …



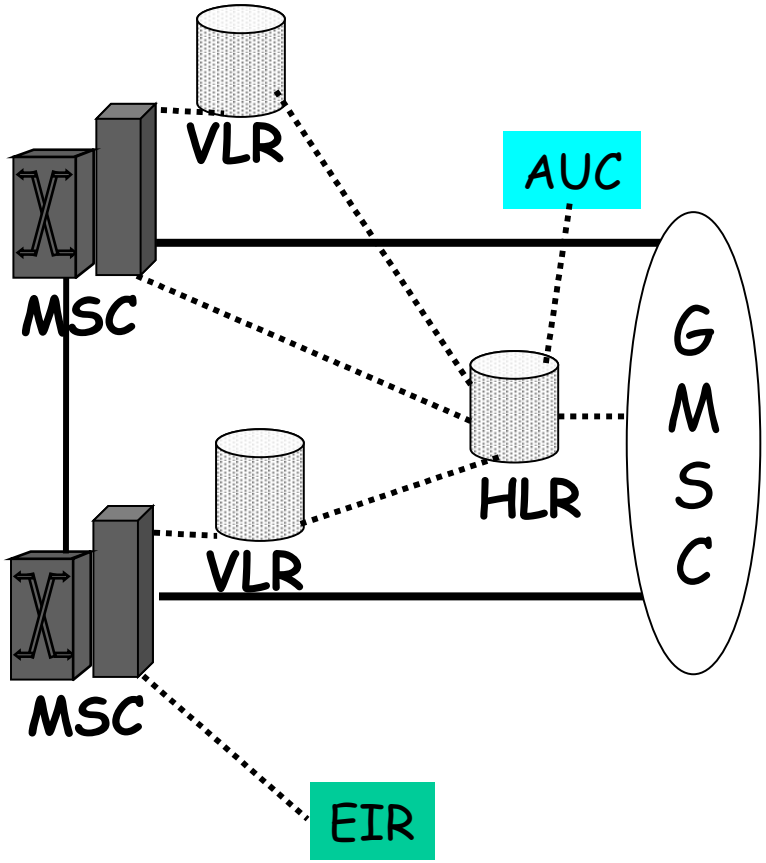
Le sous-système réseau (NSS)

- VLR : BD de localisation locale
- mémorise les informations concernant les abonnés présents dans une zone
- données identiques au HLR avec TMSI (identité temporaire) en plus
- Les informations suivent le mobile lors de ses déplacements
- séparation matérielle entre MSC et VLR rarement respectée

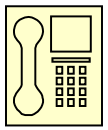


Le sous-système réseau (NSS)

- EIR
  - BD annexe contenant les identités des terminaux IMEI
  - peut refuser l'accès au réseau parce que le terminal n'est pas homologué ou qu'il a fait l'objet d'une déclaration de vol
- AUC
  - mémorise pour chaque abonné une clé secrète utilisée pour authentifier les demandes de services et pour chiffrer les communications
- EIR et AUC sont souvent considérés dans le sous-système d'exploitation et de maintenance OSS



Echanges lors d'un appel



GMSC

MSC

MSISDN →

e MSISDN est numéroté. Le réseau fixe transmet au MSC le plus proche qui agit en GMSC

MSISDN →

2. GMSC interroge le HLR pour connaître le MSC courant du mobile

IMSI →

3. HLR traduit MSISDN en IMSI et interroge le VLR

← **MSRN**

4. VLR attribue un MSRN au mobile et le transmet au HLR

← **MSRN**

5. HLR le retransmet au GMSC

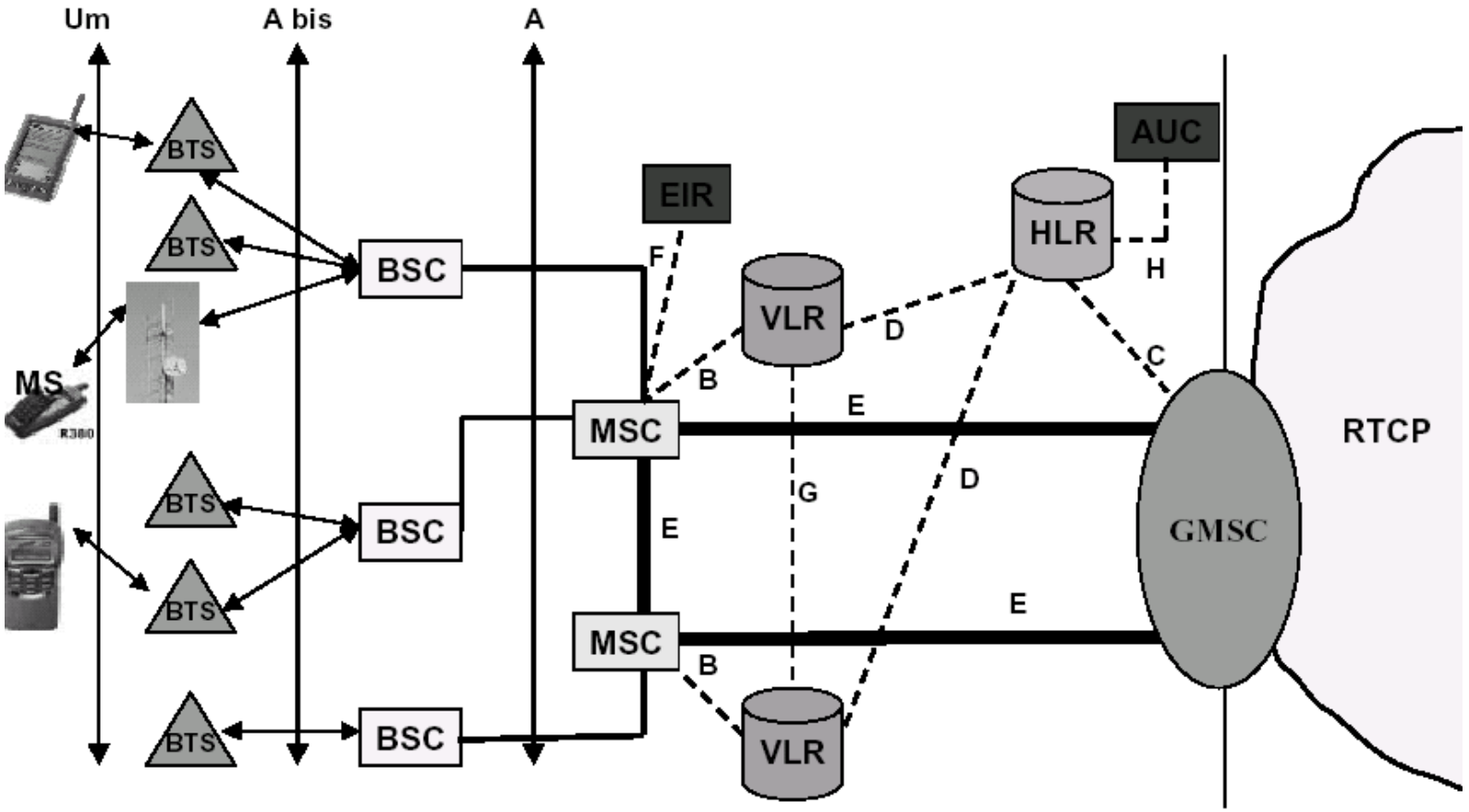
MSRN →

6. GMSC établit l'appel vers le MSC courant comme un appel tel normal (num est MSRN)

TMSI / IMSI →

7. MSC va enfin appeler le mobile en utilisant l'id temporaire TMSI

Interfaces GSM



Interfaces GSM

Nom	Localisation	Utilisation
Um	MS – BTS	Interface Radio
A bis	BTS – BSC	Divers
A	BSC – MSC	Divers
B	MSC – VLR	Divers
C	GMSC – HLR	Interrogation HLR pour appel entrant
D	VLR – HLR	Gestion des informations d'abonnés
E	MSC – MSC	Exécution des handover
	MSC – GMSC	Transport des messages courts
F	MSC – EIR	Vérification de l'identité du terminal
G	VLR – VLR	Gestion des informations d'abonnés
H	HLR – AUC	Echange des données d'authentification

- La norme GSM définis les différentes interfaces
- Le respect de l'interface D (impératif) permet à un MSC/VLR de dialoguer avec le HLR de tout autre réseau
- Le respect de l'interface A permet aux opérateurs d'avoir différents fournisseurs pour le NSS et le BSS

Les réseaux GSM : Plan

- Introduction et Historique
- Services
- Architecture
- Interface Radio
- Protocoles

Interface radio

- La transmission Radio est assurée par l'interface Radio Um, partie la plus complexe et sophistiquée dans le système, elle définit :
  - méthode d'accès multiple
  - largeur des canaux fréquentiels
  - nombre d'utilisateurs par porteuse
  - éléments de la chaîne de transmission (modulation, codage, entrelacement…)

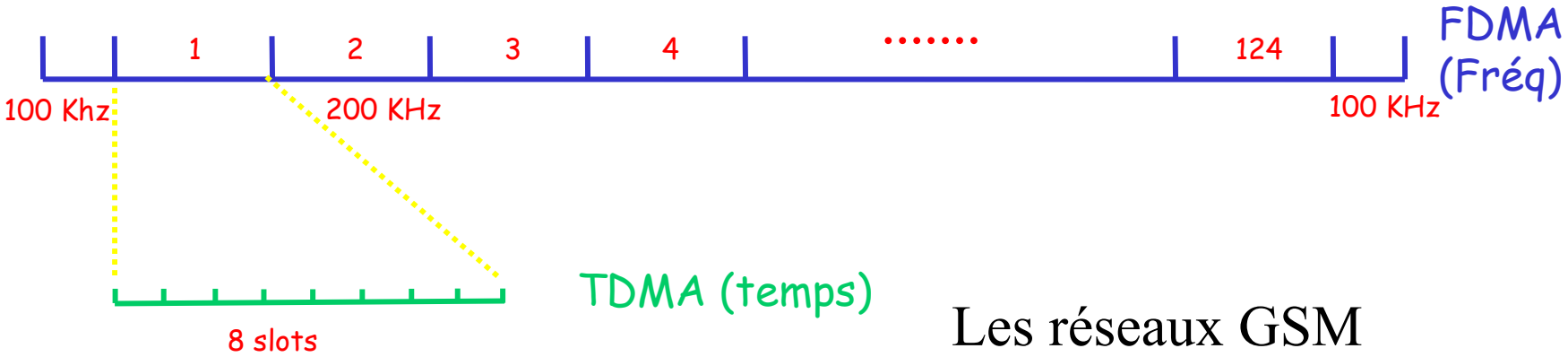
Fréquences utilisées

	GSM	DCS 1800
Bandes de Fréquences (Mhz)	890-915 ↑ 935-960 ↓	1710-1785 ↑ 1805-1880↓
Largeur simplex	2*25 Mhz	2*75 Mhz
Ecart duplex	45 Mhz	95 Mhz

