

Chapitre3 : Intégration des réseaux orientés paquets

- Architecture physique de référence
- Attachement au réseau
- Activation d'un contexte PDP
- Transmission de données dans le réseau GPRS

1. Introduction au standard GPRS

Le standard GPRS (General Packet Radio Service) est une évolution de la norme GSM, le transport des données sur le réseau GSM n'autorise qu'au mieux des débits de 9,6 kbit/s. C'est pourquoi la technologie GPRS a été définie, permettant de contourner le problème de monopolisation de canal, et par la même de résoudre le problème de la facturation à la durée, ainsi que de permettre des débits résolument plus importants.

Etant donné qu'il s'agit d'une norme de téléphonie de seconde génération permettant de faire la transition vers la troisième génération (3G), on parle généralement de 2.5G pour classer le standard GPRS.

Le standard GPRS utilise l'architecture du réseau GSM pour le transport de la voix, et propose d'accéder à des réseaux de données (notamment internet) utilisant le protocole IP ou le protocole X.25.

2. Catégories de services

Le GPRS permet de nouveaux usages que ne permettait pas la norme GSM, généralement catégorisés par les classes de services suivants :

- **Services point à point (PTP)** : c'est-à-dire la capacité à se connecter en mode client-serveur à une machine d'un réseau IP.
- **Services point à multipoint (PTMP)** : c'est-à-dire l'aptitude à envoyer un paquet à un groupe de destinataires (*Multicast*).
- **Services de messages courts (SMS).**

3. Principales caractéristiques du GPRS

3.1. Spectre des fréquences

L'interface radio du GPRS s'appuie sur celle du GSM. Elle utilise les mêmes bandes de fréquences (900 et 1800 Mhz), la même modulation, le GMSK (Gaussian Minimum Shift Keying), et les mêmes canaux physiques.

3.2. Débit

La différence entre GSM et GPRS est que GSM n'utilise qu'un time slot par trame TDMA, tandis que GPRS peut utiliser plusieurs time slots (jusqu'à 8, qui est le maximum) sur une seule trame pour transporter les données.

GPRS utilise ces time-slots de façon dynamique et peut donc justifier d'un débit beaucoup plus important que GSM.

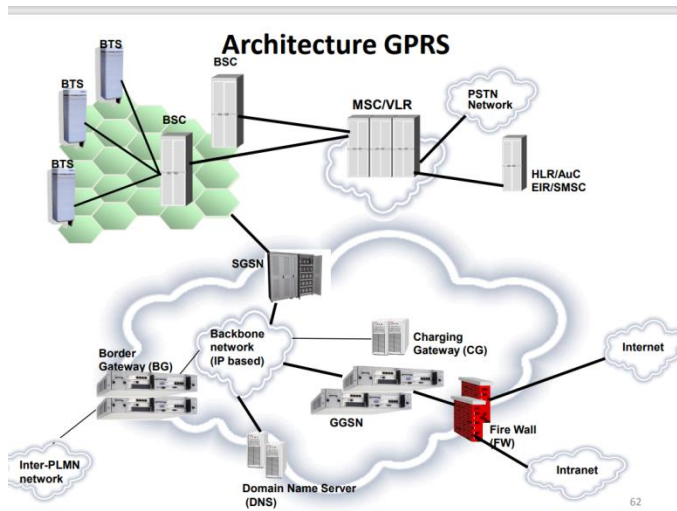
Le GPRS permet d'étendre l'architecture du standard GSM, afin d'autoriser le transfert de données par paquets, avec des débits théoriques maximums de l'ordre de 171,2 kbit/s (en pratique jusqu'à 114 kbit/s). Grâce au mode de transfert par paquets, les transmissions de données n'utilisent le réseau que lorsque c'est nécessaire.

4. Architecture physique de référence

Architecture générale du GSM/ GPRS

Le GPRS ne représente pas à lui seul un réseau mobile à part entière car il utilise les équipements du GSM pour pouvoir fonctionner, son architecture est fortement liée à ce dernier. En effet, l'architecture GSM fournit les services voix, tandis que l'architecture GPRS fournit les services de données par paquets avec un débit élevé.

Tous deux utilisent les mêmes équipements BSS, c'est-à-dire les stations de base BTS et leurs contrôleurs BSC. C'est ensuite qu'ils se distinguent. Le réseau cœur (*Core Network*) du GPRS est un réseau paquet interconnecté, pouvant être relié à divers types de réseaux de données fixes; IP (Internet Protocol), X.25 ...etc., ou encore à d'autres réseaux GPRS, exploités par d'autres opérateurs.

