Notes sur le cours Architectures des Réseaux Mobiles

DIAPO 1 :
Dans cette matière nous allons nous intéresser à l'architecture des réseaux mobiles. Ce cours va décrire les enjeux de la création et des évolutions des réseaux mobiles. Nous présenterons les architectures systèmes en termes d'équipements, les architectures protocolaires et prendrons des illustrations protocolaires.

DIAPO 2 :
Les réseaux mobiles sont des réseaux d'accès qui viennent en remplacement des accès filaires pour se raccorder à des réseaux de télécommunications. L'introduction présentera les principes généraux de fonctionnement puis on retracera les évolutions du monde 2G vers la 3G et la 4G. Les cours sur la 5G seront effectués en 3ème année dans les parcours Télécoms, Réseaux et Systèmes Embarqués. Commençons par les systèmes 2G.

DIAPO 3 :
Nous allons commencer par positionner les réseaux mobiles. En toute rigueur, on devrait parler de réseaux de mobiles car ce sont les équipements qui bougent et rarement les infrastructures. Par abus de langage, on utilisera tout de même par la suite la terminologie de réseaux mobiles qui est communément acceptée. Notons qu'il y a des réseaux dans lesquels l'infrastructure bouge aussi : si tout le monde bouge ensemble, il n'y a plus de mobilité relative mais on peut aussi envisager des configurations dans lesquelles les infrastructures bougent et les utilisateurs aussi mais avec des mobilités distinctes. Ces types de réseaux seront repris dans certains cours de 3ème année car ils sont plus compliqués encore que les réseaux que je vais vous présenter dans cette matière.

D'une manière générale, les réseaux mobiles sont construits dans un monde très orienté télécom piloté par les opérateurs et les équipementiers du monde des télécommunications. Nous allons commencer l'histoire à partir du moment où ces réseaux de mobiles ont basculé vers des transmissions numériques en passant sous silence les générations précédentes de réseaux de mobiles (de voiture essentiellement vu la taille des équipements) analogiques appelés systèmes 1G.
L'objectif premier était de remplacer le réseau d'accès filaire par un réseau d'accès sans fil dans lesquels le support hertzien était utilisé par les utilisateurs en termes de premier bond. C'est bien d'un réseau d'accès télécoms complètement dans le sens qui a été retenu dans les cours précédents concernant les réseaux de télécommunications.
La première application qui a été visée a été la parole téléphonique. Le systèmes GSM a été conçu a cet effet au début des années 90. C'est un standard européen à la base ; c'est d'ailleurs l'ETSI (partie européenne de l'ITU-T située à Sophia Antipolis) qui l'a standardisé. Il a connu le plus de succès à travers le monde. On est dans une philosophie classique de téléphonie avec un réseau qui s'apparente à une solution circuit et qui est également largement inspirée du RNIS.
Fort de ce succès, le monde télécoms a réfléchi à la mise en place de solutions dans lesquelles on se servirait de l'infrastructure du réseau d'accès GSM pour véhiculer des données et se raccorder à l'Internet. On voit une volonté assez proche de celle du RNIS mais clairement, on a tiré les enseignements du RNIS pour l'exploitation du support de communication et cela a conduit à la solution GPRS à la fin des années 90.
La suite logique, à l'instar de ce que l'on a connu globalement dans l'ensemble des réseaux et pas uniquement dans les réseaux d'accès à consister à planifier des évolutions dans lesquelles

les trafics de voix allaient devenir marginaux en termes de débit agrégés et la dualité des réseaux paquets et circuits n'était pas tenable sur le long terme car trop coûteuses en termes d'équipements et de maintenance. C'est dans ce contexte que sont apparues les solutions 3G.
La suite logique mais on le verra dans la suite du cours, seront les solutions 4G/LTE dans lesquelles les débits augmentent encore mais où on arrête le raccordement au réseau téléphonique commuté.
C'est à cet ensemble que sera consacré ce cours de réseau mobiles, mais il n'est pas la seule configuration dans laquelle le support hertzien et la mobilité sont envisagées.
Il y a par exemple tout le monde des réseaux locaux sans fil. La volonté est un peu la même que la précédente, on a voulu remplacer Ethernet par un support sans fil. On est complètement dans un contexte de réseaux locaux et l'organisme qui s'occupe de la standardisation en est l'IEEE. Les standards les plus connus sont par exemple le WiFi et toutes ses variantes au travers des standards IEEE 802.11. Il y a encore des réseaux à plus courte portée tels que les réseaux Bluetooth IEEE.802.15.1 et bien d'autres encore qui seront présentés à la fois en 2ème année et en 3ème année.
Attention l'Internet des Objets est plus transverse et plusieurs solutions sont candidates pour les créer : à la fois des solutions issues du monde télécoms ; du monde des réseaux locaux et encore d'autres SigFox ou LoRa en sont des exemples.

Le support hertzien est aussi utilisé pour la définition de la télévision numérique : j'ai cité ici les standards Digital Video Broadcasting T pour terrestre et S pour satellite… Ces réseaux présentent essentiellement des enjeux en termes de couches physiques ; ils seront présentés pour l'essentiel en 3A (surtout dans le parcours T).