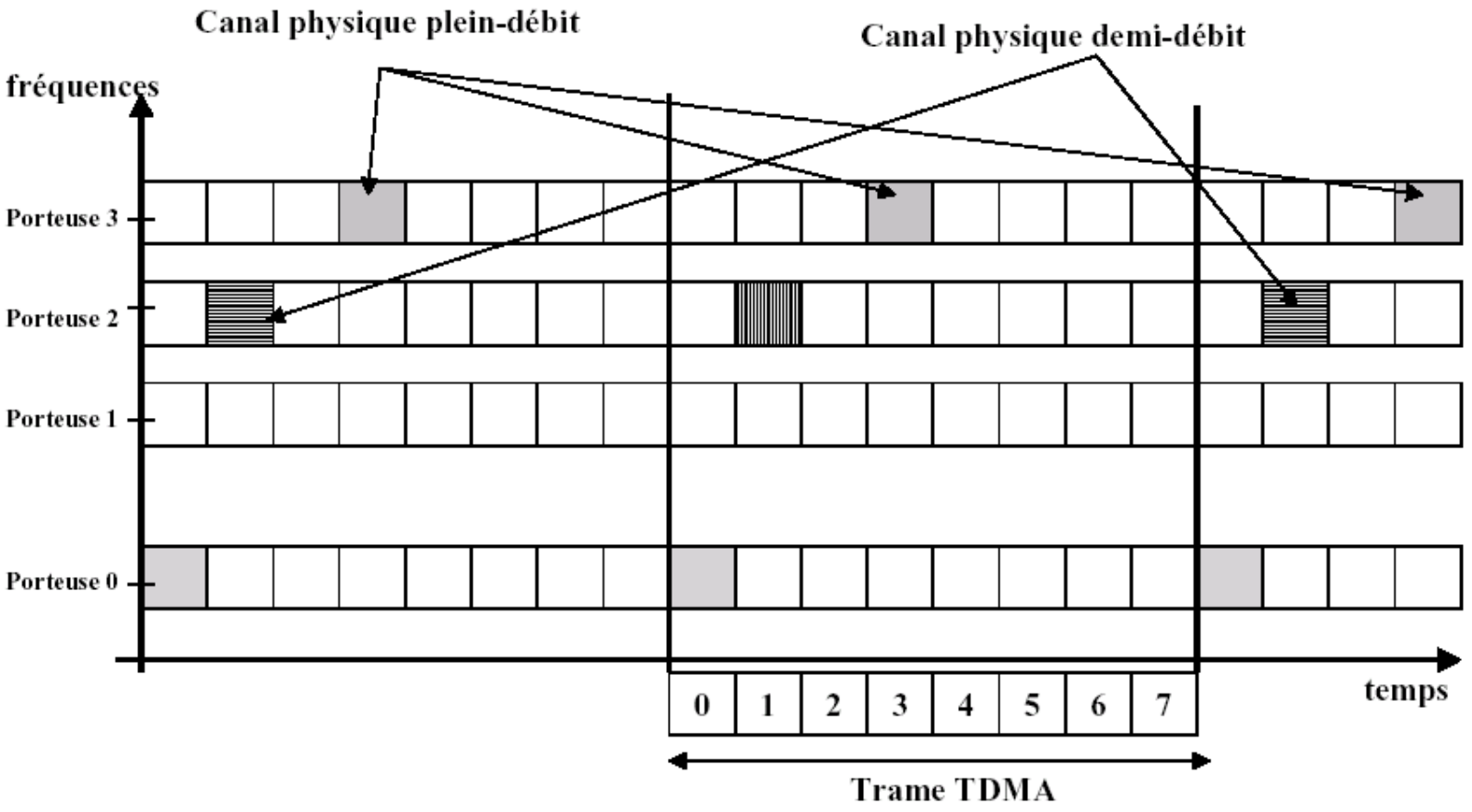
Interface radio GSM

- ↑ 890 - 915 MHz 25 Mhz
- ↓ 935 – 960 MHz 25 Mhz
- Technique d'accès : FDMA/TDMA (avec saut de fréquence)
  - FDMA : 124 canaux radio de 200 kHz par voie
  - TDMA : découpage temporelle des canaux en 8 slots ou IT (intervalle de temps) élémentaire
- Un canal physique = 1 slot / trame TDMA
- Possibilité de n'allouer qu'un slot toutes les 2 trames TDMA (canal physique demi-débit pour la parole)

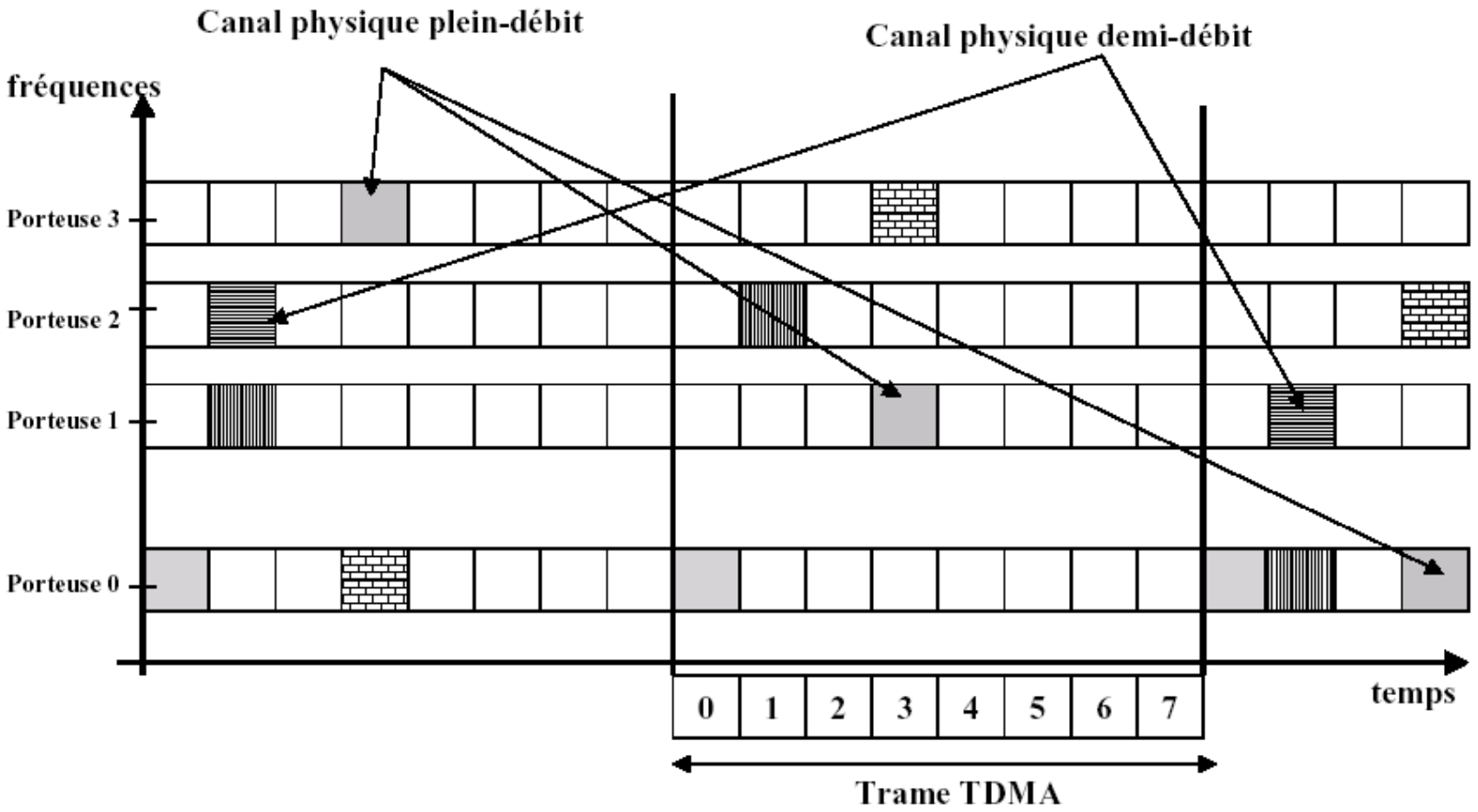
25 Mhz / 124 canaux de 200kHz + 2* 100 kHz



Canaux physiques sans saut de fréquence



Canaux physiques avec saut de fréquences



Canal physique duplex

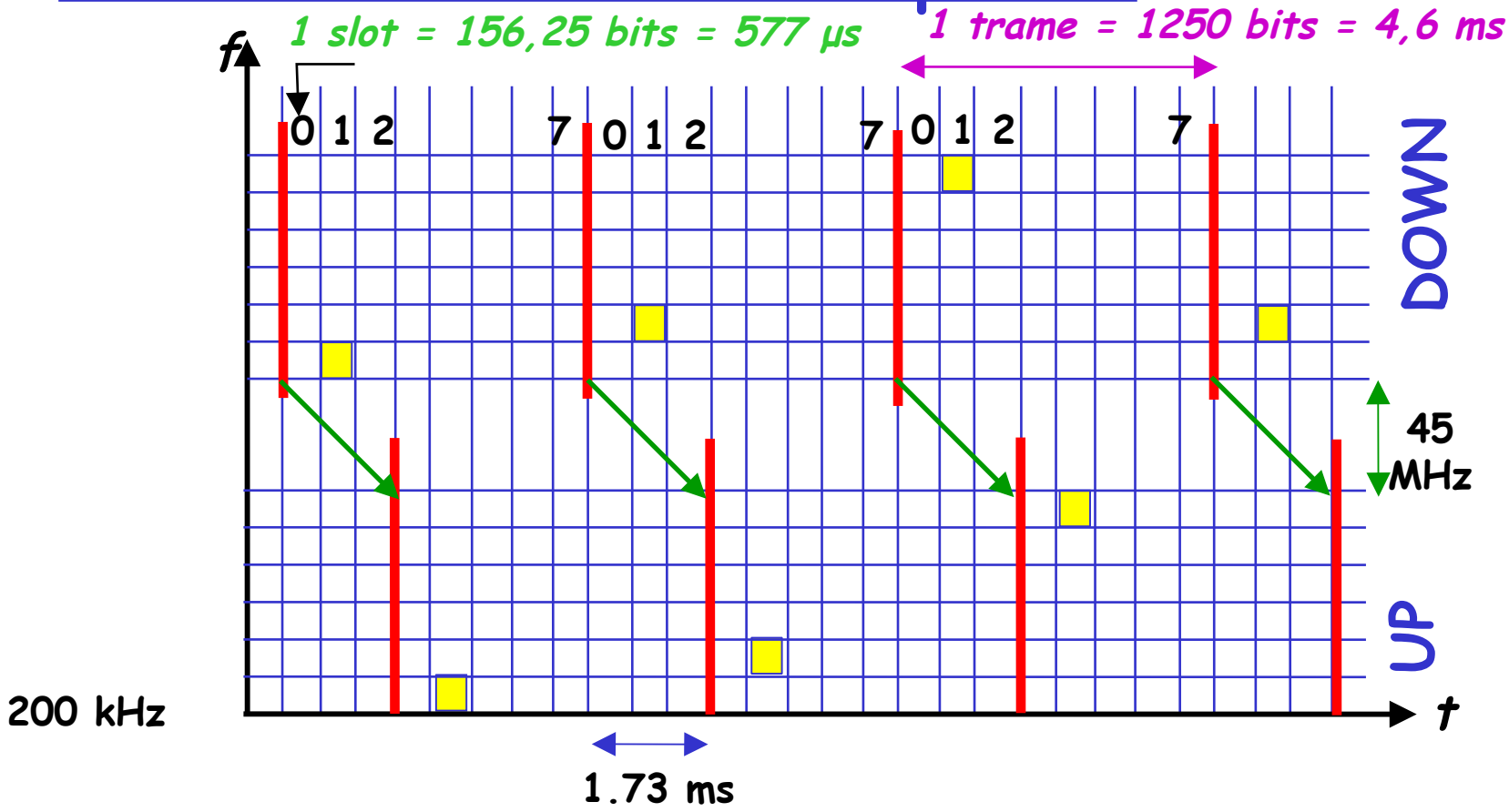
- Un canal physique simplex : 1 slot par trame TDMA (sans saut de fréquence)
- Un canal physique duplex : 2 canaux physique simplex
- Le duplexage se fait en fréquence FDD (Frequency Division Duplex)
  - Les fréquences up et down différentes

- Numérotation des porteuses (fréquences)
  - Les fréquences sont identifiées d'une manière unique par un numéro ARFCN sur 10 bits