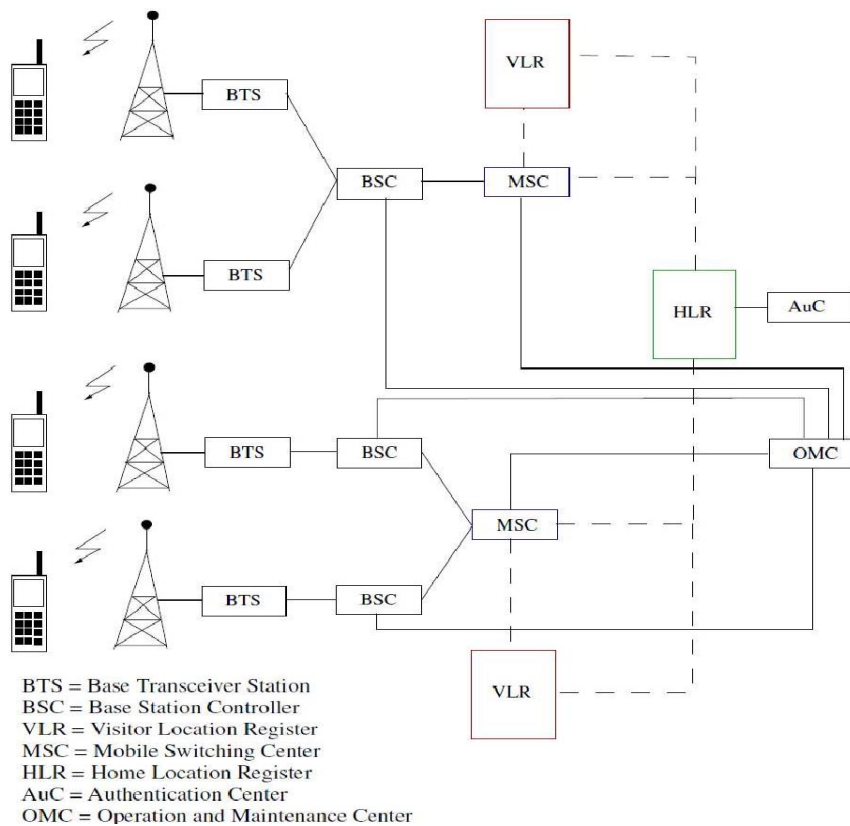


4.1.Présentation de l'architecture du réseau GSM

L'architecture d'un réseau GSM peut être divisée en trois sous-systèmes :

- Le sous-système radio : contenant la station mobile, la station de base et son contrôleur.
- Le sous-système réseau ou d'acheminement.
- Le sous-système opérationnel ou d'exploitation et de maintenance.

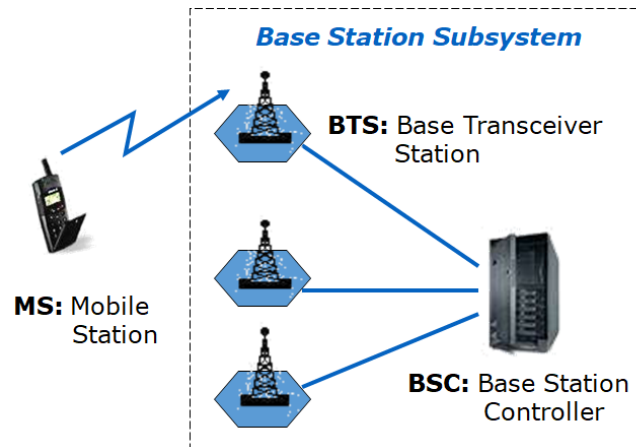
Les éléments de l'architecture d'un réseau GSM sont repris sur le schéma de la figure ci-dessous.



Architecture du réseau GSM.

4. 1.1. Le sous-système radio

Appelé aussi BSS, Base Station Sub-System, il gère la transmission radio, est constitué de : le mobile, la station de base (BTS, Base Transceiver Station) et un contrôleur de station de base (BSC, Base Station Controller).