A l'autre extrémité du spectre (ou des piles de protocoles) sont apparues aussi d'autres façon d'envisager la mobilité et le monde IP s'en est emparé. L'idée de base et la suivante, l'utilisateur se déplace et à chaque endroit où il se raccorde, il veut utiliser son adresse IP (attention cela peut être complémentaire de l'ensemble des problèmes évoqués précédemment). Dans ce cas, le routage IP étant centré sur l'adresse, il a fallu proposer des protocoles pour permettre de faire suivre les paquets vers là où se trouve l'utilisateur. Sur le principe, c'est assez séduisant, dans la vraie vie, les situations dans lesquelles on peut réellement vouloir garder son adresse sont faibles ; les adresses sont attribuées sans se préoccuper de la continuité des communications et par conséquent, on ne reviendra que très tardivement dans ce cours de Réseaux Mobiles à des configurations dans lesquelles ces protocoles peuvent réellement servir.
De la même façon, le monde de l'Internet, s'est aussi penché sur la création de réseaux mobiles sans infrastructures pour lesquels on veut envoyer des paquets entre des utilisateurs qui se déplacent, ce sont les réseaux ad-hoc Mobile Ad-hoc Networks. Ils seront repris dans les options de 3ème année.

DIAPO 4 :
On va maintenant raffiner un peu le vocabulaire. On appelle réseaux de mobiles un réseau de communication dans lequel les utilisateurs se déplacent et qui peuvent communiquer à l'extérieur de leur réseau d'origine.
Il s'agit donc d'un problème d'adressage car il faut que l'on puisse joindre l'utilisateur quand il est hors de son réseau.
La solution proposée pour le GSM et qui est toujours en vigueur dans les systèmes 3G/4G/5G va consister à garder la localisation des utilisateurs. La dissociation de l'adresse et de la localisation avait déjà été faite dans le contexte des réseaux téléphoniques dès l'apparition du SS7 avec les « numéros verts ». Ce sont les mêmes principes qui seront retenus. Les plages

d'adresse dédiées aux utilisateurs mobiles sont disjointes de celles des utilisateurs fixes. Quand on reconnaît un tel numéro dans une demande de communication, on va interroger une base de données qui va stocker la localisation courante de l'utilisateur. C'est donc sur cette partie le même principe que celui du numéro vert.
Ce qui change ce sont les millions d'utilisateurs pour un opérateur et les changements fréquents de localisation des utilisateurs. Il a donc fallu mettre en place des protocoles qui permettent la mise à jour des bases de données ; là où dans le réseau SS7, il n'y avait pas de protocoles spécifiques définis pour cela. Les opérateurs mettaient « manuellement » à jour leur base de données stockant les adresses des centres d'appel.
Pour mémoire, c'est un peu le même principe qui a régi le principe de la solution IP-mobile avec de la même façon des notions d'adresses temporaires que l'on reverra un peu plus tard dans le cours.
Cette fonction qui au départ s'appelait gestion de la mobilité est dénommée désormais gestion du nomadisme. La gestion de la mobilité correspondra plus spécifiquement à la continuité de la communication quand l'utilisateur se déplace.

Qui dit réseau sans fil ne veut pas forcément dire réseaux mobiles. Le support hertzien est utilisé dans de nombreux contextes y compris pour la téléphonie sans que l'on ait la possibilité de communiquer une fois que l'on n'est plus à portée – exemple téléphone sans cordon.
Pour la gestion du nomadisme en WiFi, je vous renvoie au cours de Réseaux Locaux Sans Fil ; la gestion de la communication en cas de changement de point d'accès est fruste !

DIAPO 5 :
Dans la suite du cours, on va s'intéresser à des réseaux sans fil cellulaires. Ce sont des réseaux avec une infrastructure d'opérateur. Des stations/points d'accès avec un certain nombre d'antennes sont disposés sur les territoires. Chaque antenne a une zone de couverture ; ces zones de couvertures se chevauchent. Le puissance du signal diminue avec la distance, ce qui permet à plusieurs utilisateurs de communiquer sur les mêmes bandes de fréquences s'ils sont assez éloignés. On va jouer sur la puissance d'émission : plus elle est faible, plus la portée sera faible et plus on pourra densifier le réseau. C'est ce principe qui a fait gagner le plus de capacité aux réseaux cellulaires en 30 ans !
L'architecture du réseau va être arborescente, les stations sont reliées à une infrastructure de réseau soit par des liens filaires soit par des liaisons RF (cela dépend des opérateurs, pour un opérateur comme Orange il n'y a presque que des liaisons filaires, pour Free, il y a beaucoup de communication sans fil). Une zone de localisation sera un ensemble contigu de cellules ; la taille de cet ensemble va jouer sur la signalisation associée. Si la zone est très petite, les utilisateurs changent souvent de zone et la signalisation dans le sens montant sera volumineuse ; si la zone est grande, c'est quand on voudra joindre un utilisateur que la signalisation sera lourde car il faudra interroger toutes les antennes pour savoir où est l'utilisateur.
Les opérateurs font des mesures de couverture pour déterminer les emplacements des stations ; il faut tenir compte de contraintes de type génie civil, coût de déploiement… Les études de couverture sont souvent assez empiriques (test avec des équipements et en se déplaçant…)

DIAPO 6 :
Pour l'essentiel et en tout cas c'est le cas en 2G, 3G, et pour l'instant 4G et 5G, les communications se font des terminaux vers l'infrastructure et de l'infrastructure vers les terminaux. C'est une topologie classique de réseaux d'accès télécoms. Le support hertzien

