Principi Generali delle Reti Cellulari

- **Introduzione**
- **Cenni evolutivi**
- **Mercato**
- **Fondamenti**

Renato Lo Cigno
www.dit.unitn.it/locigno/didattica/wn/

...Copyright

Quest'opera è protetta dalla licenza *Creative Commons NoDerivs-NonCommercial*. Per vedere una copia di questa licenza, consultare:
http://creativecommons.org/licenses/nd-nc/1.0/
oppure inviare una lettera a:
Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.

This work is licensed under the *Creative Commons NoDerivs-NonCommercial* License. To view a copy of this license, visit:
http://creativecommons.org/licenses/nd-nc/1.0/
or send a letter to
Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.



Cenni storici - 1

- La propagazione nello spazio libero è usata da quasi 100 anni per le telecomunicazioni
- I primi (rudimentali) sistemi di telecomunicazione non diffusiva con mezzi mobili appaiono durante la seconda guerra mondiale
- I primi sistemi di telefonia mobile risalgono agli anni '60, ma sono costosi, poco pratici, con bassa qualità e bassa affidabilità



Cenni storici - 2

- Nei primi anni '80 vengono installate le prime reti cellulari nel senso "moderno" del termine (1983 Chicago, 1980/2 prototipazione in Giappone)
  - reti "specializzate" (es. private di una organizzazione)
  - piuttosto costose
  - bassa capacità e versatilità
- Nella seconda metà degli anni '80 vengono installate le reti analogiche "avanzate" (AMPS, NMT, TACS) con immediato ed enorme successo commerciale



Cenni storici - 3

- **AMPS**: *Advanced Mobile Phone Service*
  - è uno standard U.S.A. (EIA-553); lavora nella banda intorno agli 800 MHz
  - **diffusione**: Stati Uniti, Canada, Messico, Australia, Nuova Zelanda, Taiwan, Corea del sud, Singapore, Hong Kong, Thailandia, Brasile, Argentina, ...
- **TACS**: *Total Access Communications System*
  - è uno standard sviluppato nel Regno Unito; lavora nella banda intorno ai 900 MHz, di fatto è un adattamento dello standard AMPS
  - **diffusione**: U.K., **Italia**, Irlanda, Spagna, Austria, Penisola Arabica, ...



Cenni storici - 4

- **NMT**: *Northern Mobile Telephone System*
  - è uno standard scandinavo, sviluppato senza relazioni con AMPS e TACS; lavora nelle bande intorno ai 450 e ai 900 MHz; ci sono notevoli differenze nel funzionamento tra le 2 bande
  - **diffusione**: Scandinavia, BeNeLux, Austria, Francia, Ungheria, Spagna, Svizzera, ...



Cenni storici - 5

- Alla fine degli anni '80 è diventato chiaro che le reti cellulari esistenti non erano in grado di sopportare la domanda di traffico e qualità a meno di:
  1. risolvere i problemi di bassa capacità a causa dell'indisponibilità dello spettro
  2. migliorare in modo significativo la qualità del servizio e la gamma dei servizi disponibili
  3. diminuire drasticamente i costi delle apparecchiature
  4. risolvere i problemi di interoperabilità tra sistemi diversi



Cenni storici - 6

- I 4 problemi da risolvere hanno spinto verso soluzioni di tipo *concertato* (standard internazionali) con tecnologia *numerica* (GSM, D-AMPS, IS-95)



Cenni storici - 7

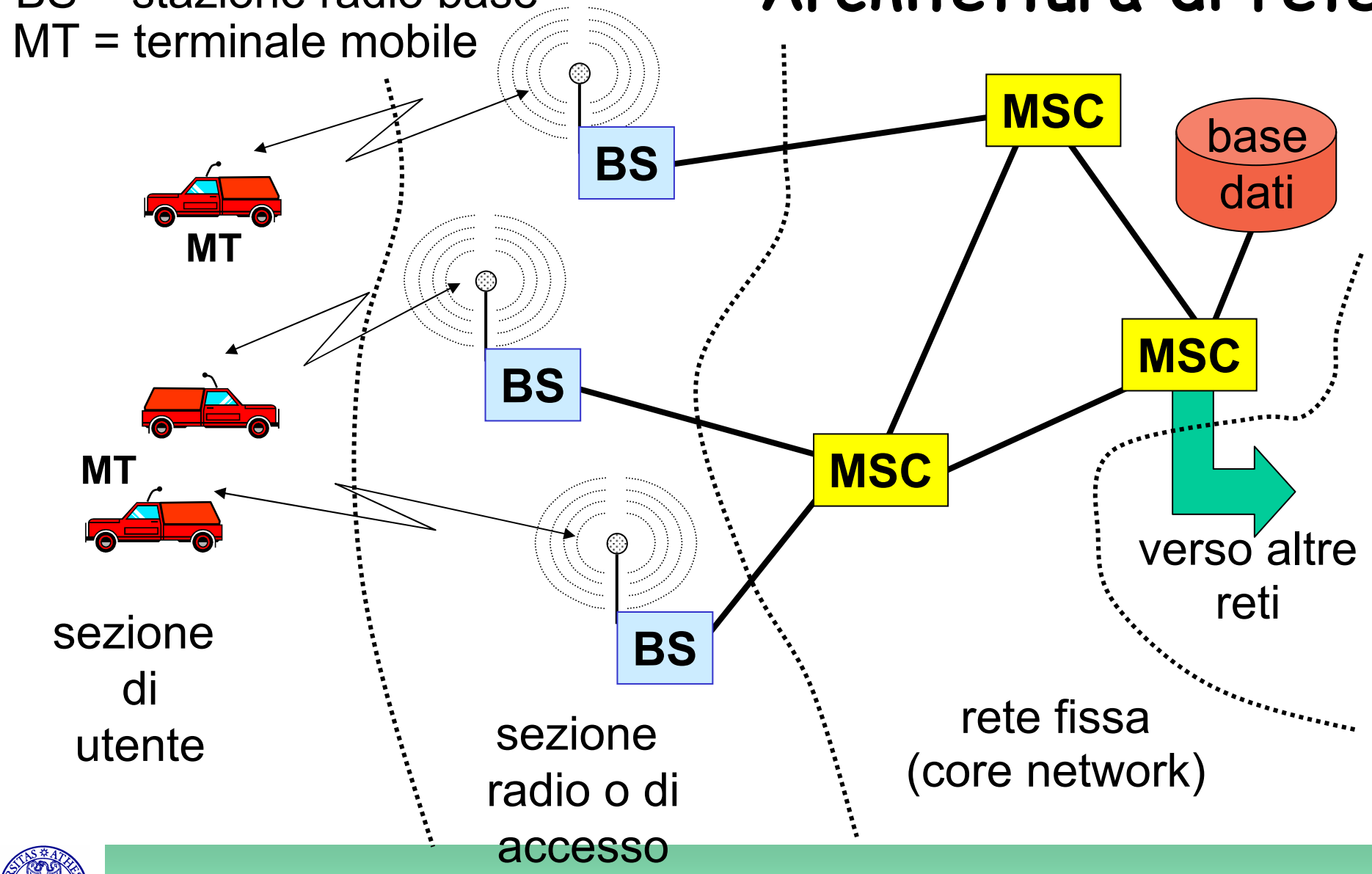
- Nel '92 e` stato introdotto GSM in Europa con un successo ed una diffusione enorme
- D-AMPS e IS-95 (CDMA) sono introdotte in USA nella meta` degli anni '90 con grande successo (meno del GSM)
- Fine anni '90 standardizzazione di reti con accesso a pacchetto
- ... oggi (o domani??) ... UMTS/IMT2000



Principi delle reti cellulari

Architettura di rete

MSC = commutatore
BS = stazione radio base
MT = terminale mobile



Gestione della mobilità

- Il supporto alla mobilità è di fatto l'elemento distintivo tra le reti cellulari ed ogni altro tipo di rete TLC
- Sono necessarie alcune procedure
  - Roaming
  - Location updating
  - Paging
  - Handover



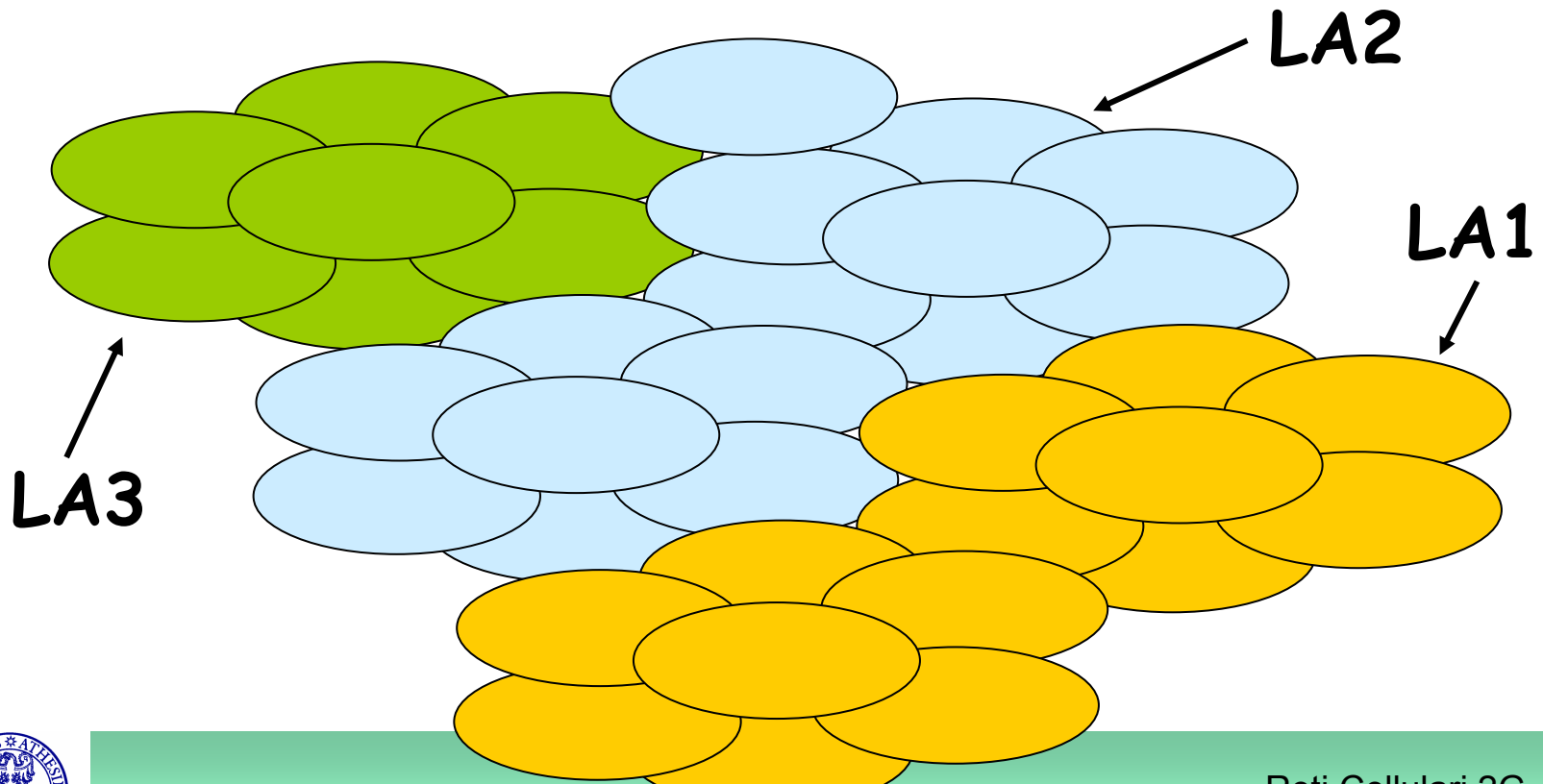
Roaming

- È la possibilità data all'utente di essere rintracciabile anche se si sposta all'interno della rete
- Il sistema deve memorizzare in una base di dati la posizione degli utenti per poterli rintracciare
- Per memorizzare la posizione dell'utente si divide il territorio in aree dette *location area* (LA) che sono insiemi di celle