❖ Station mobile

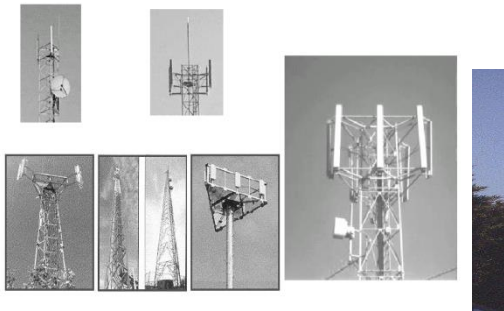
Le téléphone et la carte SIM (Subscriber Identity Module) sont les deux seuls éléments auxquels un utilisateur a directement accès. Ces deux éléments suffisent à réaliser l'ensemble des fonctionnalités nécessaires à la transmission et à la gestion des déplacements.

- La SIM est une petite carte dotée de mémoire et de microprocesseur, sert à identifier l'abonné indépendamment du terminal utilisé, sa principale fonction est de contenir et de gérer une série d'informations. Elle se comporte comme une mini-base de données.
- Elle contient des données spécifiques comme le code PIN (Personal Identification Number). L'identification d'un utilisateur est réalisée par un numéro unique (IMSI, International Mobile Subscriber Identity) différent du numéro de téléphone connu de l'utilisateur (MSISDN, Mobile Station International Subscriber Directory Number), tous deux étant incrustés dans la carte SIM. Seul le HLR connaît la correspondance entre le MSISDN et l'IMSI contenu dans la carte SIM de l'abonné.
- Le Mobile Equipment est identifié (exclusivement) à l'intérieur de n'importe quel réseau GSM par l'International Mobile Equipment Identity (IMEI), un numéro de 15 chiffres. Pour le savoir on compose (*#06#) sur le téléphone.

❖ La station de base (BTS)

- BTS (Base Transceiver Station): station de base d'émission et de réception
- Assure couverture radio d'une cellule (rayon de 200m à ~30 km)

- Prend en charge: modulation/démodulation, correction des erreurs, cryptage des communications, mesure qualité et puissance de réception



BTS rayonna

BTS ciblé (directive)



BTS (Station de métro de Kiev-Ukraine)

❖ Le contrôleur de station de base (BSC)

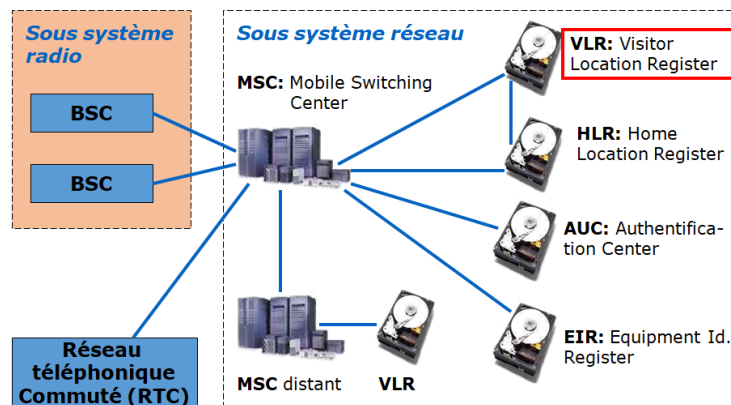
- BSC (Base Station Controller) pilote un ensemble de station de base (typiquement ~60)
- Gestion des ressources radio: affectation des fréquences, contrôle de puissance...
- Gestion des appels: établissement, supervision, libération des communications, *etc.*
- Gestion des transferts intercellulaires des utilisateurs dans sa zone de couverture (handover)

Handover :C'est-à-dire quand une station mobile passe d'une cellule dans une autre. Il doit alors communiquer avec la station de base qui va prendre en charge l'abonné et lui communiquer les

informations nécessaires tout en avertissant la base de données locale VLR (*Visitor Location Register*) de la nouvelle localisation de l'abonné.

- Mission d'exploitation.

4.1.2. Le sous-système réseau



Le sous-système réseau, appelé *Network Switching Center* (NSS), joue un rôle essentiel dans un réseau mobile. Alors que le sous-réseau radio gère l'accès radio, les éléments du NSS prennent en charge toutes les fonctions de contrôle et d'analyse d'informations contenues dans des bases de données nécessaires à l'établissement de connexions utilisant une ou plusieurs des fonctions suivantes : Chiffrement, Authentification ou Roaming.

Le NSS est constitué de :

- Mobile Switching Center (MSC)
- Home Location Register (HLR) / Authentication Center (AuC)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)

❖ Le centre de commutation mobile (MSC)

MSC (Mobile Switching Center) commutateur numérique en mode circuit.

- Le rôle principal est d'assurer la commutation entre les abonnés du réseau mobile et ceux du réseau commuté public (RTC).

