Le GSM™: Global System for Mobile communication

- Par Emanuel Corthay HB9IJI et
  Iacopo Giangrandi HB9DUL
- Présentation au club des RadioAmateurs Vaudois le 11 avril 03 : www.hb9mm.com
- © RAV 2003 version 1.3 octobre 2003

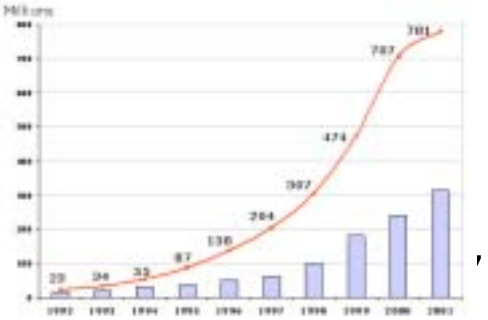
Introduction historique

- Origine
- Organisme de standardisation
- Raison de son succès
- Couverture suisse et mondiale

Historique

- WARC World Administrative Radio Conference en 1979: Ouverture du 900 Mhz
- ETSI European Telecommunication Standards Institute : Communauté EU
- Groupe Spécial Mobile
- Choix du numérique en 1987 – Standard européen – Fin de l'analogique
- Lancement commercial en 1991: NATEL D

Statistiques



- Succès mondial du standard, millions d’abonnés fin 2002 - 190 pays
- 1 milliard en 2004
- Sa force : Standard fixé au niveau EU
  - Baisse de coûts des terminaux et du réseau
  - Itinérance dans de nombreux pays
  - Plusieurs constructeurs en concurrence
  - Répond à un besoin et payé par l’appelant
  - Beaucoup de services (caller id, conférence,…)

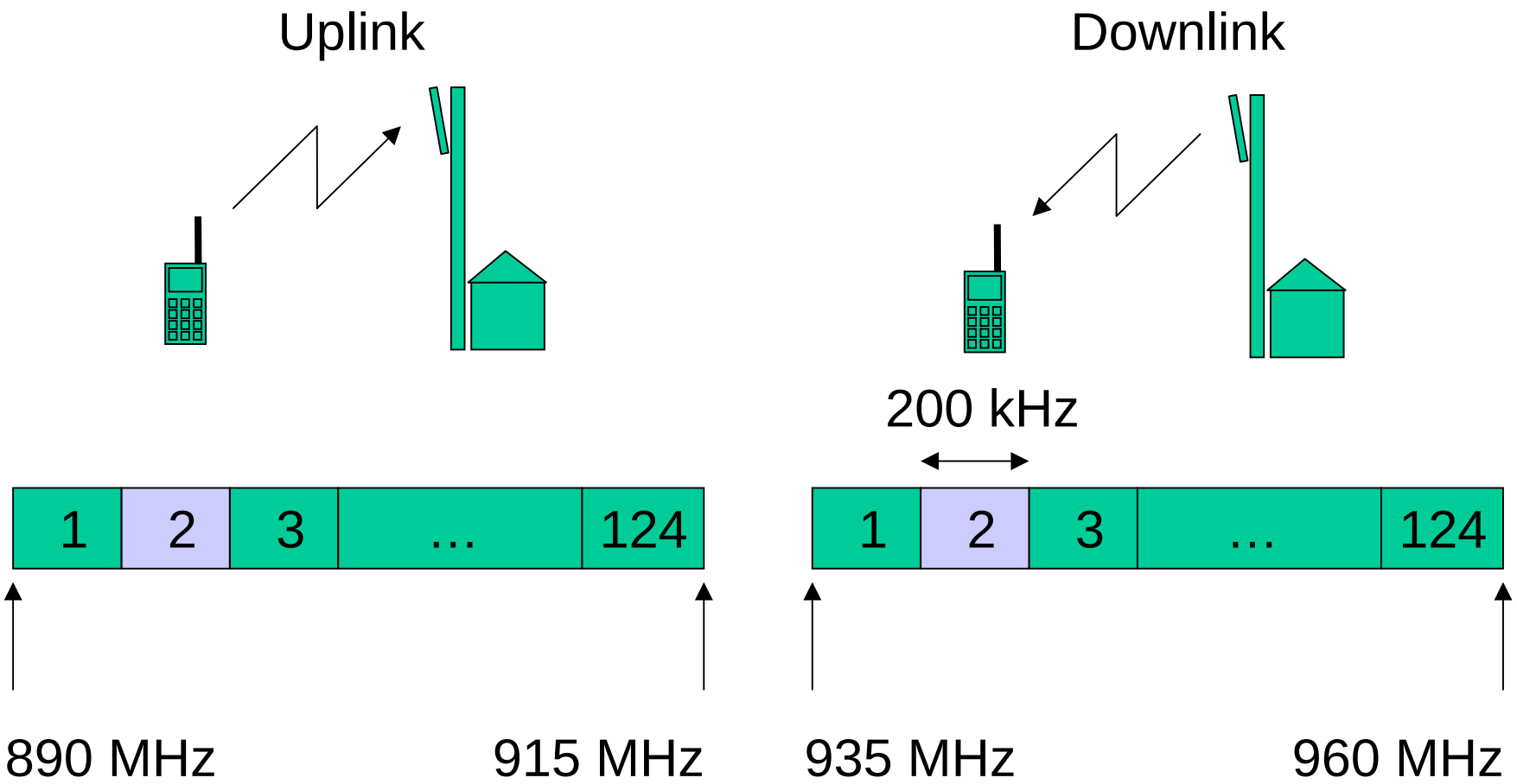
Couverture


Basel
Winterthur
St. Gallen
Zürich
Zürichsee
Biel
Neuchâtel
Luzern
Fribourg
Lausanne
Lake
Geneva

Interface radio

- Fréquences / Canaux / Bandes
- Modulation / Traitement de la parole
- Multiplexage temporel
- Canaux logiques
- Trafic / Capacité
- Réutilisation des fréquences et interférances
- Puissance

Fréquences / Canaux



Bandes / Opérateurs

GSM 900 MHz

UL : 890..915 MHz
DL : 935..960 MHz
124 Canaux (1..124)

68 53

EGSM 900 MHz

UL : 880..890 MHz
DL : 925..935 MHz
49 Canaux (975..1023)

11 22

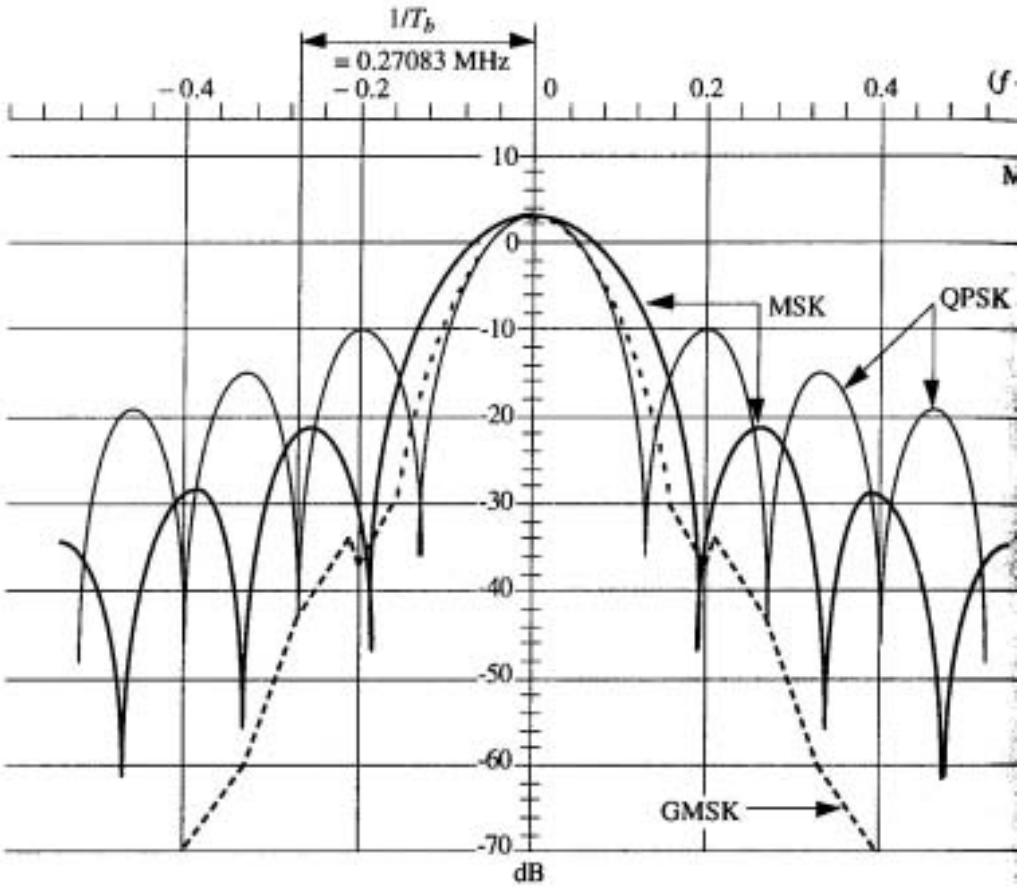
GSM 1800 MHz

UL : 1710..1785 MHz
DL : 1805..1880 MHz
374 Canaux (512..885)

61 124 59

Swisscom
Orange
Sunrise

Modulation GMSK



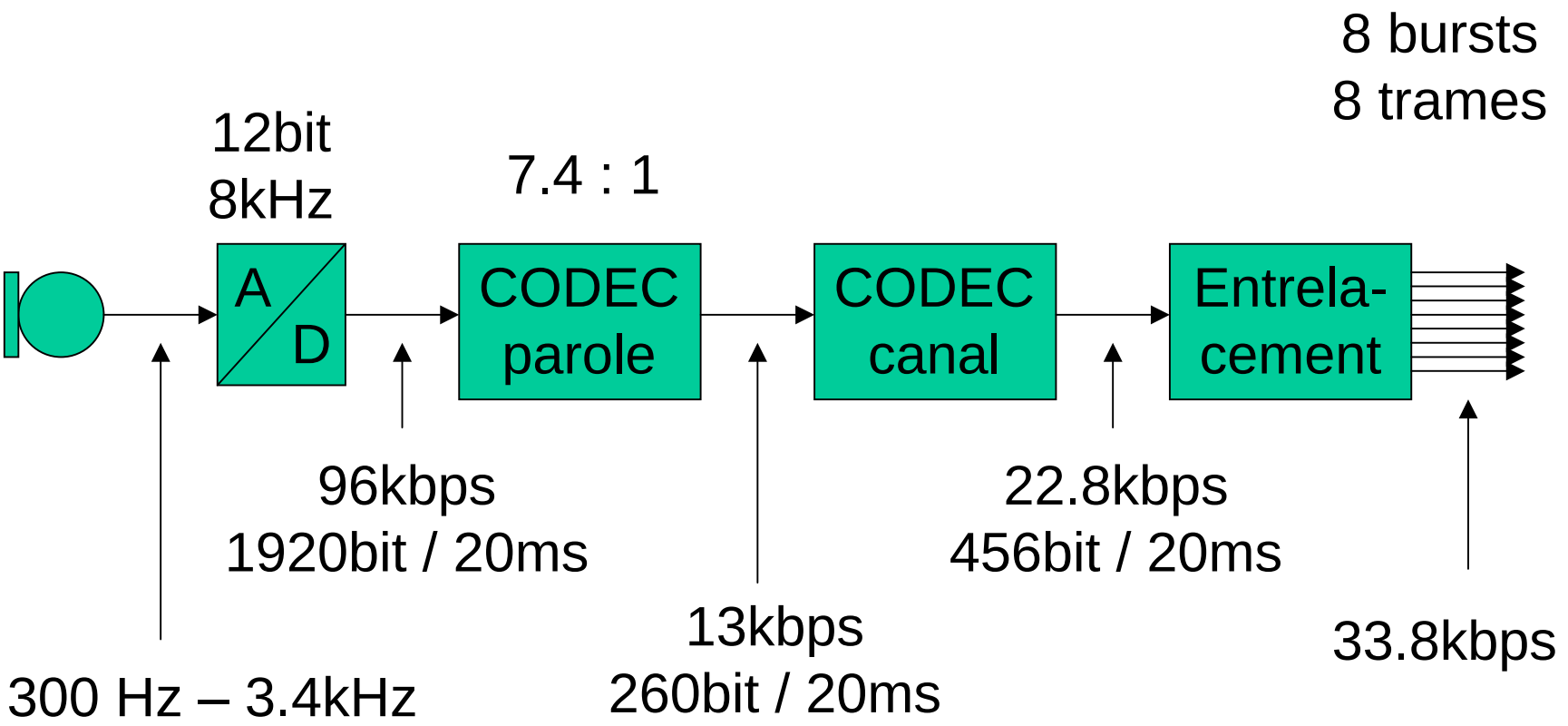
Gaussian Minimum Shift Keying ≈ combinaison de modulation de phase et de fréquence.