Roaming

- Ogni location area ha un identificativo numerico, il *location area identifier* (LAI)





Location Update

- È la procedura con cui avviene l'aggiornamento della posizione dell'utente
- In ogni LA viene diffuso il LAI su un canale di controllo
- Il terminale mobile che riceve un LAI diverso da quello precedentemente memorizzato richiede al sistema una procedura di *location update* (aggiornamento della base di dati di localizzazione)



Paging

- È la procedura con cui il sistema avvisa un terminale mobile di una chiamata in arrivo
- Il sistema invia un messaggio di paging (in broadcast) all'interno della LA in cui è localizzato l'utente



Handover

- È la procedura che consente il trasferimento di una chiamata attiva da una cella alla successiva, mentre il terminale mobile si sposta all'interno della rete
- È una operazione complessa che pone alla rete notevoli requisiti in termini di architettura di rete, di protocolli e di segnalazione per la gestione delle procedure connesse agli handover



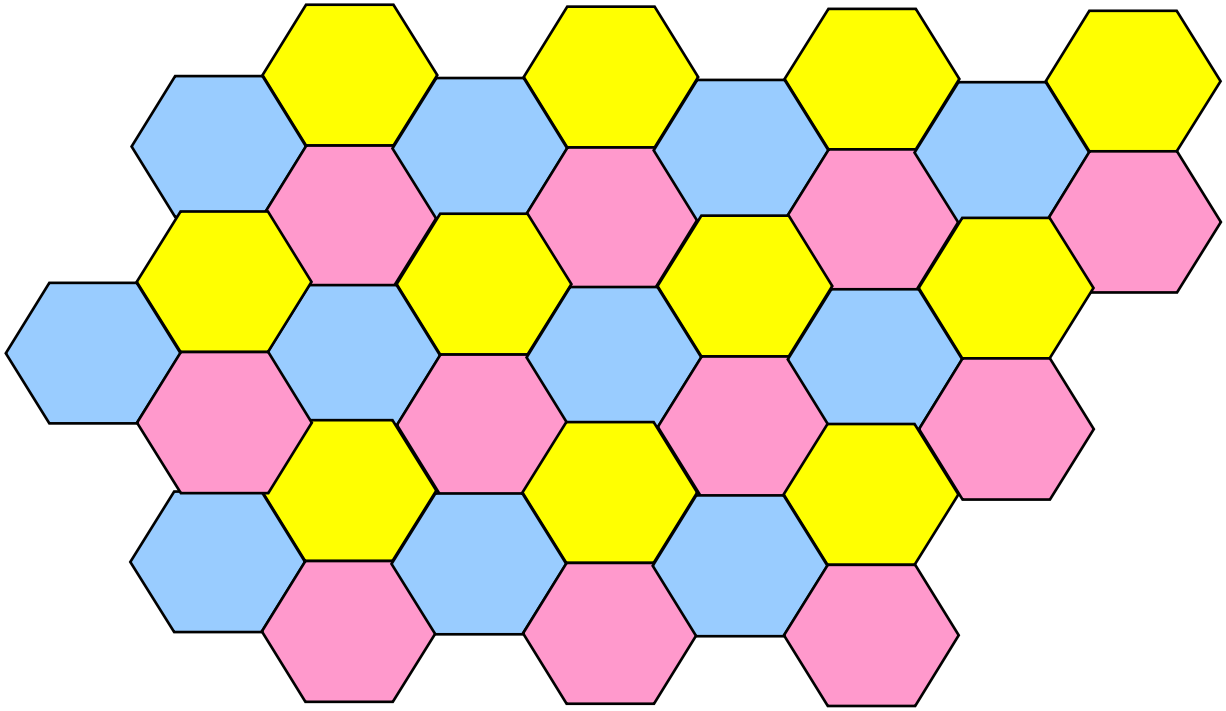
Altre funzioni: la registrazione

- E' la funzione di
  - collegamento del terminale alla rete
  - identificazione, autenticazione
- Procedura da eseguire:
  - all'accensione del terminale
  - tutte le volte che si desidera accedere ad un nuovo servizio (es. fare una nuova chiamata) con fini di autenticazione
  - serve ad associare MT alla rete



La copertura cellulare

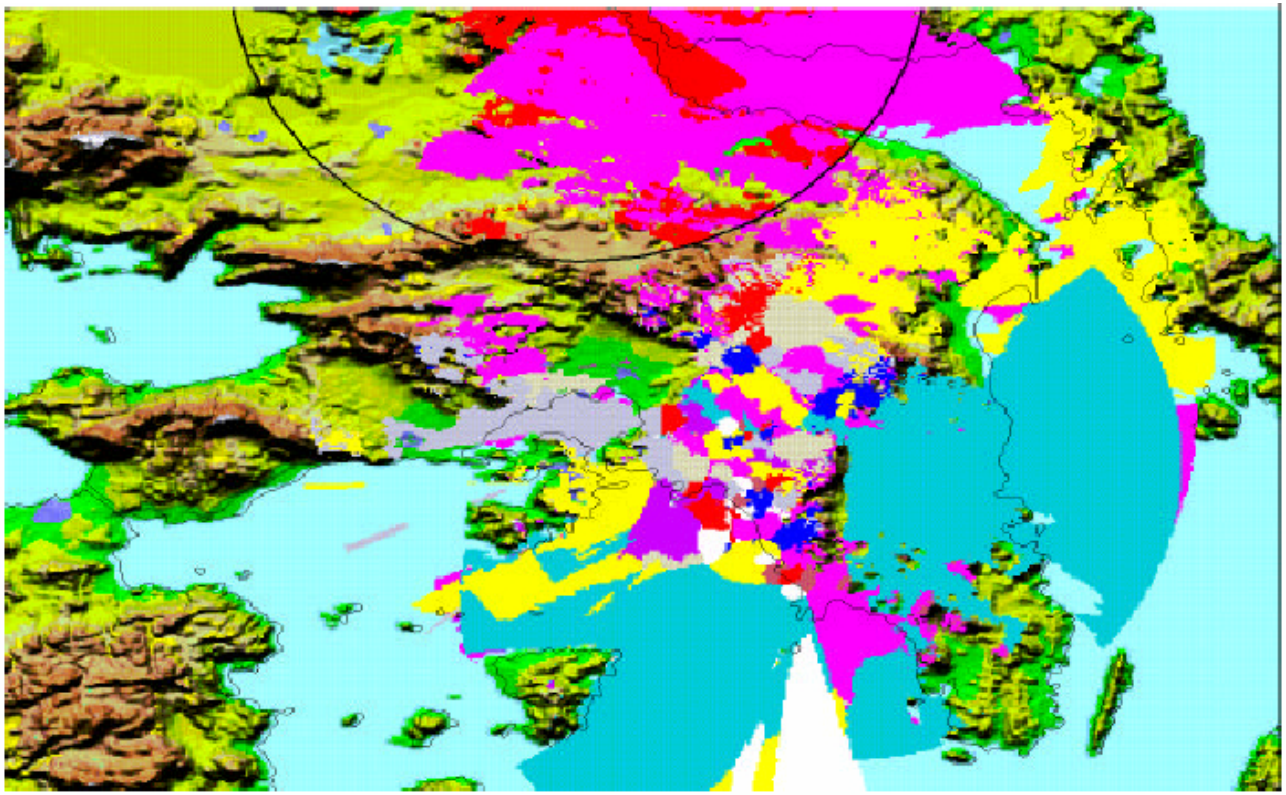
La copertura cellulare teorica



Costituita da aree esagonali regolari



La copertura cellulare reale



Le Celle

- Le celle non sono regolari (esagoni) e delle stesse dimensioni
- Forma e dimensione della cella sono determinate dalla
  - Potenza delle antenne
  - Guadagno di antenna
  - Morfologia del territorio
- Per definire la copertura cellulare si usano *modelli di propagazione* basati su mappe del territorio rilevate via satellite



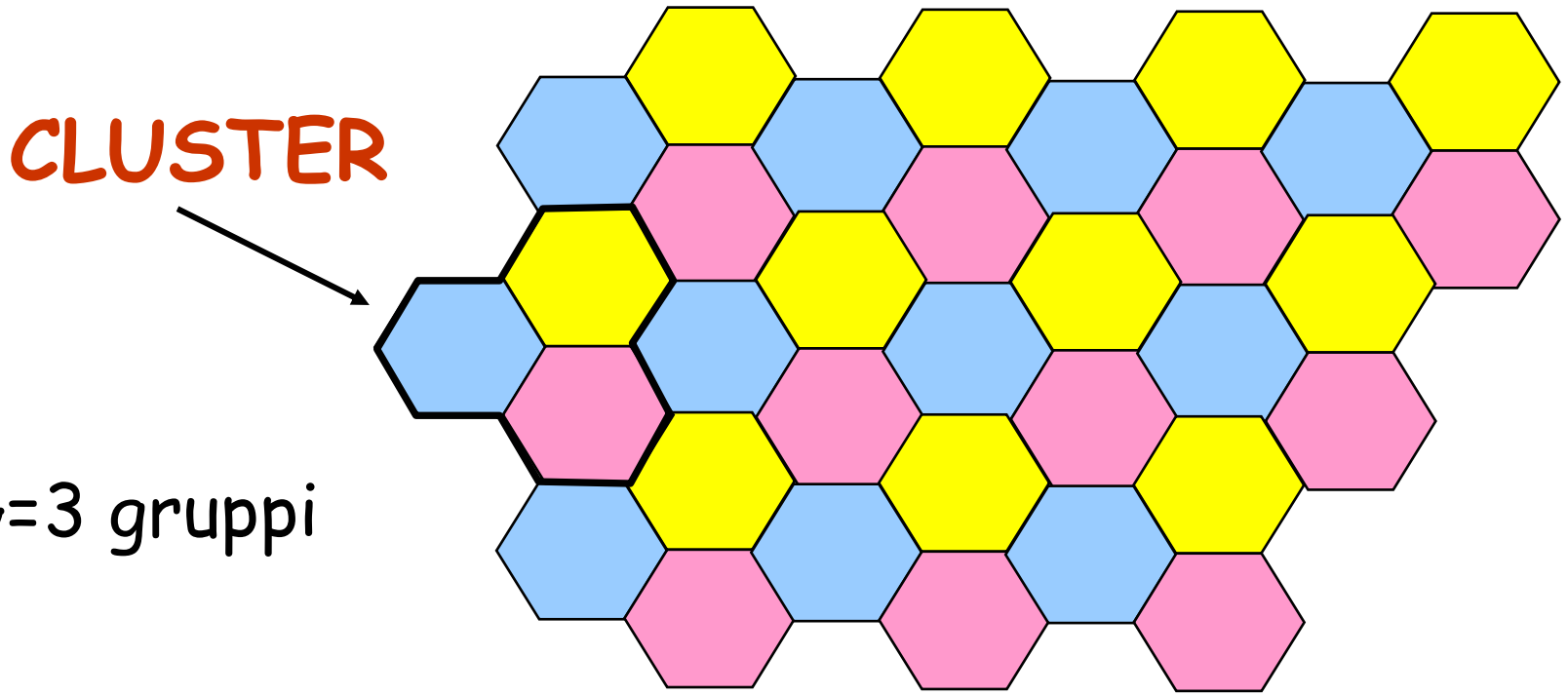
Riutilizzo delle frequenze

- Con un limitato numero di risorse radio si vogliono conseguire i seguenti obiettivi
  - Assicurare la copertura del territorio
  - Servire un elevato numero di utenti