sera partagé entre les différentes cellules et entre les différents utilisateurs. Pour le partage du support entre plusieurs utilisateurs d'une même cellule, on a mis en place successivement des techniques de partage fréquentiel, temporel, par code…
Pour la répartition des fréquences entre les cellules, plein de solutions aussi : réattribution des fréquences selon des motifs géométriques (joli problème de coloriage de graphes) ; on peut faire de la réattribution plus proche mais dans ce cas, il faut faire attention au niveau d'interférences.
Parmi les problèmes communs à tous les systèmes mobiles, il y a la sécurité en raison du fait que le support de communication est le support hertzien et que donc les signaux peuvent être captés. Vous aurez des cours de sécurité en // à ce cours de réseaux mobiles. On retiendra les besoins d'authentification des utilisateurs et de chiffrement des informations.
Il y aura aussi pour les systèmes cellulaires, le besoin de mettre en œuvre des protocoles et des algorithmes pour déclencher les transferts intercellulaires et assurer la continuité de la communication. Ces transferts sont appelés handovers (ou handoff).
Le paging est la fonction qui sera mise en œuvre pour contacter un utilisateur dont on connaît la zone de localisation.
Le contrôle de puissance sera le mécanisme en boucle ouverte ou en boucle fermée qui réglera le niveau qui devra être suffisant pour que les données soient reçues de part et d'autre ; pas trop élevé pour limiter les méfaits des interférences.
Les métriques de qualité de service ne sont pas exactement les mêmes que celles que l'on peut avoir dans des réseaux fixes car il y aura aussi des coupures potentielles en cours de communication ; on peut être amené à mettre en place des priorités – mais qui peuvent être liées au contrat !

DIAPO 7
On va maintenant se plonger plus spécifiquement sur les systèmes 2G même si les fonctions dont on va parler vont nécessairement se retrouver dans les systèmes suivants.
La première fonction et nous l'avons déjà évoquée est celle de la gestion de la mobilité « Mobility Management ». Dans les systèmes GSM, un protocole a été défini, intitulé MM qui s'occupera de mettre à jour la localisation. Deux types d'équipements sont identifiés : une base de données intitulée HLR liée à l'opérateur et qui gère votre abonnement, votre localisation… Une base de données temporaire intitulée VLR permet de servir de cache et évite par exemple pour le chiffrement de repasser à tout moment par la HLR qui peut être à des milliers de kilomètres. La HLR est unique (logiquement) ; c'est elles qui ont largement été sujet à des défaillances et à des attaques.
Comme on l'a évoqué, le bon compromis porte sur les arbitrages entre coût de mise à jour et coût du paging. Jusqu'à la 5G pas beaucoup de neuf…

La deuxième fonction est la gestion des appels. Là c'est très GSM car la notion d'appel est très téléphonique – il y aura beaucoup de signalisation et il s'agira de choses que l'on a vu en grande partie à ce que l'on a vu dans les cours précédents. La gestion des communications sera revue dans tous les autres systèmes et la signalisation sera assez différentes de celle que l'on verra dans le contexte GSM. Le protocole associé s'appelle Call Management.

La troisième fonction identifiée dans le GSM s'appelle Gestion des Ressources Radio (RR). Là encore il faut noter qu'en GSM c'est globalement plus simple car il s'agira d'allouer un débit pour la durée de la communication téléphonique. Il ne faudra pas oublier les ressources pour la signalisation.

DIAPO 8 et 9

Si l'on regarde l'architecture système, il y a plusieurs maillons dans les communications. On s'est jusque là focaliser sur le lien sans fil entre le terminal et l'antenne mais il y a d'autres équipements avant de raccorder au réseau téléphonique.
Au-delà des équipements, il a fallu définir les piles de protocoles qui vont être mis en œuvre. On retrouve ici les interfaces qui avaient déjà été évoquées dans les cours de réseaux de télécommunications et qui au-delà des piles de protocoles utilisées de part et d'autre, délimite des zones de compétence des acteurs présents.
On note qu'à l'intérieur des équipements terminaux (là un téléphone), il y a des cartes SIM et une interface entre la carte SIM et le téléphone. On a ensuite l'interface radio avec le réseau d'accès. Le réseau d'accès sera raccordé à un réseau cœur (ici le réseau téléphonique) avec de nouveau une interface.
Sur la diapo 9, j'ai mis des noms sur les équipements et les interfaces (j'ai juste enlevé l'interface avec la carte SIM que l'on traitera peu par la suite).
Le terminal (MS) communique avec l'Interface Air avec une station de base (BS). Les stations base ont plusieurs antennes. Ces stations de base ont été conçues avec une idée de peu les charger fonctionnellement, l'essentiel des fonctions protocolaires seront plus loin dans le réseau. Une station de base sera pilotée par un contrôleur de station de base (BSC). Le lien peut être filaire (fibre) ou sans fil (RF). Le contrôleur est plus complexe d'un point de vue fonctionnel comme on l'illustrera sur les piles de protocoles à suivre.
Il sera à son tour raccordé à un MSC qui jouera le rôle de commutateur de raccordement vers le réseau téléphonique. C'est à partir de là que l'on aura accès au réseau sémaphore. Ce réseau sémaphore sera mis à contribution pour la mise en place des appels téléphoniques mais comprendra aussi les bases de données que sont les VLR et HLR. Le réseau d'accès s'arrête donc sur le MSC (et les équipements du réseau d'accès ne sont pas représentés dans le réseau sémaphore). Le MSC est une passerelle et là on retrouve ce que l'on a dit dans le cours d'interconnexion de réseaux.

DIAPO 10 : Principaux protocoles du GSM
Comme vous l'avez compris le GSM a été fait pour faire de la téléphonie. Par conséquent, la transmission de la voix sur le réseau d'accès ne donne pas lieu à des protocoles spécifiques : on en reste avec le codage de source et le codage canal pour mettre les échantillons de voix sur les ressources radio qui ont été attribuées.
Les principaux protocoles qui sont utilisés sont donc liées aux fonctions que l'on a évoquées sur les diapo précédentes.
Si on regarde l'interface radio, on voit apparaître les trois protocoles CM, MM, RR qui vont passer sur le protocole LAPD-m… qui a du mal à cacher son origine !
Sur le lien entre la station de base et son contrôleur, on retrouve le protocole LAPD. De façon surprenante sur le lien entre le contrôleur de station de base et le commutateur de raccordement, on trouve une pile de protocoles connue : celle du SS7. La surprise est que l'on n'est pas dans le réseau sémaphore !