- D'un point de vue fonctionnel, il est semblable à un commutateur de réseau RTC, mis à part quelques modifications nécessaires pour un réseau mobile.

- De plus, il participe à la fourniture des différents services aux abonnés tels que la téléphonie, les services supplémentaires et les services de messagerie.

- Il permet encore de mettre à jour les différentes bases de données (HLR et VLR) qui donnent toutes les informations concernant les abonnés et leur localisation dans le réseau.

- Les commutateurs MSC d'un opérateur sont reliés entre eux pour la commutation interne des informations.

- Des MSC particuliers servant de passerelle (Gateway Mobile Switching Center, GMSC) sont placées en périphérie du réseau d'un opérateur pour à assurer une interopérabilité entre les autres réseaux mobile ou fixes.

Exemple d'un centre MSC



❖ **L'enregistreur de localisation nominale (HLR)**

Il existe au moins un enregistreur de localisation (HLR) par réseau (PLMN). Il s'agit d'une base de données avec des informations essentielles pour les services de téléphonie mobile et avec un accès rapide de manière à garantir un temps d'établissement de connexion aussi court que possible.

Le HLR contient :

- Toutes les informations statiques relatives aux abonnés : le type d'abonnement, la clé d'authentification (K_i) cette clé est connue d'un seul HLR et d'une seule carte SIM., les services souscrits, le numéro de l'abonné (IMSI), etc.
- Ainsi qu'un certain nombre de données dynamiques telles que la position de l'abonné dans le réseau .en fait, son VLR. et l'état de son terminal (allumé, éteint, en communication, libre, . . .).

❖ **Le centre d'authentification (AuC)**

- AUC (AUTHentication Center) contrôle l'identité des abonnés et assure les fonctions de cryptage
- Authentification de l'abonné: Subscriber Identity Module (carte SIM) contient plusieurs clés secrètes
- Cryptage des données au niveau du terminal

❖ **L'enregistreur de localisation des visiteurs (VLR)**

Cette base de données ne contient que des informations dynamiques et est liée à un MSC. Il y en a donc plusieurs dans un réseau GSM. Elle contient des données dynamiques qui lui sont transmises par le HLR avec lequel elle communique lorsqu'un abonné entre dans la zone de couverture du centre de commutation mobile auquel elle est rattachée. Lorsque l'abonné quitte cette zone de couverture, ses données sont transmises à un autre VLR ; les données suivent l'abonné en quelque sorte.

- VLR mis à jour à chaque changement de cellule d'un abonné.

❖ **L'enregistreur des identités des équipements (EIR)**

- EIR (Equipment Identity Register) empêche l'accès au réseau aux terminaux non autorisés (terminaux volés)
- A chaque terminal correspond un numéro d'identification: le IMEI (International Mobile Equipment Identity)
- A chaque appel, le MSC contacte le EIR et vérifie la validité du IMEI

4.1.3. Le sous system d'exploitation et de maintenance

Appelé aussi OSS, *Operation Sub-System*, cette partie du réseau regroupe trois activités principales de gestion : la gestion administrative, la gestion commerciale et la gestion technique. Le réseau de maintenance technique s'intéresse au fonctionnement des éléments du réseau. Il gère notamment les alarmes, les pannes, la sécurité, . . .

4. 2- Architecture générale de réseau GPRS

De nouveaux éléments de réseau doivent donc être ajoutés au GSM pour offrir le GPRS. Ils sont le SGSN (*Serving GPRS Support Node*), côté sous-système radio et le GGSN (*Gateway GPRS Support Node*), côté réseau de données public ; ce sont des routeurs paquet dotés de fonctionnalités dédiées à la gestion d'un réseau mobile. Ils sont responsables de la livraison et du routage des paquets de données entre la station mobile (MS, mobile station) et des réseaux de données externes.

L'interface radio du GPRS s'appuie sur celle du GSM, mais les réseaux cœur sont séparés.