- GSM : pour $1 \leq n \leq 124$ Fdown = 935 +(0,2 x n) (??? + 0,1)
  - GSM 124 paires de porteuses
- DCS : pour $512 \leq n \leq 885$ Fdown = 1805,2 +(0,2 x (n - 512))
  - DCS " 374 paires de porteuses

- La numérotation des canaux est commune dans GSM 900 et DCS 1800
  → Possibilité de réseaux mixtes avec des terminaux bi-bande

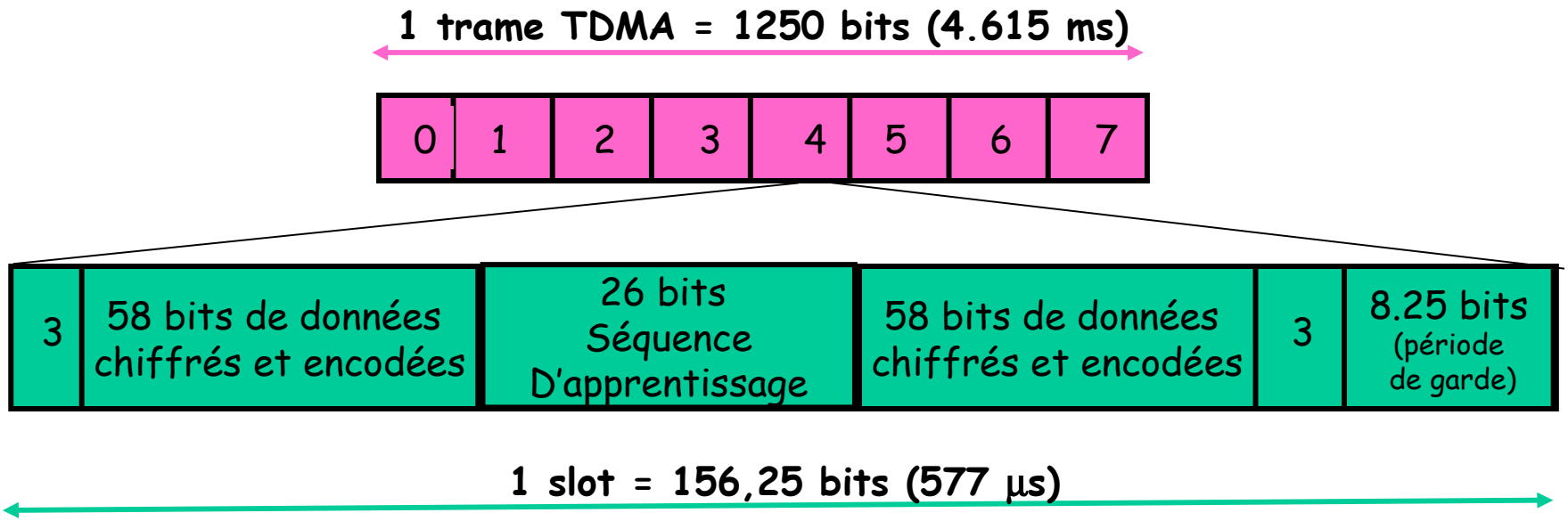
Transmission/Réception



- Les voies montante et descendante sont séparées par l'écart duplex:
  - Fdown = Fuplink + 45 Mhz
- Emission et réception décalée dans le temps de 3 slots (sinon terminal plus cher)

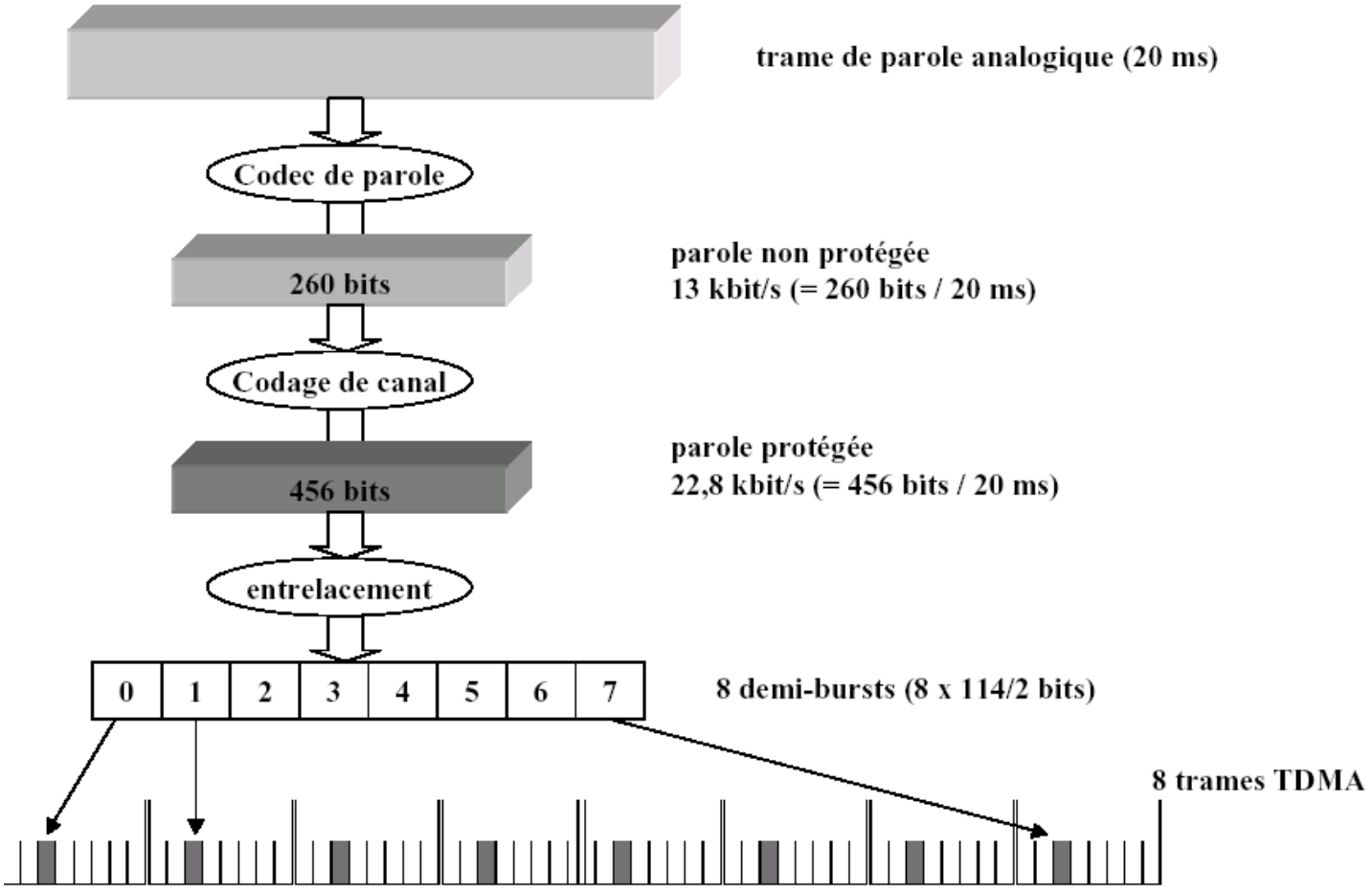
Organisation d'un burst

- Unité de transmission est le burst (slot)
  - Plusieurs structures
- Burst normal :

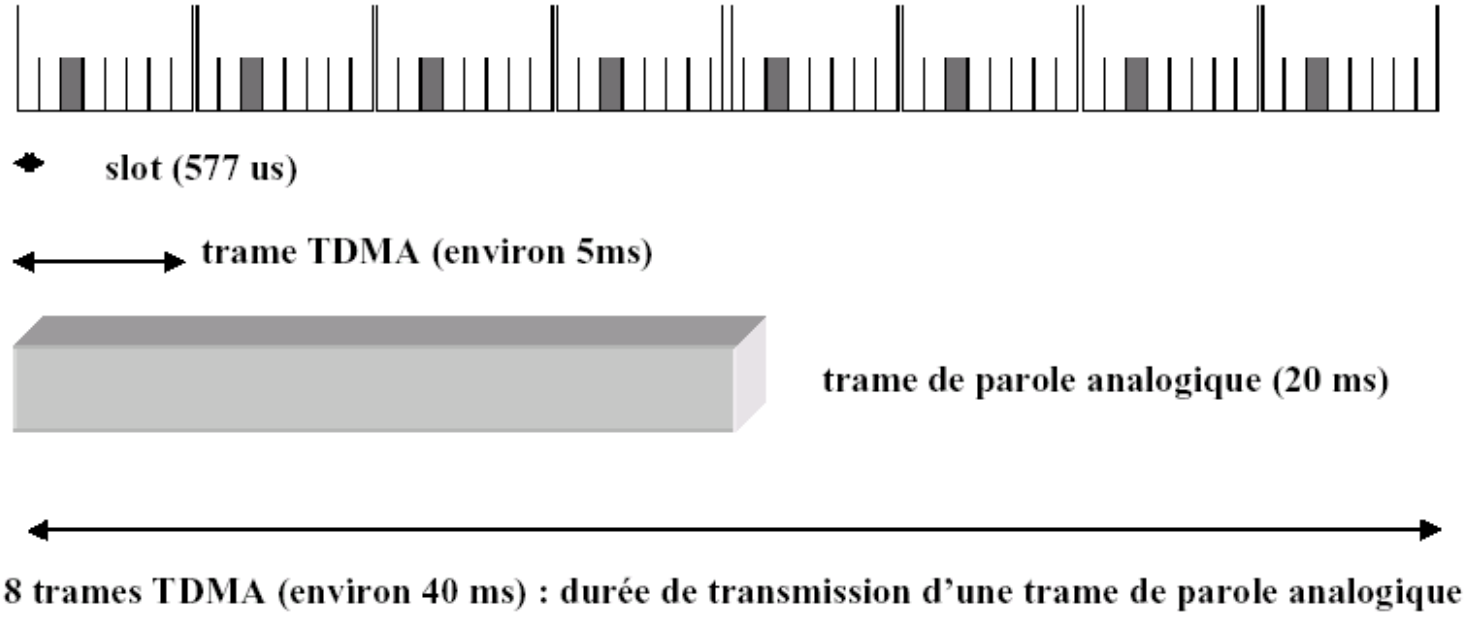


- 3 bits début et fin : augmenter et diminuer la puissance de l'émetteur
- Séquence d'apprentissage : synchronisation (minimise l'apparition d'erreurs)
- Délais de garde : protège le slot suivant des inexactitude d'alignement temporel
- 2 * 58 bits de données utilisateurs ou de signalisation (1er bit indique la présence éventuelle de signalisation)