DIAPO 11 : Les canaux du GSM
Une des raisons qui nous a poussé à conserver encore une séance sur le RNIS provient de ce passage. Dans le GSM, le partage du support de communication se fait sur un double découpage temporel et fréquentiel : on parle alors de MFTDMA (MultiFrequency Time Division Multiple Access). Chaque station de base exploite une certain nombre de bandes de fréquences, elles-mêmes redécoupées temporellement.
Un canal physique du GSM correspond à une bande de fréquence et à une plage temporelle. Ces canaux physiques vont alors être utilisés pour plusieurs fonctions qui sont retracées dans ce tableau. Le découpage est réalisé de façon figée. Chaque canal logique aura droit à un

« débit » (nombre d'intervalles de temps par unité de temps) constant ; mais tous ces canaux n'ont pas le même débit.
C'est un peu le même principe que ce que l'on a vu en RNIS avec des canaux à débit différent MAIS ici l'unité d'allocation est l'intervalle de temps.
Donc sur une trame de la couche physique tous les canaux ne seront pas systématiquement représentés.
Le schéma est parfaitement périodique… sur une échelle de plusieurs trames de la couche physique !
Là où l'on avait essentiellement les canaux B et les canaux D, là il y a une plus grande diversité de fonction et donc de protocoles associés. Attention, le passage à la 3G, 4G et la 5G n'a pas fait disparaître cette notion de canaux ! Ce sera leur façon de les exploiter qui évoluera.
Les canaux du GSM sont découpés en 4 groupes. Dans ce tableaux sont recensés les différents canaux, les flèches font référence au sens de la communication.
On va commencer par les plus simples : les canaux de données. Ils sont plus simples car ils sont majoritairement utilisés pour faire transiter de la voix et par conséquent pas de protocoles. Ils sont bidirectionnels. Bon on s'en est servi pour faire de la transmission de données… bon là c'est comme le RNIS, peu d'intérêt d'avoir des canaux attribués en mode circuit et à débit si faible (bcp plus que le RNIS).
On va remonter d'un cran. C'est la catégorie des canaux de signalisation dédiés. Naturellement, on va avoir de la signalisation et donc naturellement, on va avoir des canaux séparés pour la signalisation. Les originalités par rapport aux canaux D du RNIS, c'est que la signalisation va passer majoritairement sur ces canaux qui sont des canaux dédiés. On aurait pu faire un peu comme pour le canal D mais les débits sont faibles et y remettre un accès aléatoire à la mode Canal D n'était pas raisonnable. Les canaux de signalisation seront donc attribués à un utilisateur. Ils sont bidrectionnels encore une fois. La deuxième nouveauté est la présence de canaux de contrôle associés à ces canaux de signalisation. Ils sont utilisés pour envoyer des mesures périodiques qui sont particulièrement utiles (niveau de puissances reçus, taux d'erreur…) en particulier quand il s'agira de déclencher des transferts intercellulaires. On termine par les canaux dédiés justement à la signalisation liée au transfert intercellulaire.
Les canaux SDCCH et FACCH se partagent les mêmes ressources ; c'est le seul cas en GSM où il y aura un partage dynamique, le FACCH apparaîtra lors des phases de transferts intercellulaires.
Les nouveautés sont plutôt sur les canaux au-dessus. La troisième catégorie, ce sont des canaux de signalisation partagés.
On va en premier trouver les canaux de paging qui sont dans le sens descendant pour savoir où se situe l'utilisateur.
Les seconds sont les canaux en accès aléatoire. Sans surprise, il est nécessaire d'offrir la possibilité aux terminaux de rentrer dans le réseau. On a donc ajouté un canal dans le sens montant ! Ce canal est partagé car justement, on ne peut pas les préattribuer. Les terminaux ne s'entendent pas… donc on a mis une méthode d'accès aléatoire de type Aloha Discrétisé. Ces intervalles de temps laissés à l'entrée des terminaux dans le réseaux apparaissent périodiquement.
Bon naturellement, Aloha ne suffit pas à régler le problème de l'entrée. Cet accès aléatoire peut donner lieu à des collisions et, dans la mesure où justement les terminaux ne sont pas encore entrés dans le réseau, ils envoient des messages en clair. Il faut donc faire passer le moins d'informations possibles sur ces canaux RACH.
On va donc compléter par un canal descendant AGCH sur lequel on attribuera les ressources.

Le canal AGCH permet donc de traiter aussi la méthode d'accès. Les collisions et les erreurs de transmission se traduiront par une absence de retour. D'où l'accès aléatoire qui se traduira par un tirage uniforme au bout duquel on relancera la requête.
Le canal RACH peut être vu comme un canal sur lequel l'utilisateur va juste lever le doigt et ensuite on se servira des autres canaux pour faire passer la signalisation U-U et U-N.
Pour finir un canal descendant pour envoyer des SMS à tous les terminaux à portée (je ne sais pas si cela a été réellement utilisé).

Pour terminer des canaux de broadcast sont présents uniquement dans le sens descendant et qui se traduit par des informations purement couche physique pour assurer la synchronisation temporel et le calage fréquentiel. Les canaux qui nos intéresseront d'un point de vue réseaux sont les canaux BCCH où le réseau va donner des informations systèmes aux utilisateurs liés à la cellule. C'est par exemple là que circulent les informations sur la zone de localisation qui permettront à l'utilisateur de mettre à jour les informations auprès de la HLR. Ces informations sont envoyées en clair. Les utilisateurs sont couverts par plusieurs cellules, ils pourront ainsi repérer le niveau de puissance depuis les cellules voisines, cela permettra de déclencher les transferts intercellulaires.

