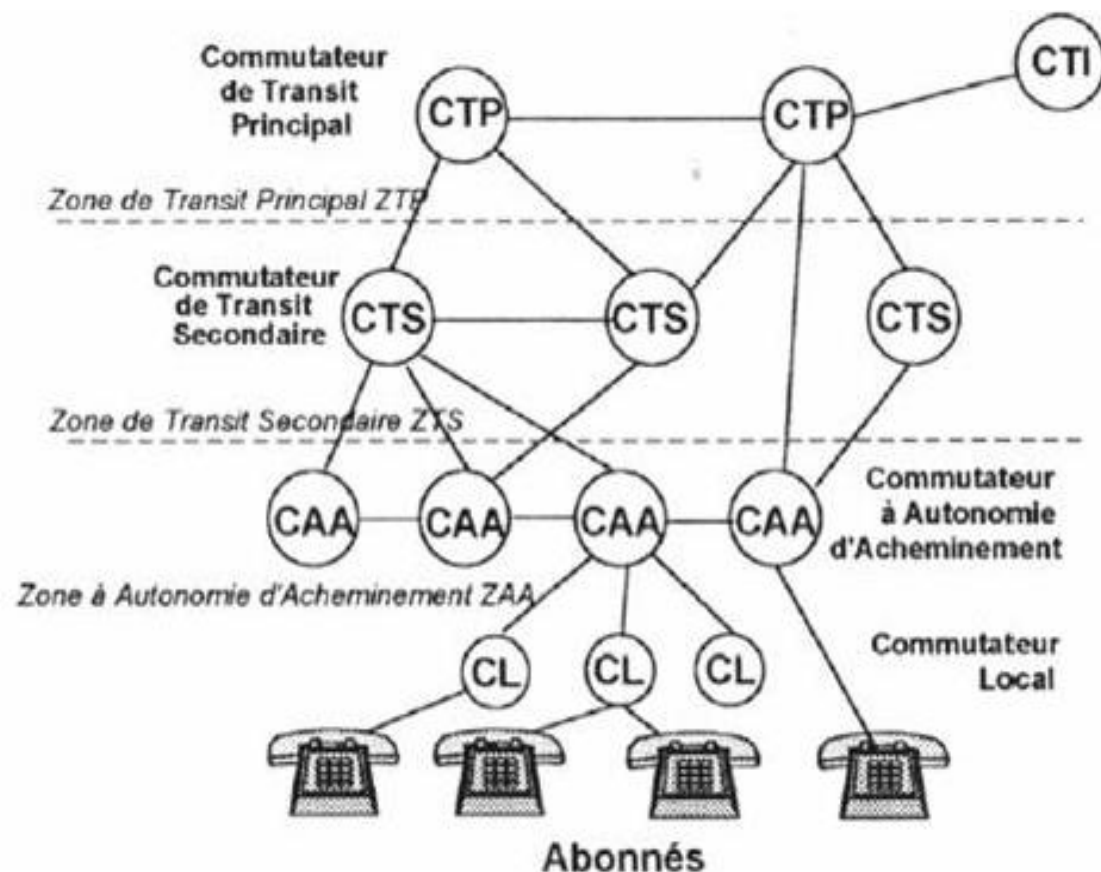


La téléphonie mobile

- Introduction
- GSM
- GPRS (EDGE)
- UMTS
- LTE – LTE advanced
- 5G



Téléphonie fixe



Architecture
présente sur le
territoire

- Liaison analogique vers le Commutateur Local, et aussi le CAA
- Liaison numérique autrement
- Fibre optique entre les différents équipements

Fin commercialisation ligne RTC : début 2019 → passage en VoIP

Correspondances bande/fréquence

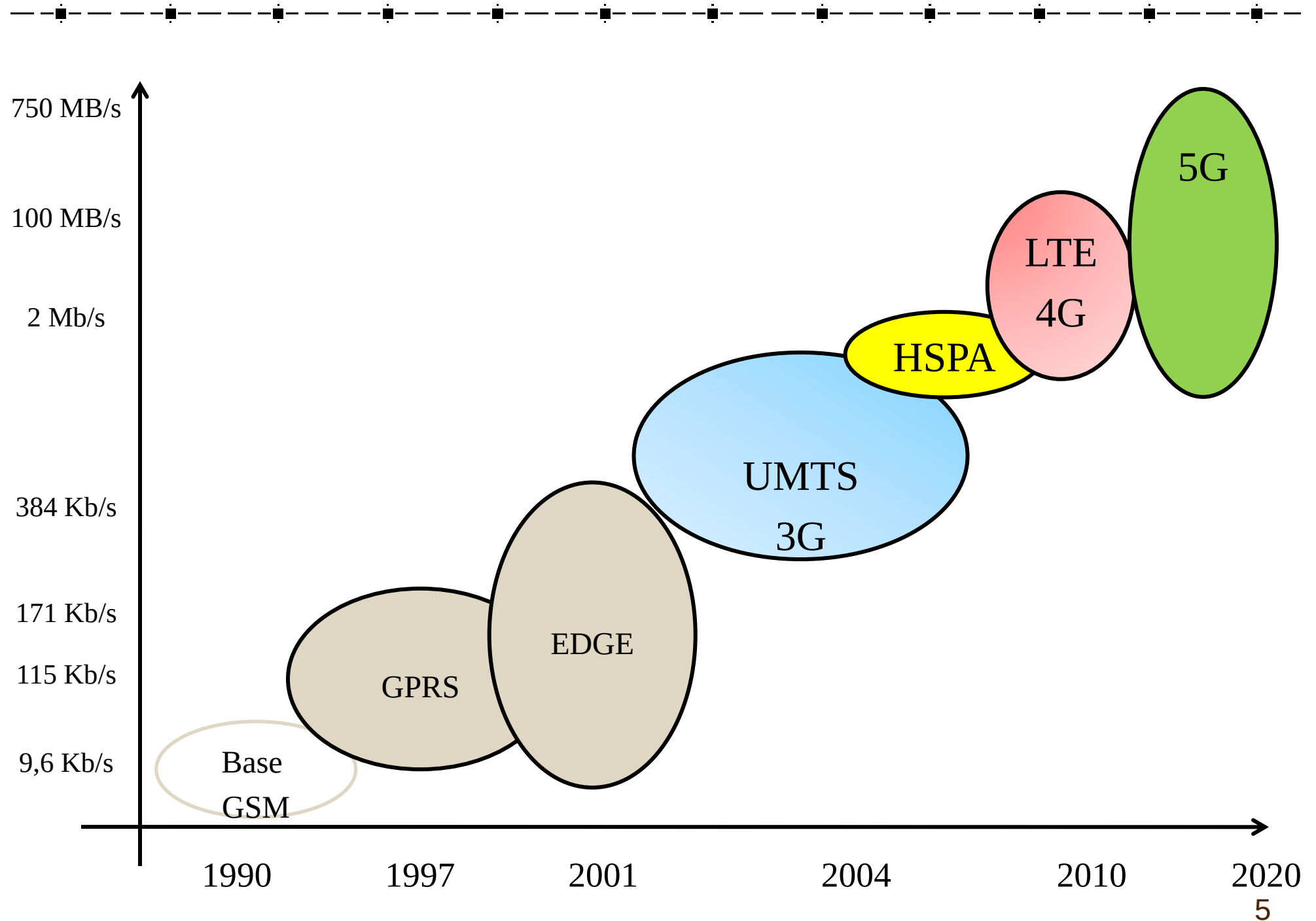
Bande de fréquences possibles en téléphonie (actuellement)

Bandes	Fréquences	Bandes	Fréquences
B1	2 100 Mhz	B18	800 Mhz
B2	1 900 Mhz (PCS)	B19	800 Mhz
B3	1 800 Mhz	B20	800 Mhz (DD)
B4	1 700 Mhz	B21	1 500 Mhz
B5	850 Mhz	B25	1 900 Mhz
B7	2 600 Mhz	B26	850 Mhz
B8	900 Mhz	B28	700 Mhz (APT)
B9	1 800 Mhz	B30	2 300 Mhz
B11	1 500 Mhz	B38	2 600 Mhz (TD)
B12	700 Mhz (ac)	B39	1 900 Mhz (TD)
B13	700 Mhz (c)	B40	2 300 Mhz (TD)
B17	700 Mhz (bc)	B41	2 500 Mhz (TD)

Génération de réseaux mobiles

Génération	Services	Nom	Type d'accès	Période de vie
1	Téléphonie	R2000, NMT,..	Analogique, FDMA	1980-1995
2	Téléphonie, SMS	GSM	TDMA	1991-
2,5	Téléphonie, SMS Accès IP 100kb/s	GPRS, EDGE	TDMA + accès paquet	2000-
3	Téléphonie, SMS, Accès IP 1 Mb/s	UMTS	CDMA	2002-
3,9	Téléphonie, SMS, Accès IP 10 Mb/s	HSDPA	CDMA+ nouvelle modulation	2008-
4	Accès IP à 100 Mb/s	LTE	OFDM	2010-
5	Accès IP à 1Gb/s	5G	OFDM, MIMO	2020-

Comparaison



Les réseaux cellulaires

✦ Un téléphone est associé à une fréquence
=> mais nombre de fréquences limitées.