Usare le stesse risorse in punti geografici diversi



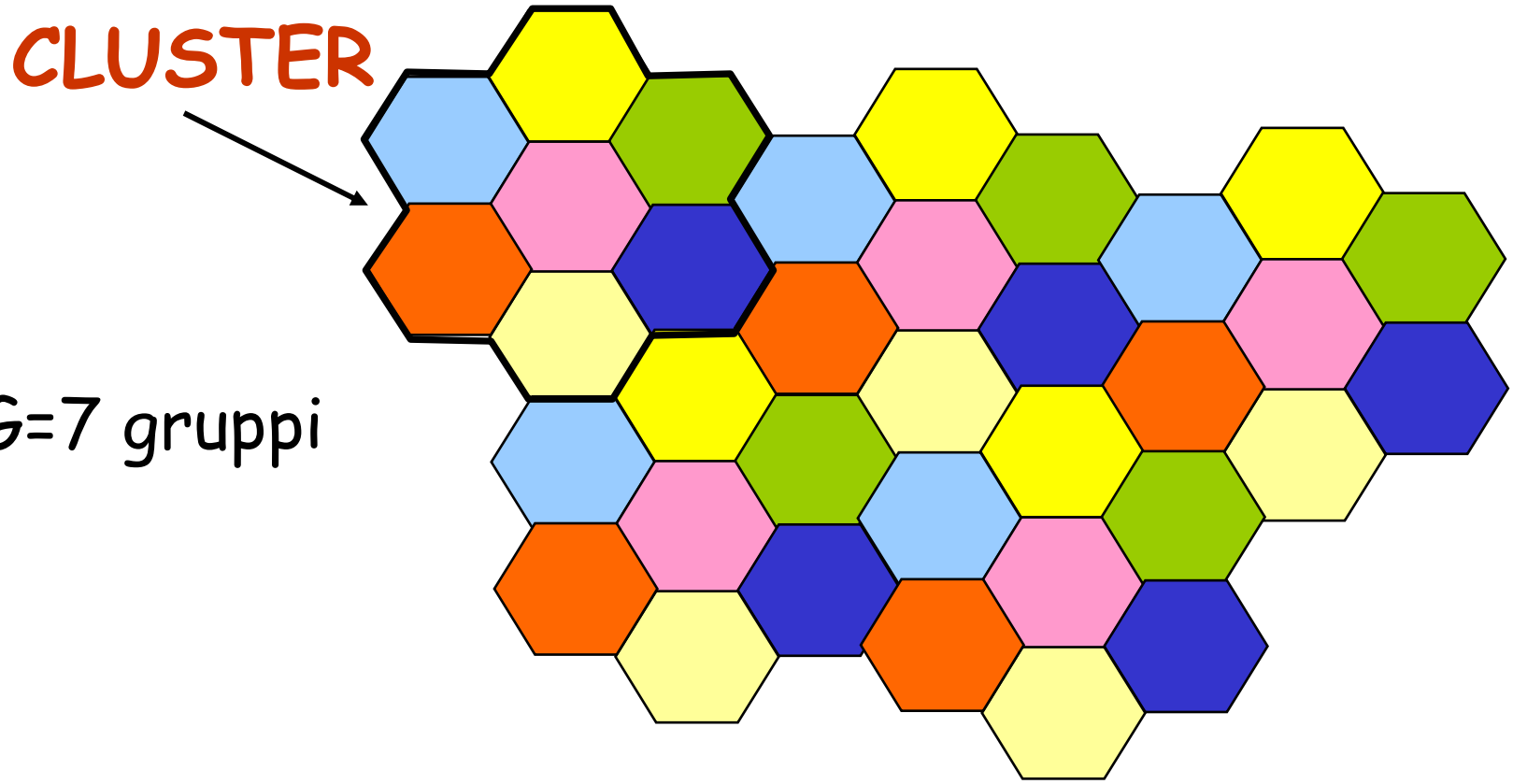
Cluster con 3 celle



- G=3 gruppi

- L'insieme dei canali nel gruppo blu, giallo e rosa sono disgiunti

Cluster con 7 celle



- *G=7 gruppi*

Dimensione tipica del cluster

- Sistemi analogici con accesso FDMA (AMPS, TACS, NMT):
  - cluster di 19 o 21 celle
- Sistemi numerici con accesso di tipo TDMA o misto FDMA/TDMA (GSM, D-AMPS, JCD):
  - cluster di 7 o 9 celle
- Sistemi numerici con accesso CDMA (IS-95/UMTS):
  - cluster di una cella (almeno in linea di principio)

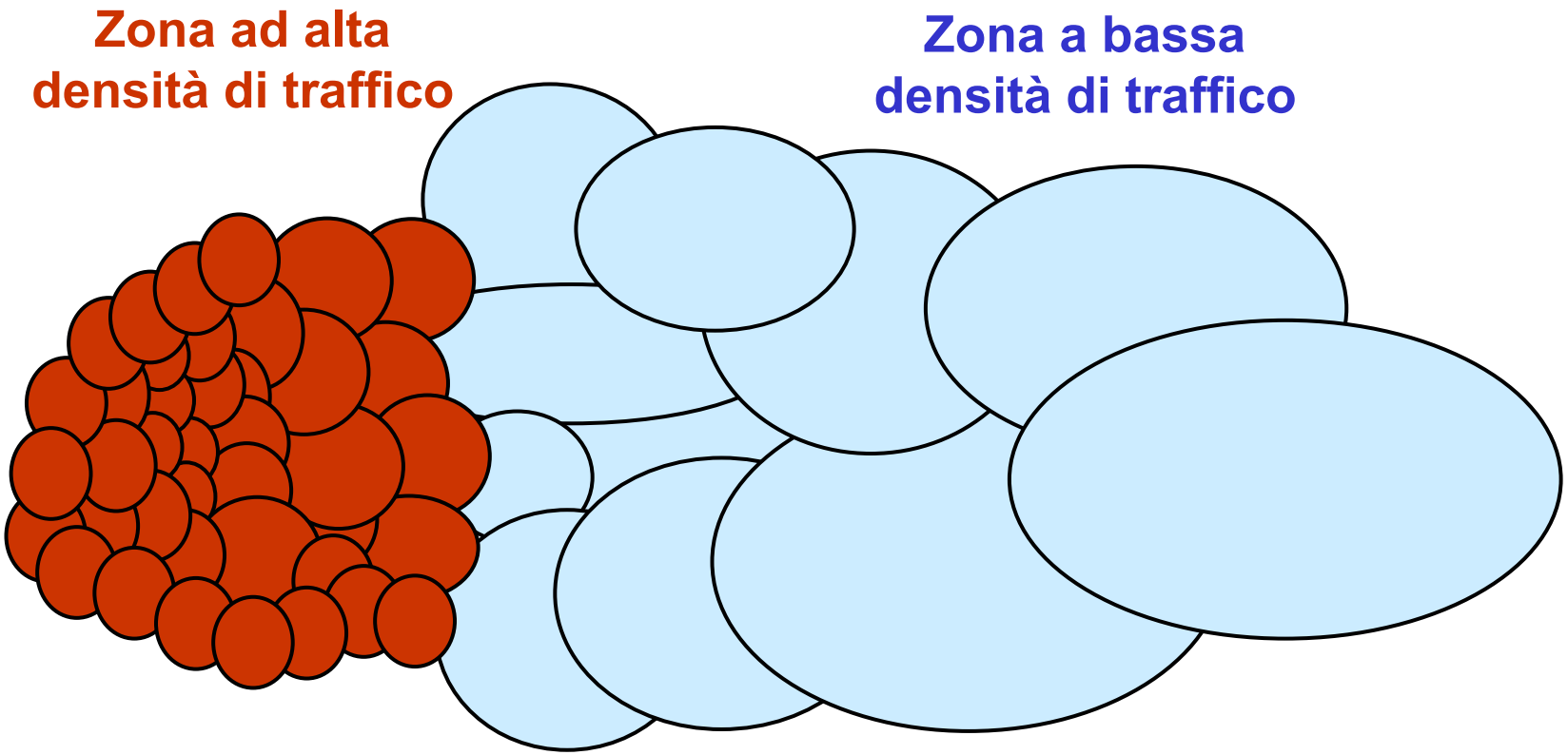


Tecniche di Copertura Cellulare

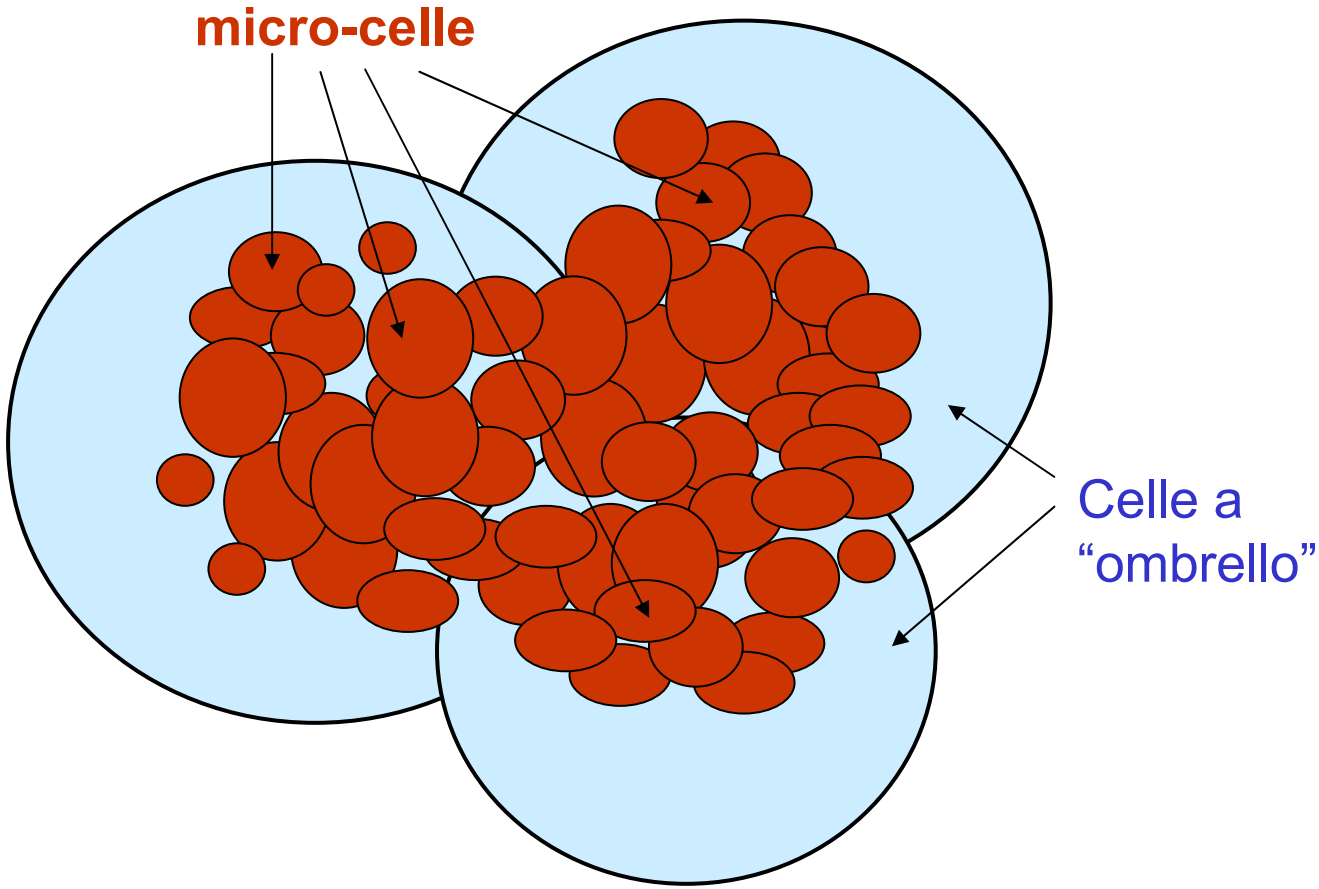
- È possibile usare antenne direzionali per avere celle di forma e dimensione particolare
- Celle di dimensione (e forma) diversa
- Celle "stratificate" (celle a ombrello)
- Sono allo studio tecniche per ottenere celle "puntiformi" che "inseguono" il terminale mobile