4.2.1. SGSN (*Service GPRS Support Node*)

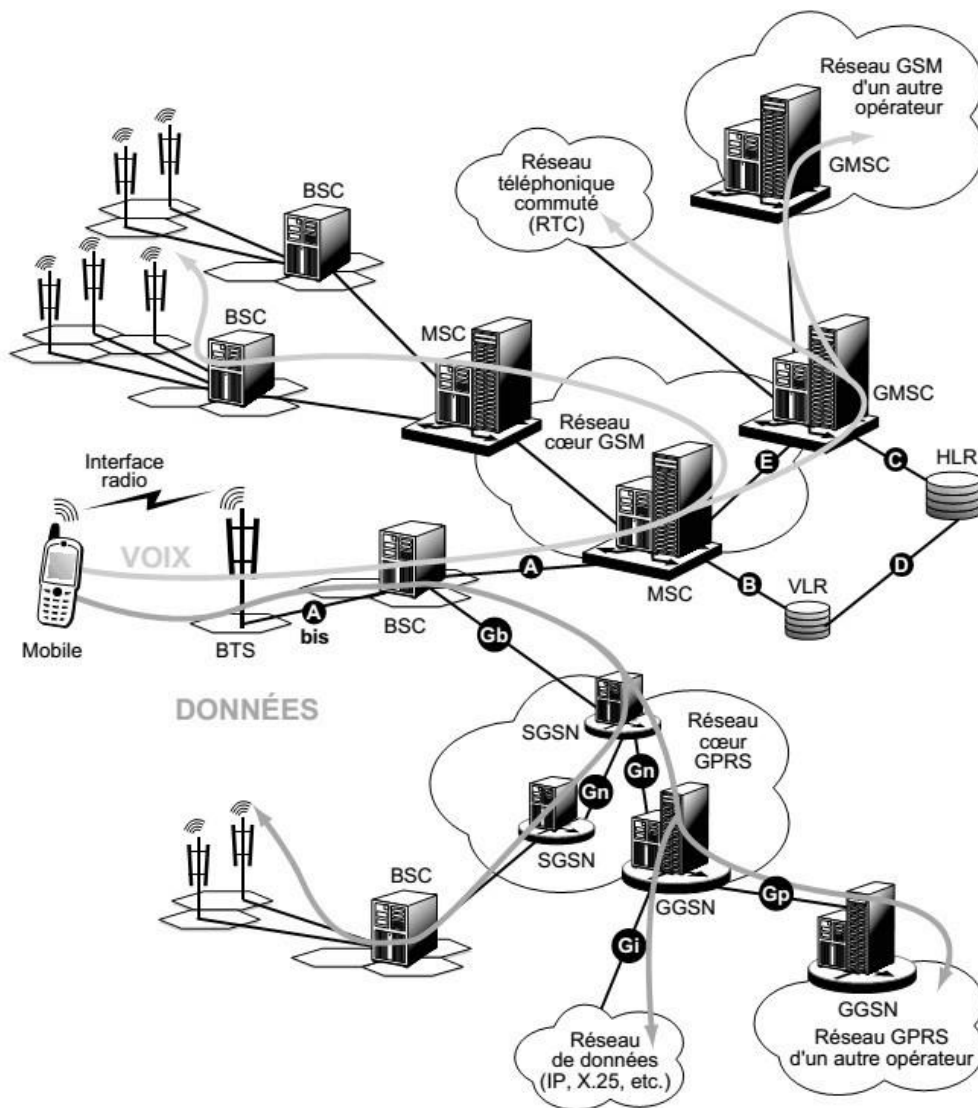
L'entité SGSN (*Service GPRS Support Node*) se charge dans son aire de service des transmissions de données entre les stations mobiles et le réseau. Il gère en conséquence les

contextes de mobilité et de sécurité du mobile, ainsi qu'un contexte caractéristique du réseau de données avec lequel le mobile est connecté, le contexte PDP (Packet Data Protocol), où la conversion des données du terminal en paquets de type IP (et réciproquement).

Le SGSN est connecté à plusieurs BSC et présent dans le site d'un MSC.

Le SGSN :

- Authentifie : prend en charge l'enregistrement (attachement) les stations mobiles GPRS ;
- Prend en charge la gestion de la mobilité des stations mobiles. En effet, une station mobile doit mettre à jour sa localisation à chaque changement de zone de routage ;
- Etablit, maintient et libère les contextes PDP, qui correspondent à des sessions de données permettant à la station mobile d'émettre et de recevoir des données ;
- Relais les paquets de données de la MS au réseau externe ou du réseau à la station mobile ;
- S'interface à d'autres nœuds (HLR, MSC, BSC, GGSN, ...).



4.2.2. Le GGSN (*Gateway GPRS Support Node*)

L'entité GGSN joue le rôle d'interface à des réseaux de données externes **PDN** (*Packet Data Network*) (X.25, IP).