✦ Solutions envisagées:

- ✦ Chaque terminal peut utiliser **différentes fréquences** qui lui sont attribuées par l'opérateur, en fonction des ressources disponibles
- ✦ **Création de cellules**, où chaque cellule utilise des fréquences différentes
 - Puissance des terminaux limitée
 - 2 cellules adjacentes ne doivent pas pouvoir interférer
 - Réutilisation des fréquences pour des cellules lointaines
 - Les cellules ont des tailles différentes (macro-cellule, micro-cellule)
- ✦ **Passage d'une cellule à l'autre => Handover**
- ✦ **Utilisation d'un opérateur étranger => Roaming**

Identification de l'utilisateur

- ✦ Avant utilisation d'une carte SIM (Subscriber Identity Module), valable pour la 2G
- ✦ Actuellement **USIM** (Universal SIM)
 - ✦ Contient **IMSI (Internationale Mobile Subscriber Identity)**
 - ✦ IMSI :
 - MCC (Mobile Country Code) 3 chiffres
 - MNC (Mobile Network Code) 2-3 chiffres
 - MSIN (Mobile Subscriber Identification Number) 9-10 chiffres

Ex : France 208 01=ORANGE, 10 =SFR, 15=FREE

-> numéro unique qui caractérise un usager

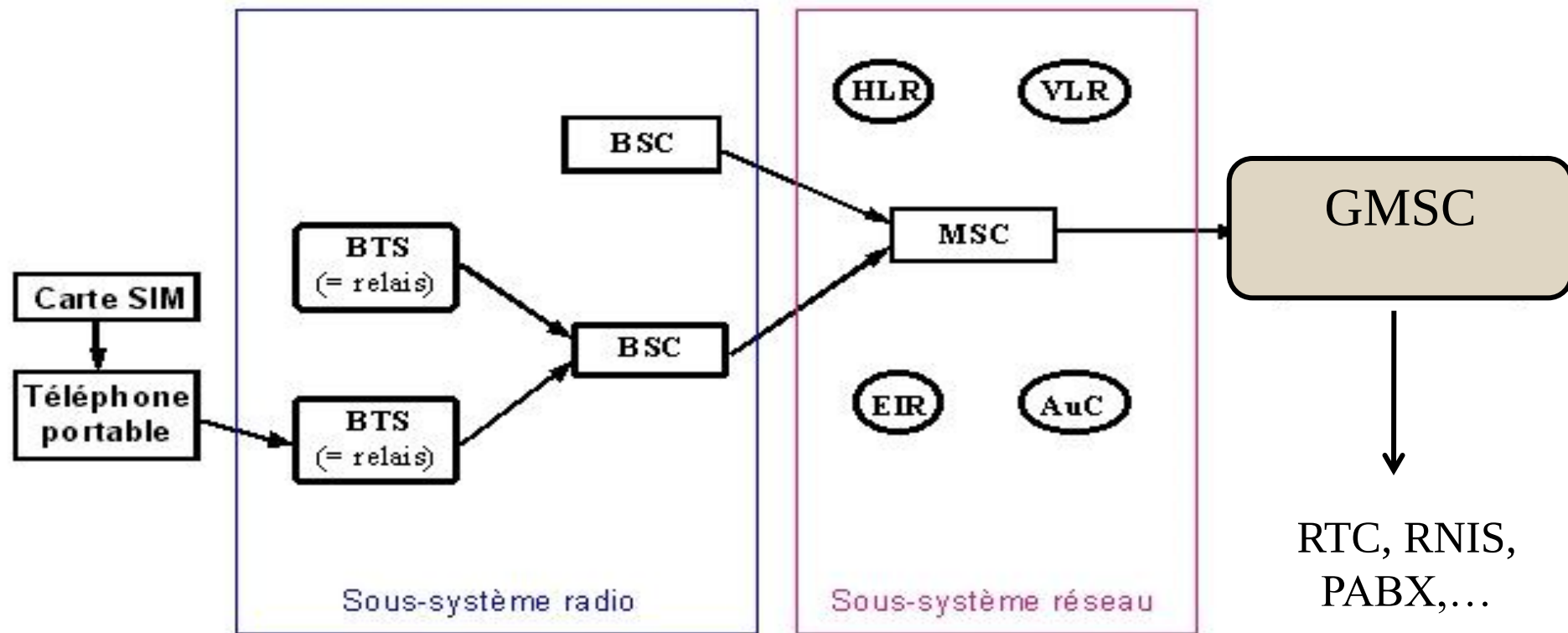
Le réseau GSM

GSM = Global System for Mobile communications

- ✦ Norme adoptée en 1986
- ✦ En **1987 13 pays Européens** se mettent d'accord pour développer un réseau **GSM** sur la bande des 900 Mhz
- ✦ En **1990** une adaptation dans **la bande 1800 Mhz est mise en place: DCS1800 (Digital Communication System).**
- ✦ De leur côté **les Américains** reprennent une version du GSM dans la bande des 1900 Mhz, le **DCS 1900**

- ✦ Mode commutation de circuit
- ✦ **Un mobile : appareil portatif en version 2 Watts**
 - ◆ Mobile dual-bande ou tri-bande
 - ◆ Mobile possède un n° d'identification internationale IMEI (*#06#) -> BD EIR
 - ◆ Obligation d'une carte SIM pour pouvoir utiliser toutes les fonctionnalités.

Architecture du réseau GSM (1)



BTS (Base Transceiver Station) : station de base (relais)
BSC (Base Station Controller) : contrôleur de station de base
MSC (Mobile Services Switching Center) : Centre de commutation radio mobile
VLR (Visitors Location Register) : Registre de localisation des visiteurs
EIR (Equipment Identity Register) : Registre d'identité des équipements
AuC (Authentication Center) : Centre d'authentification
HLR (Home Location Register) : Registre de localisation nominal
GMSC (Gateway Mobile Service Center)

Architecture du réseau GSM (2)

✦ Les stations de base (BTS)

- ✦ La fonction essentielle d'une **station de base (BTS ou Base Transceiver Station)** est d'assurer la transmission d'un signal radio entre les radiotéléphones et le réseau de l'opérateur.
- ✦ 1 BTS représente 1 cellule.
- ✦ Ainsi la BTS fournit aux utilisateurs présents dans la cellule **un point d'accès dans le réseau pour pouvoir recevoir ou émettre des appels.**
- ✦ La capacité maximale d'une BTS est de 12 TRX (Transmission/Reception Unit).
 - Pour améliorer la capacité de trafic on réduit au minimum la puissance de ces BTS en ville de manière à couvrir une zone plus petite.
 - Mais cela entraîne évidemment une multiplication importante des coûts: **une BTS coûte en moyenne 300 000 Euros**

Exemple le réseau SFR compte plus de 6 000 BTS en France.

Architecture du réseau GSM (3)

✦ Différentes BTS

- Les BTS rayonnantes (pour les larges espaces)
- Les BTS ciblés (zones à forte densité d'abonnés)
- Les micro BTS (lieu très peuplé)
- Les antennes peuvent être : omnidirectionnelles, bidirectionnelles ou tri-sectorielles (les plus fréquentes)

Nécessité d'une étude approfondie pour le placement d'une BTS

Toute BTS est raccordée à un BSC (Contrôleur de station)



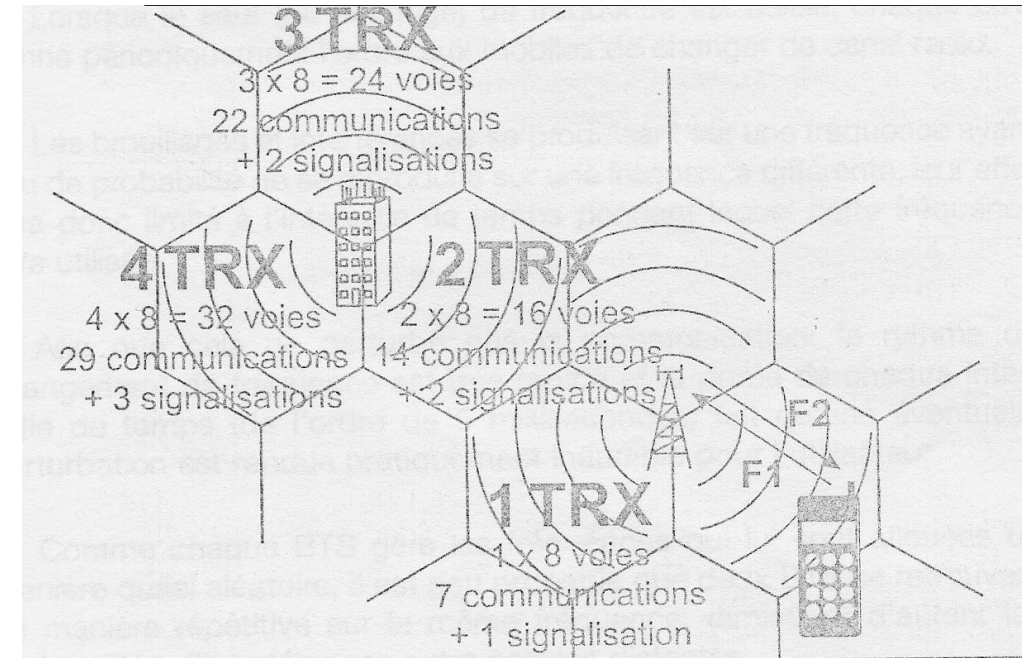
Joue le rôle de concentrateur

La liaison est en générale filaire (Fibre optique, cuivre,...)