Exemple de transmission : codage de la parole

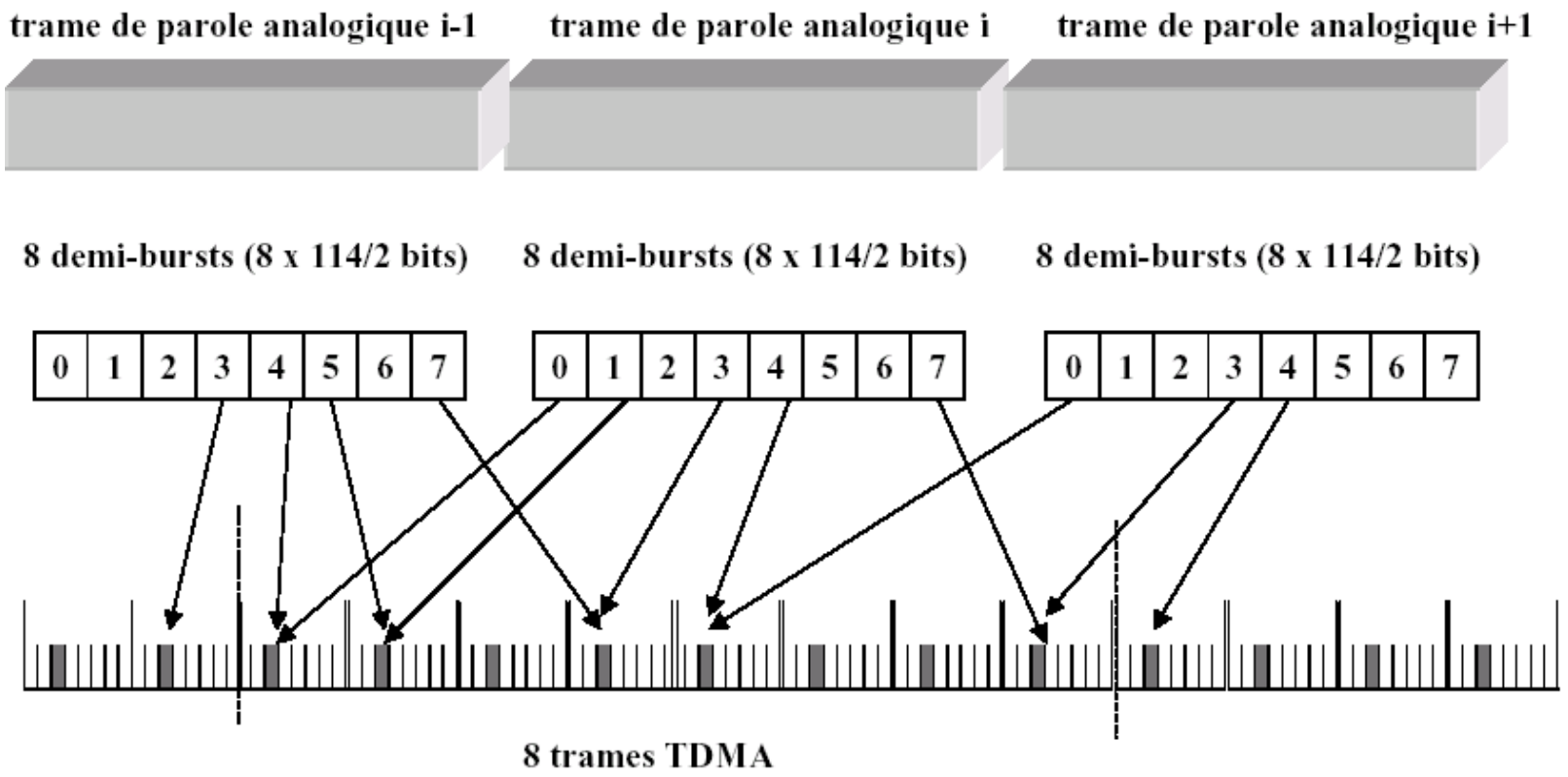


Exemple de transmission : codage de la parole

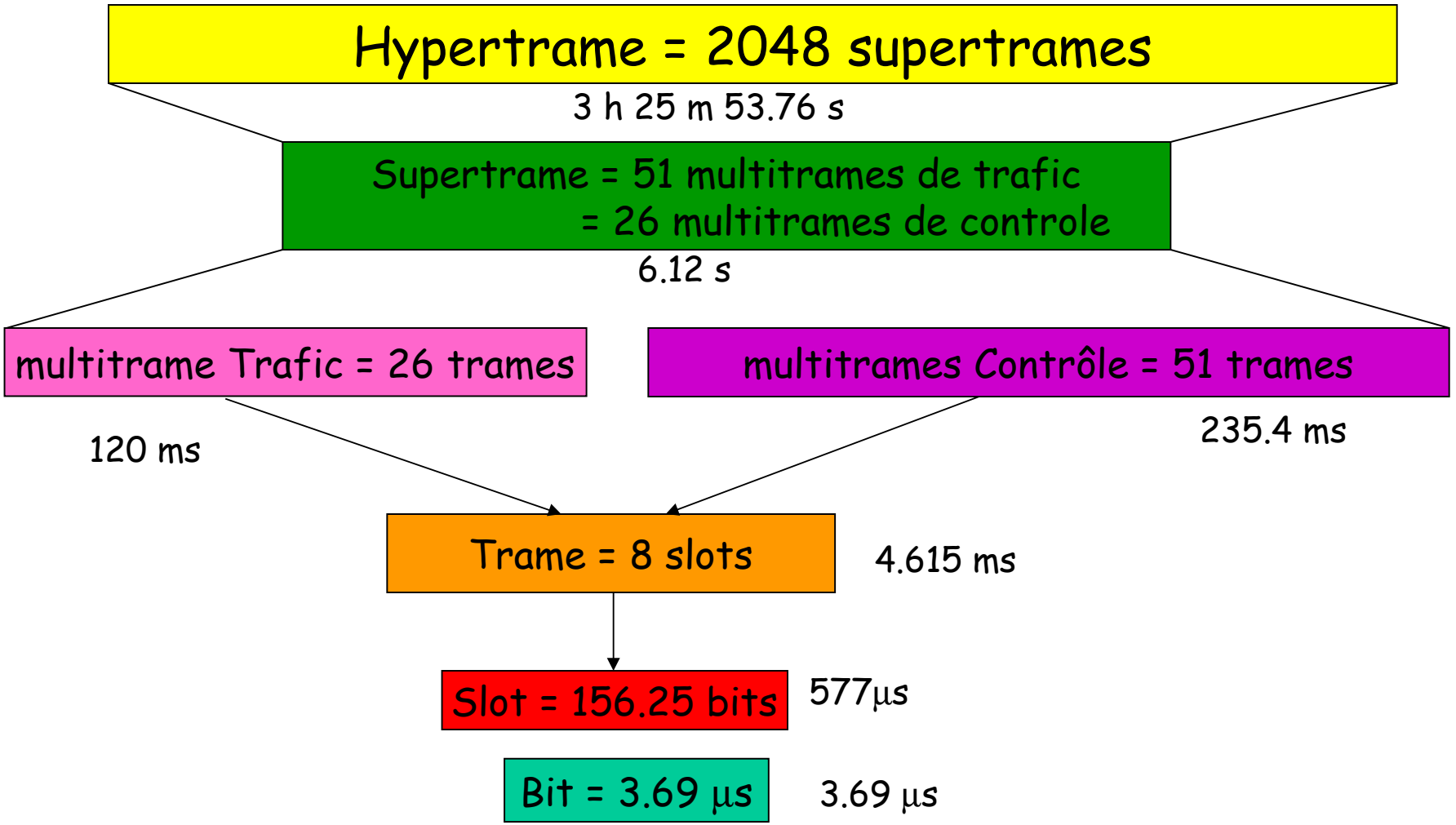


→ paquétisation introduit donc un délai de 20 ms

Exemple de transmission : codage de la parole



Organisation des trames



Les canaux logiques

- Les canaux de contrôle ne sont pas acheminés sur un canal physique dédié par souci d'économie mais de temps en temps

- Plusieurs types de canaux :
  - Canaux dédiés
    - échanges d'information (TCH) + signalisation téléphonique
  - Canaux de contrôle (SACCH)
    - Contrôle de présence mobile, puissance, mesures …
  - Canaux contrôle diffusés :
    - voie balise

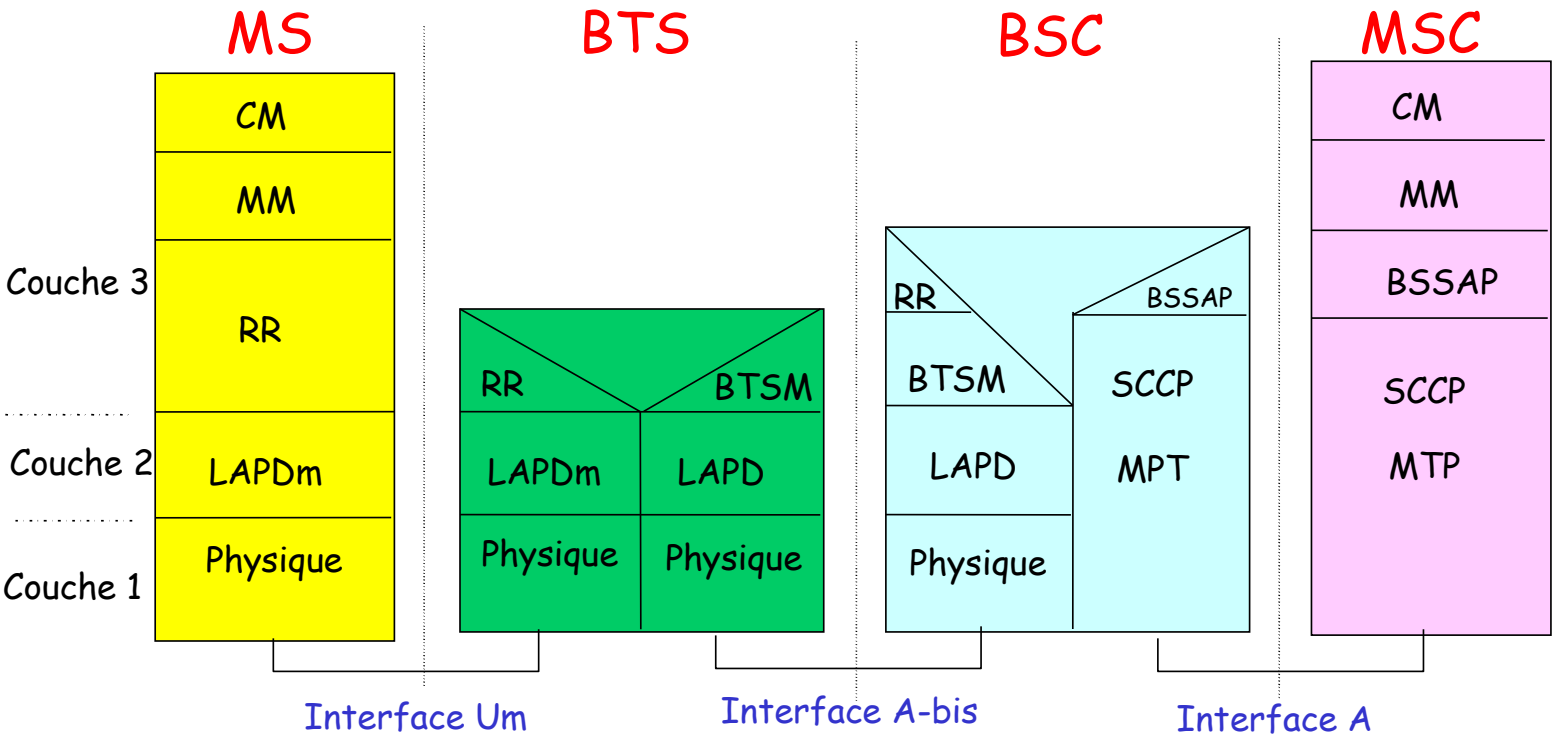
Les canaux logiques

Catégorie	Nom	Sens	Rôle
Diffusion (commun)	BCCH (Broadcast Control CHannel)	Descendant	Diffusion d'info. système spécifique à la cellule
	FCCH (Frequency Correction CHannel)	Descendant	Synchronisation fréquentielle
	SCH (Synchronization CHannel)	Descendant	Synchronisation temporelle et identification de la cellule
Contrôle (commun)	AGCH (Access Grant CHannel)	Descendant	Réponse du réseau à l'accès initial
	CBCH (Cell Broadcast CHannel)	Descendant	Diffusion de messages courts
	PCH (Paging CHannel)	Descendant	Appel du mobile
	RACH (Random Access CHannel)	Montant	Accès initial du mobile
Contrôle (dédié)	FACCH (Fast Associated Control CHannel)	Bidirectionnel	Signalisation rapide
	SACCH (Slow Associated Control CHannel)	Bidirectionnel	Contrôle de transmission
	SDCCH (Stand-alone Dedicated Control CHannel)	Bidirectionnel	Signalisation
Trafic (dédié)	TCH (Traffic CHannel)	Bidirectionnel	Transmission de données