Largeur de bande: 200 kHz

Débit binaire: 270.833 kbps

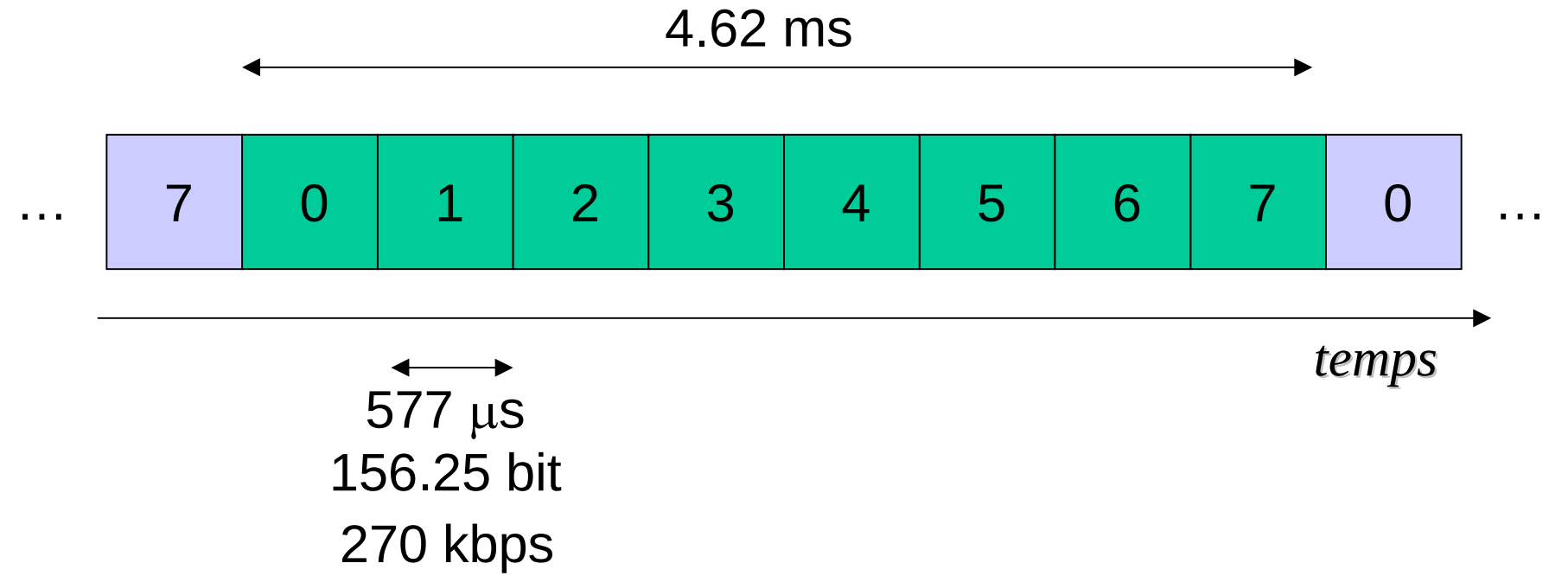
1 bit = 3.7 μs

Traitement de la parole



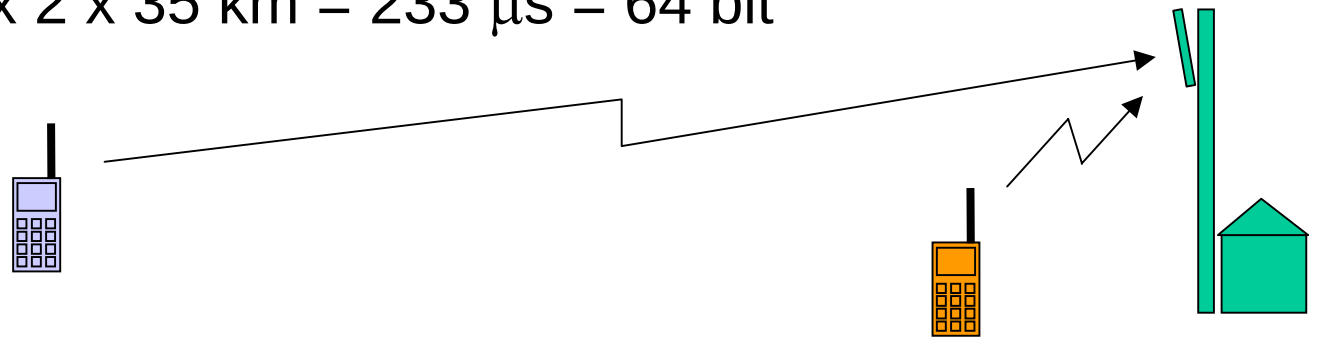
Multiplexage temporel : TDMA

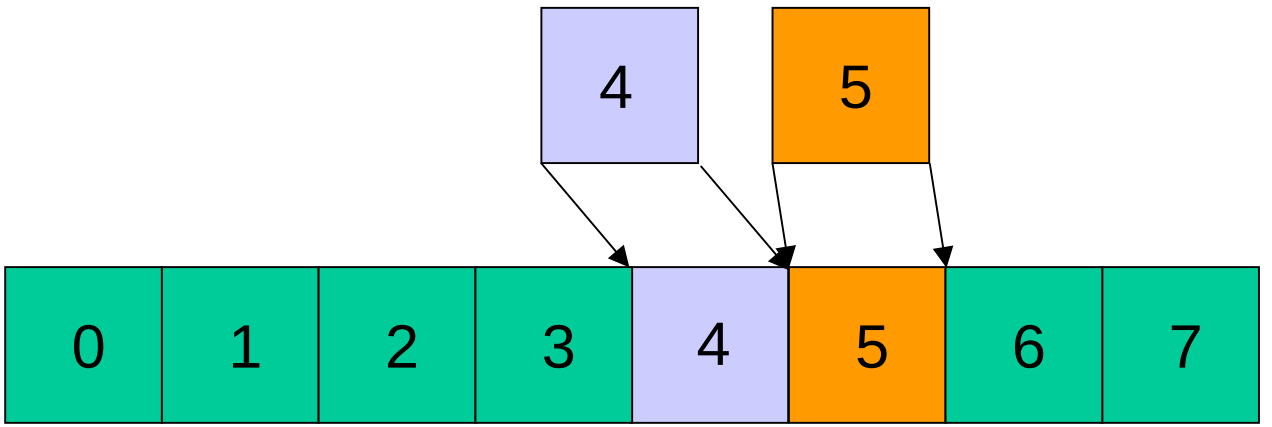
8 Time Slots par canal



Timing Advance

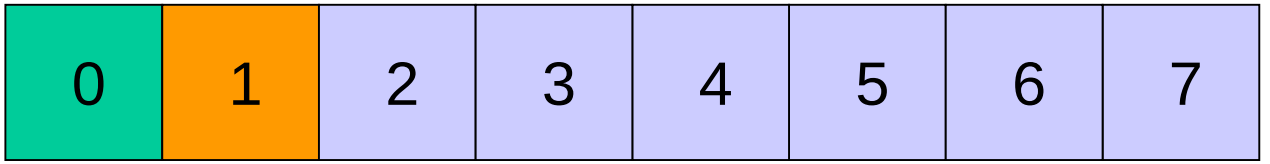