Architecture du réseau GSM (4)

♦ La planification des fréquences:

- Une BTS comporte 1 ou plusieurs modules émetteurs-récepteurs
- Chaque module ou **TRX** est constitué d'un couple de fréquences (une pour recevoir les données, l'autre pour les envoyer)
- Un **TRX** permet 8 communications simultanées: parole, données ou signalisation.
- Max : 12 TRX par antenne (en réalité, 9)



Le MSC est un commutateur d'un réseau mobile, il redirige les appels vers :

- les autres opérateurs
- le réseau RTC
- un autre BSC



Joue le rôle de CAA

Le GSM : l'interface radio (1)

✧ Bandes de fréquences:

✧ Du mobile vers l'antenne : voie montante

- Pour le GSM, de 890 Mhz à 915 Mhz (extension entre 880 Mhz et 890 Mhz)
(donc 25 Mhz)
- Pour le DCS 1800, de 1710 Mhz à 1785 Mhz
(donc 75 Mhz)

✧ De l'antenne vers le mobile : voie descendante

- Pour le GSM, de 935 Mhz à 960 Mhz (extension entre 925 Mhz et 935 Mhz)
- Pour le DCS 1800, de 1805 Mhz à 1880 Mhz

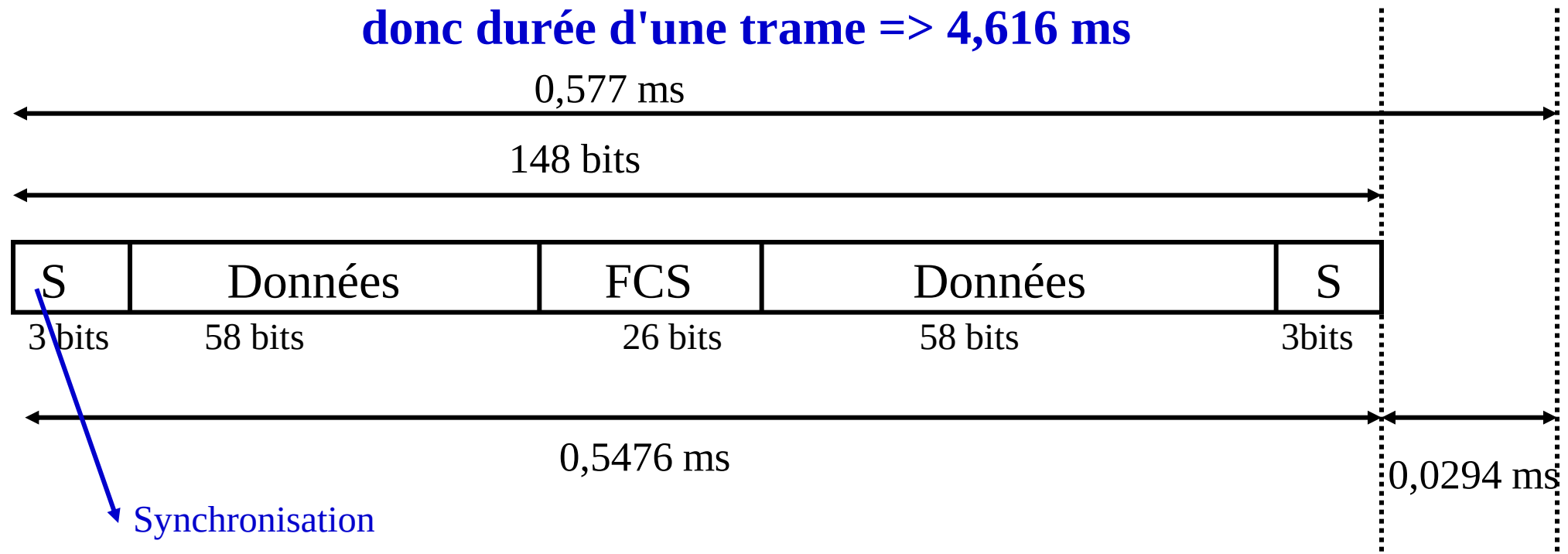
✧ Pour émettre, une porteuse utilise une bande de fréquence de **200 Khz**

⇒ **en GSM, 125 fréquences à se répartir entre les opérateurs** ($125 * 200 \text{ Khz} = 25 \text{ Mhz}$)

Le GSM : l'interface radio (2)

✦ Partage en temps TDMA

- ✦ Chaque porteuse est divisée en 8 intervalles de temps ou **slot** (slot 0 réservé en général pour la signalisation)
- ✦ La durée élémentaire d'un slot est de **0,577 ms**
donc durée d'une trame => 4,616 ms



Pour chaque trame, changement de fréquence

=> permet une meilleure réception

GSM (Mise sous tension)

✦ 3 étapes:

✦ Sélection de PLMN (Public Land Mobile Network)

- Plusieurs PLMN par pays (chaque opérateur propose un PLMN)
- PLMN = Mobile Country Code + Mobile Network Code (cf transparent 9)
ex : France : MCC=208, MNC_orange=01, MNC_SFR=10
- A la mise sous tension, récupération de la liste des PLMN dispo
 - ✦ Carte SIM indique PLMN prioritaire => choix du PLMN
 - ✦ Si aucun PLMN possible, N° urgence seule

✦ Sélection de la cellule

- Recherche des cellules candidates
- Liste ordonnée des cellules via le signal de réception

✦ Inscription sur le réseau

- Contacte le HLR, EIR et AuC

GSM : établissement d'un appel (1)

✧ Autres équipements actifs : Deux bases de données:

- ✧ **HLR (Home Location register)** qui contient les caractéristiques des abonnés, ainsi que le MSC et VLR de rattachement (actuel)
- ✧ **VLR (Visitor Location Register)** qui localise les mobiles traversant la zone du MSC.
- ✧ **AuC** : chargé de l'authentification de l'abonné, ainsi que du chiffrement de la communication. Le AuC se base sur le HLR afin de récupérer les informations relatives à l'utilisateur et pour ainsi créer une clé d'identification.

✧ Etablissement d'un appel depuis un mobile:

- ✧ La **BTS transmet le numéro** appelé au MSC, via un BSC
- ✧ Le **MSC vérifie** auprès de son VLR et HLR si la demande est réalisable en fonction des caractéristiques de l'abonné
- ✧ Après accord le MSC effectue deux choses:
 - **Autoriser la BTS à allouer un canal** pour transporter la voix
 - **Établir une connexion vers le destinataire** et gérer la signalisation

GSM : établissement d'un appel (2)

✦ Réception d'un appel sur le mobile

- ✦ **Demande arrive sur le MSC** le plus proche de l'appelant
- ✦ **Le MSC interroge le HLR:**
 - S'il est autorisé à acheminer la communication
 - Pour obtenir les références du MSC dont le VLR a localisé le mobile
- ✦ Le **MSC établit une connexion vers le MSC destinataire** en recherchant le chemin optimal
- ✦ Le **MSC destinataire** en fonction de la LAC (Location Area Code) récupérée via le VLR **établit une liaison avec les BSC et BTS.**
- ✦ Lorsque le mobile répond, la signalisation **établit les circuits nécessaires à l'acheminement de la communication** vers la cellule concernée