DIAPO 12
Le système GSM conduit à des trames de couche physique de durée constante. Une trame comporte plusieurs (8) slots et plusieurs fréquences seront utilisées en même temps. La durée d'un slot est constant et courte. La périodicité de l'ensemble n'est pas très simple comme on le voit. Les emplacements des intervalles de temps dédiés à chaque (type de) canal sont connus à l'avance et sur une périodicité qui n'est pas la même pour la signalisation et le contrôle.

DIAPO 13 et 14
Sans grande surprise les piles de protocoles utilisées ne sont pas les mêmes sur les différents types de canaux…
Par exemple, si on regarde la couche 2, pour certains canaux, il n'y a rien. Les canaux de Broadcast sont dans ce cas (sauf BCCH), on s'arrête à la couche PHY. Pour les canaux TCH, rien non plus.
Pour d'autres canaux, ce sera transparent (CCH et BCCH) : pour les canaux unidirectionnels, cela ne sert à rien de mettre en place de la fiabilisation. Donc on met directement le message à émettre dans le slot dédié. Remarquons que pour RACH, on n'est pas identifié donc on ne va pas avoir une fiabilisation intrinsèque. Ce sera le canal AGCH qui permet de terminer le protocole d'accès.
Finalement, on ne va avoir de protocoles de niveau 2 que sur les canaux DCCH. Le protocole utilisé est LAPDm. C'est un cousin de LAPD. Ce qui change, c'est que le code d'erreur est traité par la couche physique ; pas de FCS en fin de trame. Le slot a une durée constante. On aura alors une taille de trames constante et courte (la différence avec les valeurs de la diapo précédente, c'est justement le traitement couche PHY). Taille constante implique qu'il n'y a plus besoin de délimiter mais aussi du padding pour terminer le remplissage. Il est donc nécessaire d'indiquer la partie réellement utilisée. La taille est très faible et les messages que l'on va faire passer dessus sont plus grands (demande d'appel téléphonique par exemple). Il faut donc prévoir de faire de la segmentation. Ces informations sont indiquées dans le champ longueur.
Le reste est plus classique et en particulier le champ de contrôle… Le champ d'adresse est plus spécifique. Les canaux sur lesquels ce protocole est utilisé sont des canaux dédiés. Il n'y a donc pas de doute sur l'adresse du terminal. Ce que l'on va laisser en revanche, ce sera le

SAPI que l'on avait vu dans le LAPD. Peu de SAPI ont finalement été retenus : un pour la SIG (SAPI=0) et ceux pour envoyer les SMS (SAPI=3).
Peu de surprise ensuite…
La possibilité d'envoi de données avec et sans connexion sont présentes. Le choix est le suivant : pour toute la signalisation, on utilisera le mode connecté qui permettra de faire du contrôle de flux et de la reprise sur erreur. Le mode non-connecté est utilisé lors des phases de transferts intercellulaires comme on l'illustrera par la suite mais aussi pour les envois de mesures sur les canaux SACCH. Si on rate l'une de ces mesures, on fera sans. Le terminal en remonte suffisamment régulièrement.

DIAPO 15
La couche 3 (je n'ai ni écrit ni dit réseau) va s'occuper de traiter les différents protocoles de signalisation. On y retrouve sans surprise les protocoles RR, CM et MM déjà évoqués précédemment. Les formats de message sont en fait ceux de Q.931 dont on retrouve encore une des forces. En particulier dans les en-têtes, on a un identifiant de protocole. C'est lui qui permettra de savoir de quel protocole il s'agit. On n'a pas voulu encapsuler CM sur MM sur RR. Ce sont bien trois protocoles séparés au dessus de LAPDm.
Ce problème aurait pu être traité différemment par exemple en ayant des points d'accès au service au-dessus de LAPDm… ce n'est pas ce qui a été retenu.
Pour le reste, je vous renvoie à la description des messages Q.931 : type de messages, champ obligatoire, optionnel, Type/Longueur/Valeur
Identificateur de transaction pour faire du double appel… déjà vu !

DIAPO 16
La couche RR permet de gérer les ressources radio. Les ressources sont attribuées par le réseau à l'utilisateur pour toute la durée voulue. Elle permet d'allouer les canaux de signalisation dédié DCCH et les canaux de données TCH. Attention, il faut rétablir les ressources en cas de transfert intercellulaire.
C'est une nouveauté par rapport au RNIS où l'on avait pas ces mécanismes. Les canaux B étaient établis implicitement lors des mises en place des connexions.
C'est de la signalisation Usager/Réseau qui est uniquement cantonnée au réseau d'accès.

La couche MM est également nouvelle. C'est elle qui permettra de mettre à jour la localisation des utilisateurs mais c'est aussi elle qui permettra de mettre en œuvre les principes de la sécurité : authentification et chiffrement. Les messages sont transparents pour le réseau d'accès et seront échangés entre le terminal d'une part et la VLR/HLR. Attention MM est un protocole de réseau d'accès. C'est de la signalisation Usager/Réseau.

La couche CM est la moins nouvelle. Elle permet de gérer les connexions et elle comprend plusieurs parties : CC – la signalisation de base téléphonique, SS – les services supplémentaires de type double appel/transfert d'appel. Tout va bien c'est de la signalisation U-U de réseau d'accès et qui va avoir pour objet de déclencher la signalisation sémaphore ISUP. De façon un peu originale, c'est aussi là qu'ont été implantés les SMS. C'est un peu surprenant car justement les SMS sont des messages qui devraient être dans le plan de données car ils sont à échanger entre utilisateurs. En revanche, comme leurs noms l'indiquent ce sont des messages et les contraintes de qualité de service sont identiques à celles de la SIG : pas de contrainte de délai mais contrainte de fiabilité… Attention, on est sur des canaux de SIG et l'on décrira ensuite comment on les traitera une fois que l'on sera arrivé au MSC. Tous ces messages sont traités de façon transparente par le réseau d'accès.