Max 2 x 35 km = 233 μs = 64 bit





Résolution: 1 bit = 3.7 μs = 2 x 550 m

Canaux logiques

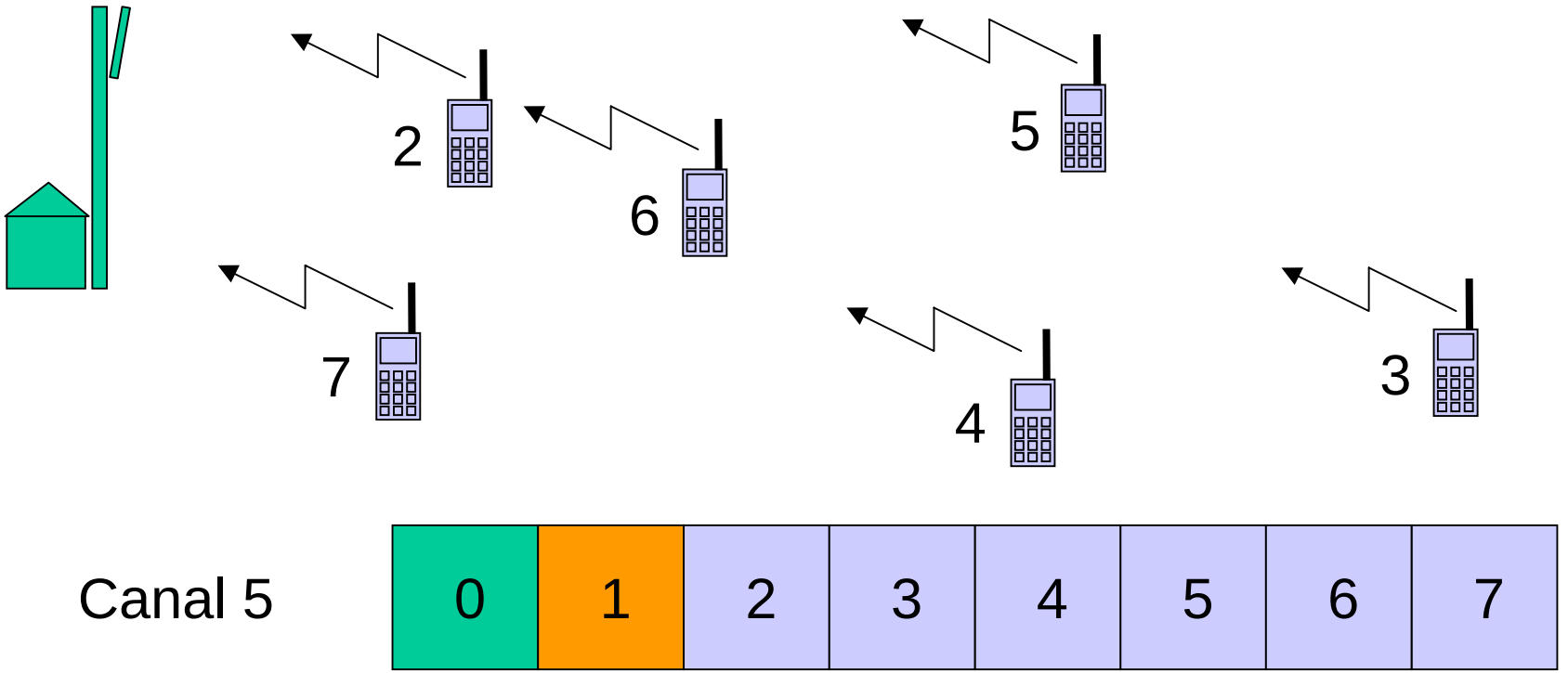


TCH: Traffic CHannel

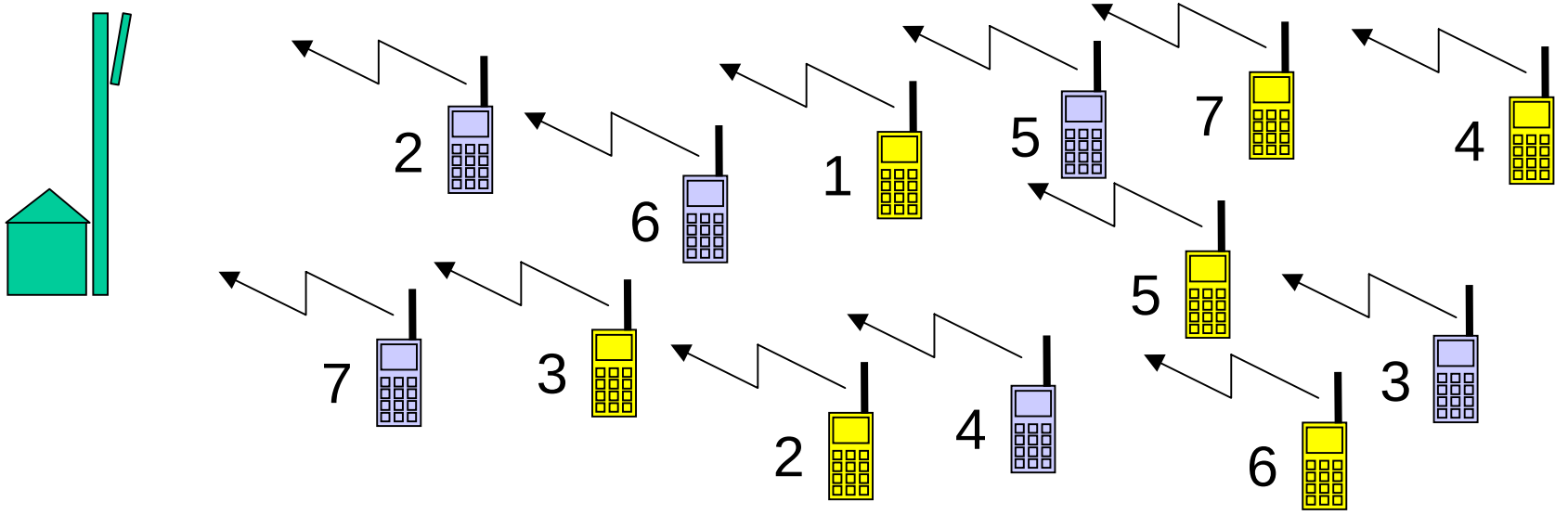
SDCCH: Standalone Dedicated Control CHannel

BCCH: Broadcast Control CHannel

Trafic / Capacité (1/2)

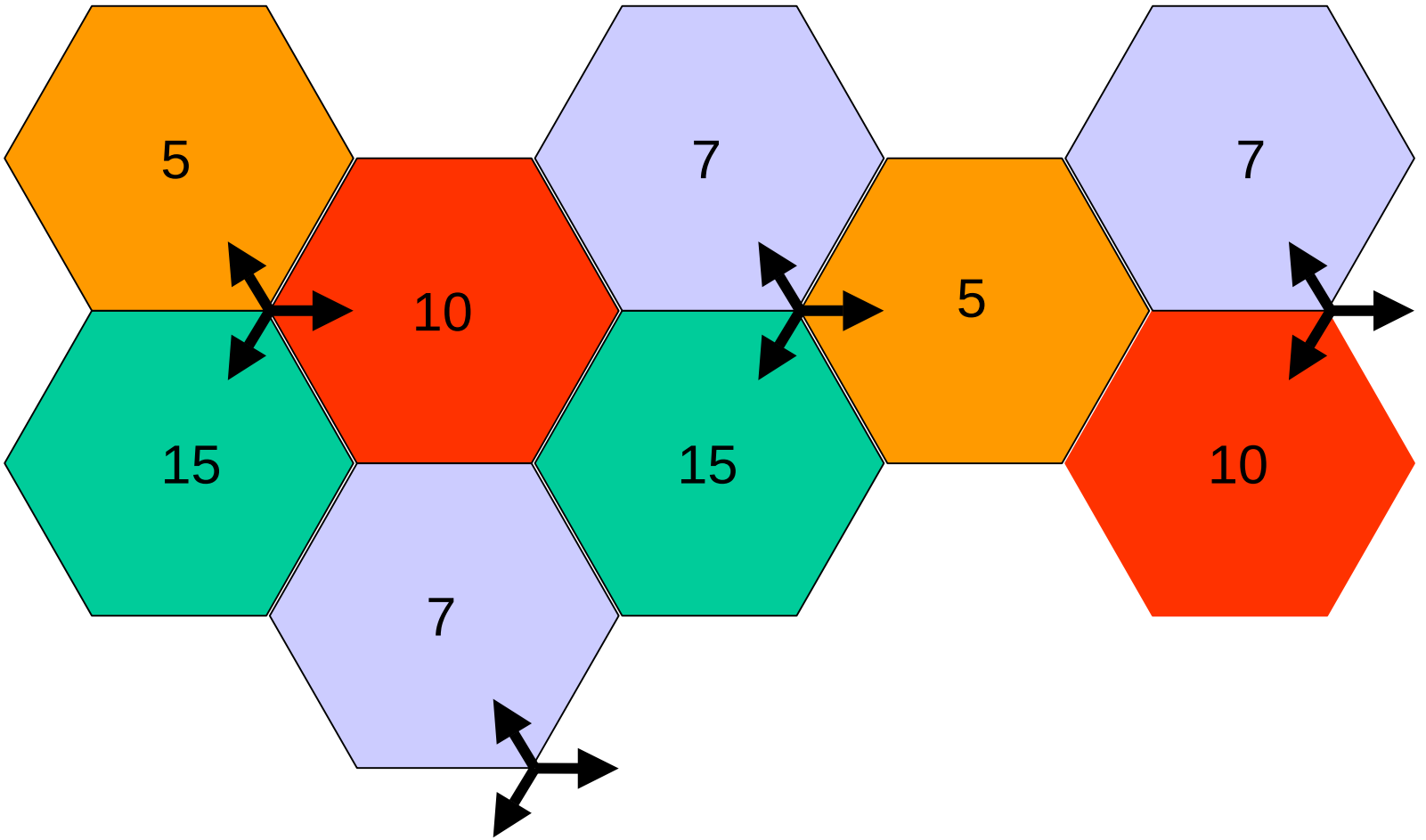


Trafic / Capacité (2/2)