Elle décapsule des paquets GPRS provenant du SGSN les paquets de données émis par le mobile et les envoie au réseau externe correspondant. Egalement, le GGSN permet d'acheminer les paquets provenant des réseaux de données externes vers le SGSN du mobile destinataire, les encapsule dans des nouveaux paquets IP. Le GGSN est généralement présent dans le site d'un MSC. Il existe un GGSN ou un nombre faible de GGSN par opérateur.

Le GGSN :

- Joue le rôle d'interface aux réseaux externes de type IP ou X.25 même si en pratique seule l'interface vers des réseaux IP est mise en œuvre ;
- Ressemble à un routeur. D'ailleurs dans de nombreuses implantations, il s'agit d'un routeur IP avec des fonctionnalités supplémentaires ;
- Route les paquets émis par la station mobile à la destination appropriée ;
- Filtre le trafic usager.

4.2.3. Le PCU (*Packet Control Unit*)

Pour déployer le GPRS dans les réseaux d'accès, on réutilise les infrastructures et les systèmes existants. Il faut leur rajouter une entité responsable du partage des ressources et de la retransmission des données erronées, et qui fait la différence entre les données "circuit" de GSM et les données "paquet" de GPRS ; c'est l'unité de contrôle de paquets (PCU, *Packet Control Unit*) par une mise à jour matérielle et logicielle dans les BSCs.

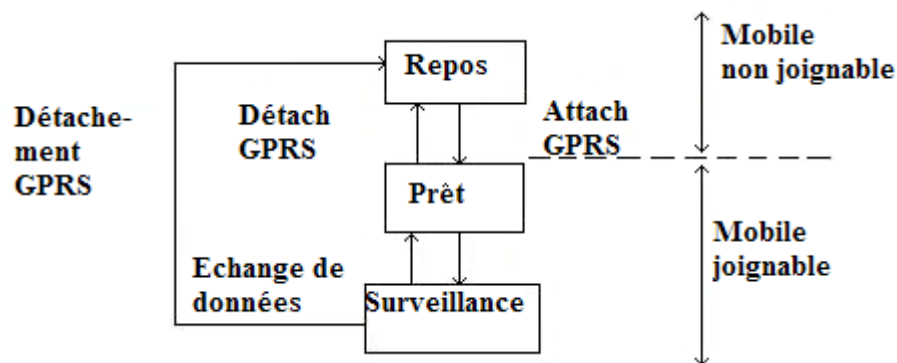
5. L'état du mobile

Le service GPRS distingue entre 3 états probables pour un mobile :

- **Etat « repos » : Idle** ; le mobile est hors réseau ou tout simplement éteint.
- **Etat « surveillance » : Stand-by** ; (être prêt à intervenir): le terminal est dans un état intermédiaire dans lequel il est prêt à émettre et recevoir des données.
- **Etat « prêt » : Ready** ; le terminal émet ou reçoit des communications, il est localisé à la cellule prés.

Lorsqu'un mobile au repos essaye de s'attacher au réseau GPRS, il passe directement à l'état « prêt ». L'émission et la réception des données est possible. Si aucun échange n'est effectué pendant une durée prolongée, le mobile se met alors en mode « surveillance ».

Le mobile retrouve son état « repos » dès qu'il se détache du réseau.



Les identités temporaires :

Pour plus de sécurité, et pour que le mobile ne dévoile jamais son identité IMSI, le GPRS associe à chaque MS des identités temporaires P.TMSI (*Packet Temporary Mobile Subscriber Identity*) et le TLLI (*Temporary Link Layer Identity*)

- La P.TMSI est une identité courte qui permet au réseau de différencier entre les abonnés sous le même SGSN, mais cette identité n'est attribuée au mobile qu'après son attachement au réseau.
- La TLLI est une identité aléatoire attribuée au mobile par le SGSN au cours de son attachement au réseau afin d'échanger de la signalisation avec celui-ci, mais une fois le mobile attaché, elle est actualisée et confondue avec la P-TMSI.

6. Attachement du mobile au réseau :

Pour accéder au service GPRS, le mobile doit d'abord s'attacher au réseau selon la procédure de « GPRS Attach ».