DIAPO 17 :
Après l'interface radio, on va maintenant regarder l'interface entre la station de base et son contrôleur.
Pour le plan de données, il s'agit ici simplement de la parole téléphonique qui est envoyée en mode circuit entre le contrôleur et la station de base, pas de protocole supplémentaire.
Pour la signalisation, c'est un peu plus complexe.
Le contrôleur doit piloter ses stations de base. Il y a donc des messages de contrôle qui doivent être échangés entre la station de base et son contrôleur pour gérer les ressources… (on distingue les messages de supervision/maintenance de la station de base d'une part et les messages de gestion de la liaison).
Par ailleurs, il y aura des messages qui auront vocation à être envoyés sur l'interface radio (ou qui dans l'autre sens viennent des utilisateurs). Ces messages-là qui proviennent des protocoles RR, CM et MM transitent de façon transparente sur la station de base.
Pour tous ces messages, on va utiliser le protocole LAPD du RNIS en mode connecté qui permettra de fiabiliser l'ensemble.
On distingue ces différents flux au travers de SAPI différents – ce qui permet de savoir ce que l'on doit faire des messages au niveau de la station de base dans le sens descendant.
Il y aussi un identifiant de terminal dans LAPD – TEI. Ce qui a été retenu a consisté à regrouper l'ensemble des messages qui sont destinés aux utilisateurs qui sont sur la même fréquence sur le même TEI.

DIAPO 18
Si maintenant on regarde la pile de protocole, on retrouve une pile un peu particulière car les messages RR sont soit traités directement par la station de base. Pour d'autres, c'est le contrôleur de station de base qui les traitera (on le verra au travers d'exemple).
Entre la station de base et son contrôleur, c'est la couche BTSM qui gère les communications.
Les autres messages sont dans les « couches supérieures » au niveau du contrôleur de station de base passent de façon transparente sur la station de base. Pour ces messages, la Station de Base joue un rôle de pont mais il ne peut pas être complètement transparent car en raison du multiplexage qui est mis en œuvre sur le lien BTS-BSC, on doit regarder dans le message pour savoir le terminal destinataire et donc envoyer le message sur le bon canal (SDCCH).

DIAPO 19 et 20
Bon on va gagner un peu de temps sur ces deux diapos… On retrouve sensiblement les mêmes principes sur l'interface entre le BSC et le MSC que ceux que l'on vient de voir.
Pour le plan de données, rien de mieux.
Pour le plan de contrôle, on aura des messages de contrôles à échanger entre le contrôleur de station de base et le commutateur de raccordement et messages qui passent de manière transparente sur l'interface car ils vont poursuivre leur vie. La seule curiosité est l'utilisation des protocoles du monde SS7 alors que l'on n'est pas dans le réseau sémaphore.

DIAPO 21
On va passer maintenant à des illustrations protocolaires. Comme vous vous doutez, il y a beaucoup de protocoles et de messages. On va se concentrer sur certaines phases-clé.
Le premier exemple qui est un peu la brique de base, c'est celle qui permet à un utilisateur de demander un canal de signalisation.
La première étape, l'utilisateur lève le doigt sur le canal RACH. C'est un message RR qui est envoyé : pas de protocole de niveau 2.

S'il gagne l'accès aléatoire, on va lui attribuer un canal de signalisation SDCCH. La décision n'est pas du ressort de la station de base mais de son contrôleur. C'est le protocole BTSM qui est utilisé… un peu bavard (bon on ne détaille pas LAPD à ce niveau-là).
La réponse à la requête RR est envoyée par un message RR sur le canal AGCH. On donne les informations sur le canal SDCCH qui est attribué.
L'utilisateur ouvre une connexion LADm sur le canal en question et il va ensuite préciser le service qu'il veut activer.
Dans la suite, toute cette diapo sera représentée sous la forme d'une simple flèche bidirectionnelle.

DIAPO 22
On va maintenant décrire le paging. L'utilisateur est repéré à une zone de localisation près mais pas à la cellule près. Quand on essaye de le joindre, un message est diffusé à l'ensemble des cellules qui sont dans la zone de localisation – donc à tous les contrôleurs de station de base (pas repéré ici) et à toutes les stations de base. Le message de Paging est relayé par ces stations de base et envoyé en Broadcast et en clair sur le canal PCH.
L'utilisateur qui se reconnaît va chercher à répondre. Il lève le doigt sur le canal RACH pour dire qu'il veut parler. On lui attribue un canal SDCCH et il répondra sur ce canal.
Attention là c'est en clair. On ne relâche pas le canal SDCCH car si on lui a envoyé un message de paging.
Ces accès aléatoires initiaux et ce paging n'ont guère bougé avec les systèmes 3G, 4G – les couches basses si !

DIAPO 23
On va illustrer maintenant des mécanismes plus sophistiqués.
On commence par l'appel sortant (du coup d'un mobile vers un fixe).
L'utilisateur commence cf. diapo 21. Il va alors dire qu'il veut téléphoner. Pour l'instant tout est en clair. On va alors l'authentifier.
Le principe repose sur des clés publiques. On jette un nombre aléatoire à l'utilisateur ; lui seul peut répondre correctement.
Les choix possibles auraient été que la VLR puisse vérifier en déroulant l'algo mais cela pose des problèmes de confidentialité – la VLR peut ne pas appartenir à l'opérateur auprès duquel on est abonné et il ne faut pas lui donner la clé de chiffrement.
Ce nombre aléatoire est le paramètre de l'algorithme qui est déroulé sur le terminal et qui permettra de répondre. La VLR stocke le nombre aléatoire et la réponse. On ne le rejoue plus.