GSM : le handover

✧ BCCH : Broadcast Control Channel

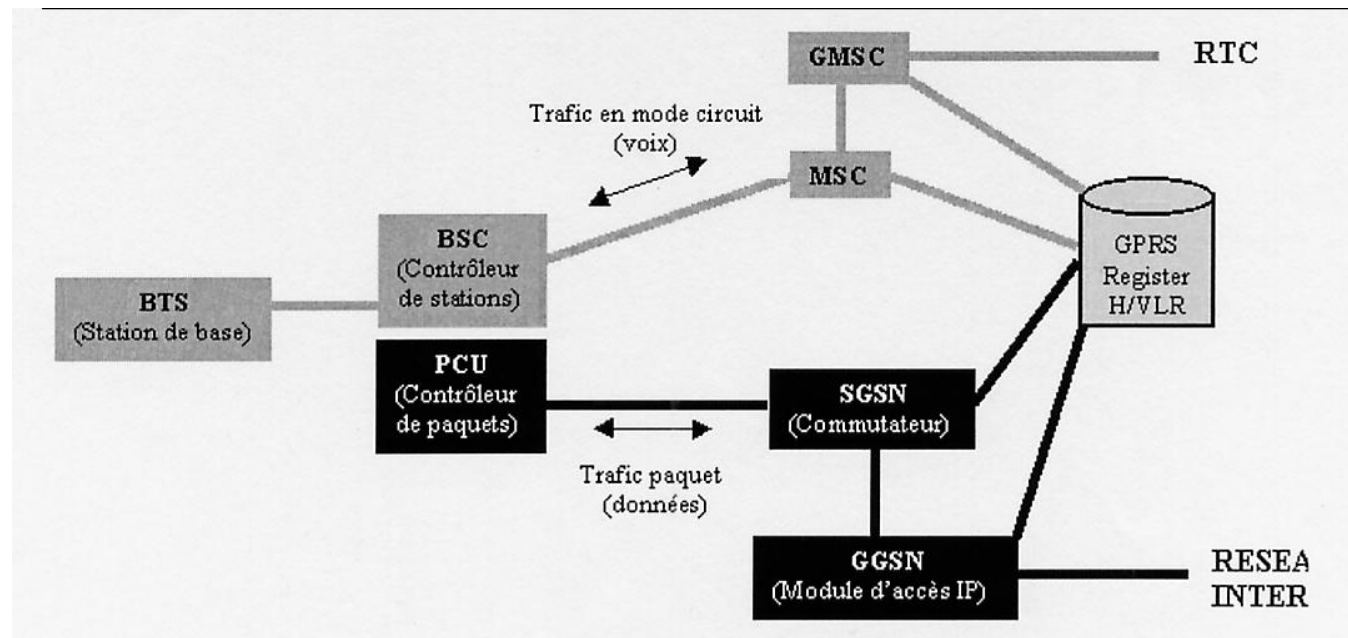
- Envoyé par chaque BTS
 - Utilise un slot d'une porteuse -> code identification antenne, N° cellule,...
- ✧ Un mobile se connecte toujours à l'antenne permettant de recevoir le signal le moins atténué -> connu par le BCCH
(envoie de l'information au MSC -> HLR)
- ✧ Quand le signal faiblit, le mobile écoute toutes les BCCH
- La BTS renseigne le mobile sur les cellules voisines (fréquences utilisées)
 - Le mobile calcule la puissance de réception de chaque BTS voisine.
 - Le mobile envoie ses conclusions au BTS
 - La BTS décide du handover
=> certaines fois de BSC.

GPRS : General Packet Radio Service

- ✧ Le GPRS constitue une **transition** vers la troisième génération des réseaux mobiles.
- ✧ Le GPRS ne constitue pas un réseau mobile à part entière mais une couche supplémentaire **rajoutée au réseau GSM existant**.
- ✧ Ainsi le GPRS utilise les bandes de fréquences attribuées au GSM.
- ✧ Le GPRS **appelé aussi GSM2+** repose sur la transmission en mode paquet.
- ✧ **EDGE (Enhanced Data for Global Evolution)** : Evolution du standard GPRS qui permet le transfert de données en mode paquets, à haut-débit (3x GPRS)
- ✧ Le GPRS offre un débit de 171 Kbit/s au maximum

Architecture du réseau GPRS

- ✧ Les **stations de base** ont seulement une évolution logicielle
- ✧ Le contrôleur de stations de base doit être doublé par un contrôleur de paquet **PCU** (**Paquet Controler Unit**).
- ✧ Ensuite intervient un **commutateur de paquet SGSN (Serving GPRS Support Node)**: il a pour fonction de vérifier l'enregistrement des abonnés, les authentifier et autoriser les communications.
- ✧ Et enfin le **GGSN (Gateway GPRS Support Node)** qui est la passerelle d'accès au réseau IP (Internet ou Intranet).



FIN GSM et GPRS → fin 2025

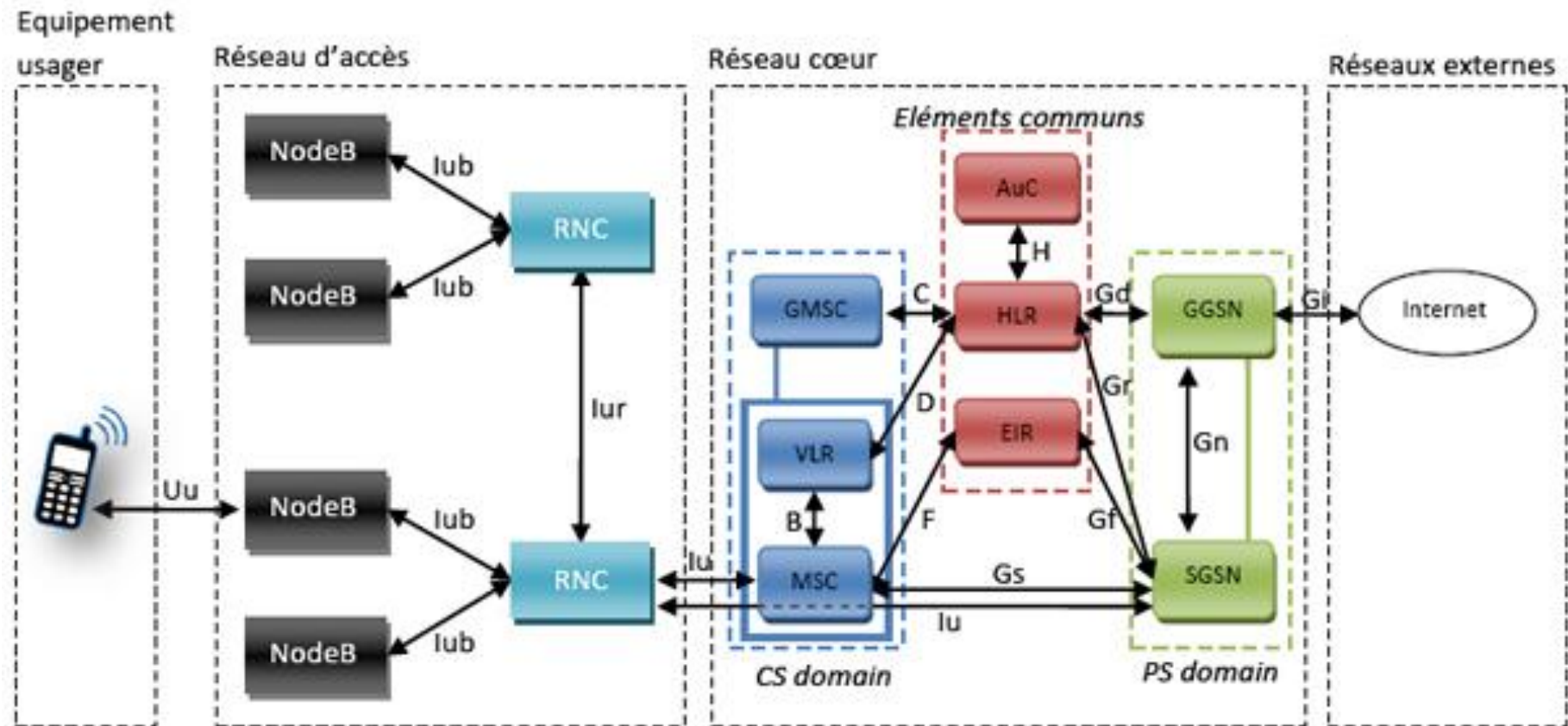
UMTS

✦ Système de radiotéléphonie de troisième génération

- ✦ Respecte les recommandations de l'IMT 2000
 - Europe : UMTS : Universal Mobile Telecommunication System (W-CDMA)
 - Amérique : CDMA-2000
 - Japon : W-CDMA (Wideband Code Division Multiple Access)
- ✦ Débit maximum de 2 Mb/s (static)
 - Mobilité permise -> débit max 384 Kbits/s
 - Couverture très réduite pour 2 Mb/s (pico-cellule)
- ✦ Bande passante
 - De 1900 Mhz à 1980 Mhz et de 2010 Mhz à 2170 Mhz
2 modes d'accès : FDD (Frequence) et TDD (Time Division Duplex)
- ✦ Mise en place d'un contrôle de puissance sur les téléphones

Architecture UMTS

Réseau UTRAN : UMTS Terrestrial Radio Access Network



Le cœur du réseau ne change pas => évolution faite avec GPRS

MAIS toutes les stations de base et les contrôleurs doivent changer

→ NodeB = BTS, RNC= BSC

Inscription auprès d'un réseau

✦ Après choix PLMN et cellule, 2 inscriptions possibles:

- ✦ Inscription au domaine CS (Circuit switched) -> téléphone
- ✦ Inscription au domaine PS (Packet Switched) -> data

(utilisation de différents protocoles : MAP –Mobile Application Part-..)