Les réseaux GSM : Plan

- Introduction et Historique
- Services
- Architecture
- Interface Radio
- Protocoles

Architecture de protocole



- CM : Connection Management
- MM : Mobility Management
- RR : Radio Ressource Management

- LAPD : Link Access Protocol / canal D
- MTP : Message Transfer Part
- SCCP : Signaling Connection Part
- BSSAP : BSS Application part

Architecture de protocole

- La couche 1 : définit l'ensemble des moyens de transmission et de réception physique de l'information (A bis : MIC, Um gestion du multiplexage, codage correcteur d'erreur, mesures radio)
- Couche 2 : fiabilise la transmission entre deux équipement par un protocole LAPD et LAP mobile
- Couche 3 : établit, maintient et libère des circuits commutés avec un abonné du réseau fixe et est divisée en 3 sous-couches
  - Radio ressource mangement RR
  - Mobility Management MM
  - Connection Management CM

La couche 3

- RR : Gestion des ressources Radio
  - Sélection de cellule (choix de la porteuse), ouverture d'une connexion, contrôle en cours de communication, handover, terminaison
- MM : Gestion de la mobilité MM
  - Gestion de l'itinérance, procédure de mise à jour de zone de localisation
  - Gestion de la sécurité
    - Protéger l'utilisateur et le réseau
    - usurpations d'identité, écoutes frauduleuses, utilisations abusives
    - Authentification
    - Cryptage
- CM : Gestion des connexions
  - Établissement et relâchement des appels

RR : Sélection d'une cellule

- Écoute des fréquences
- Détection des infos sur le canal BCCH
- Inscription à la cellule
- Effectuer régulièrement des mesures des fréquences des cellules voisines
- Se caler sur la meilleure cellule

RR : Contrôle durant un appel

- Garantir une bonne qualité de la liaison
- Contrôle de puissance (via SACCH)
- Le BSS détermine les niveaux de puissance adéquats (grâce aux mesures)
- Utilisation du SACCH pour la compensation temporelle (ou *timing advance*)
  - Compenser les différences de temps de propagation suivant la position du mobile dans la cellule
  - Compensation coder sur 6 bits → valeurs de 0 à 63 * 3,7 µs (233 µs).
  - La valeur max correspond à une cellule de max de 35 Km

RR : Le handover (HO)

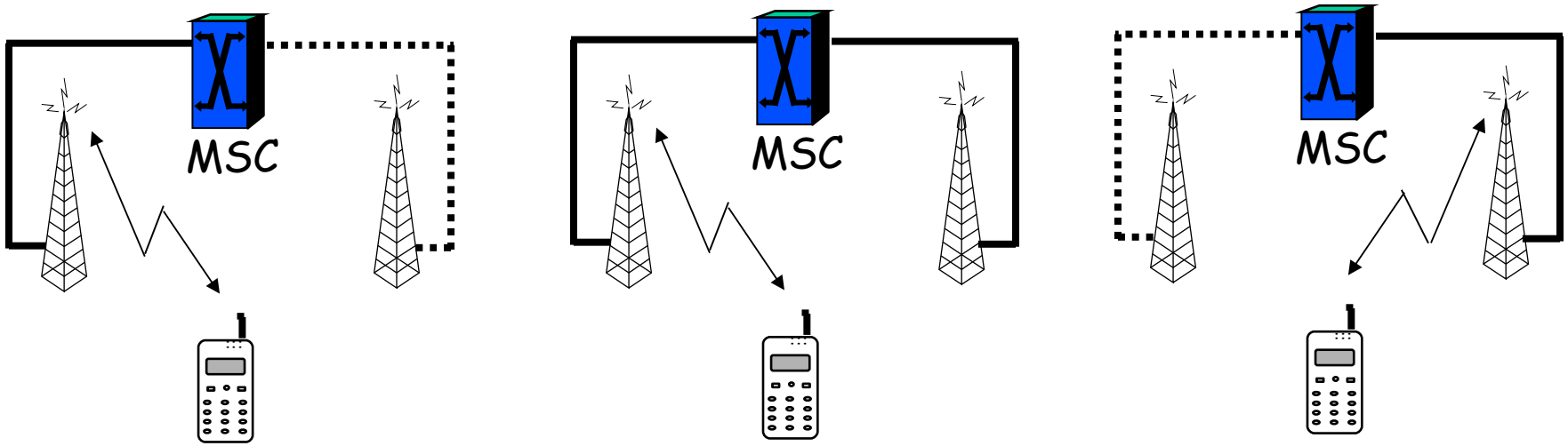
- Changement du lien radio
- Les causes :
  - Transfert cellulaire (mobilité de l'utilisateur)
  - Éviter la rupture du lien
  - Équilibrer le trafic
  - Minimiser la consommation d'énergie
- Pas d'algorithme imposé dans la norme GSM
  - Le HO est décidé par le réseau
  - Chaque opérateur établit une liste de critères

RR : Le handover (HO)

- Pendant la communication
  - Le lien radio est mesuré
  - Si la qualité passe sous un seuil : déclenchement
- Après la décision d'effectuer le HO
  - L'ancienne station transmet à la nouvelle les paramètres de transmission (clé de chiffrement, débit,…)
  - Réservation (éventuelle) des ressources sur les liens BSC-BTS et MSC-BSC
  - Le réseau transmet au mobile un message (référence sur le nouveau canal de transmission)
  - L'ancien canal est libéré
  - Si pas de ressources disponible : *échec de handover* (*call dropped*)
    - Réservation

RR : Hard Handover

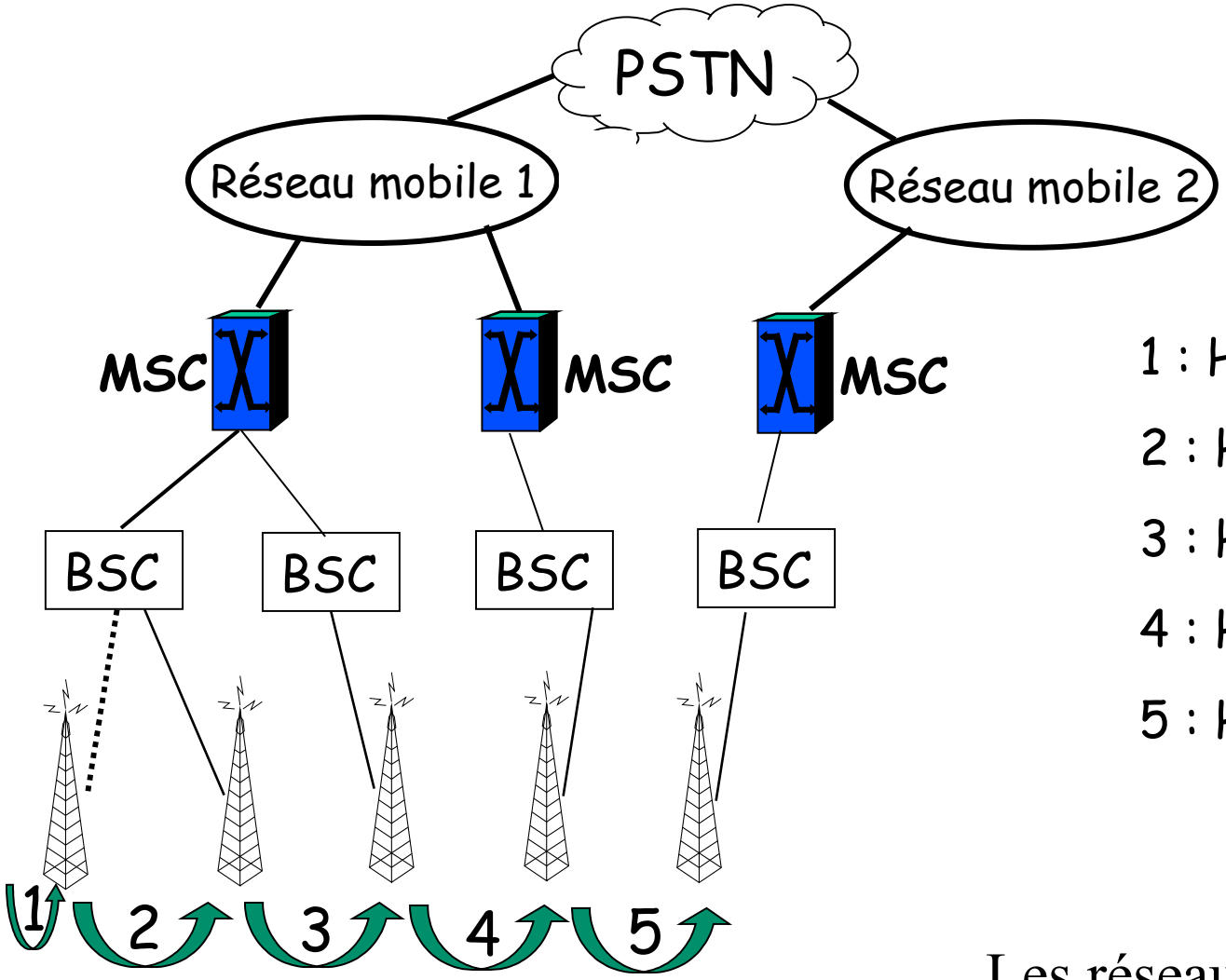
- Si déclenchement
  - Etablissement du nouveau canal
  - Transfert de la connexion vers le nouveau lien
  - Libération de l'ancien