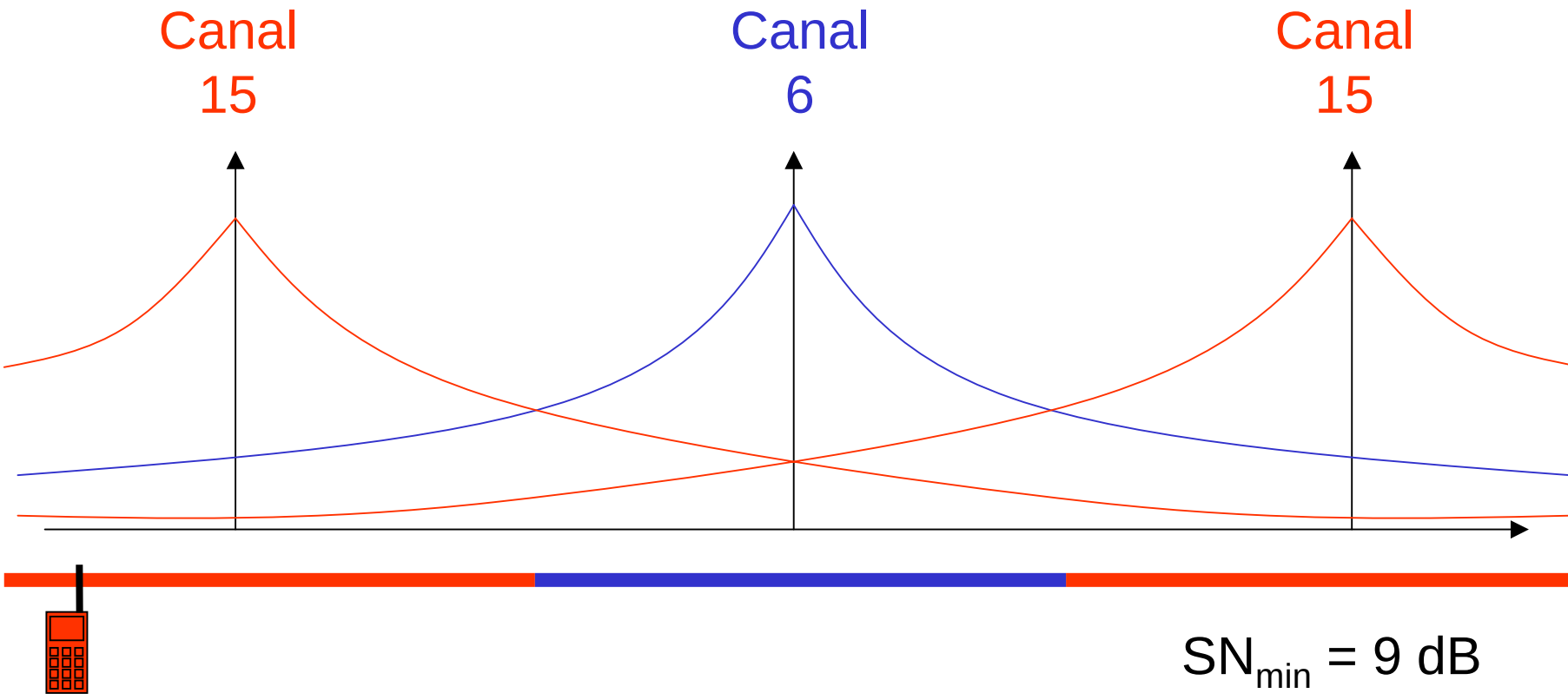


Canal 5	0	1	2	3	4	5	6	7
Canal 18	0	1	2	3	4	5	6	7

Réutilisation des fréquences

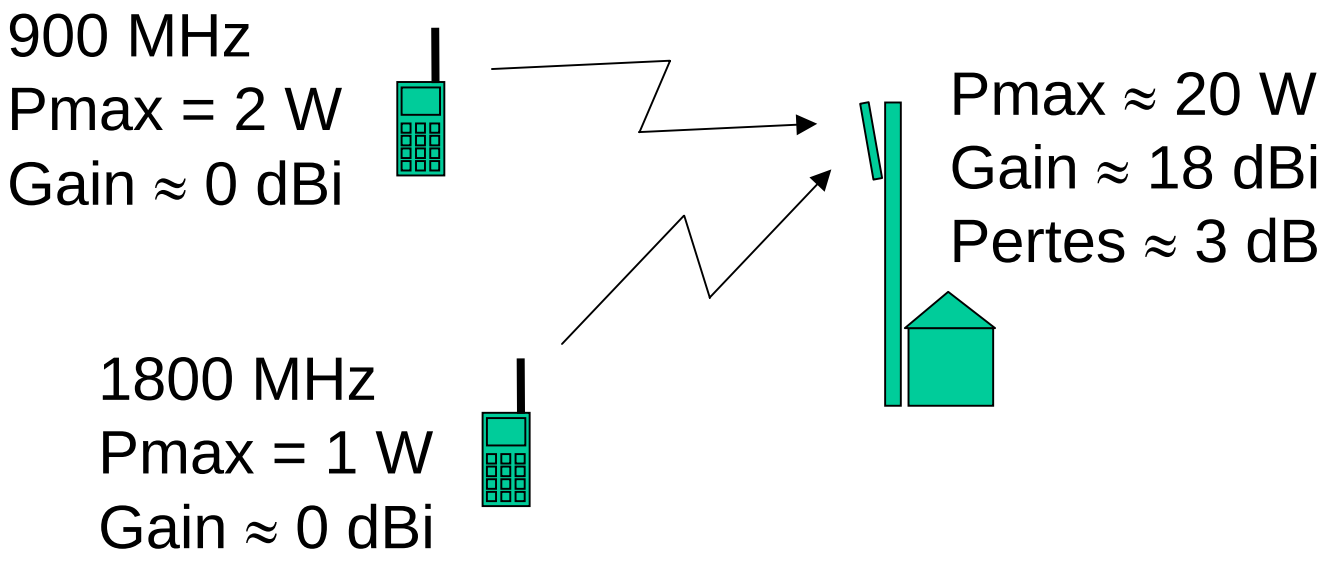


Réutilisation et interférences



SN_{min} = 9 dB

Puissance



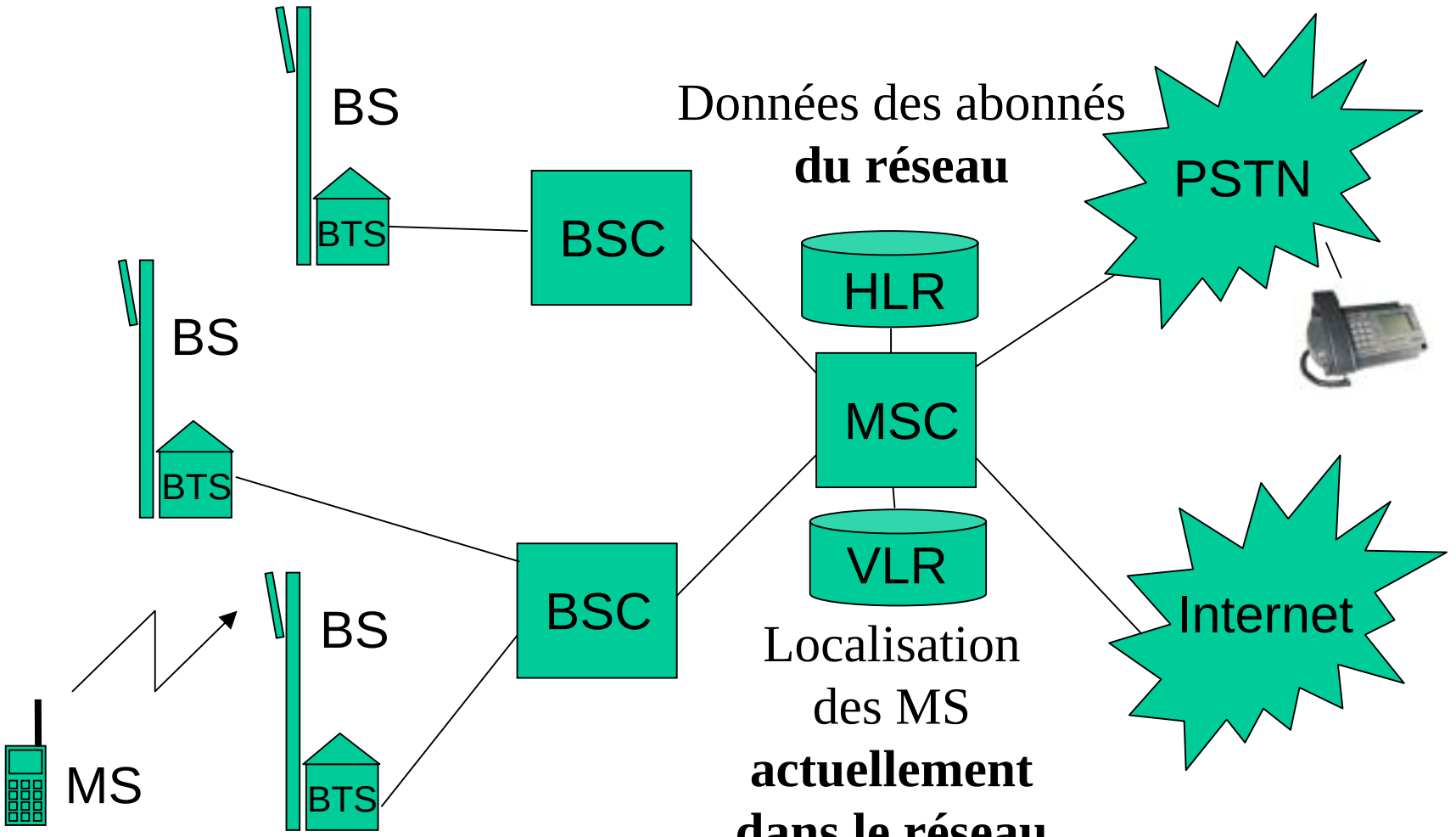
La puissance est variée continuellement par pas de 2 dB jusqu'à une réduction maximale de 20 dB (99%).

• Structure du réseau

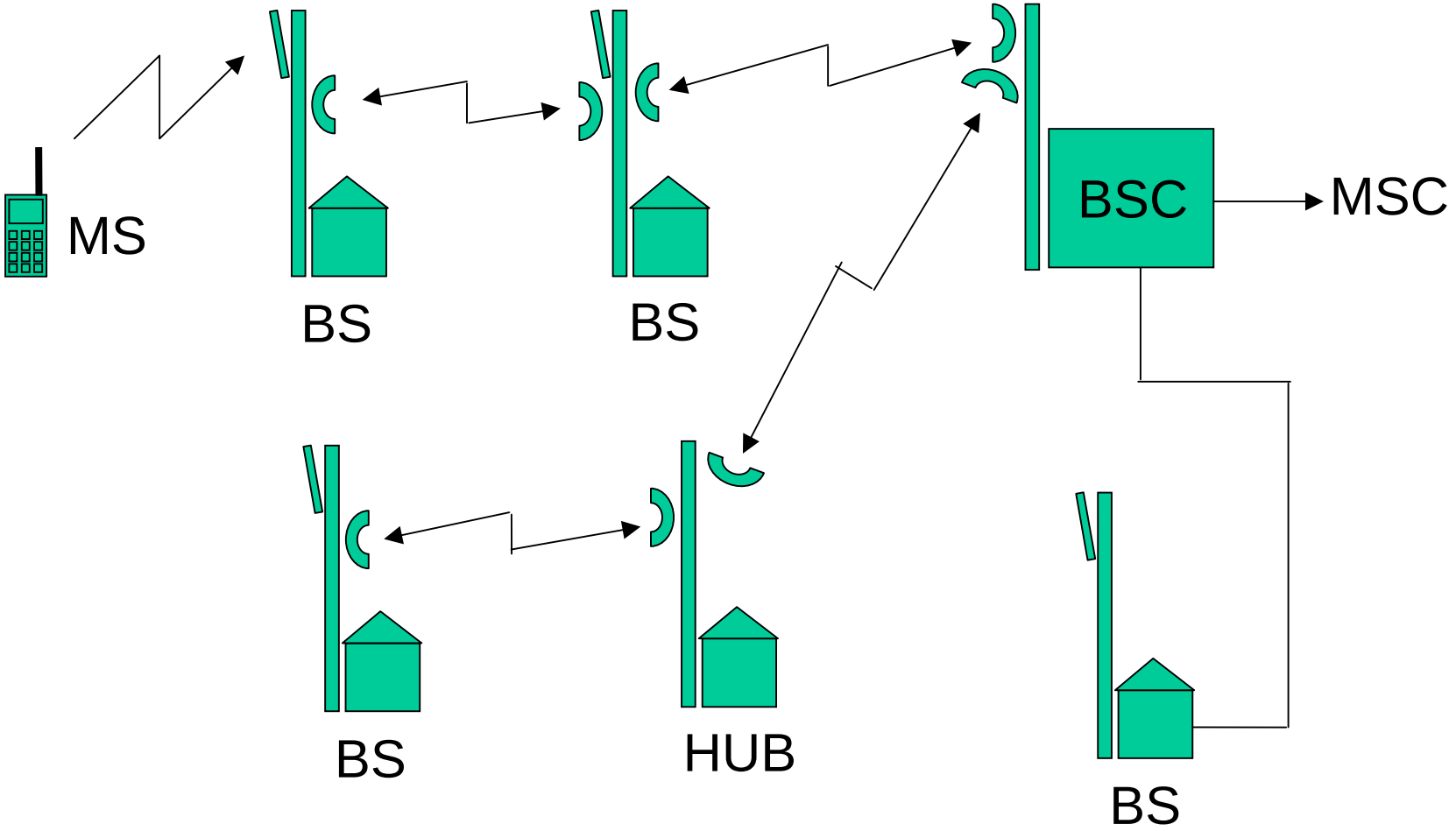
- Structure générale :

  Mobile**S**tation, **B**ase**S**tation**C**ontroller, **M**obile**S**witching**C**enter
  - **B**ase**T**ransceiver**S**tation
  - **H**ome**L**ocation**R**egister / **V**isitor**L**ocation**R**egister
  - **S**ubscriber**I**dendity**M**odule
- Structures terrestres :
  - Liaisons micro-ondes
  - Liaisons par lignes louées
  - Liaisons hertziennes

MS / BTS / BSC / MSC



Liaisons MW / LL



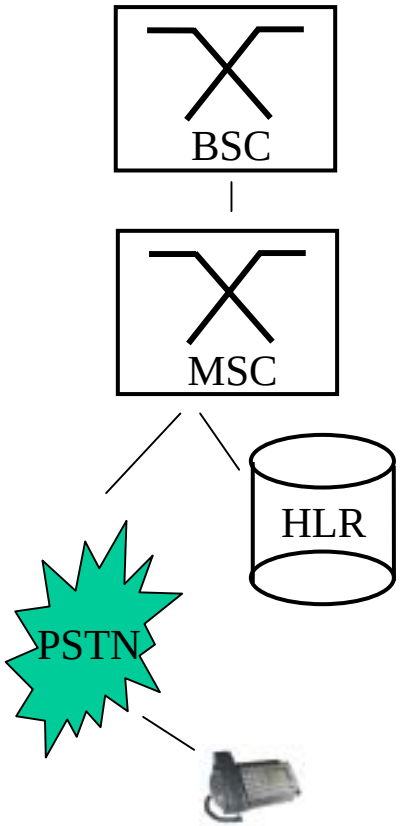
Liaisons par lignes louées

- Utilisation d’une ligne de cuivre HDSL.
- Débit de 2 Mbit/s = 12 x 8 timeslots.
- Qualité indépendante de la météo.
- Frais d’installation importants.
- Frais de location importants.