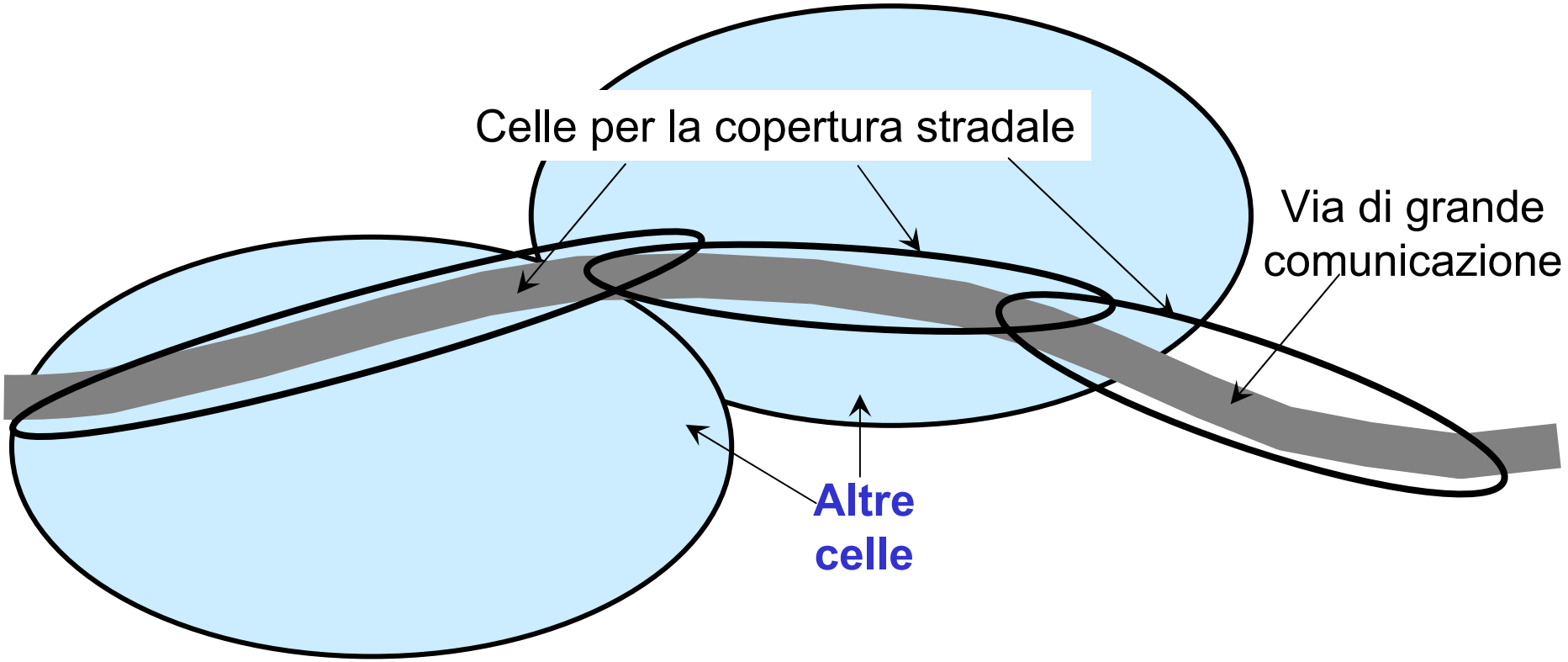
Copertura cellulare con celle di dimensione diversa per aree a diversa intensità di traffico



Copertura cellulare stratificata



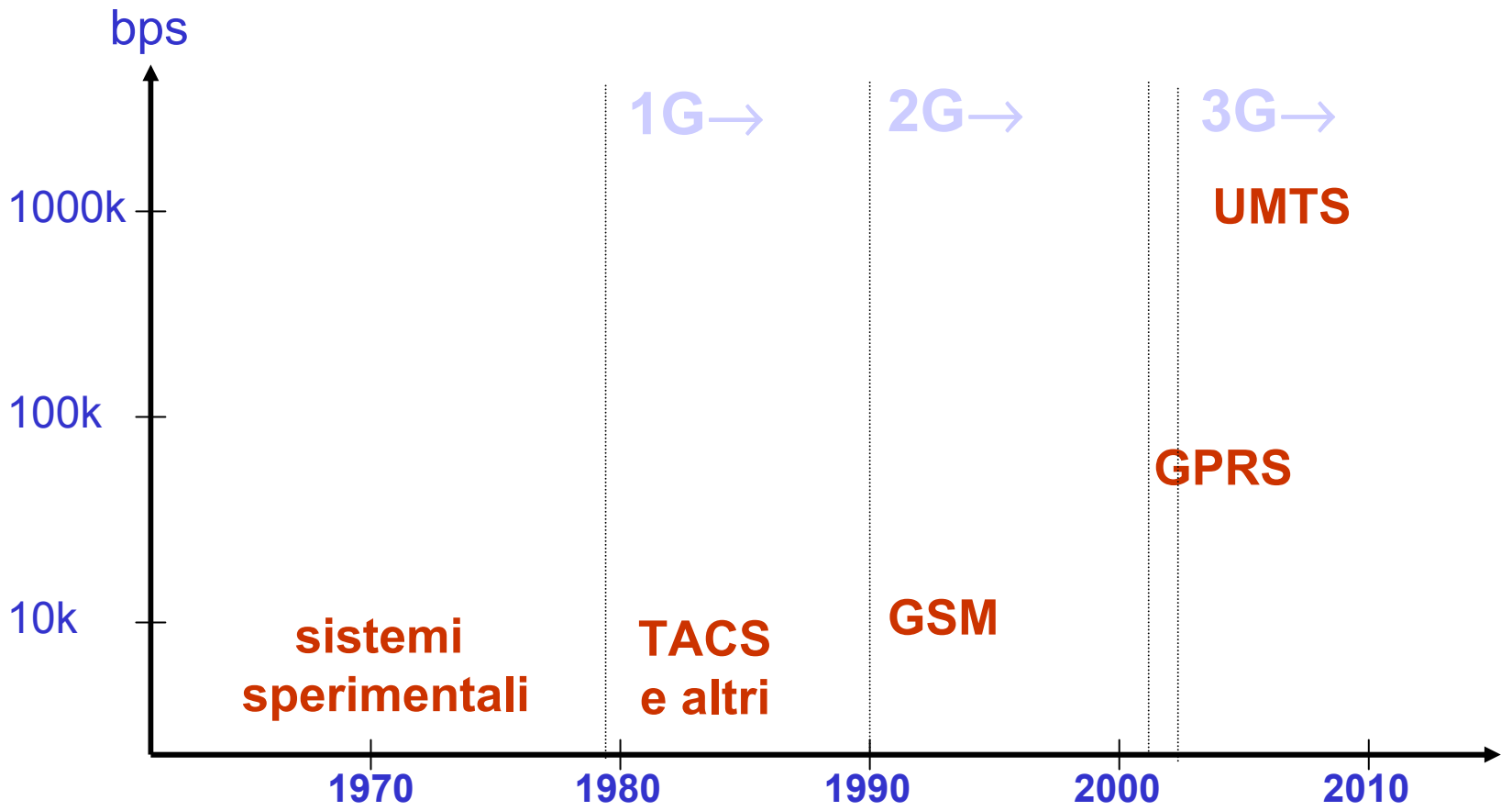
Copertura cellulare di tipo autostradale



Evoluzione della telefonia cellulare

Renato Lo Cigno
www.dit.unitn.it/locigno/didattica/wn/

Evoluzione della telefonia cellulare



Miniaturizzazione

Nokia
10 kg



1984

Nokia
900 gr



1987

Ericsson
2 kg



1990

Motorola
285 gr



1993

Motorola
110 gr



1996

Reti commerciali di prima generazione

- Tecnologia analogica
- Tecnica di accesso FDMA
- Solo servizio di telefonia
- Copertura del territorio con celle di grandi dimensioni
- Bassa qualità del servizio offerto
- Bassa efficienza nel riuso delle frequenze, e bassa capacità complessiva della rete



Reti commerciali di prima generazione

- Vari standards, fra loro incompatibili
- Reti in esercizio (in fase di dismissione): AMPS, TACS, NMT
- In Italia:
  - TACS, dal 1990
  - Gestito solo da TIM (è in stato di dismissione)



Reti commerciali di seconda generazione

Differenza fondamentale è il passaggio da trasmissione analogica a **digitale**. Vantaggi:

- Integrazione di servizi diversi
- Crittografia sul canale radio (riservatezza)
- Dimensione tempo per sfruttare risorse radio
- Tecniche di codifica vocale per ridurre banda richiesta
- Tecniche di segnalazione per servizi avanzati



Reti commerciali di seconda generazione

- Trasmissione digitale
- Tecnica di accesso FDMA/TDMA
- Tre bande di frequenza (900, 1800, 1900 MHz)
- Celle di dimensioni più contenute (raggio delle celle da alcune centinaia di metri ad alcune decine di km)
- Efficienza complessiva abbastanza buona, riuso delle frequenze da buono ad accettabile
- Alto grado di riservatezza e di sicurezza (PIN, trasmissione criptata)