Inscription au domaine PS :

1 - Demande d'inscription entre le mobile et le SGSN, via le RNC

2 - Le SGSN demande au HLR les données de l'utilisateur et aussi au mobile (code IMEI, IMSI)

-> vérification de la correspondance

-> vérification dans le fichier EIR pour le portable

3 – Inscription du mobile dans le HLR

-> le HLR renvoie les infos de l'abonné au SGSN pour suivre le contrat

(Puis récupération @IP via le GGSN)

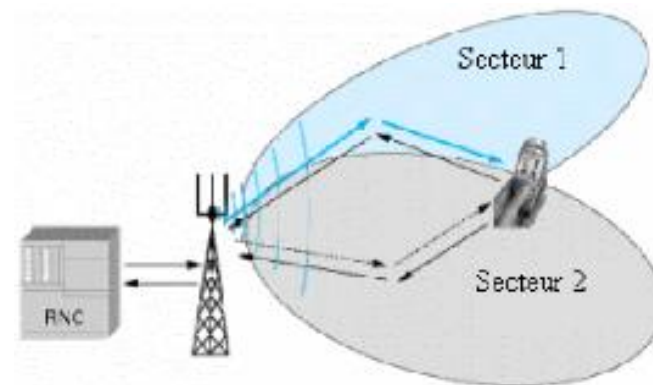
UMTS : handover (1)

✧ Remarque pour l'UMTS:

-> plusieurs canaux utilisés pour améliorer la communication

✧ Softer handover

- ✧ L'appareil mobile utilise plusieurs canaux de différentes antennes pour améliorer son signal
 - > on garde alors le meilleur canal lors du déplacement



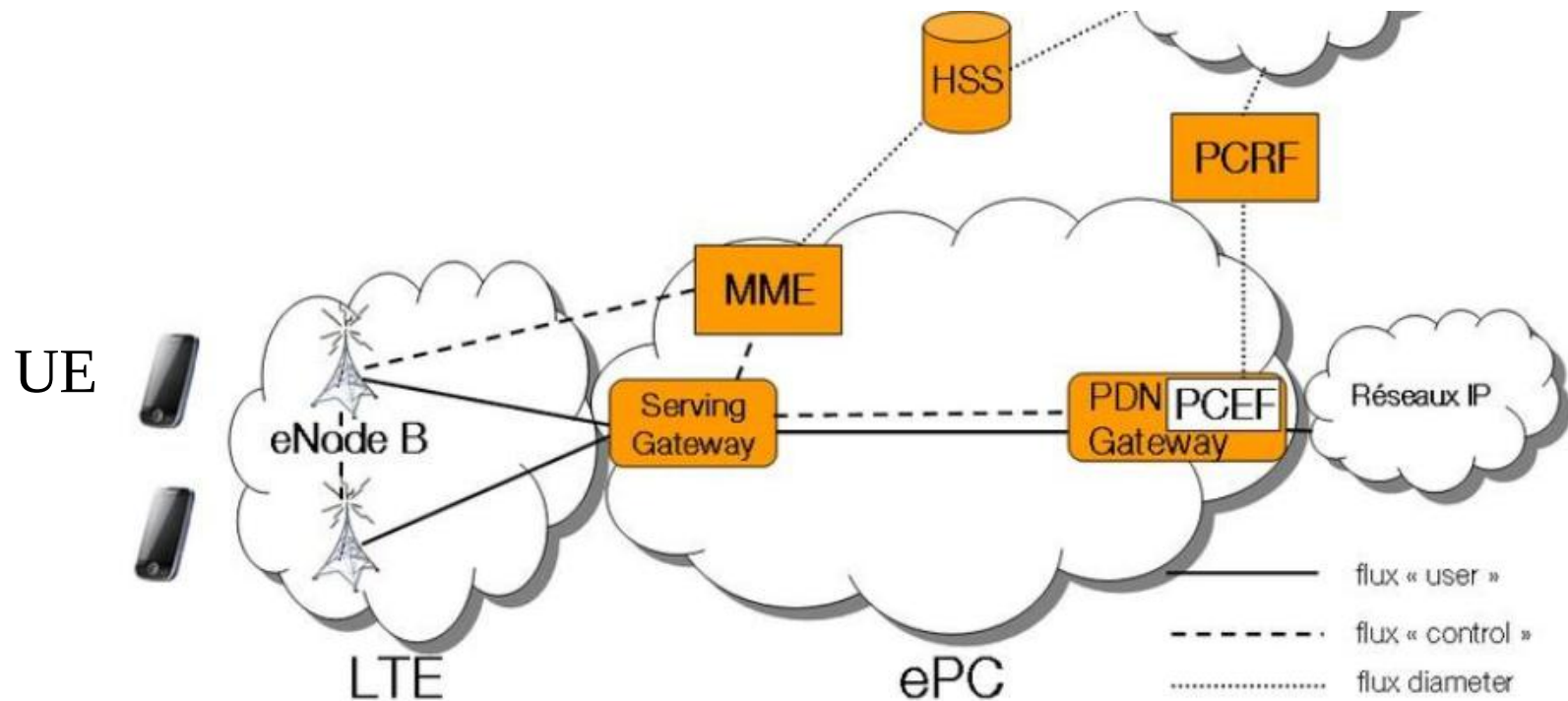
✧ Soft handover

- ✧ L'appareil mobile utilise plusieurs canaux appartenant à deux nœud B.
 - > on garde le meilleur canal lors du déplacement
 - **Le choix est fait par le RNC qui synchronise les émissions des 2 antennes.**
- ✧ Si les nœuds B font intervenir 2 RNC, création d'une liaison entre RNC
 - Discussion entre les RNC pour faire le handover

60 % des handovers en UMTS sont dans ces 2 catégories

4G : LTE (1)

- ✦ Tout en IP (abandon du CS), utilisation de VoLTE (volp sur LTE)
- ✦ Nouvelle architecture :



Enode B : evolved Node B (108000)

MME : Mobility Management Entity

HSS = HLR + Auc

ePC : Evolved Packet Core

SGW : Serving Gateway

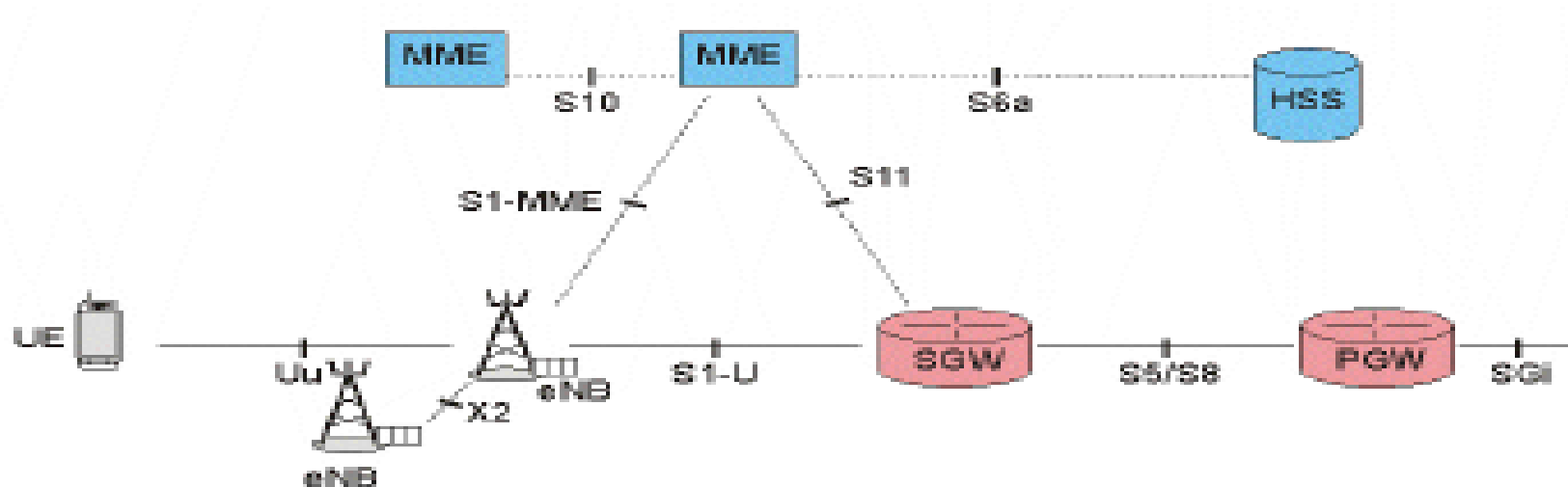
PGW : PDN Gateway, Packet Gateway

UE : User equipment

→ liaison IP avec routeur

4G : LTE (2)