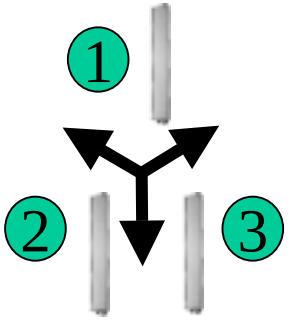
Liaisons hertziennes

- 15 GHz 30 km
- 23 GHz 10 km
- 38 GHz 2 km
- 58 GHz 500 m

MSC : Mobile Switching Center



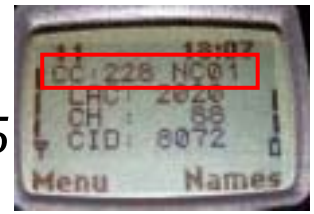
BTS : Base Station Subsystem

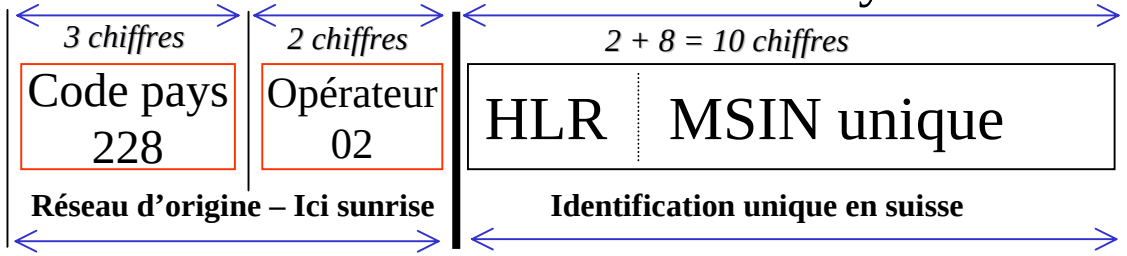


3 secteurs = minimum 3 antennes et
3 TRX (ensemble émetteurs récepteurs à 1 fréquence porteuse)

Terminal mobile (MS)

- Différentiation
  - « Numéro d'abonné »
    - Mobile Station ISDN number : *+41 7x 555 55 55*
  - « Identité du client mobile » : IMSI
    - **I**nternational **M**obile **S**ubscriber **I**dentity dans la SIM





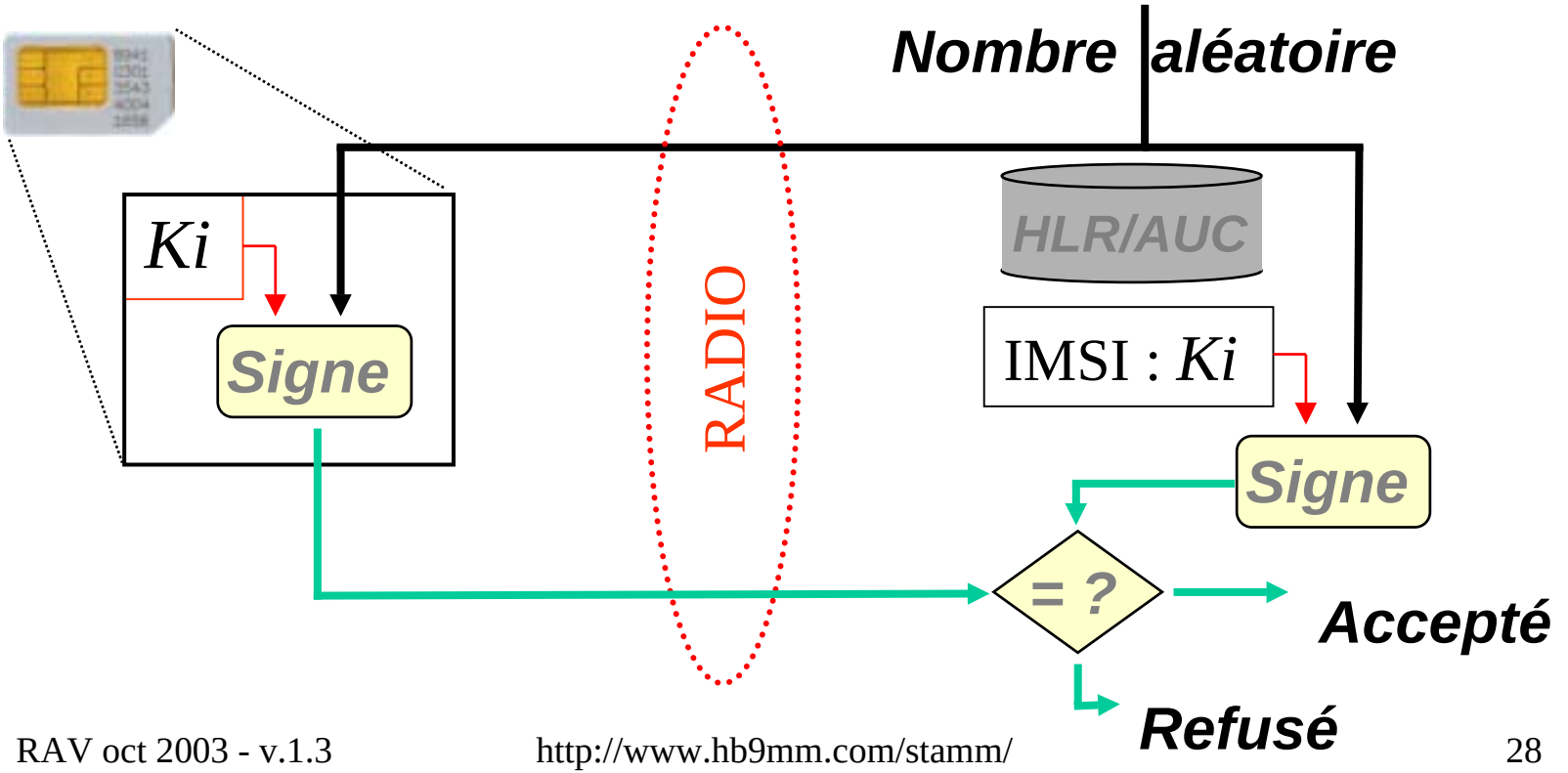
  - « Numéro de série du terminal mobile » : IMEI
    - **I**nternational **M**obile **E**quipement **I**dentity dans le terminal mobile (± modifiable)

Carte SIM et sécurité

- La SIM est un mini-ordinateur, capable de stocker des données, et de faire des calculs
- Possède un compteur interne et un premier niveau de protection, le PIN
- La carte SIM et la base de donnée d'abonné du réseau **d'origine** (HLR) partage un algorithme de cryptage secret *Ki*
- Cette clé n'est jamais transmise par radio, et il est « impossible » d'y accéder dans la SIM

Authentification de l'abonné

- A chaque accès au réseau, génération d'un nombre aléatoire et signature par la SIM



Chiffrement et sécurité

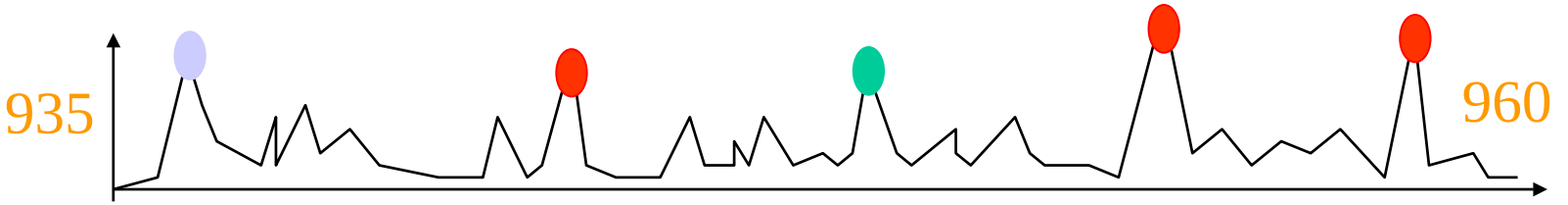
- Seul le premier lien radio est crypté
- Utilisation d'identité temporaire TMSI
- Algorithme de chiffrement et de signature choisit par l'opérateur
- Certain réseau ont été vendu avec une faible protection (A5/2)
- Station de base « pirates »
- Clonage de carte SIM possible par cryptanalyse (COMP128 v.1)

• Fonctionnement

- Initialisation du terminal
- Appels entrants et sortants
- SMS et roaming
- Mobilité en cours d’appel ; Hand-overs
- Localisation (précision)
- Gestion de la puissance et qualité
- Codage de la voix

Initialisation du terminal

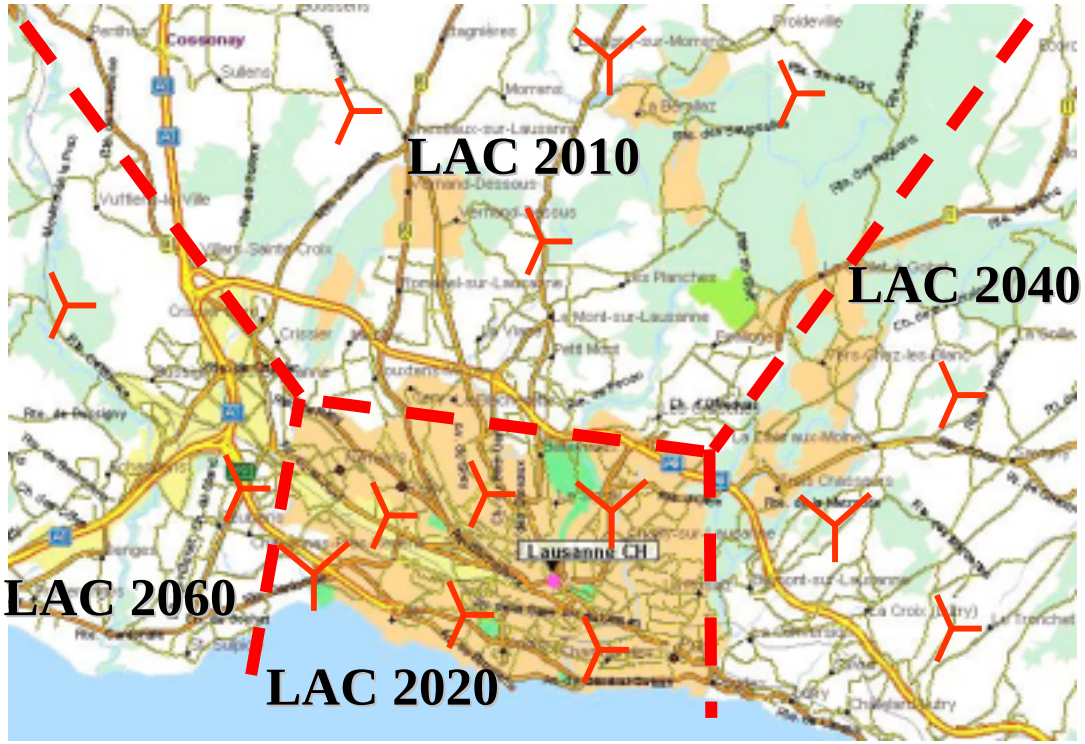
- Scanne les fréquences disponibles

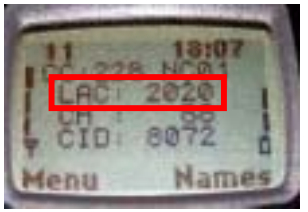


- Mémorise les 30 plus forts signaux, se synchronise et analyse le code du réseau
- Stocké dans la SIM pour un redémarrage plus rapide
- Averti le réseau : IMSI attach / detach

Location update

- Un groupe de BTS définissent une région ; la LAC, transmise dans la signalisation