Le MS ne gère qu'un seul canal

Le handover

- Différents type de HO vus du réseau



1 : HO intra-cellulaire

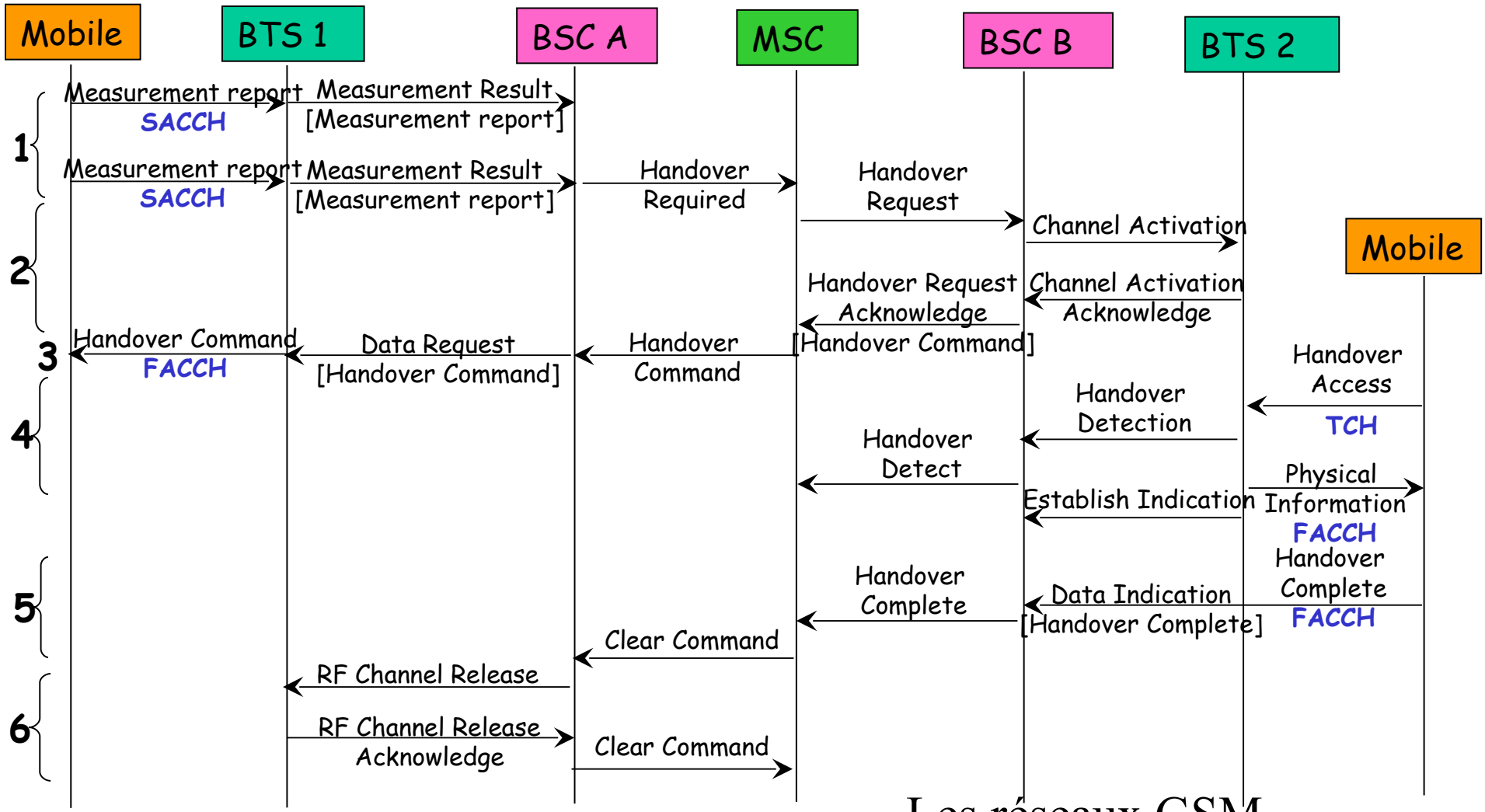
2 : HO intra-BSC

3 : HO intra-MSC

4 : HO inter-MSC

5 : HO inter-réseau

Déroulement d'un Ho type

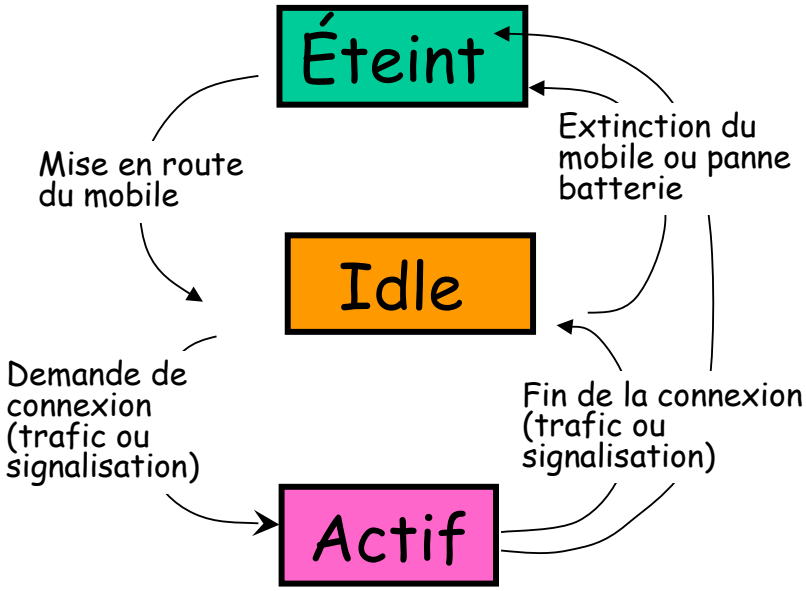


Déroulement d'un Ho type

1. Phase préliminaire d'observation (remontée des mesures) et décision d'exécution du HO : le BSC A remonte au MSC l'identité de la cellule cible : le MSC informe le BSC dont dépend la cellule cible (BSC B) et lui demande la permission d'exécuter un HO
2. Réservation des ressources du côté de la cellule cible (BTS 2), après quoi le BSC cible informe le MSC que l'exécution du HO est possible
3. Exécution du HO : Ce message redescend du MSC jusqu'au mobile et contient les informations essentielles suivantes : fréquences et BSIC de la voie balise BCCH de la cellule cible, description du nouveau canal dédié (signalisation SDCCH/trafic TCH, n° timeslot, fréquence), n° de référence du HO et puissance d'accès
4. Arrivée du mobile dans la cellule cible : Le mobile envoie à la BTS 2 le n° de référence de son HO et reçoit en échange la valeur du timing advance : le mobile est détecté dans la nouvelle cellule. La BTS envoie ensuite un message d'initialisation, comme s'il s'agissait d'un début de communication classique
5. Réussite du HO : Le lien est bien établi
6. Libération des ressources sur la BTS1 pour pouvoir les allouer à une autre communication

MM : Gestion de la mobilité

- Gestion de l'itinérance et de la sécurité
- États d'un mobile
  - Éteint
    - mémorisation de la dernière localisation connue
    - Commutation sur la messagerie
  - Idle
    - Informe régulièrement le réseau de ses changements de localisation (IMSI-attached)
  - actif
- Procédure d'attachement
  - pour indiquer le retour du mobile dans le réseau



MM : Mise à jour de la localisation

- Permet de connaître la localisation d'un abonné
- Deux mécanismes de base :
  - Localisation à la cellule prés
    - Connaître la position exacte du mobile
    - Lourde charge de signalisation
    - Coût de localisation important mais pas de recherche (rapidité)
  - Localisation vaste
    - Localisation sur un vaste ensemble de cellules
    - Recherche avec *paging* : émettre des messages d'avis de recherche dans les cellules visitées dernièrement
    - Coût de recherche élevé (signalisation élevée) mais coût de localisation faible
- Remarque : un VLR peut gérer plusieurs zones de localisation

MM : Mise à jour de la localisation

La procédure de mise à jour de localisation :

- Elle est à l'initiative du mobile
- Elle est périodique
- Elle est activée également quand le mobile se déplace et entre dans une cellule appartenant à une nouvelle zone de localisation
- Résumée par :

  - Le mobile sait qu'il change de zone de localisation grâce au canal BCCH qui contient la référence de la zone de localisation
  - Il transmet son TMSI au nouveau VLR
  - Le nouveau VLR, qui peut être l'ancien, récupère auprès de l'ancien le profil du mobile
  - Le VLR informe le HLR de la nouvelle zone de localisation du mobile
  - Le HLR demande à l'ancien VLR d'effacer les infos relatives au mobile (si VLR différent)

MM : Sécurité

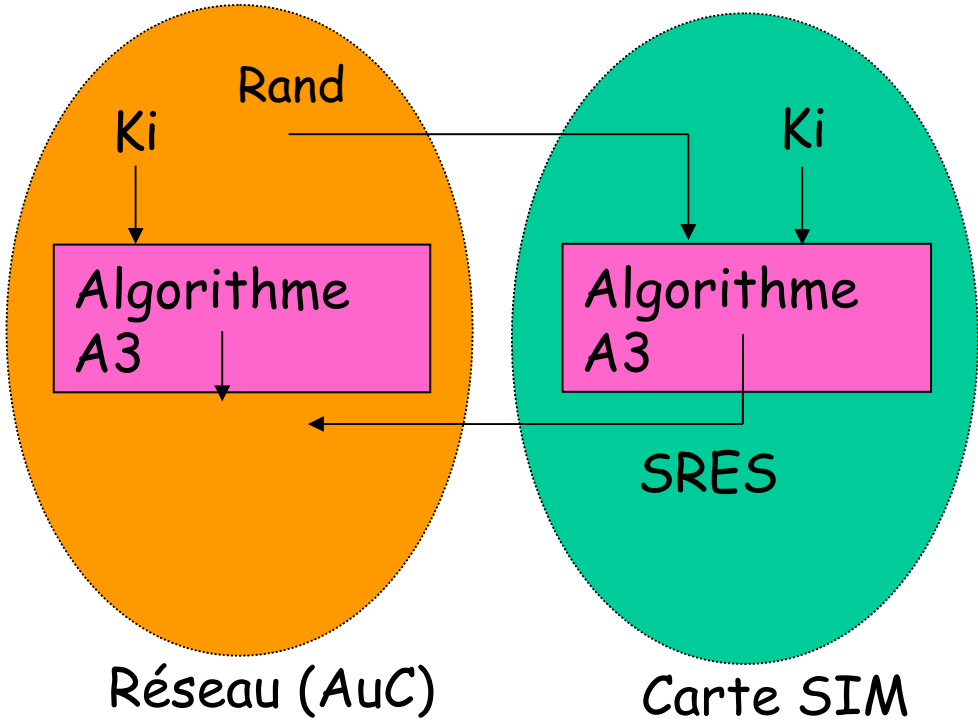
- Sécurité : protection de l'utilisateur et du réseau
  - Usurpations d'identité, écoutes frauduleuses, utilisations abusives
- Authentification du terminal
  - Grâce au numéro IMEI
  - EIR : contient la liste des terminaux volés ou impropres à l'utilisation
- Authentification de l'abonné
- Cryptage de la communication

MM : Authentification

- Authentification
  - A l'initiative du réseau
  - Permet de vérifier que l'utilisateur (SIM) est bien celui qu'il prétend être
  - La vérification peut être faite à n'importe quel moment
  - Principe : poser une question dont la réponse est connue que de l'abonné visé (sa carte SIM)

MM : Principe d'authentification

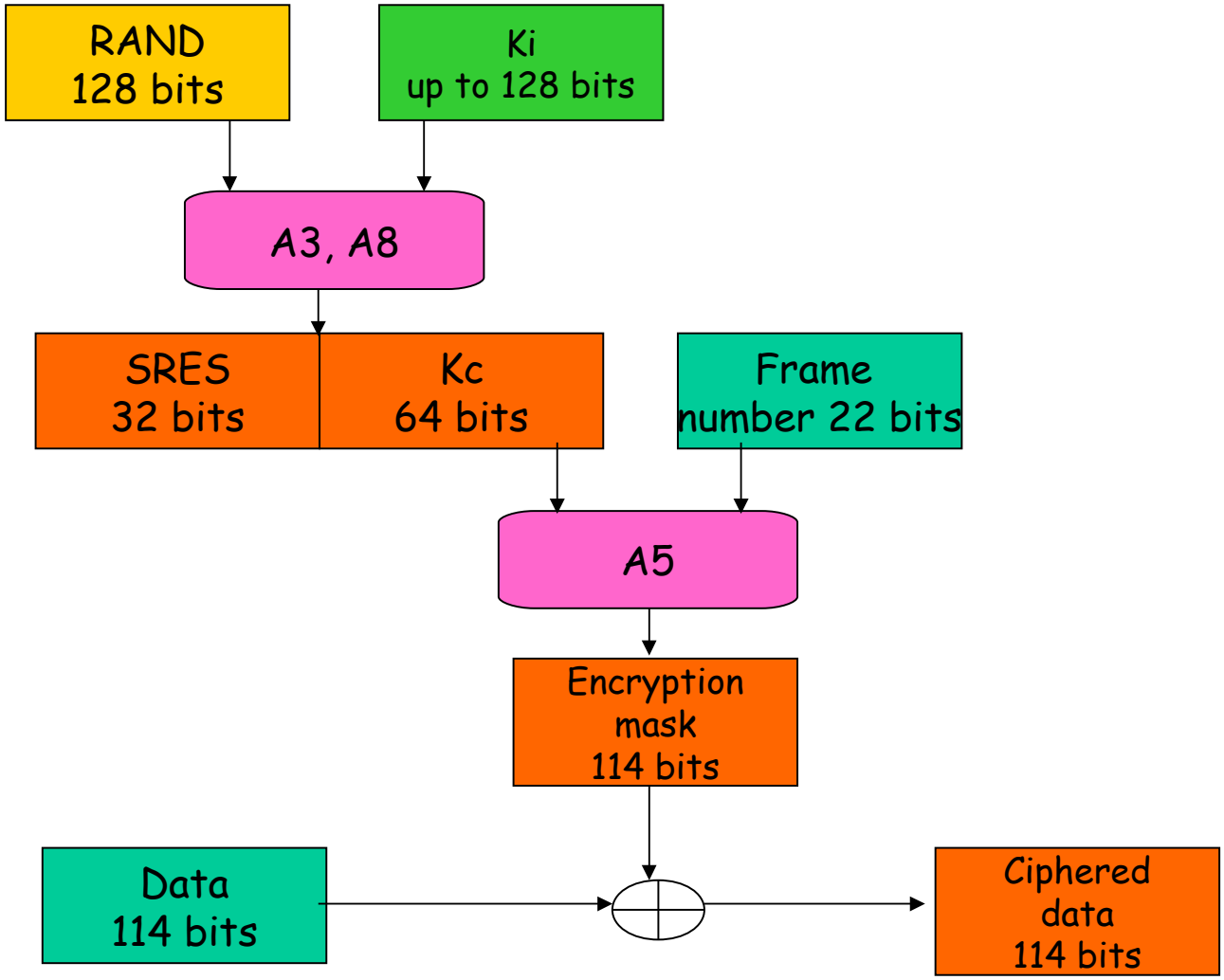
- Authentification
  - L'AuC (Authentification Center) transmet un nombre aléatoire Rand (128 bits)
  - Calcul : mobile et réseau
  - Transmission du résultat SRES
  - Ki secrète n'est connu que du réseau et de la carte SIM (jamais transmise)