✧ Interface de communication



S5 : entre SGW et PGW du même opérateur S8, pour 2 opérateurs différents

Communication : UE s'attache au MME

- vérification envoyée du MME vers le HSS du **IMSI**
- retour vers le MME du profil d'activité (APN, Access Point Name) qui contient le type Ipv?, l'@IP du PGW
- connexion du MME vers le SGW puis du SGW vers le PGW
- établissement d'une connexion IP entre le PGW<-> SGW<->eNB<->UE

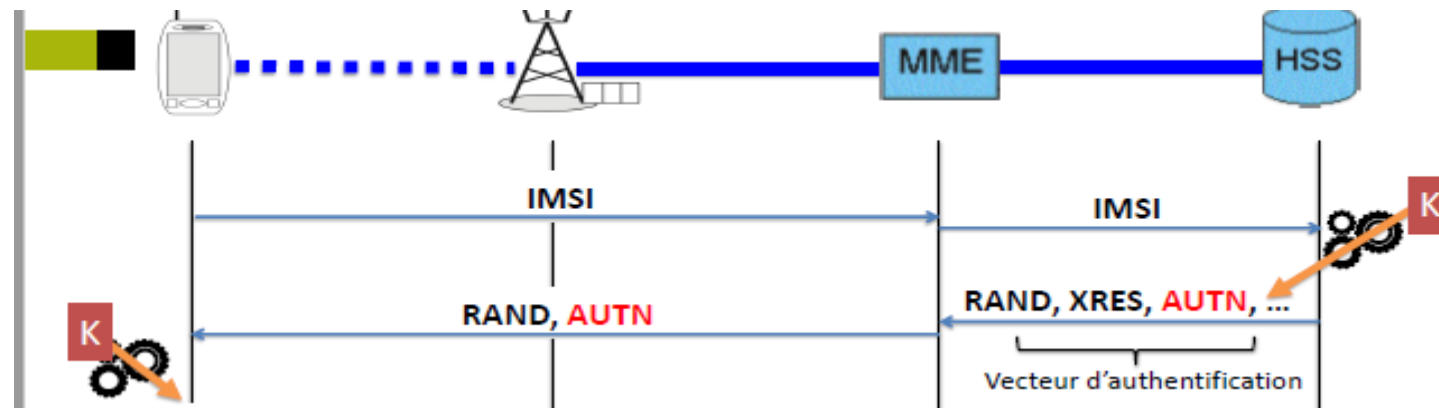
4G : sécurité

✦ Problème :

- ✦ Utilisation frauduleuse du réseau
 - Nécessité d'authentification
- ✦ Ecoute des échanges
 - Chiffrement (utilisation de clé et du chiffrement AES ou SNOW 3G)
- ✦ Modification des messages
 - Vérification de l'intégrité, que pour la signalisation
- ✦ Suivi/localisation d'un terminal
 - Mise en place d'une identité temporaire
 - Mécanisme pour diminuer le nombre de messages de localisation d'une UE
 - ✦ Paging via le TMSI

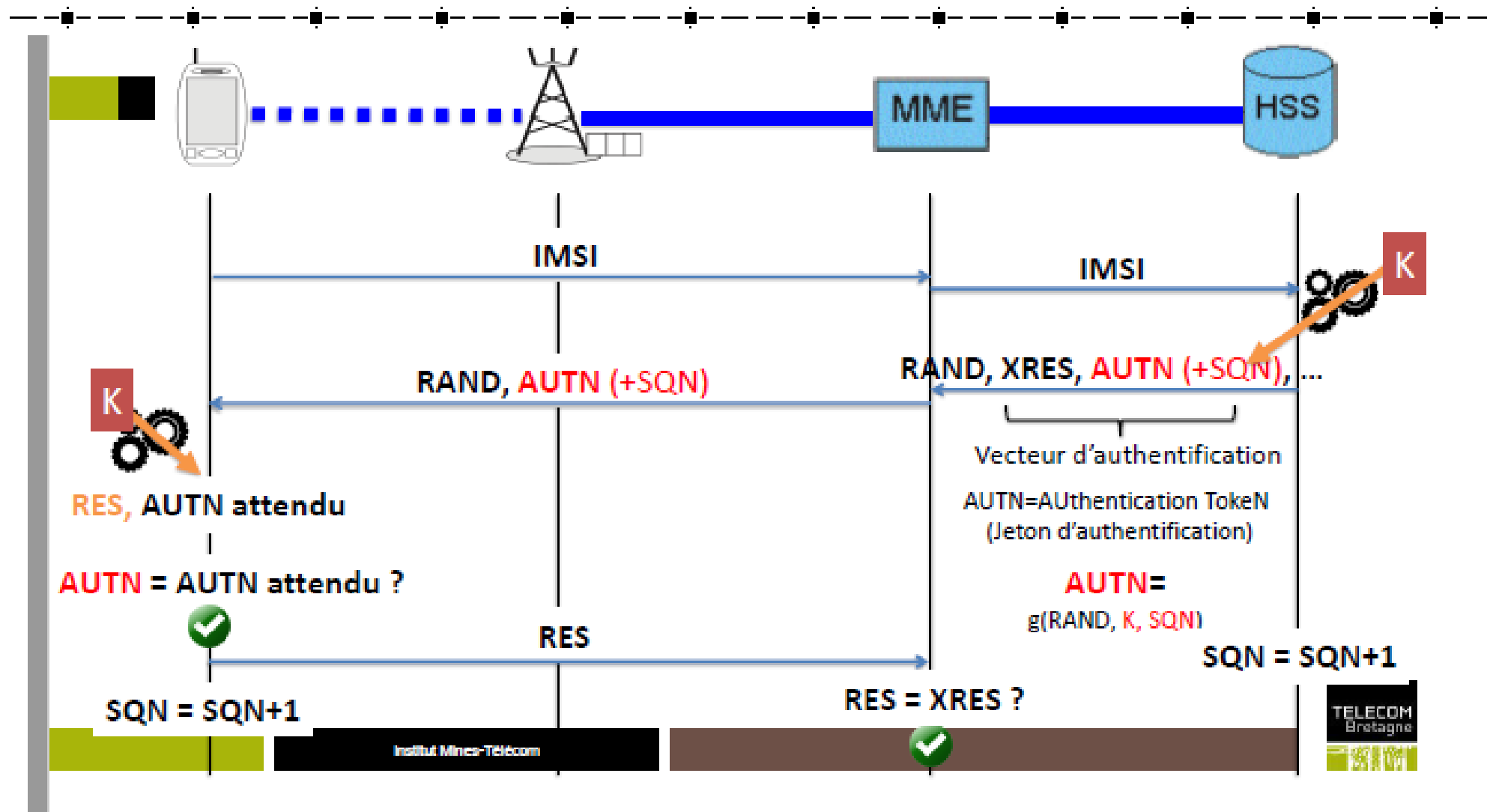
Authentication (1)

- ✦ S'assurer que l'UE peut se connecter sur le réseau, et pour l'UE, que c'est le bon réseau.
- ✦ Utilisation d'une clé secrète **K** partagée entre la SIM et le HSS.



- ✦ UE envoie son IMSI en clair, HSS tire aléatoirement un nombre RAND, et le chiffre avec clé K par l'algorithme $f \rightarrow XRES$, et par l'algorithme $g \rightarrow AUTN$
- ✦ UE connaît algorithme f et g , donc peut calculer les valeurs XRES et AUTN
- ✦ Clé connue seulement de HSS. Pour simplifier et ne pas toujours demander à HSS, envoi d'une clé dérivée K_{asme} (Access Security Management Entity) au MME
 - ◆ Dérivation des clés suivantes à partir du K_{asme}
 - ◆ K_{asme} est aussi calculé sur l'UE.

Authentication (2)



- ✧ Vérification du AUTN (coté UE) puis du XRES (côté réseau)
- ✧ Ajout d'un numéro de séquence pour éviter le replay.