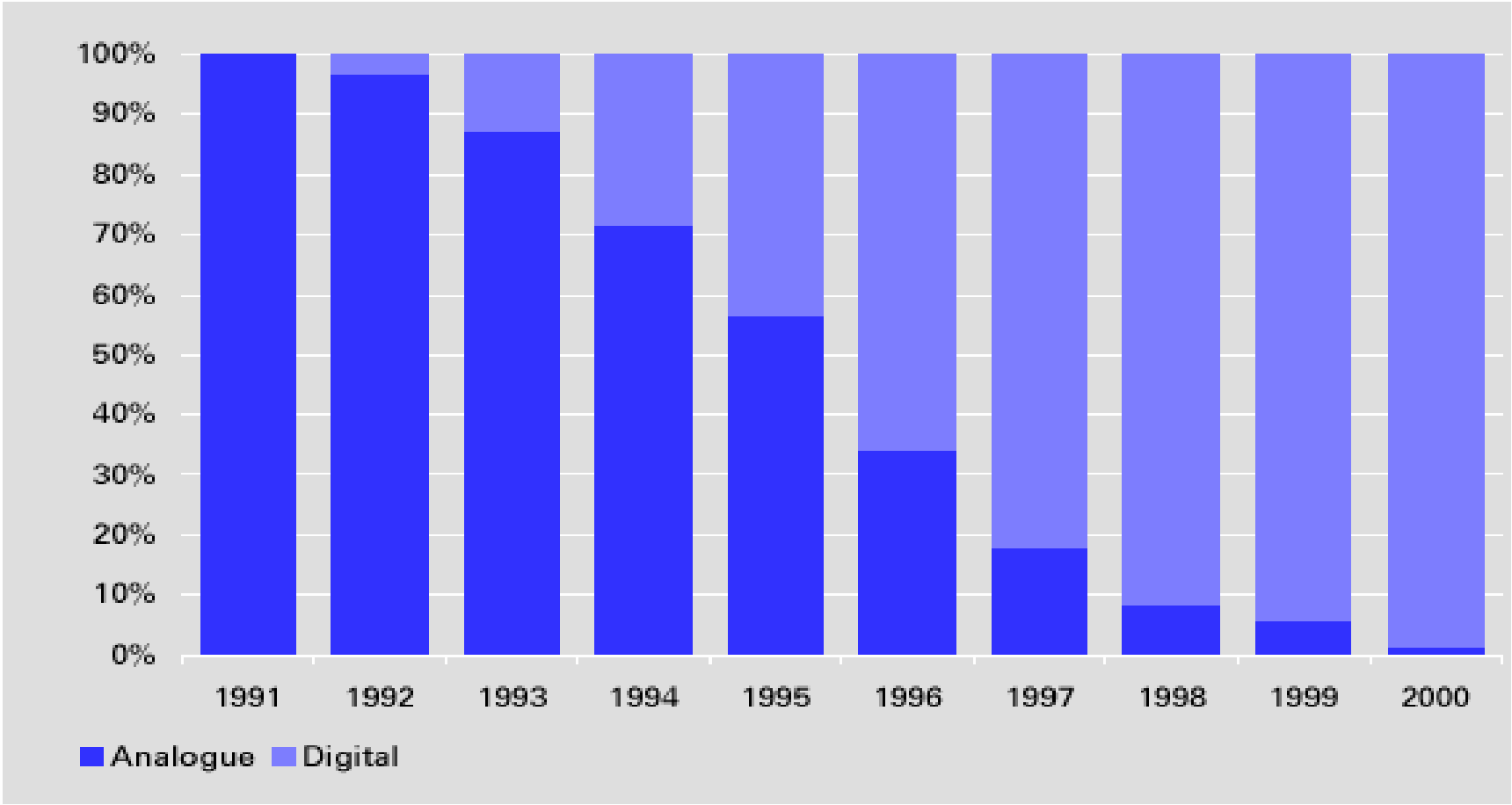


Reti commerciali di seconda generazione

- Per la trasmissione dati velocità molto basse (9600 bps per GSM)
- Invio e ricezione di SMS (*Short Message Service*) di max 160 caratteri (dal 1992)
- Il servizio inizia nel 1991; ora è adottato da più di 160 Paesi
- Reti in esercizio: D-AMPS (o ADC) e IS-95 in USA, GSM in Europa, PDC in Giappone
- In Italia le licenze sono state assegnate a 4 operatori: TIM, Omnitel-Vodafone, Wind, Blu (assorbita da Wind)



Customer migration from analogue to GSM in Western Europe



Source WestLB Panmure

Reti di seconda generazione "estese"

- Sfruttano la stessa architettura e la stessa tecnologia delle attuali reti di seconda generazione
- Sono una prima fase commerciale: GPRS in Europa, IS-95B in USA, DoCoMo in Giappone
- Servizi dati
  - A pacchetto
  - A velocità elevata (fino a 170 kbps in GPRS)
  - Tariffazione in base al volume di traffico



Terminali GPRS: esempi







Convergenza PDA / cellulare



Accoppiamento
PDA - cellulare





NTT DoCoMo: i-mode

- Tecnologia di accesso wireless a Internet a commutazione di pacchetto, basata su un subset di HTML (9,6 Kbps)
- Funziona solo sulla rete di DoCoMo (Giappone), il maggiore operatore mondiale di telefonia mobile
- Lanciata da febbraio 1999, successo esplosivo in Giappone: 24 milioni di utenti in due anni
- Basso costo: flat fee di $2,4 al mese



Reti di terza generazione

- Progettate per fornire servizi "multimediali"
- Tecnica di accesso CDMA, W-CDMA o A-TDMA (Advanced-TDMA, una evoluzione della tecnica FDMA/TDMA del GSM)
- Copertura cellulare "stratificata", con celle di piccole dimensioni per avere elevata capacità e celle a ombrello sovrapposte per consentire elevata mobilità
- Uso della diversità spaziale (comunicazione contemporanea con più stazioni fisse) per maggiore qualità/affidabilità
- Elevata velocità (fino a 2Mbps)



Reti di terza generazione

- Elevata integrazione di molte sottoreti specializzate per fornire migliore qualità di servizio
- Richiede grandi investimenti
- Possibilità di handover tra sottoreti differenti
- Reti "previste":
  - UMTS (Universal Mobile Telecommunication System) - ETSI in Europa, Giappone, Cina, ...
  - CDMA2000 (IS-95C) in USA



IL SISTEMA GSM

Renato Lo Cigno
www.dit.unitn.it/locigno/didattica/wn/

Breve Storia - 1

1982: la CEPT (Conférence Européenne des Administrations des Postes et des Télécommunications) istituisce un gruppo speciale per lo studio di un insieme uniforme di regole per lo sviluppo di una futura rete cellulare pan-europea: il Groupe Spécial Mobile da cui **GSM**

1984: istituzione di 3 Working Parties (WP1-3) per la definizione di servizi da offrire in GSM: l'interfaccia radio, i formati di trasmissione e i protocolli di segnalazione, le interfacce e l'architettura di rete



Breve Storia - 2

1985: definizione della lista di raccomandazioni che il GSM deve produrre (finiranno per essere circa 130: 1500 pagine in 12 volumi! ... piu` tutti quelli relativi all'evoluzione, cioe` le fasi 2+ e 3 di GSM, rilasciati in anni successivi)

1986: viene istituito il cosiddetto *nucleo permanente* con lo scopo di coordinare il lavoro del GSM, soprattutto visto il forte interesse da parte dell'industria



Breve Storia - 3

1987: viene firmato un primo Memorandum of Understanding (MoU) tra operatori Telecom in rappresentanza di 12 Nazioni (europee) con i seguenti obiettivi:

- coordinare lo sviluppo temporale delle reti GSM europee e verificarne lo standard
- pianificare l'introduzione dei servizi
- concordare le politiche di instradamento e la tariffazione (modalità e prezzi)



Breve Storia - 4

1988: con l'istituzione di ETSI (European Telecommunication Standards Institute) il lavoro su GSM viene "spostato" in questo foro

1990: viene deciso di applicare le specifiche GSM anche al sistema DCS1800 (Digital Cellular System on 1800 MHz), un sistema di tipo PCN (Personal Communication Networks) inizialmente sviluppato in U.K.

1991: (luglio) il lancio commerciale del GSM, pianificato per questa data, viene rimandato al 1992 per la mancanza di terminali mobili conformi allo standard



Breve Storia - 5

1992: viene rilasciato lo standard definitivo relativo a GSM, che a questo punto diventa l'acronimo di
Global System for Mobile communications

1992: introduzione ufficiale dei sistemi GSM commerciali

1993: il MoU raccoglie 62 membri di 39 paesi; inoltre altre 32 organizzazioni in rappresentanza di 19 paesi partecipano come osservatori in attesa di firmare il MoU



Breve Storia - 6

1994-95: introduzione di SMS

1995-97: introduzione del servizio a 1800MHz

1996: standardizzazione dei codificatori enhanced sia full-rate che half-rate

1997: terminali dual-band con codificatore enhanced

1999: standard GPRS (lo tratteremo a parte) per la trasmissione a pacchetto;
primi terminali WAP (Wireless Access Protocol) su circuito commutato

2000/01: introduzione del servizio GPRS

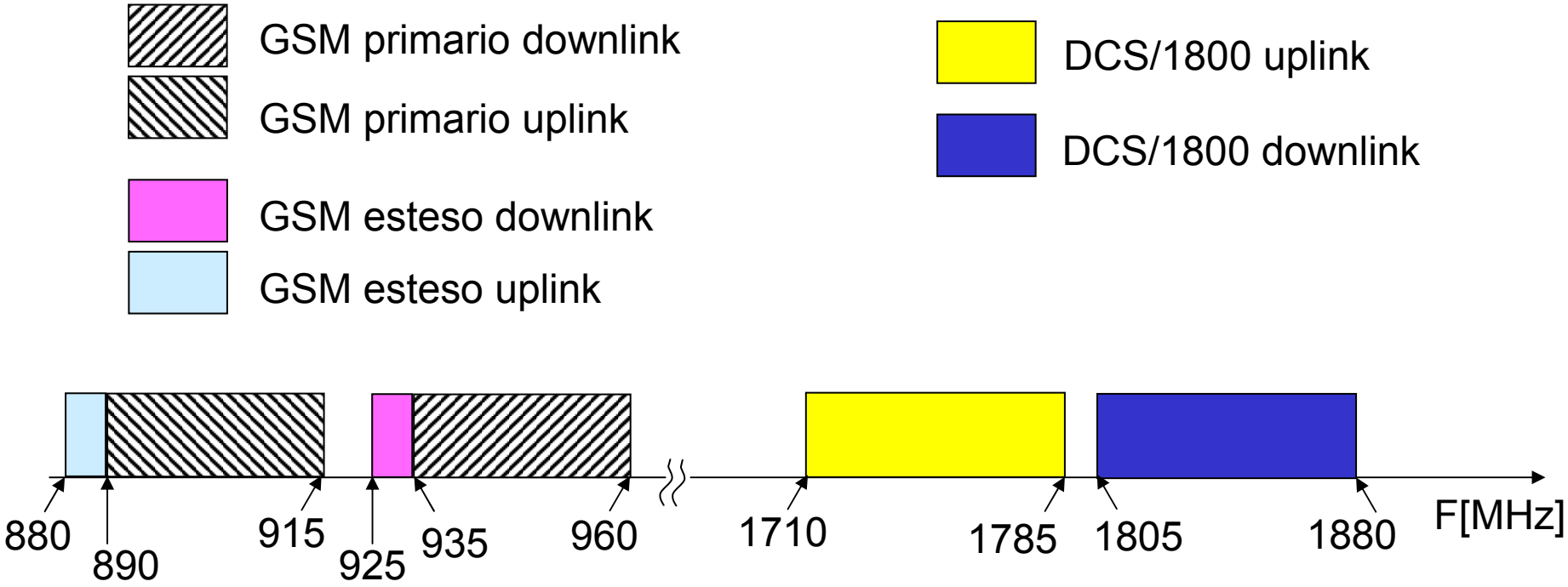


Breve Storia - 7

1993-2003: GSM diventa la rete cellulare piu` diffusa al mondo, con quasi 100M utenti in Europa e oltre 200M a livello mondiale (quasi 40M solo in Cina), una penetrazione non marginale anche in USA con una decina di operatori, che hanno una quota di mercato seconda solo a AMPS/D-AMPS.
GSM e` diventato una standard mondiale, influenzando in modo significativo l'evoluzione verso le reti di 3ª generazione e contribuendo a determinare il fallimento commerciale delle reti satellitari