MM : Principe de cryptage

- Cryptage
  - Protection contre les écoutes inopportunes
  - De Ki + Rand + A8 est calculée la clé Kc
  - Kc : 64 bits
  - Séquence générée par A5 : Kc,numéro de trame
  - Combinaison avec la séquence à émettre
  - Kc est stockée par le mobile et par la station de base lors de la procédure d'authentification, mais il est utilisé plus tard lors de communication

MM : Sécurité


RAND
128 bits
Ki
up to 128 bits
A3, A8
SRES
32 bits
Kc
64 bits
Frame
number 22 bits
A5
Encryption
mask
114 bits
Data
114 bits
Ciphered
data
114 bits

CM : Gestion des connexions

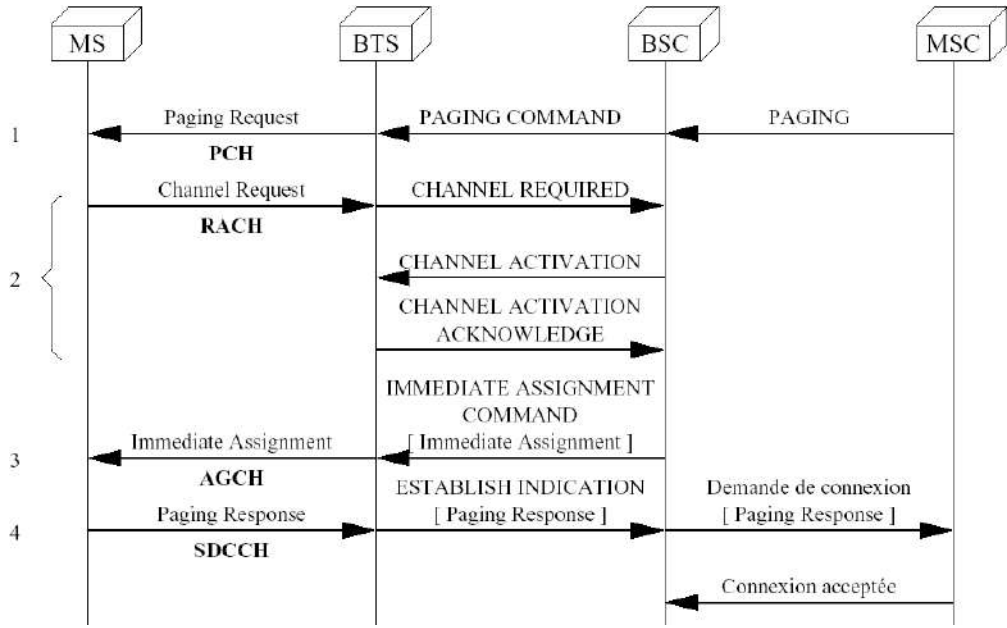
- CM gère l'établissement et le relâchement des connexions
- Utilise les standard des réseaux fixes et signalisation SS7
- L'établissement d'un appel diffère suivant son origine
- Appel issu du mobile
  - Allumer le portable
  - Parcourt des fréquences
  - Sélectionne la cellule et le PLMN
  - État Idle
  - Signalisation périodique pour la localisation
  - Composition d'un numéro
  - Envoi d'une demande de connexion via RACH
  - Allocation d'un canal dédié de signalisation SDCCH via AGCH
  - Procédures d'authentification et d'autorisation d'appel
  - Le réseau route la demande vers le RTCP (SS7)

CM : Gestion des connexions

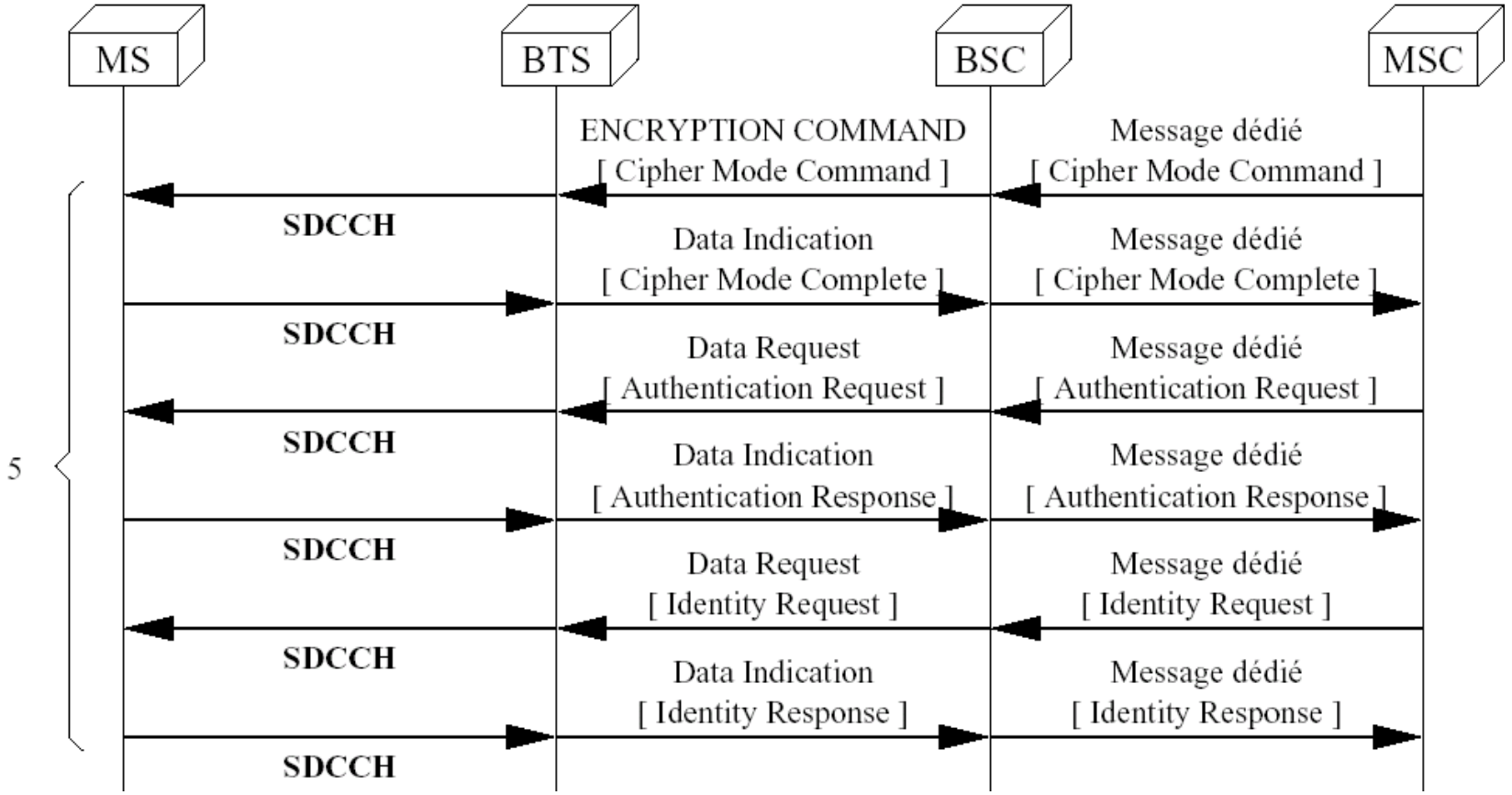
- Appel vers un mobile
  - Appel en utilisant le MSISDN
  - Appel acheminé jusqu'au GMSC le plus proche
  - Le HLR du mobile est interrogé pour
    - trouver le VLR courant
    - vérifier les caractéristiques de l'abonnement
    - traduction du MSISDN en IMSI
  - Le VLR diffuse le message de paging PCH dans la zone de localisation
  - Réponse du mobile (demande d'ouverture de canal (via RACH, réponse paging)
  - Établissement comme précédemment (entre GMSC et le mobile via VLR-MSC)

Appel type vers le mobile (1)

1. Recherche de l'abonné, décidée par le MSC et diffusée par toutes les BTS de la zone de localisation sur leur canal de *paging* PCH.
2. Réponse du mobile sur le canal RACH réservé à cet effet. La BTS informe le BSC d 'un nouvel arrivant ; en réponse, elle reçoit l'ordre de réserver pour ce mobile un canal de signalisation dont toutes les caractéristiques sont précisées dans le message : fréquence, numéro de *timeslot* et type de l 'activation.
3. Basculement sur un canal dédié de signalisation : le mobile est informé sur un canal AGCH commun à tous les mobiles de la cellule qu'il doit basculer vers le canal SDCCH qui lui a été réservé lors de l'étape précédente.
4. Etablissement de la connexion sur le canal dédié et transmission de la raison de la connexion : réponse à un appel entrant.