Chiffrement/Intégrité

✧ A partir de la clé K_{asme}

- ✧ Dérivation de plusieurs clés entre UE et ENodeB et entre UE et MME
 - Intégrité
 - Chiffrement
- ✧ Chiffrement
 - Codage AES ou SNOW 3G pour la confidentialité
- ✧ Intégrité
 - Calcul d'un hachage sur 32 bits à partir de K_{eNB}
 - Utiliser que pour la signalisation
 - MAC (Message Authentication Code)

Identité temporaire

✦ IMSI -> unique au monde..... Permet de suivre un UE

✦ Création d'un autre identifiant par le MME

- TMSI : Temporary Mobile Subscriber Identity (4 octets)
- Passage valeur TMSI chiffré entre UE et MME

✦ Création du GUTI (Globally Unique Temporary UE identity)

MCC	MNC	MME group ID	MME Code	TMSI
-----	-----	--------------	----------	------

✦ Communication en clair via le GUTI

- Tout le monde peut voir le TMSI, mais seul un MME peut avoir la correspondance entre TMSI et IMSI.
- Utilisation du GUTI pour faire une requête vers le réseau
- Utilisation du TMSI pour contacter un UE par le réseau.
(Un UE se met en veille -> ECM_idle)

GTP – GPRS Tunneling Protocol

- ✦ Permettre une communication entre réseau distant et UE via PGW
 - ◆ Passage dans un réseau contenant SGW, ENodeB via @IP
 - ◆ 2 adresses IP : source : UE, destination : @IP quelconque
- ✦ Pour gagner du temps, utilisation de GTP
 - ◆ Encapsulation du paquet IP dans un paquet GTP (niveau applicatif)
 - ◆ Lui-même encapsulé dans UDP, encapsulé dans IP



Entre UE et ENodeB

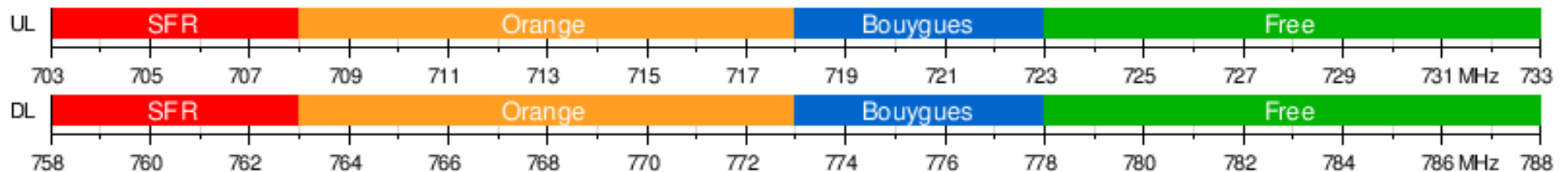
Entre ENodeB et SGW

Entre SGW et PGW

4G : Fréquence

✧ Fréquences possibles

- ✧ Chaque pays a choisi ses fréquences
- ✧ En France, fréquence vers 800 Mhz et 2600 Mhz, mais évolution au cours du temps
- ✧ Répartition sous forme de bandes : de 1 à 44
 - France : bande 3, 7, 20 et 28



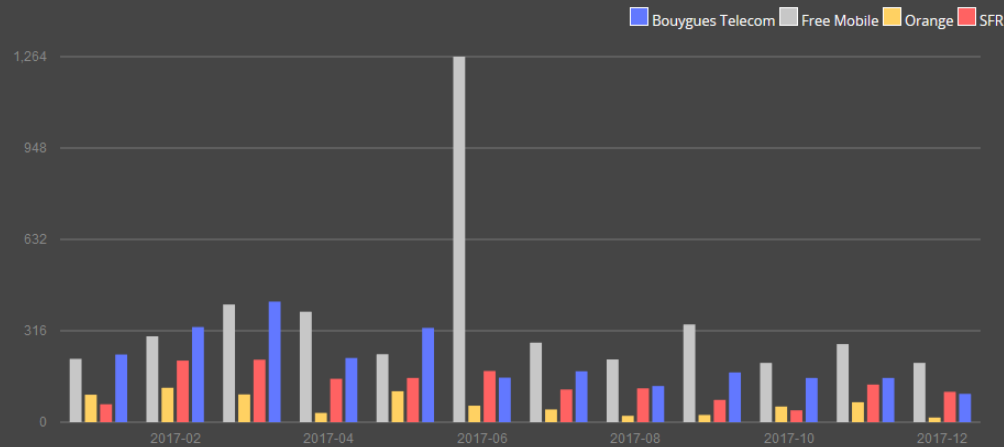
- ✧ Utilisation de OFDMA pour transmettre les données, ou sa variante SC-FDMA.

(orthogonal frequency-division multiple access)

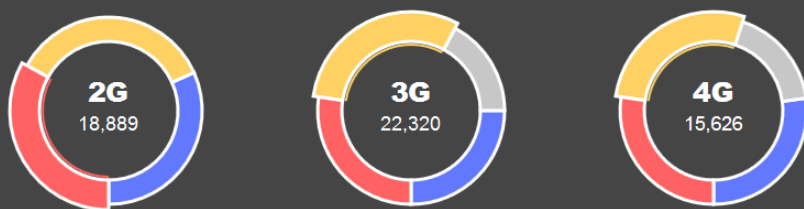
- Multiplexage fréquentiel et temporel
- Augmentation du débit
- Débit théorique : 300 Mb/s