Frequenze assegnate al GSM (Europa)



- In UK e USA si usano bande intorno a 1900MHz anziché intorno a 1800MHz.
- Esistono terminali "tri-band"

Frequenze assegnate al GSM (Europa)

- I canali uplink e downlink sono sempre accoppiati in modo fisso e distano
  - ✓ 45 MHz a 900
  - ✓ 95 MHz a 1800
- A 900 dispone di 124 (125-1) canali FDM nella parte primaria dello spettro più 50 canali nella parte estesa
- A 1800 dispone di 374 (375-1) canali FDM
- Il canale all'estremo inferiore non è **mai** usato
- Se possibile sia a 900 che a 1800 anche i canali all'estremo superiore sono usati come "guardia"



Frequenze assegnate al GSM (Europa)

- La banda assegnata a GSM è parzialmente sovrapposta a quella dei servizi TACS, creando qualche problema di "convivenza"
- Esiste un sistema di numerazione assoluto dei canali (ARFCN - Absolute Radio Frequency Channel Number), che consente di identificare in modo univoco il canale da usare (o in uso) indipendemente dal fatto che sia GSM/900 o DCS/1800
- I canali GSM-900 hanno ARFCN da 0 a 124 (primario) e da 974 a 1023 (esteso)



Dati generali

- Distanza tra portanti 200 KHz
- Accesso TDMA/FDMA, 8 timeslot per portante
- Codifica voce a 13 kb/s (full rate) o 6.5 kb/s (half rate), 12.6 e-gsm
- Modulazione GMSK (Gaussian Minimum Shift Keying)
- Uso di controllo di potenza
- Definizione di interfacce standard (non proprietarie) tra elementi della rete



Servizi offerti

Teleservizi:

- telefonia sia full rate (13 kbit/s, 12.6 Enhanced coder), sia half rate (6.5 kbit/s)
- telefax
- messaggi sia unicast che multicast
- messaggi brevi (SMS, MMS)

Servizi supplementari: praticamente tutti quelli della rete PSTN (inoltro di chiamata, richiamata su occupato,...)



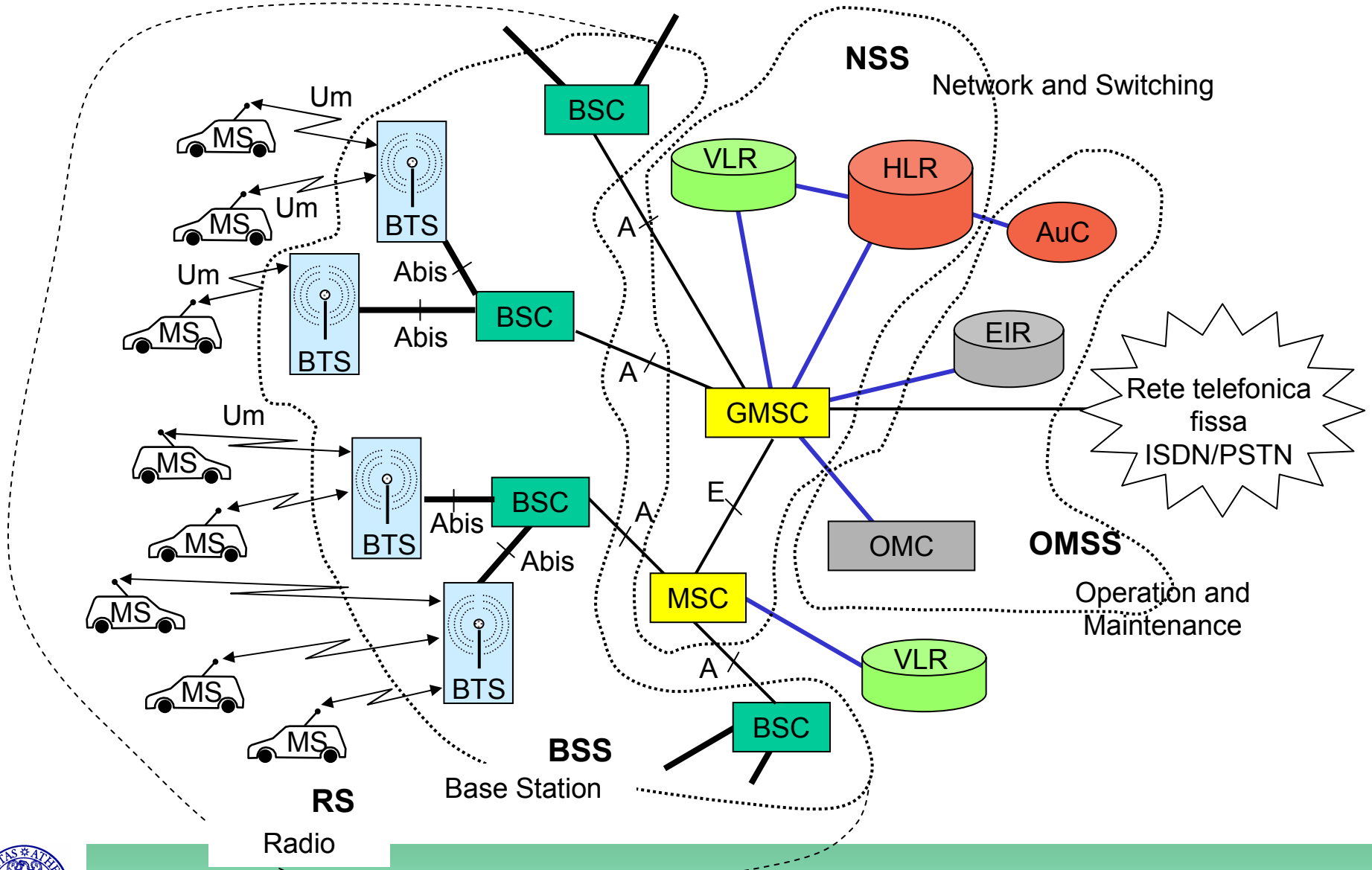
Servizi offerti

Servizi di trasporto:

- trasmissione dati (non strutturata) sincrona e asincrona tra 300 bit/s e 9.6 kbit/s
- trasmissione dati a pacchetto sincrona con velocità compresa tra 2.4 e 9.6 kbit/s
- trasmissione dati con affasciamento di canali (HSCSD) fino a 76.8 kbit/s



Architettura del GSM



Architettura del GSM

4 componenti

- **Terminali utente**
- **Base Station Subsystem (BSS)**: si occupa degli aspetti radio: copertura, comunicazione con il terminale utente, etc.
- **Network and Switching Subsystem (NSS)**: gestisce la mobilità degli utenti, il controllo delle chiamate, supporto ai servizi
- **Operation and Maintenance Subsystem (OMSS)**: si occupa di gestione e manutenzione della rete





Terminale Mobile (Mobile Station, MS)

- È il terminale di utente
- Ne esistono molti tipi diversi, a seconda delle applicazioni e dei luoghi di installazione
- Tre categorie a seconda della potenza nominale:
  - veicolari: possono emettere fino a 20 W all'antenna
  - portatili: fino a 8 W all'antenna, sono trasportabili, ma hanno bisogno di una notevole fonte di alimentazione per il funzionamento (es. PC portatili, fax, etc.)
  - personali (hand-terminal): fino a 2 W all'antenna, è il "telefonino"; GSM1800 prevede in genere i un limite di potenza a 0.8 W

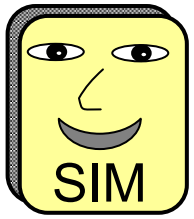




Terminale Mobile (MS)

- *Multi-Band*: se funziona su più bande (es., dual-band opera a 900 MHz e 1800 MHz)
- *Multi-slot*: può trasmettere su più canali (fino a 8) della stessa portante (es., per il GPRS)
- MS è solamente "hardware", per poter funzionare e collegarsi alla rete ha bisogno di una scheda di abilitazione: la **SIM**
- MS è abilitato a chiamare i numeri di emergenza anche senza la SIM

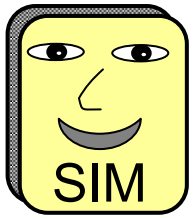




Modulo di Identificazione Utente (Subscriber Identity Module - SIM)

- È una scheda intelligente (con processore e memoria) di tipo *smart card* che rende "operativo" un qualunque MS
- Deve essere inserita nell'apposito *lettore* di SIM
- Sono ammessi 2 possibili formati: tipo carta di credito e un formato ridotto (*plug-in* SIM, attualmente la più diffusa)



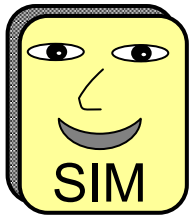


Modulo di Identificazione Utente (Subscriber Identity Module - SIM)

Memorizza

- Identificativo univoco SIM
- Identificativo utente (IMSI: International Mobile Subscriber Identity)
- Chiave di autenticazione
- Chiave di cifratura (per la trasmissione su tratta radio)
- Altre caratteristiche dell'utente (# telefonico, servizi accessibili, etc.)





Modulo di Identificazione Utente (Subscriber Identity Module - SIM)

- Memorizza messaggi brevi inviati dalla rete (più evolve la tecnologia maggiori capacità potranno essere associate alla SIM) tra cui gli SMS
- La SIM viene abilitata attraverso un codice di 4 cifre (**PIN** - Personal Identification Number)

L'insieme MS+SIM fa un **terminale mobile (TM)**



IMSI

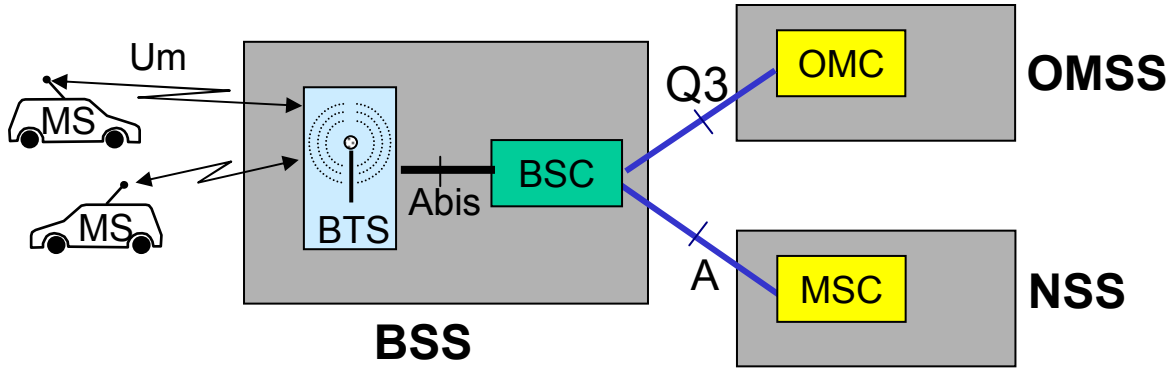
- Numero di identificazione dell'utente
- Composto da 3 campi:
  - **MCC**: Mobile Country Code (3 cifre)
  - **MNC**: Mobile Network Code, che identifica l'operatore che fornisce il servizio (2 cifre)
  - **MSIC**: Mobile Subscriber Identification Number, che identifica la SIM (fino a 10 cifre)
- Es: 222 01 4572228769, identifica una SIM italiana (222) del gestore TIM (01)
- Il numero di telefono dell'apparato in questione è completamente scorrelato dall'IMSI