On passe alors en mode chiffré. On fait appel à une cryptographie à clé privée. C'est la même clé qui est utilisée entre le MSC et le terminal mobile. Cette clé ne circule pas. Elle est déduite par le terminal au vu du nombre aléatoire qui a été envoyé. Pour la même raison que pour l'authentification, la VLR ne fait pas le calcul de la clé de chiffrement. Elle est calculée par l'opérateur et stockée dans le VLR. La VLR stocke donc des triplets : nombre aléatoire, réponse à apporter et clé de chiffrement.
On passe ensuite à du plus connu : signalisation CM – Q.931 de demande d'appel téléphonique.
Attention, on voit aussi l'attribution d'un canal TCH à l'utilisateur de façon explicite (protocole RR). Comme on le voit, la signalisation U-U et la signalisation U-N sont complètement disjointe contrairement à ce que l'on avait vu en RNIS.

DIAPO 24 : Appel Entrant

Là c'est plus compliqué ! L'appelant est fixe, l'appelé mobile. L'appelant compose le numéro de téléphone du destinataire. L'appel téléphonique est routé dans le réseau téléphonique en fonction du numéro de téléphone qui est composé. Hors ce numéro est un numéro E.164 avec le code pays. Les plages de numéro réservé aux utilisateurs mobiles dépendent d'un pays à l'autre. Par conséquent, on route l'appel vers le bon pays. C'est en arrivant dans le bon pays que l'on découvre qu'il s'agit d'un utilisateur mobile. Il faut atteindre une passerelle vers le bon opérateur mobile et la bonne HLR. C'est grâce au numéro qui est composé que l'on découvre l'opérateur et que l'on pourra router l'appel vers la bonne passerelle GMSC (qui permettra d'atteindre la bonne HLR).
La mise en place de l'appel téléphonique s'arrête là et on va maintenant interroger la HLR. Le protocole utilisé est MAP (Mobile Application Protocol) qui se positionne sur TCAP/SCCP/MTP1-3 (cf. cours de téléphonie). On ne téléphone pas à la base de données.
La HLR stocke la localisation de l'utilisateur. On veut prolonger l'appel dans le RTC pour atteindre la MSC qui le gère. La solution qui a été proposée (très inspirée du numéro vert) est de fournir un numéro de téléphone temporaire qui lui est parfaitement géographique et lié au MSC courant. Le mérite est que l'on n'a absolument pas à changer le routage dans le RTC et les modifs dans le SS7 sont indolores (on a juste eu à introduire ce nouveau protocole MAP).
Le numéro de téléphone temporaire va être fourni par la VLR. On aurait pu attribuer ce numéro de téléphone temporaire au moment de l'enregistrement de la mise à jour de la localisation mais cela aurait imposé de bloquer le numéro de téléphone. Un MSC ne dispose que de 10.000 numéros ce qui est peu. Un même MSC gère plutôt 10 fois plus d'utilisateurs que cela. La VLR est donc interrogée ; elle fournit ce numéro temporaire à la HLR qui la restitue à la GMSC. On reprend la mise en place de l'appel téléphonique avec ce numéro de téléphone temporaire jusqu'à atteindre le MSC. Celui reconnaît le numéro de téléphone temporaire et va chercher à contacter l'utilisateur. On fait du paging… et après c'est assez proche à ce que l'on a vu pour l'appel entrant.
On voit un peu la lourdeur induite et surtout la non-optimisation globale du routage téléphonique obtenu. On aurait pu améliorer en mettant en place une communication MAP directement entre le CA de l'appelant et la HLR de l'appelé… mais pour cela, il aurait fallu que les adresses des HLR soient connues partout ainsi que la connaissance des plages de numéros de tous les opérateurs dans le monde. Les opérateurs n'étaient pas très chauds.
Une remarque encore concernant la portabilité du numéro, si on change d'opérateur la HLR de l'opérateur d'origine renvoie vers la HLR du nouvel opérateur.

DIAPO 25 ; Handover
La topologie du réseau mobile est arborescente. On peut envisager lors d'un transfert intercellulaire à changer de stations de base, de contrôleur de station de base ou de commutateur de raccordement.
Attention, il s'agit bien de la topologie logique, la topologie physique est souvent en anneau SDH par exemple.
On ne va détailler que le plus simple : le changement de station de base. On expliquera ensuite plus rapidement les modifications pour les autres.
Le déclenchement du handover donne lieu à de l'algorithmique : quand déclencher le handover, vers quelle cellule l'envoyer et à des protocoles.
Les algorithmes ne sont pas normalisés. Le plus souvent, on utilisera des critères de qualité de signal. Mais il faut que la différence de la qualité des signaux reçus depuis la nouvelle station de base soit significativement meilleure et pendant une durée suffisante pour que cela ait un intérêt. On peut aussi envisager de déclencher un handover pour faire de l'équilibrage de charge.