Antennes

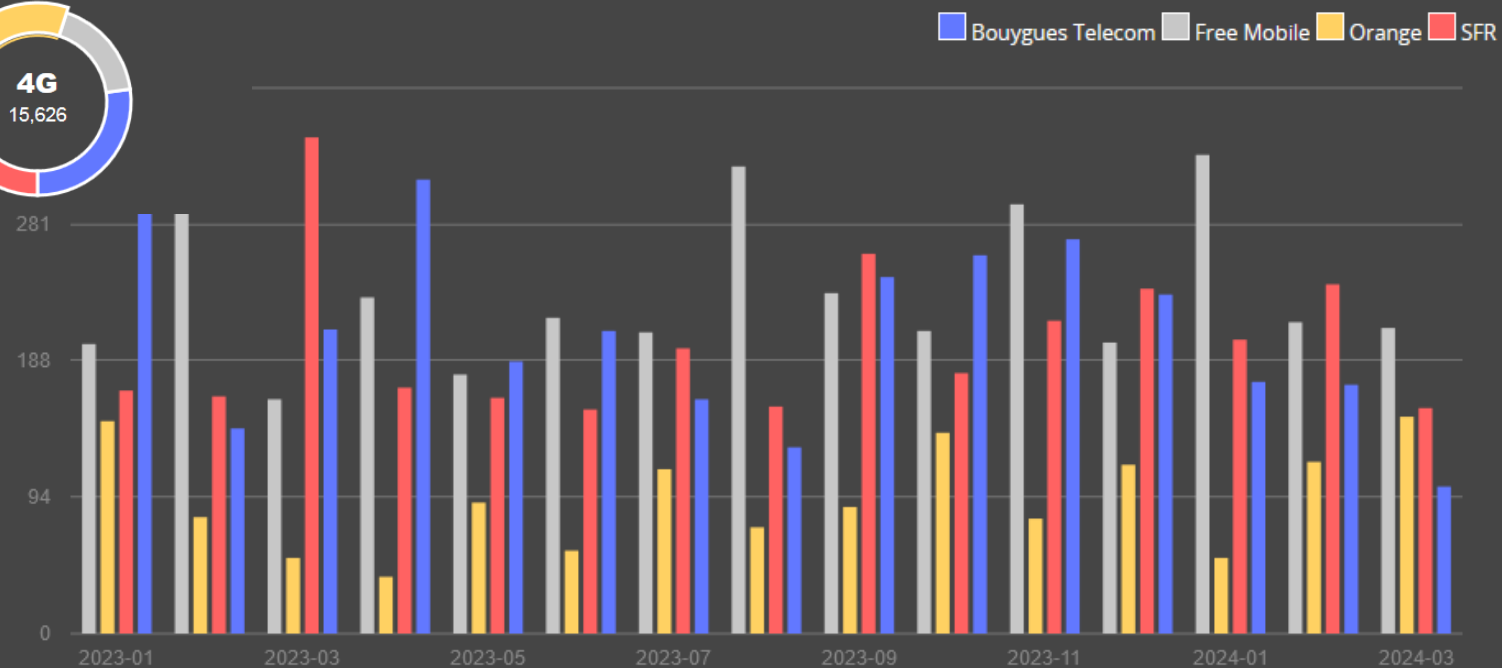
NOMBRE D'ANTENNES 3G DECLAREES PAR MOIS



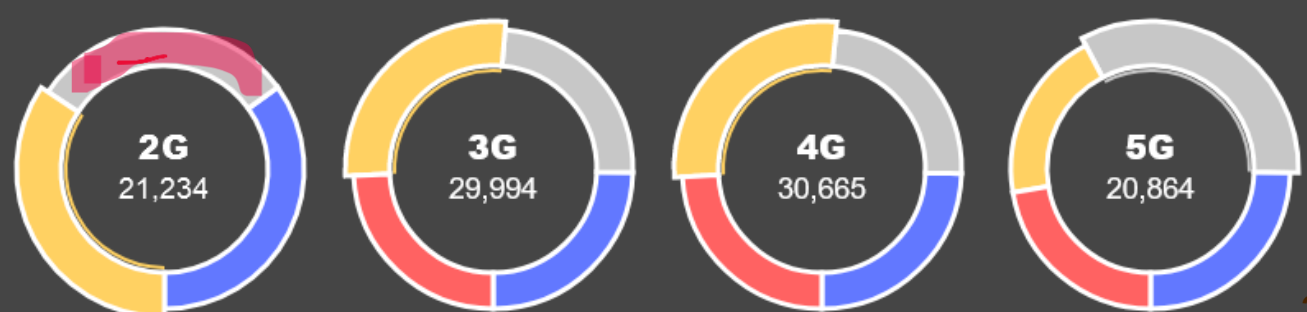
NOMBRE D'ANTENNES DECLAREES PAR RESEAU



NOMBRE D'ANTENNES 3G DECLAREES PAR MOIS



NOMBRE D'ANTENNES DECLAREES PAR RESEAU



5G

✦ Aperçu d'une partie de la 5G

- ✦ La 5G, pas 1 service mais 3 (3GPP rel 15 et 16)
 - eMBB (enhanced Mobile Broadband) → utilisation pour téléphone mobile
 - mMTC (Massive Machine Type Communication) → pour les IOT
 - URLLC (Ultra Reliable Low Latency Communication)

Suivant le service, on a :

- ✦ Débit ≥ 1 Gb/s
- ✦ Latence très faible < 1 ms (actuellement 500 ms)
- ✦ Minimisation de la consommation d'énergie
- ✦ Technologie MIMO
 - Utilisation des ondes millimétriques
 - Utilisation de « small cells » en milieu dense
- ✦ Bande passante
 - Distribution des fréquences à partir de 2020 en France

Attribution fréquence 5G

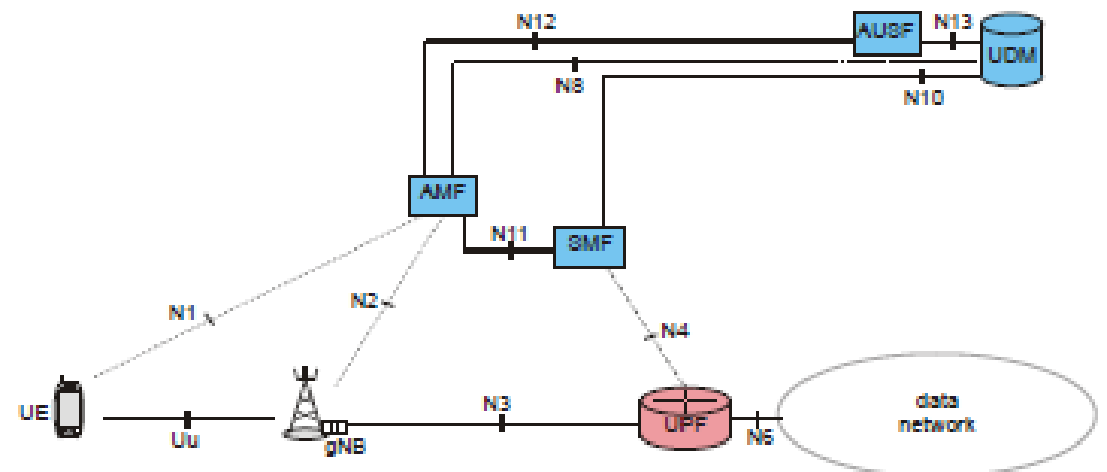
- ✦ Mise aux enchères bande de 3,4 à 3,8 Ghz par l'ARCEP
 - ✦ Pour avoir accès , achat de 50 Mhz à 350 Millions €
 - ✦ 4 entreprises OK : free, Bouygues, Orange, SFR
 - ✦ 11 * 10 Mhz à se répartir aux enchères entre les différentes entreprises
 - ✦ Final : Free : 2 Bouygues : 2 Orange : 4 SFR : 3
 - ✦ L'état récupère environs 3 milliards €

Candidat	Bouygues Telecom	Free Mobile	Orange	SFR	Total
Fréquences	3570 - 3640 MHz	3640 – 3710 MHz	3710 – 3800 MHz	3490 – 3570 MHz	-
Quantité de fréquences	70 MHz	70 MHz	90 MHz	80 MHz	310 MHz
Montant	602 000 000 €	605 096 245 €	854 000 000 €	728 000 000 €	2 789 096 245 €

- ✦ Bolloré libère les fréquences Wimax (90 Mhz à distribuer....)

5G (suite)

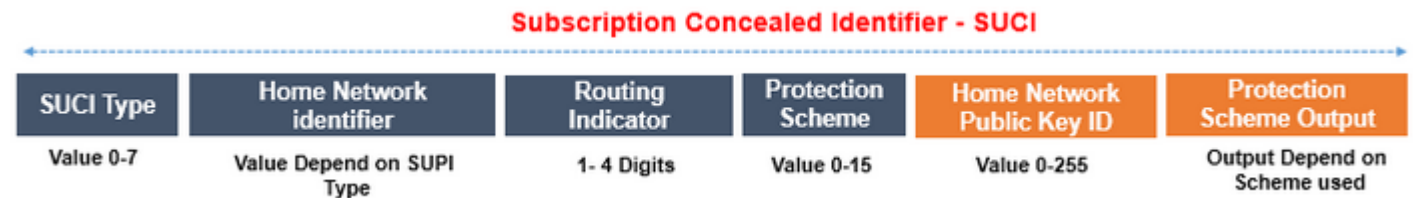
- ✦ Architecture assez similaire à la 4G
- ✦ Mais moins de tunnel
- ✦ Possibilité de communiquer sans IP, directement @MAC
- ✦ Changements équipements internes
 - ◆ User Plane Fonction (UPF) remplace le SGW et PGW
 - ◆ Le MME est remplacé par l'Access and Mobility Function (AMF) et par le Session Management Function (SMF)
 - ◆ Le HSS est séparé en 2 :
 - AUSF : Authentication Server Function
 - UDM : Unified Data Management



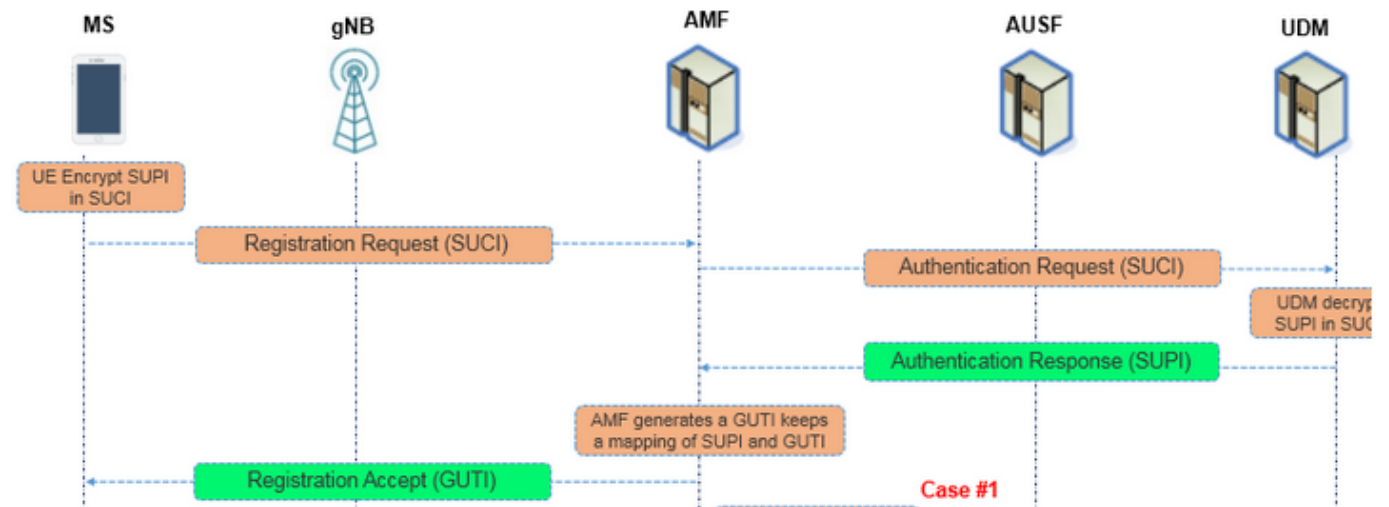
5G

✦ SUPI (Subscription Permanent identifier)

- ✦ Remplace l'IMSI, mais même information : MCC+MNC+MSIN
- ✦ Apparition du SUCI : Subscription Concealed Identifier pour cacher le SUPI



- ✦ Début d'identification pour la première connexion



Communiquez avec tout le monde → 6G 38