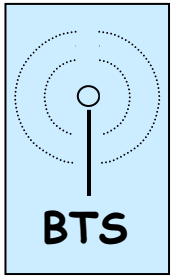


Base Station Sub-system

2 funzioni fondamentali:

- Rice-trasmissione: realizzata da **Base Transceiver Station (BTS)**
- Controllo delle risorse radio: realizzata da **Base Station Controller (BSC)**

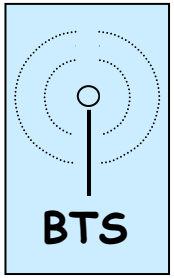




Stazione Radio Base (Base Tranceiver Station - BTS)

- È il punto di accesso alla rete di TLC, o se si vuole, la "controparte" di MS
- È collocata in un punto opportuno della cella (al centro per celle circolari, nel vertice delle celle settorizzate, ad un estremo delle celle oblunghe per la copertura stradale...)
- Dalla potenza del BTS dipende l'effettiva dimensione fisica della cella: grazie a questa caratteristica è possibile "aggiustare" in modo dinamico le dimensioni delle celle

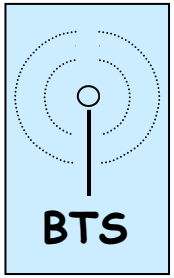




Stazione Radio Base (Base Tranceiver Station - BTS)

- Ciascuna BTS può avere da 1 a 16 interfacce radio, corrispondenti a diverse portanti
- Ciascuna interfaccia radio corrispondente a 8 canali (TDM)
- Effettua la codifica di canale e la cifratura
- Modula/demodula i segnali
- Realizza il frequency hopping





Stazione Radio Base (Base Tranceiver Station - BTS)

- Effettua misure di qualità dei canali up-link e riceve da MS le misure relative al down-link, le invia al BSC che decide il controllo di potenza e l'handover
- Implementa i protocolli di livello fisico per il corretto scambio di informazioni tra MS e BTS



BSC

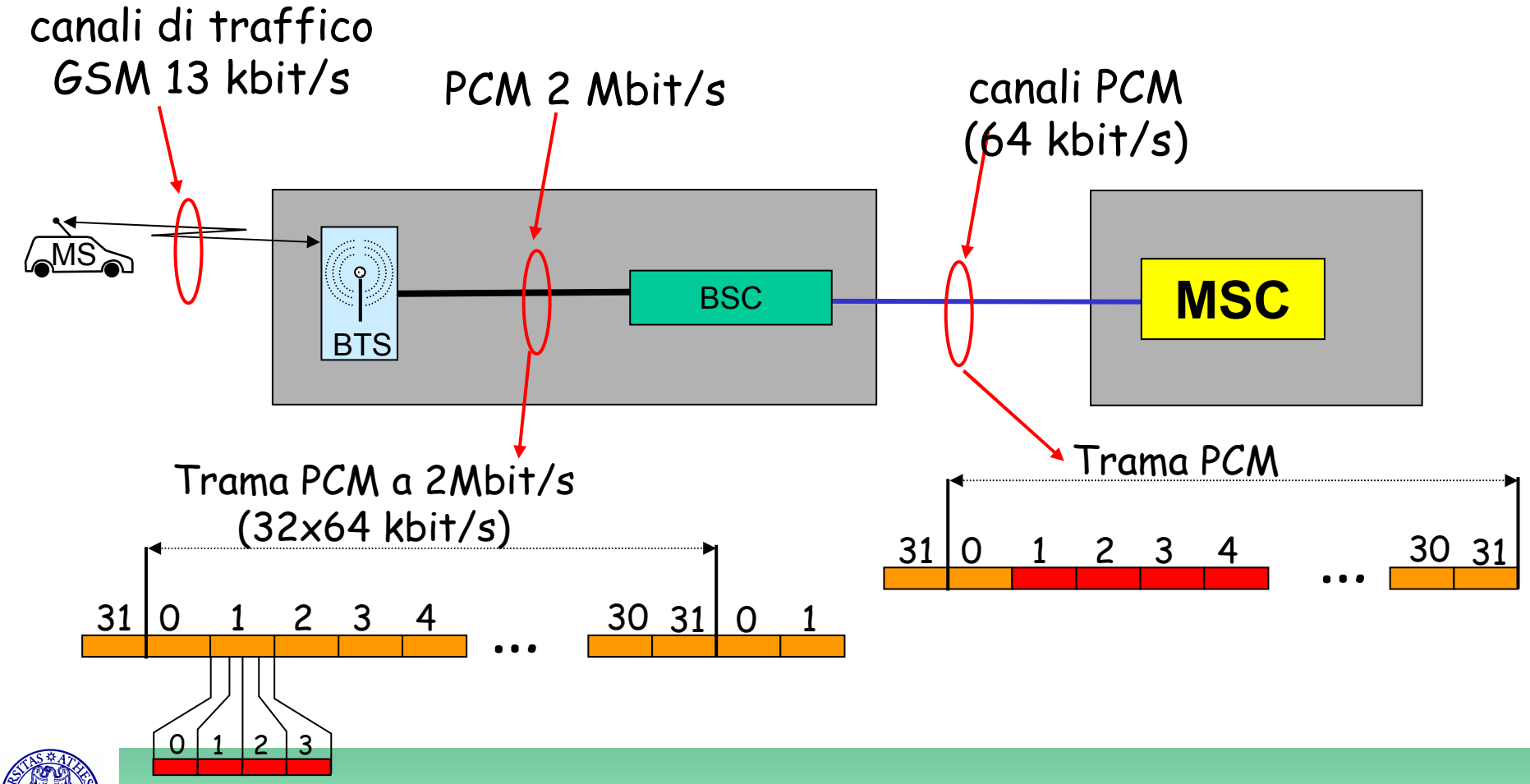
Controllore della Stazione Radio Base (Base Station Controller- BSC)

- Un BSC può controllare un numero elevato di BTS: da alcune *decine* ad alcune *centinaia*
- Quando sono distanti, BTS e BSC sono collegati da collegamenti a 2 Mb/s (31 canali PCM)
- Un canale PCM del collegamento a 2Mb/s viene usato per trasportare 4 canali di traffico GSM, a 13 kb/s
- La transcodifica della voce GSM (13 kb/s) $\Leftrightarrow$ PCM (64 kb/s) e viceversa è fatta dal BSC



BSC

Controllore della Stazione Radio Base (Base Station Controller- BSC)



BSC

Controllore della Stazione Radio Base (Base Station Controller- BSC)

- I compiti principali del BSC sono:
  - transcodifica della voce GSM $\Leftrightarrow$ PCM
  - analisi delle misure di qualità del segnale sulla tratta radio
    - Decisione se è il caso di fare handover
    - Gestione dell'handover tra BTS controllate dallo stesso BSC o richiesta al NSS (al MSC)
  - gestione delle frequenze, che possono essere assegnate in modo dinamico alle varie BTS



BSC

Controllore della Stazione Radio Base (Base Station Controller- BSC)

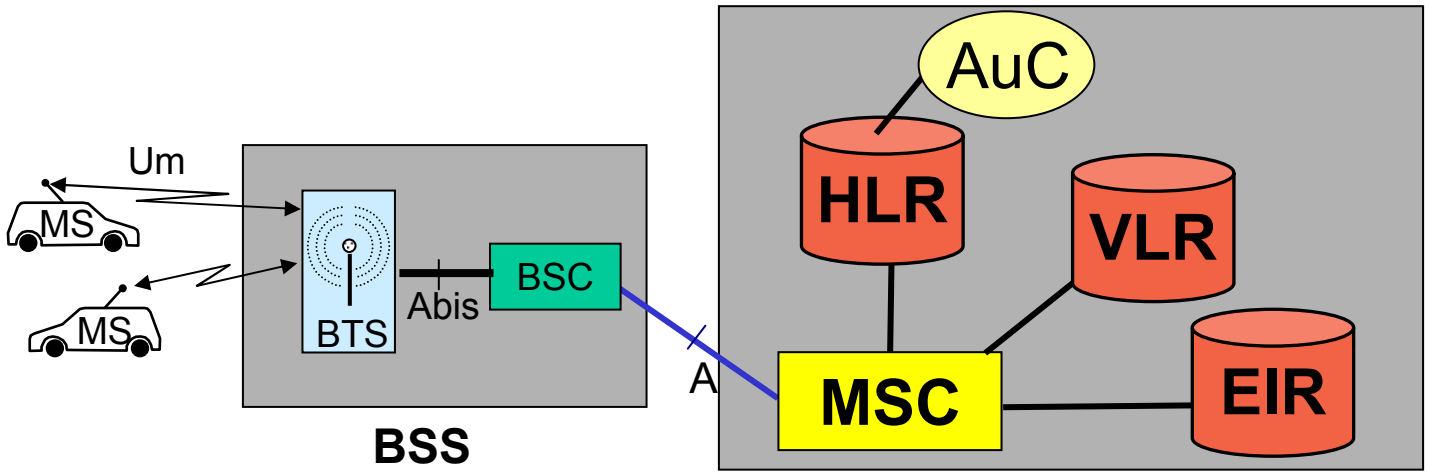
- I compiti principali del BSC sono:
  - concentrazione del traffico verso un MSC e smistamento del traffico verso le BTS
  - gestione del paging
  - manutenzione del BSS



Network and Switching Sub-system (NSS)

Noto anche come Switching and Management Sub-system (SMSS), svolge funzioni fondamentali:

- Gestione della mobilità
- Controllo delle chiamate
- Supporto ai servizi forniti



Network and Switching Sub-system (NSS)

- Mobile Switching Center (MSC): è la centrale di commutazione che gestisce i terminali mobili
- Home Location Register (HLR): è il data base con
  - i *dati permanenti* degli utenti
  - i *dati dinamici* per gestire la mobilità (identificativo del VLR, etc.)
- Visitor Location Register (VLR): è il data base con
  - le infomazioni relative ai MS attualmente presso l'area di competenza del MSC
- Equipment Identity Register (EIR): è il data base degli apparati rubati o difettosi
- Authentication Center (AuC): genera chiavi di cifratura



(G)MSC

(Mobile Switching Center - MSC)
Centro di Commutazione dei Servizi Mobili

- Sono "normali" commutatori PCM (commutatori a circuito) cui sono state aggiunte le funzionalità di segnalazione per la gestione della mobilità
- Funzioni fondamentali
  - Gestione della mobilità
  - Controllo delle chiamate (con autenticazione)
  - Supporto ai servizi
  - Interworking con altre reti
  - Funzioni di gateway
  - Funzioni di gestione delle risorse



(G)MSC

(Mobile Switching Center - MSC)
Centro di Commutazione dei Servizi Mobili

- Consente l'instradamento delle chiamate da un MS ad un altro o verso telefoni fissi
- Un caso particolare di MSC è il **G**MSC (*Gateway*-MSC), che costituisce l'interfaccia tra la rete GSM e le reti fisse (PSTN)
- GMSC e` anche il "punto di partenza" per la ricerca degli MS nella rete cellulare

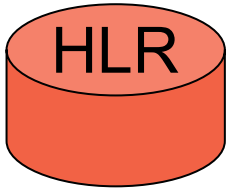


(G)MSC

(Mobile Switching Center – MSC)
Centro di Commutazione dei Servizi Mobili

- A seconda delle dimensioni della rete e del numero di utenti, un operatore può avere uno o più GMSC a cui sono associati in modo fisso i terminali mobili (TM)
- Una chiamata entrante verso un TM passa sempre attraverso il "suo" GMSC
- Le funzioni legate alla sicurezza e all'autenticazione sono effettuate presso gli MSC

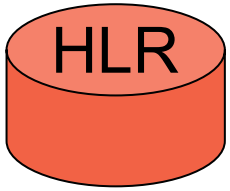




Registro di Localizzazione Principale (Home Location Register)

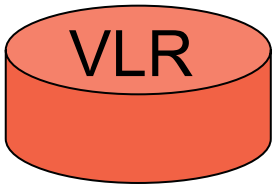
- È una base dati ***permanente*** associata in modo univoco a un MSC
- Memorizza le informazioni relative a tutti gli MS la cui localizzazione **di *default*** è presso il MSC considerato
- HLR memorizza informazioni permanenti come l'IMSI (International Mobile Subscriber Identity), il numero di telefono della SIM associata (che **NON** sono la stessa cosa) e la sua chiave di autenticazione, i servizi supplementari a cui l'utente è abilitato, . . .