Cette procédure consiste à établir un lien logique entre le mobile et le nœud de service SGSN, elle comporte les étapes suivantes :

- 1) Le mobile utilise le canal d'accès aléatoire PRACH (Packet Random Access Channel) pour

- avoir un canal dédié. Il transmet alors son identité TLLI aléatoire ;
- 2) Si la MS a changé de zone de routage, le SGSN ne reconnaîtra pas son TLLI. Il envoie à l'ancien SGSN une demande d'identification, si l'identification échoue, le SGSN et le mobile entament une procédure d'identification classique par l'utilisation d'IMSI.
 - 3) Authentification de l'utilisateur (peut-il accéder aux services GPRS ?). Cette procédure peut impliquer le HLR dans lequel sont stockés les renseignements relatifs à l'utilisateur.
 - 4) Le SGSN met à jour la localisation du mobile,
 - 5) Le SGSN envoie au MS « Attach Accept » et lui attribue un TLLI, cet envoi se fait sur le canal PAGCH (Packet Grant Channel), un canal de garantie d'accès pour la MS (disponibilité des ressources).
 - 6) Le mobile acquitte. Le canal dédié peut être fermé.

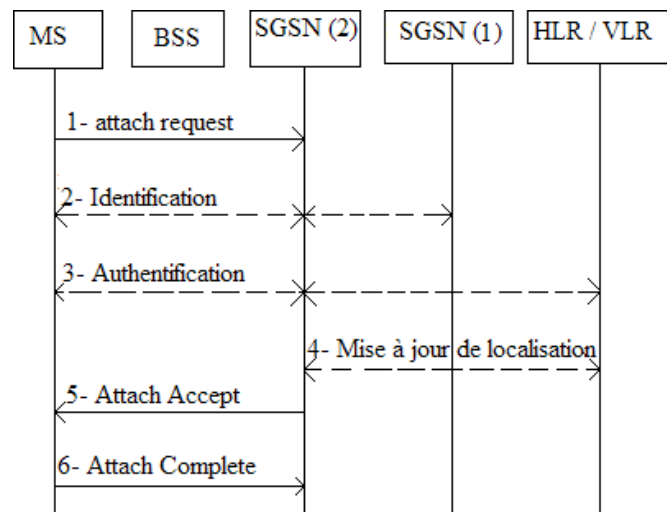


Figure .Procédure d'attachement au réseau GPRS.

7. Contenu du contexte PDP d'une session « Internet » :

Pour ouvrir une session réseau (Internet par exemple), des informations spécifiques sont stockées dans la station Mobile, le SGSN et le GGSN pour permettre des échanges de données entre la MS et le réseau externe concerné. Ces informations sont regroupées dans un contexte appelé « PDP (*Packet Data Protocol*) context ».

Le contexte PDP contient :

- 1) **Le type de réseau PDP utilisé** : pour une connexion à Internet, le réseau est un réseau IPv4 ou IPv6 .
- 2) **L'adresse PDP du terminal** : c'est l'adresse IP assignée au mobile de l'abonné qui veut se connecter à Internet. Cette adresse peut être statique attribuée à l'abonné lors de la

souscription de l'abonnement, ou dynamique fournie lors de la connexion pour la durée de la session.

- 3) **L'adresse IP du SGSN** qui gère la zone où se trouve l'abonné,
- 4) **Le point d'accès au service réseau utilisé** NSAPI (*Network Service Access Point Identifier*).
- 5) **La qualité de service QoS négociée**.
- 6) **L'APN (*Access Point Name*)** : il sert à identifier le type de service qui est fourni par la connexion. Exemple : Internet, WAP.....

Le contexte PDP peut être activé à l'initiative de l'abonné ou du réseau. Pour l'accès à Internet, il ne peut être activé que par le mobile.

7.1. Activation du contexte par le mobile

Après attachement au réseau, le mobile peut activer le contexte PDP, le déroulement de la procédure est comme suit :

1. La MS envoie au SGSN le message « **ACTIVATE PDP CONTEXT REQ** », celui-ci contient toutes les informations du contexte mis-à-part l'adresse IP du SGSN ;
2. Grâce à ces informations, le SGSN retrouve l'IMSI et le GGSN concerné par le contexte,
3. Il transfère alors le contexte PDP et le IMSI au GGSN dans un message « **GTP CREATE PDP CONTEXT REQUEST** » ; (GTP :GPRS Tunneling Protocol)
4. Le GGSN est maintenant prêt à échanger des données entre le mobile et le réseau de données externe.

8. Transmission de données dans le réseau GPRS

Lorsqu'un utilisateur désire transmettre des paquets vers un réseau de données en mode paquet, il utilise le protocole **PDP** (*Packet Data Protocol*).

8.1. Emission de données

Imaginons qu'un utilisateur GPRS désire envoyer des paquets de données à un utilisateur situé sur le réseau Internet.

Voici un descriptif des étapes à réaliser pour cette situation, et ceci dans l'ordre chronologique.