Les protocoles le sont… L'utilisateur en communication, puisque c'est bien là que l'on parlera de handover, envoie des messages périodiques sur le canal SACCH. Ces mesures sont remontées au contrôleur de station. Quand il le juge opportun, il déclenche le handover.
Dans le monde des réseaux mobiles, les handovers sont complètement pilotés par le réseau. Pour cela il prévient l'utilisateur en lui attribuant les ressources dans la nouvelle cellule. On voit apparaître l'utilisation du canal FACCH.
Attention si l'utilisateur a récupéré les informations relatives à ses nouvelles ressources, il n'est pas encore calé temporellement par rapport à sa nouvelle cellule. Pour ce faire, il va commencer à envoyer des messages sur le canal TCH mais en n'utilisant pas tout les slots, on n'utilise que le centre du slot pour éviter d'empiéter sur des slots qui sont attribués aux autres utilisateurs. La nouvelle station de base peut alors estimer la distance qui la sépare de l'utilisateur en regardant les instants où elle reçoit le message. Elle finit par détecter le nouvel utilisateur, elle en réfère à son contrôleur. Elle va alors envoyer cette estimation de distance au terminal par des trames UI et de nouveau FACCH. Quand l'utilisateur réussit à en exploiter une, il termine la réalisation du handover en mettant en place une connexion sur FACCH et envoyant un message de fin de réalisation du handover.
Pour ce qui est du plan de données, on ne fait rien ; les échantillons de voix qui sont en souffrance dans le réseau, sont purgées… l'oreille humaine s'en accommode. Il faut que ce soit assez court.

Si maintenant on essaye de regarder ce qui se passe en cas de contrôleur de station de base, il y aura en plus de la signalisation qui sera échangée entre l'ancien contrôleur et le nouveau. Ils ne sont pas reliés directement ; donc ça remonte par le MSC.
Plus compliqué le handover avec changement de MSC. En effet, jusque là, il n'y avait aucun impact sur le réseau de transport. Là, on avait deux choix : les refuser – on coupe la communication ou mettre en place des mécanismes plus sophistiqués. C'est ce que l'on a fait. Attention, peu de MSC donc ça n'arrive pas tout le temps mais lors d'un trajet en train…
Donc la particularité si changement de MSC, c'est qu'il va falloir reprendre de la signalisation sémaphore. On ne peut pas reprendre une mise en place d'appel téléphonique complète qui prend des secondes. On va donc simplement prolonger l'appel à partir de l'ancien MSC vers le nouveau… ils sont reliés par des liens. On ne fait toujours rien dans le plan de données, mais il faut relancer de la signalisation ISUP pour cela pour réserver un intervalle de temps entre l'ancien et le nouvel MSC. Pour éviter des boucles (retour vers un ancien), on redétricote.

DIAPO 26 : Mise à jour de localisation
Le principe va reposer sur la diffusion des zones de localisation par le canal BCCH – identifiant LAI. Le terminal stocke l'identifiant de la dernière zone où il s'est enregistré. Si les identifiants qu'il perçoit ne sont pas les bons, c'est qu'il faut mettre à jour. Il commence de nouveau par dire qu'il veut parler… bcp de choses déjà vues.
Comme ici les infos sont encore en clair, il va utiliser un identifiant temporaire de terminal TMSI qui lui a été attribué dans son ancienne zone de localisation.
L'obtention de l'ancienne zone de localisation permet à la nouvelle VLR d'aller interroger l'ancienne pour récupérer les triplets de sécurité non encore utilisés liés à cet identifiant. L'ancienne VLR fournit l'identifiant du terminal qui permettra d'aller mettre à jour la localisation.
On authentifie l'utilisateur. (Attention, si plus de triplet disponible, l'IMSI permet de déterminer l'opérateur et donc obtenir des nouveaux triplets.)
Quand l'authentification a fonctionné, on en réfère à la HLR pour qu'elle mette à jour la localisation et qui va s'adresser à l'ancienne VLR pour effacer le précédent enregistrement –

attention les VLR ne peuvent pas l'imposer à d'autres VLR. On met alors en mémoire cache dans la VLR des infos relatives à l'abonnement de l'utilisateur et on finit par lui changer son TMSI.

DIAPO 27 : Architecture pour SMS
Les SMS ne sont pas envoyés directement entre les terminaux mais stockés dans un centre de stockage de message qui est en dehors du réseau sémaphore. Les SMS sont envoyés comme de la signalisation sur des canaux dédiés qui sont irrémédiablement envoyés vers le réseau sémaphore. Quand on regarde l'architecture protocolaire, on voit plusieurs parties :

- sur le réseau d'accès : on utilise la pile de protocoles présentée précédemment, mais en plus on fiabilise entre le terminal et le MSC ;
- sur le réseau sémaphore : on utilise MAP avec de nouveau de la fiabilisation ;
- on ajoute une couche de transport entre le terminal et la passerelle vers le centre de stockage ;
- la partie entre la passerelle et le centre de stockage sort de la normalisation – ce qu'on veut TCP/IP/Ethernet par exemple mais avec un protocole applicatif.

DIAPO 28 : Illustration protocolaire gros grain d'envoi de SMS
On voit les différentes phases et les différents niveau d'accusés de réception entre extrémités et sur les différents segments

DIAPO 29 : Illustration de réception de SMS
Là ce qui est plus compliqué c'est encore une fois la localisation de l'utilisateur. Il y a beaucoup d'analogie avec ce que l'on a évoqué pour l'appel entrant… ce qui change, c'est qu'on n'appelle pas pour envoyer un SMS. Il va donc s'agir de router un message de signalisation entre le SMS-GMSC et le MSC. On a donc juste besoin de récupérer l'adresse du MSC (SCCP). Du coup pas besoin de numéro de téléphone temporaire.

DIAPO 30 : Un zoom sur les couches plus basses
L'utilisateur dit qu'il veut parler. On lui alloue un canal SDCCH. Il met en place une connexion sur le SAPI 0. Il dit qu'il veut envoyer un SMS. Il met en place une connexion sur le SAPI 3 LAPDm. Il peut envoyer plusieurs SMS. Quand c'est fini, on peut de façon implicite déconnecter la connexion sur le SAPI=0.
Et encore on n'a pas illustré la segmentation et toutes les trames I, RR…