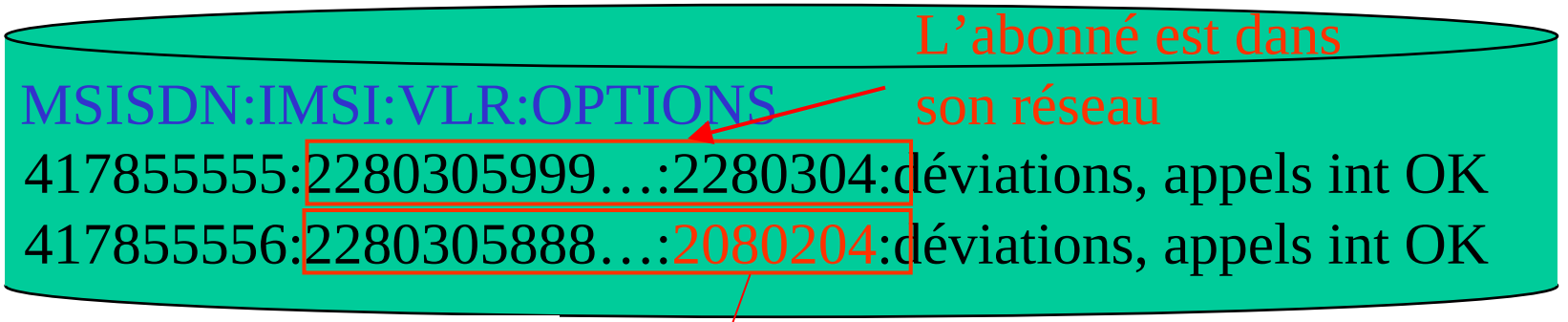


• Mise à jours périodique selon l'opérateur (timer)

Mise à jours du HLR et VLR

- Mémorise les caractéristiques d'un abonné

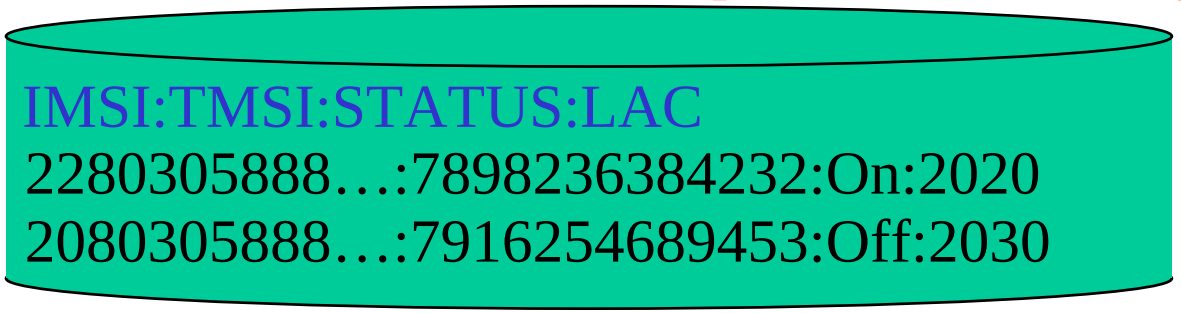
Base de donnée des abonnés « locaux » : HLR 05 réseau orange



Signalisation SS7

Base de donnée localisation : VLR 04 du réseau 208 03 (Bouygues)

L'abonné visite un réseau partenaire (roaming)



Mémorise la position de l'abonné

Appels entrants

MSISDN

+41 7x 555 55 55

MSC

HLR/VLR

IMSI/TMSI et LAC

BSC

LAC

- Paging dans le LAC
- Écoute la meilleure cellule
- Répond en faisant un accès aléatoire
- Allocation du canal, authentification
- Chiffrement

Roaming

- Le réseau d'origine ne connaît plus la position du mobile, mais la base de localisation (VLR) à laquel l'appel doit être acheminé
- Échange d'un certain nombre de couple <défi-réponse> pour l'authentification
- Ensuite, plus de contact avec le réseau d'origine pour un certain temps
- Échange d'informations de facturation environ tous les jours

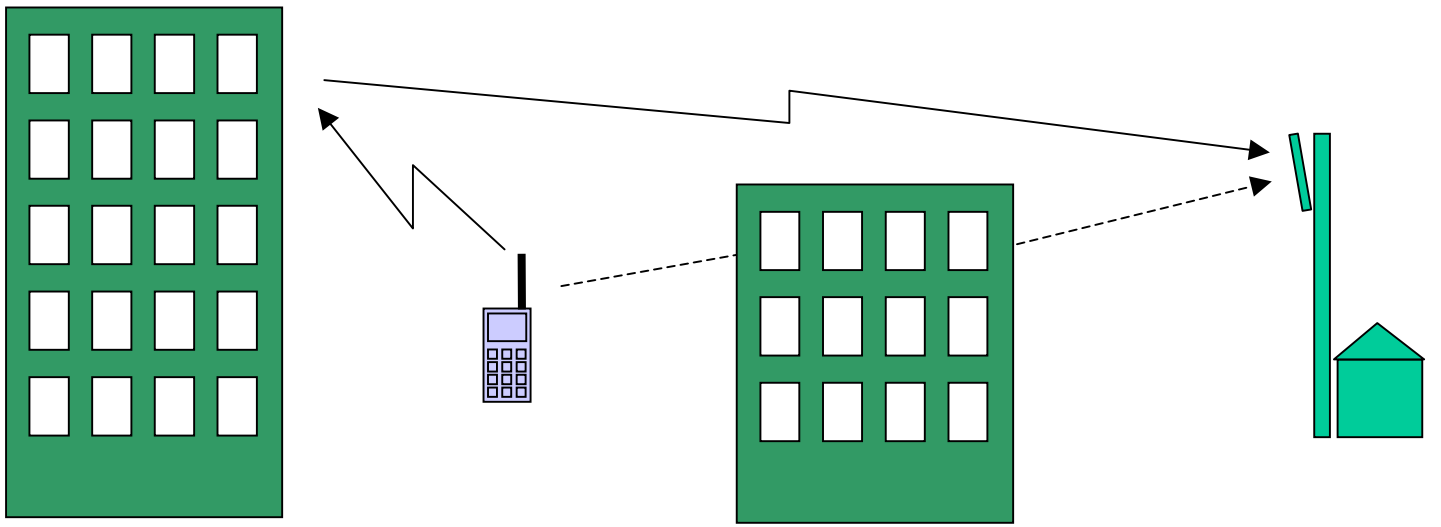
Appels sortants

- Se cale sur la cellule la plus forte
- Accès aléatoire sur slot de signalisation
- Échange d'information sur l'appel
- Assignement d'un canal dédié
- Authentification et chiffrement
- Théoriquement, vérification de l'IMEI (*#06#) pour bloquer les terminaux volés
- Conversation

Handover

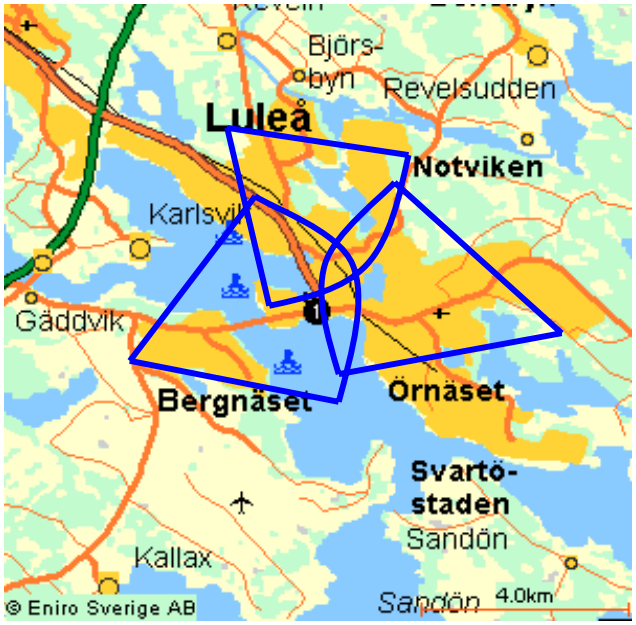
- La BTS active envoie une liste de cellules adjacente à « surveiller »
- La MS renvoie les mesures de la puissance du signal reçue pour les voisines
- Le BSC décide d'un handover – Changement de cellules

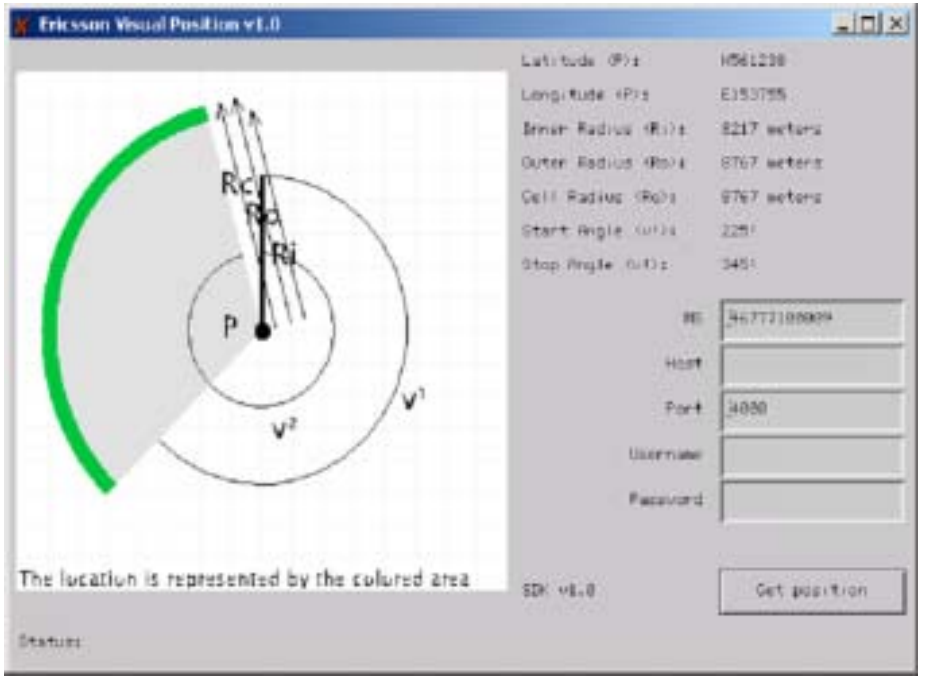
Distance électrique



Positionnement

- En tout temps, l’opérateur connaît le LAC
- En cas d’appels, la cellule et les voisines
- Moyennant quelques calculs, précision 550 m





Gestion de la puissance

- Mesure la qualité de la liaison en permanence – Adapte la puissance
- DTX
- Confort noise

- Raison des interférences sur les appareils fort au début, intermittent, et faible ensuite