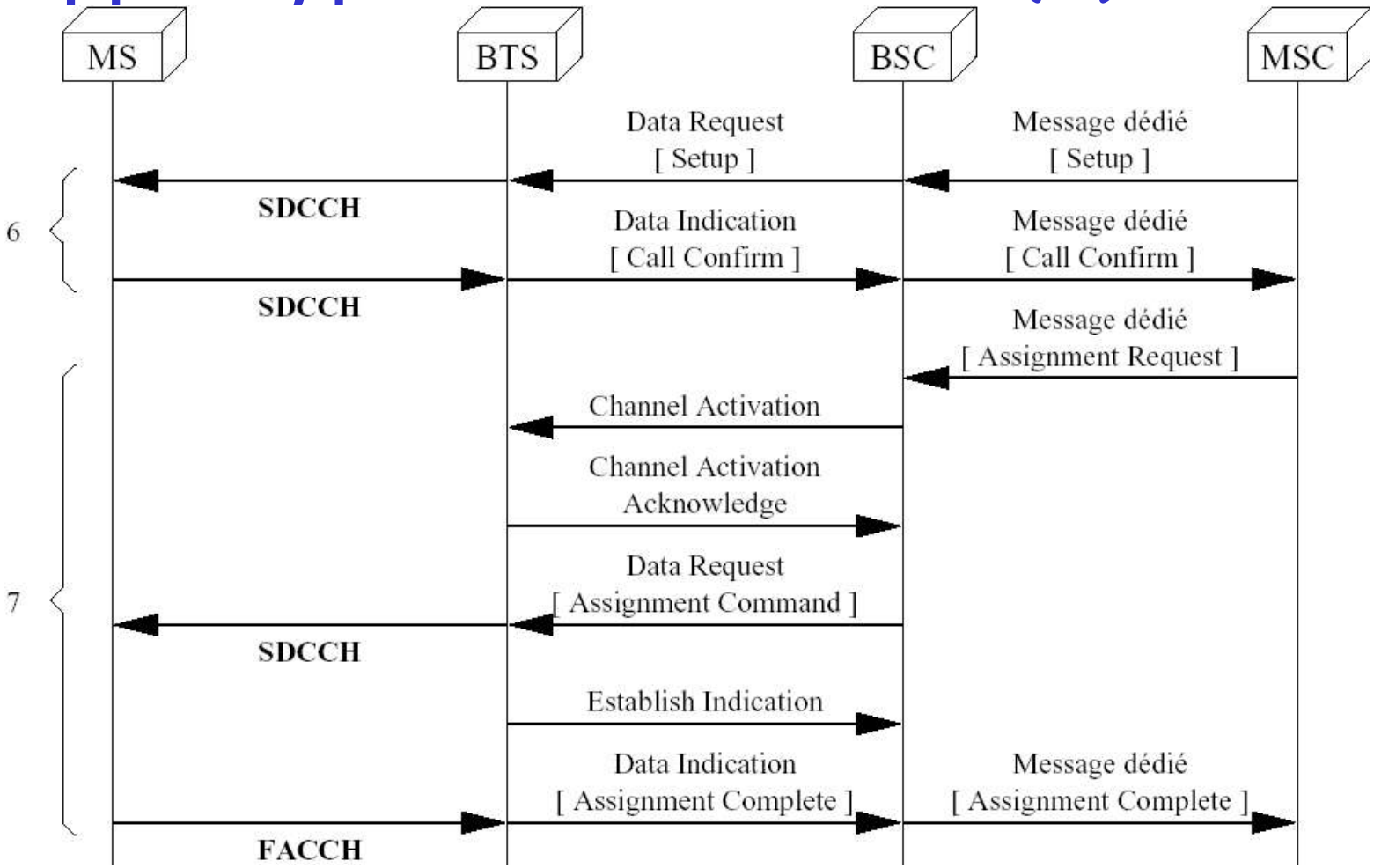


Appel type vers le mobile (2)



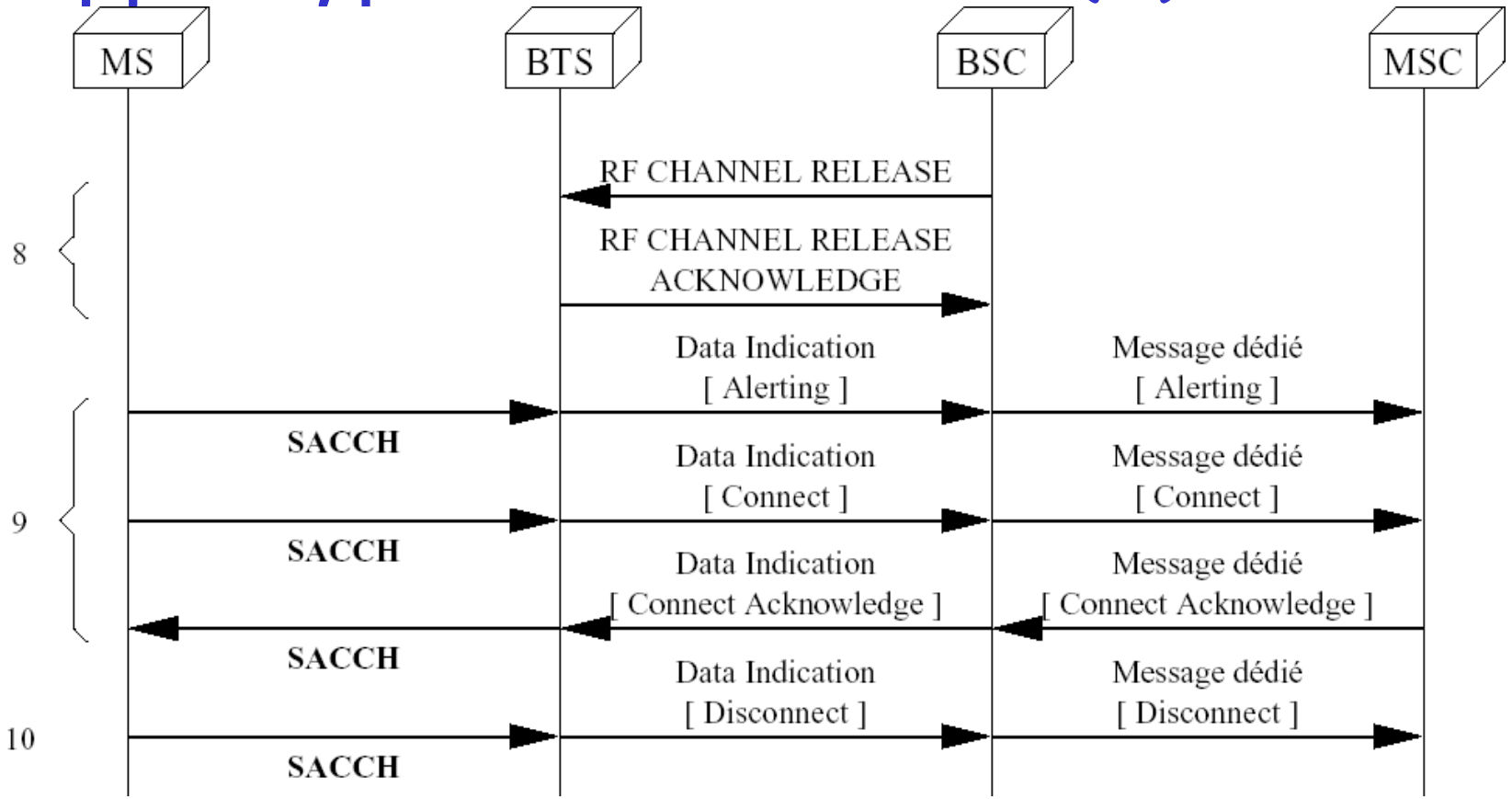
5. **Procédures d'authentification**, de chiffrement et éventuellement d'identification.

Appel type vers le mobile (3)



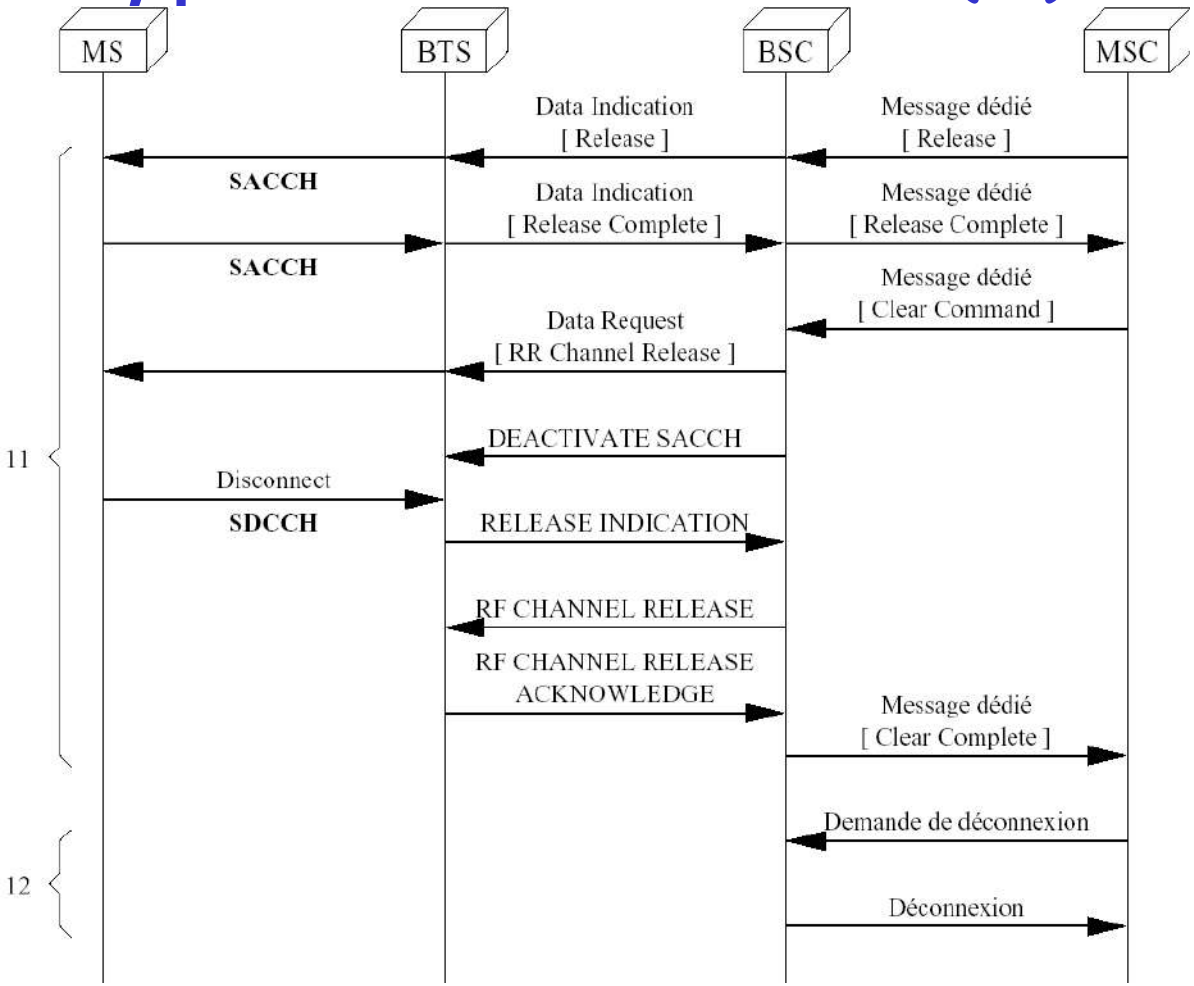
6. **Acheminement du numéro** jusqu'à l'appelé (et éventuellement de tous les services supplémentaires : numéro de l'appelant, etc.) et confirmation par le mobile.
7. **Basculement sur un canal dédié de trafic** TCH+SACCH.

Appel type vers le mobile (4)



8. **Libération du lien SDCCH.**
9. **Avertissement de la sonnerie** jusqu'au décrochage par l 'appelé. La conversation se déroule ensuite normalement jusqu'à la déconnexion des interlocuteurs, avec éventuellement un ou plusieurs *handovers*.
10. **Fin de connexion au niveau des couches hautes** du protocole.

Appel type vers le mobile (5)



11. **Fin de connexion du lien radio** entre le mobile et le réseau : désactivation du canal de trafic par basculement sur un canal SDCCH, puis relâchement de ce dernier canal.
12. **Fin de connexion au niveau des couches basses** du protocole.

Le GSM (bis)

- AGCH : *Access Grant CHannel*
- BSC : *Base Station Controller*
- BTS : *Base Transceiver Station*
- FACCH : *Fast Associated Control CHannel*
- MSC : *Mobile-services Switching Center*
- PCH : *Paging CHannel*
- RACH : *Random Access CHannel*
- RF : *Radio Frequency*
- RR : *Radio Resource management*
- SACCH : *Slow Associated Control CHannel*
- SDCCH : *Slow Dedicated Control CHannel*