L'établissement de la liaison montante :

1. le terminal mobile doit récupérer le BCCH (Broadcast Control CHannel) de la cellule afin de déterminer si un canal GPRS est présent (terminal en état IDLE).

2. le terminal mobile effectue un GPRS Attach (procédure permettant de déclarer le mobile sur le réseau GPRS et établi un lien logique entre lui et le SGSN) afin d'établir un contexte GPRS avec le SGSN, en précisant : son identité ainsi que la qualité de service désirée.

3. Après négociation de ces paramètres avec la BTS, le SGSN la charge de **la réservation du canal** (les times slots) et de l'établissement de la liaison.

4. le terminal reçoit des informations concernant le canal alloué sur le BCCH et passe à l'état STANDBY.

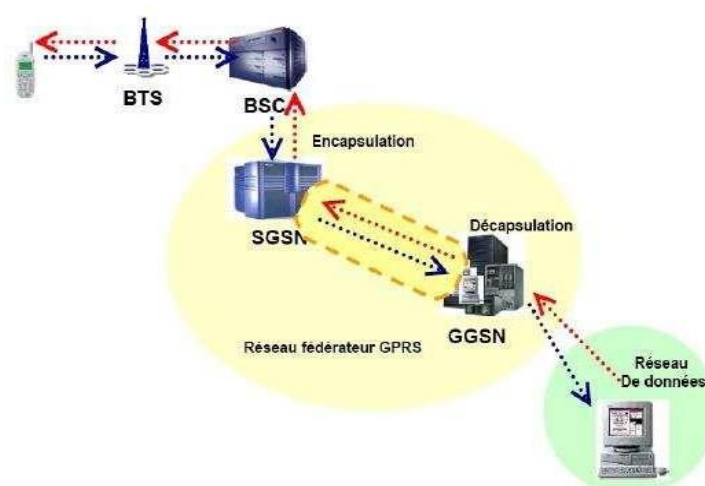
5. le terminal passe à l'état READY en transmettant au SGSN un message identifiant le canal courant (Uplink).

Un échange de paquets commence :

- les données sont transmises dans les times slots réservés.
- un accusé de réception positif est envoyé par la BTS si l'ensemble des données a été bien reçu.
- les données sont décapsulées et envoyées au SGSN.
- le SGSN encapsule les données à l'aide du protocole GTP et les envoie au GGSN.
- le paquet est décapsulé, et l'adresse et le protocole sont vérifiés afin que la bonne route soit sélectionnée.

Le paquet est alors envoyé via le réseau de données externe jusqu'au destinataire.

Ce transfert se termine par un message d'accusé réception de la part du SGSN qui peut être positif ou négatif.



8.2. Réception de données

Imaginons qu'un utilisateur désire envoyer des paquets de données IP à un utilisateur GPRS.

Voici un descriptif des étapes à réaliser pour cette situation, et ceci dans l'ordre chronologique.

- les paquets venant du réseau de données externe sont acheminés jusqu'au GGSN du réseau GPRS.
- le GGSN effectue les conversions de formats de données, de protocoles de signalisation et d'informations d'adresses.
- le GGSN vérifie s'il possède un contexte GPRS pour ce terminal mobile :
 - ✓ si le terminal mobile est dans l'état IDLE, le trafic paquet sera rejeté.
 - ✓ si le terminal mobile est dans l'état STANDBY ou ACTIF, le GGSN achemine le paquet, dans un format encapsulé, vers le SGSN (utilisation du GTP).
- si le terminal mobile est en état STANDBY, le SGSN demande au MSC de réaliser un paging GPRS dans la zone de routage du terminal.
- le terminal mobile répond au paging en précisant la cellule dans laquelle il est situé, et se met dans le mode ACTIF.
 - le paquet est acheminé du SGSN via la MSC à la station de base une fois que la route a été établie.
 - la station de base réserve un time slot sur le PDCH (Packet Data CHannel), encapsule le paquet et l'envoie au terminal mobile.
 - Si cette donnée est reçue correctement, un accusé de réception positif est généré.
 - le terminal décapsule le paquet, et l'envoie au destinataire final, par exemple l'application sur un ordinateur portable connecté au téléphone mobile.

Pour tous les paquets qui seront ensuite envoyés pendant une période de temps donnée, le terminal mobile restera dans un mode ACTIF et indiquera au réseau lorsqu'il change de cellule. Le chemin vers le terminal mobile est connu, donc tous les paquets seront acheminés vers ce terminal comme via un tunnel.