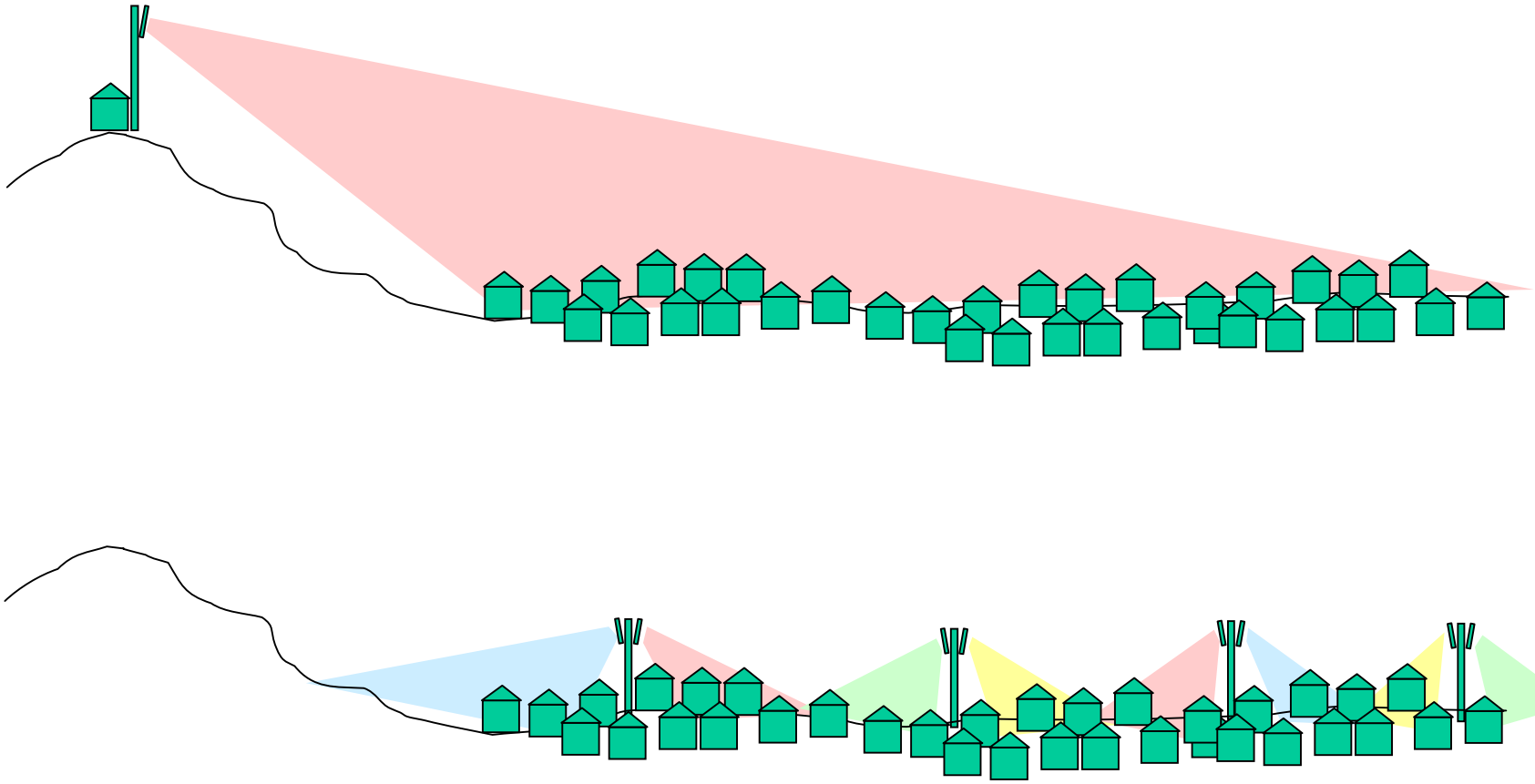
SMS

- Comme lors d'un appel, le destinataire/émetteur est authentifiée (GSM)
- Lors que le message vient d'un autre réseau, pas de contrôle du champs « De »
- Passerelles internet -> SMS avec possibilité de modifier le champs « De »

• Déploiement et maintenance

- Antennes
- Couverture
- Drive tests
- Trafic
- Télésurveillance

Choix des sites

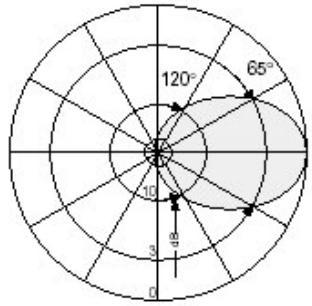


Antennes

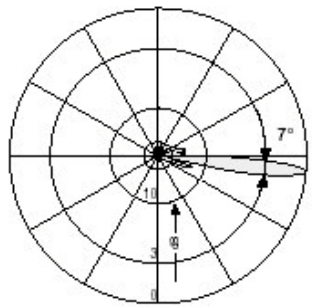
XPol F-Panel 1710–1990 65° 18dBi 6°T

Type No.	739 496
Frequency range	1710 – 1990 MHz
Polarization	+45°, –45°
Gain	2 x 18 dBi
Half-power beam width Copolar +45°/–45°	Horizontal: 65° Vertical: 7°
Electrical tilt	6°, fixed
Sidelobe suppression for first sidelobe above horizon	≥ 14 dB
Front-to-back ratio, copolar	> 30 dB
Isolation, between ports	> 30 dB
Impedance	50 Ω
VSWR	< 1.4 (1710 – 1880 MHz) < 1.5 (1880 – 1990 MHz)
Intermodulation IM3 (2 x 43 dBm carrier)	< –150 dBc
Max. power per input	200 Watt (at 50 °C ambient temperature)
Input	2 x 7-16 female
Connector position	Bottom
Weight	6 kg
Wind load (at 150 km/h)	Frontal / Lateral / Rearside: 310 N / 110 N / 250 N
Max. wind velocity	200 km/h
Height/width/depth	1302 / 155 / 49 mm

Mounting accessories are not included in the scope of delivery (see page 165 – 175)



Horizontal Pattern



Vertical Pattern

– 6° electrical downtilt
– first null-fill below horizon better or equal –25 dB below maximum gain

Couverture

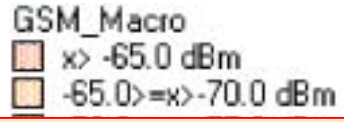
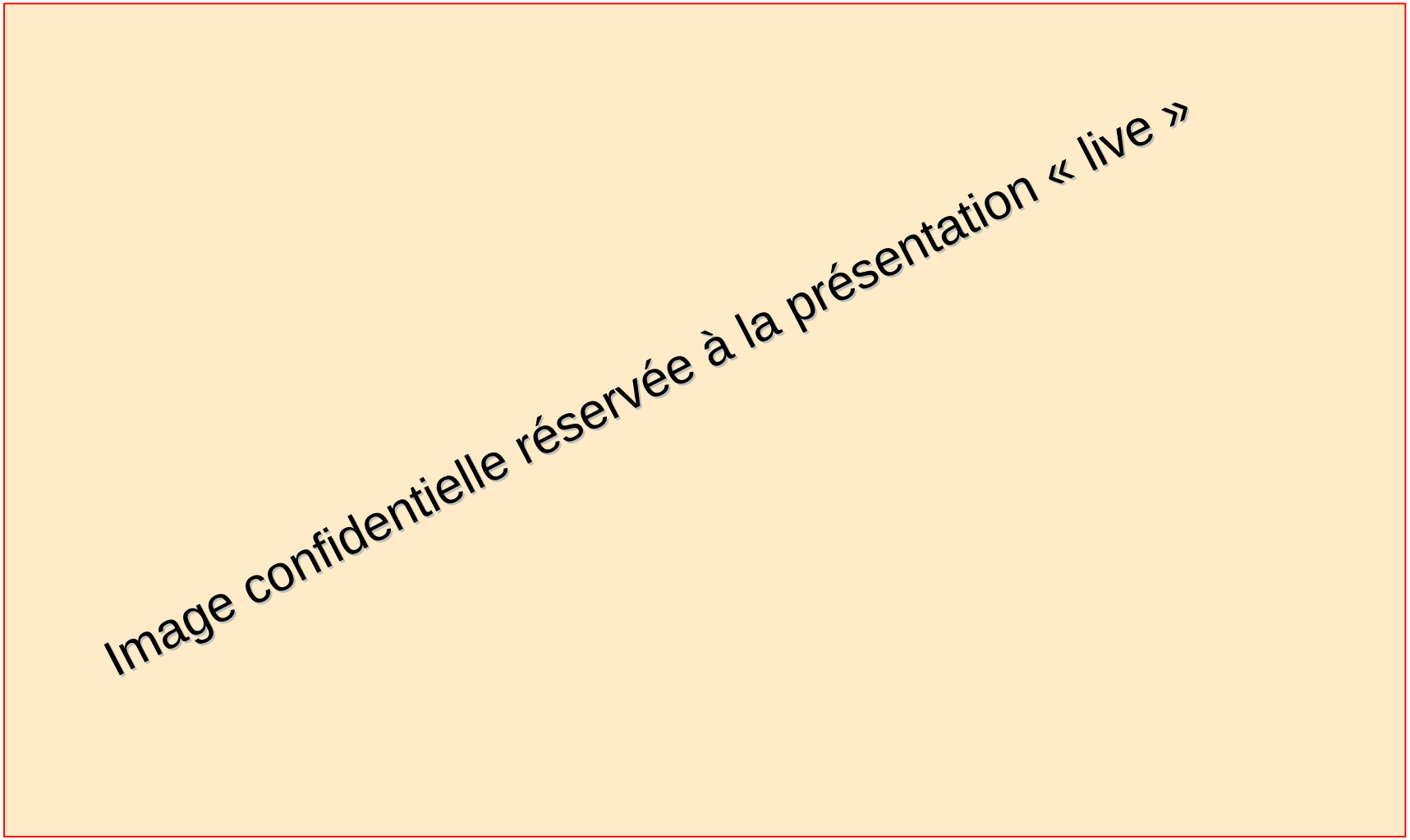


Image confidentielle réservée à la présentation « live »

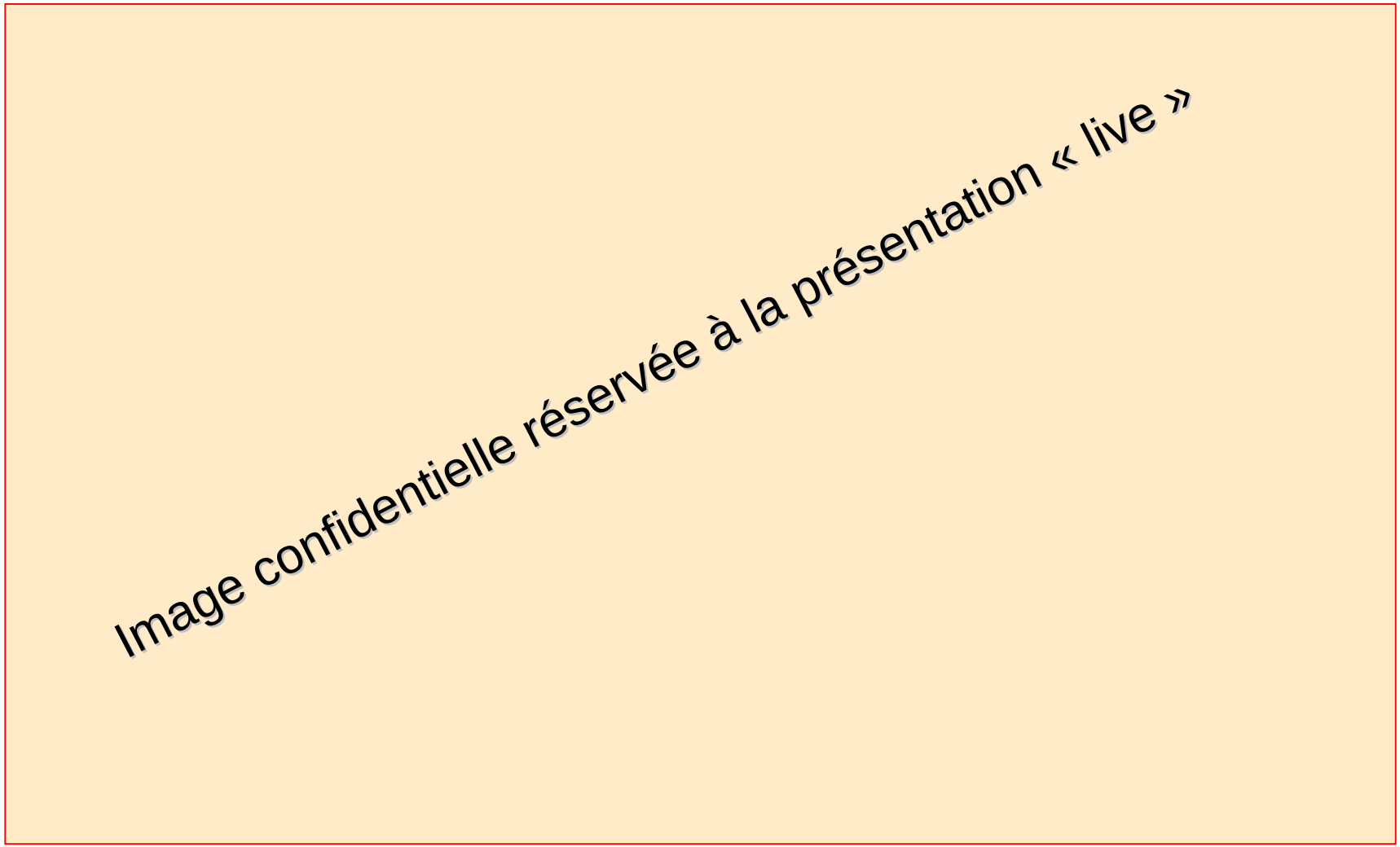
Drive tests

Image confidentielle réservée à la présentation « live »

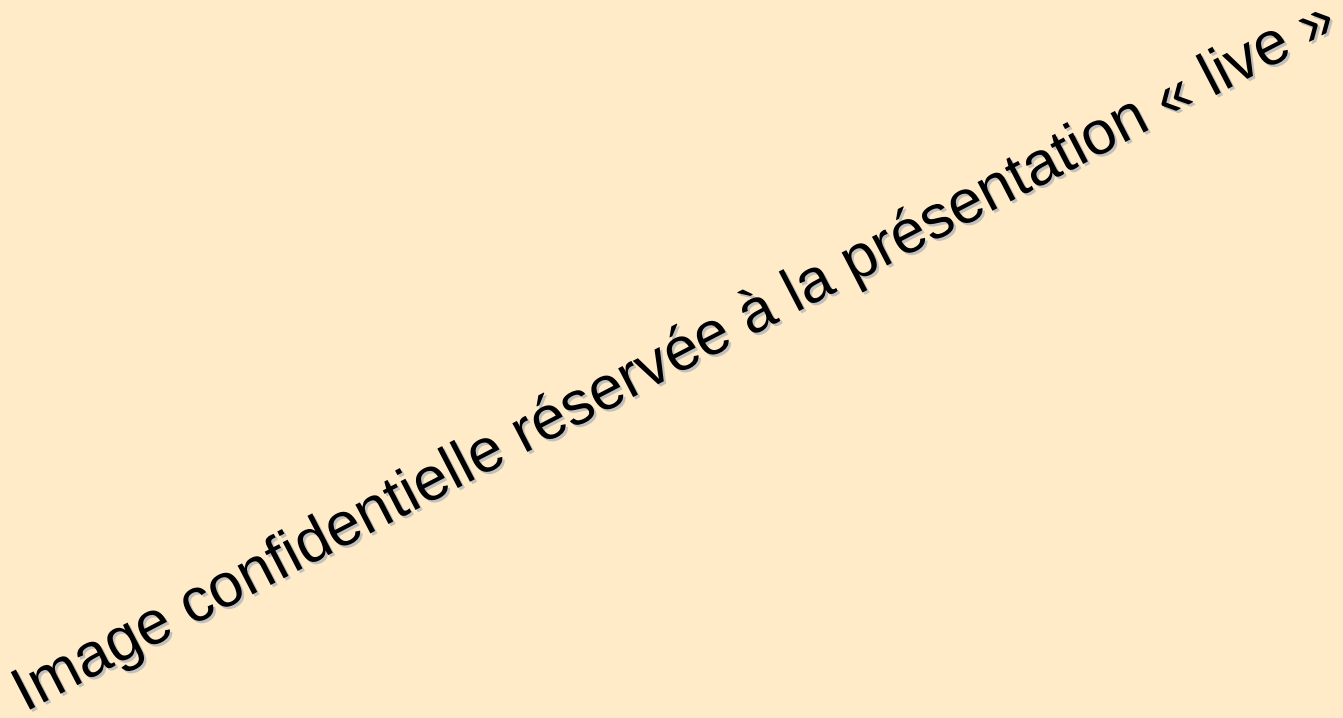
Trafic



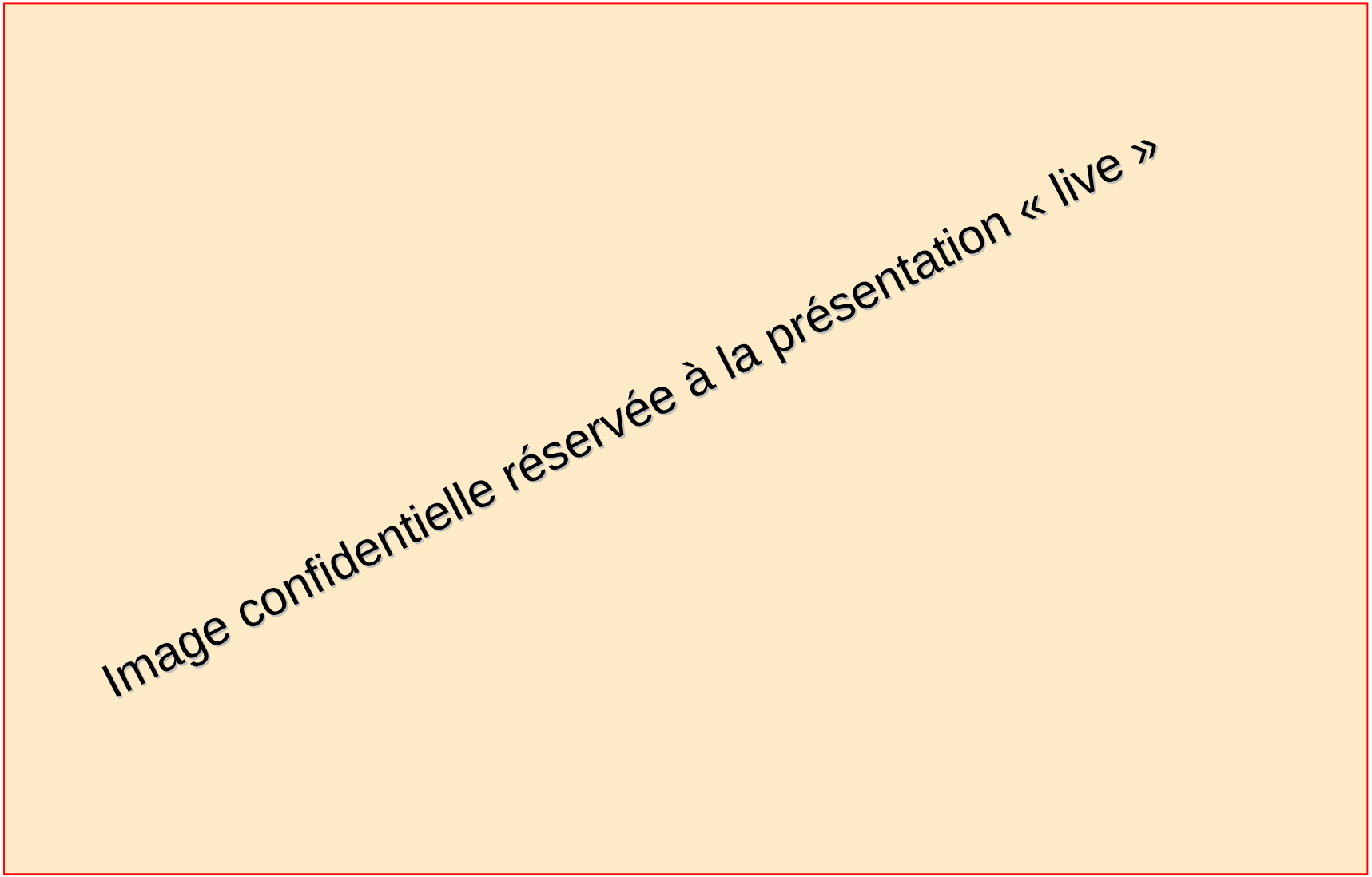
Télésurveillance



Outils logiciels



Suite…



6. Avenir du réseau

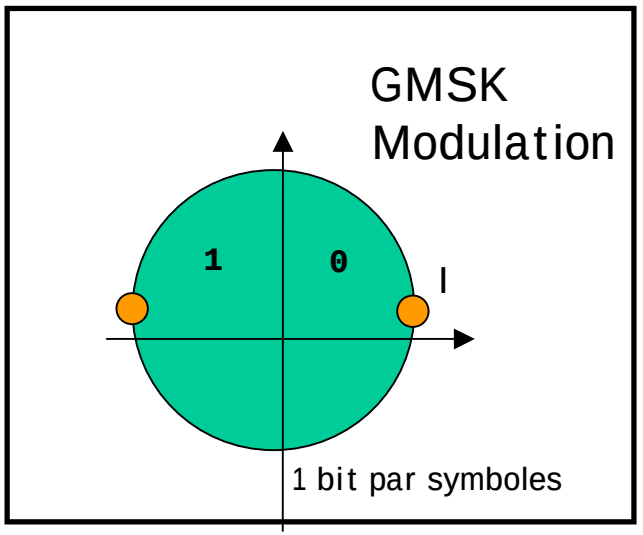
- GPRS et MMS
- EDGE : Schéma modulation
- UMTS : 3GPP et recherche de « l’application qui tue »

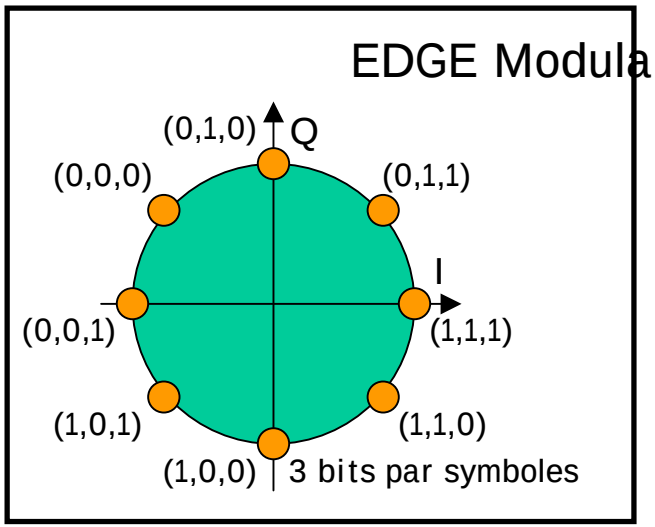
GPRS

- Échange de données en mode paquets
- Facturé au débit - MMS
- 1 timeslot partagé par plusieurs utilisateurs
- Sur les 7 timeslot d’un TRX, certains sont alloués au GPRS, mais la voix à toujours la priorité
- Utilise la capacité libre

EDGE

- En projet, nécessite le remplacement des émetteurs-récepteurs et terminaux
- Compatible avec le reste des équipements





UMTS

- Fédèrent les différents systèmes existants
- WCDMA : Modulation comme le GPS
- Large bande
- Départ difficile
- Premier réseau commercial mars 2003
- Les opérateurs sont devenus frileux
- Cherchent « l’application qui tue »

7. Conclusions

- Amélioration de la présentation
- Stamm de « rattrapage » prévu en juin + GE
- Projet de dossier papier
- Autre sujets prévus :
  - Présentation GPS (déjà présenté par Yves)
  - Wireless LAN 802.11b
  - UMTS
  - Les radioamateurs, projet d'électronique, modulation, … Le votre ici!

Références et Remerciements

- Réseaux GSM, Xavier Lagrange, Philippe Godlewski et Sami Tabbane, éd. Hermes.
- Merci à Didier HB9DUC et nos collègues radioamateurs pour leur aide précieuse!
- Merci aussi aux autres, après tout ☺
- Version papier = expurgée des illustrations trop confidentiels

Réponses aux questions

- Site web des RadioAmateurs Vaudois : http://www.hb9mm.com/
- Emanuel Corthay HB9IJI – hb9iji@sked.ch
- Iacopo Giangrandi HB9DUL – hb9dul@giangrandi.ch
- Didier Divorne HB9DUC – hb9duc@allo.ch
- Comparatif des opérateurs suisses par Didier: http://www.allo.ch/
- Possibilité de nous inviter pour faire la présentation chez vous ☺

Copyright

Architecture réseau GSM