Registro di Localizzazione Principale (Home Location Register)

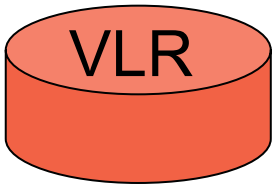
- HLR memorizza anche informazioni volatili:
  - indirizzo del VLR presso cui può essere reperito l'utente
  - parametri transitori per identificazione e crittografia
  - eventuale numero di telefono per l'inoltro delle chiamate
  - stato dell'MS (acceso, spento, ...)
  - ...



Registro di Localizzazione Visitatori (Visitor Location Register - VLR)

- È una base dati ***temporanea*** associata a tutti gli MSC, anche ai GMSC
- Contiene i dati essenziali per il servizio dei terminali mobili attualmente sotto la giurisdizione del MSC cui il VLR è associato
- Si noti che per una questione di uniformità viene usato il VLR anche per i terminali mobili che si trovano presso il proprio MSC: l'informazione memorizzata nell'HLR viene "duplicata" localmente





Registro di Localizzazione Visitatori (Visitor Location Register - VLR)

- Nel VLR vengono duplicati tutti i dati permanenti di un utente
- L'IMSI viene "mappato" su un TMSI (Temporary Mobile Subscriber Identity) per non trasmettere regolarmente l'IMSI via radio (protezione da intrusioni)
- Il TMSI viene modificato frequentemente ed è legato anche alla posizione del mobile



TMSI

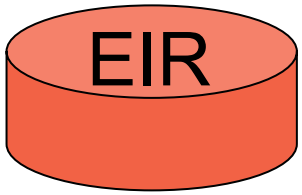
- Numero assegnato temporanemente dalla rete (VLR) a ogni MS per ottenere privacy e protezione; è strutturalmente uguale all'IMSI
- Permette al MS di non trasmettere in chiaro il proprio IMSI; è memorizzato nella SIM
- E legato al VLR (in effetti, alla Location Area)
- Viene cambiato spesso: ad ogni uso, ad ogni location update
- E' trasmesso in chiaro dal MS per autenticarsi, viene ri-assegnato dalla rete dopo aver instaurato un canale sicuro (crittografato), così che una eventuale intercettazione è inutile



IMEI

- International Mobile station Equipment Identity
- Numero di identificazione dell'apparato; serve per la protezione da furti e utilizzi non autorizzati
- E' memorizzato in modo sicuro dentro l'apparato

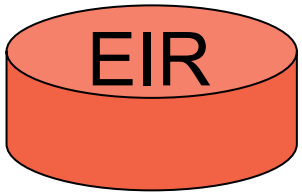




(Equipment Identity Register)
Registro di Identificazione apparati

- È una base dati il cui uso è a discrezione dell'operatore
- Contiene l'identificativo e le caratteristiche di tutti gli apparati GSM (MS - l'hardware) prodotti, insieme al produttore, al paese di fabbricazione, etc.
- E' usato per proteggere la rete dall'uso di apparecchiature non a norma, rubate, esportate illegalmente, ...





(Equipment Identity Register)
Registro di Identificazione apparati

L'EIR contiene 3 elenchi:

- White list: identifica tutti i terminali operativi
- Grey list: identifica i terminali difettosi o non omologati
- Black list: identifica apparati rubati o non autorizzati





Centro di Autenticazione (Authentication Center - AuC)

- È associato a ciascun HLR
- È il "motore" per l'autenticazione delle SIM
- È in grado di effettuare correttamente le operazioni di codifica che sono associate a ciascuna SIM
- Genera le chiavi di cifratura necessarie per la trasmissione sicura sull'interfaccia radio



Instradamento delle chiamate

Fa uso di due numeri:

- MSISDN: Mobile Station International ISDN Number … il numero di telefono
- MSRN: Mobile Station Roaming Number
  - ✓ numero usato dalla rete per l'instradamento delle chiamate; è un identificatore temporaneo assegnato dal VLR
  - ✓ memorizzato presso l'HLR, identifica il VLR dove si trova il terminale mobile, quindi anche l'eventuale operatore di roaming



Instradamento delle chiamate

- Dall'analisi del MSISDN le centrali di telefonia creano una connessione fisica verso il GMSC che gestisce quel numero
- Il GMSC richiede il MSRN al MSC su cui risiede l'HLR dell'utente
- Tramite il MSRN, il GMSC instrada la chiamata verso il MSC che contiene il VLR che ha in carico l'utente
- Il MSC crea la connessione fino al MS



Procedure di sicurezza
L'autenticazione

L'autenticazione ha 2 obiettivi:

- Proteggere da tentativi di utilizzo fraudolento della rete da parte di persone non autorizzate
- Proteggere da tentativi di accesso non autorizzato ai dati da parte di utenti regolari

Durante l'autenticazione viene anche generata la chiave di cifratura usata poi per la trasmissione sulla tratta radio



Procedure di sicurezza
L'autenticazione

1. La rete invia al MS un numero casuale (RAND) generato da AuC
2. MS calcola la risposta (SRES) in base a un algoritmo prefissato (algoritmo A3) usando RAND e Ki, una chiave memorizzata sia nella SIM che in AuC
3. MS spedisce SRES alla rete
4. La rete confronta SRES con il risultato del calcolo svolto da AuC (usando RAND e Ki)
5. Se i risultati coincidono è concesso l'accesso



Procedure di sicurezza
La cifratura

L'obiettivo è la riservatezza (proteggere contro le intercettazioni)

- L'algoritmo di cifratura (A5) è contenuto nei MS e nelle BTS e utilizza una chiave Kc
- Kc è generata da un algoritmo prefissato (A8) sia da MS che da AuC in fase di autenticazione, utilizzando RAND



Aree del GSM

- **Cella:**
  - Identificata da un Cell Global Identifier (CGI)
  - Servita da una BS, identificata con un Base Station Identity Code (BSIC)
- **Location Area:**
  - Insieme di celle in cui un MS si muove senza cambiare le informazioni nel VLR
  - Identificata da un LAI



Aree del GSM

- **MSC/VLR service area:**
  - Insieme di location area servite dallo stesso MSC e dal VLR associato al MSC
  - Quando un MS cambiare MSC/VLR service area deve aggiornare il VLR e il puntatore al VLR nell'HLR
- **Public Land Mobile Network (PLMN):**
  - Una rete GSM di un gestore
- **GSM service area:**
  - Insieme di tutte le aree servite da PLMN



Riepilogo. I dati di utente

- IMSI: itentifica l'utente
- MSISDN: è il numero di telefono
- TMSI: è l'identificativo temporaneo usato al posto dell'IMSI sulla tratta radio
- MSRN: è il numero usato dal GMSC per instradare una chiamata
- LAI: identifica la Location Area su cui è l'utente
- Identificativo del VLR presso cui è memorizzato
- Identificativo del HLR presso cui è registrato



OMC

Operation and Maintenance Sub-system (OMSS)

- È la sede di tutte le operazioni di gestione della rete
  - Gestione dei guasti
  - Gestione della manutenzione
  - Configurazione degli elementi di rete (configura le singole BTS tramite le BSC)
  - Controllo delle prestazione degli elementi di rete
  - Gestione della sicurezza del sistema
  - Raccolta dei dati relativi alla tariffazione
  - Gestione della ripartizione della tariffazione tra gestori diversi per chiamate inter-gestore



GSM - Parte II

Il livello fisico dell'interfaccia radio (Um)

Renato Lo Cigno
www.dit.unitn.it/locigno/didattica/wn/



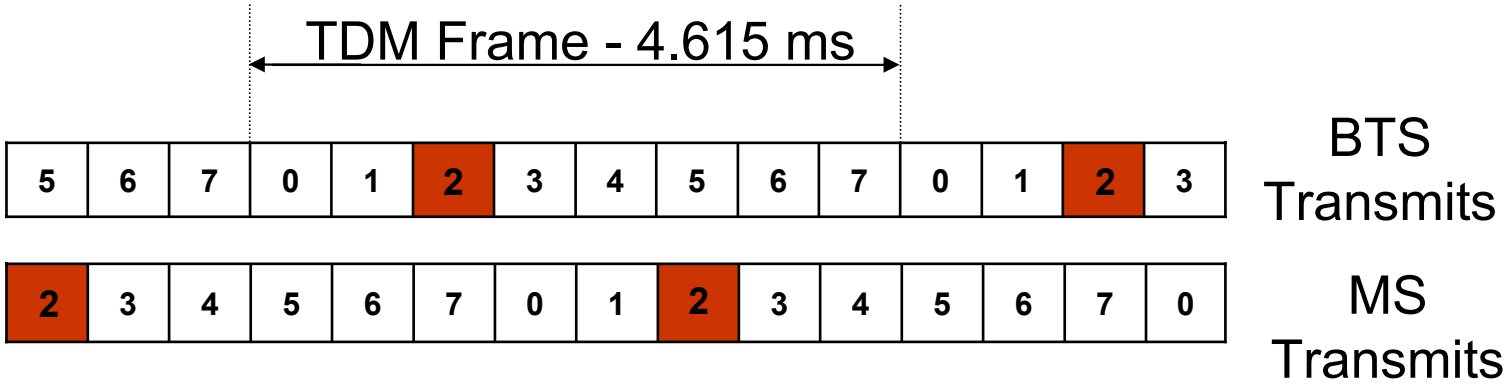
Tecnica di Accesso e Struttura dei Canali

- GSM usa una tecnica di accesso mista a divisione di tempo e frequenza (FDMA/TDMA)
- La porzione di spettro disponibile è suddivisa in canali FDM di 200 kHz l'uno
- Ciascun canale FDM è ulteriormente suddiviso in 8 canali con tecnica TDM
- La trasmissione è organizzata in *"burst"*
  - ogni MS trasmette un blocco di dati in un intervallo temporale (1 canale TDM) e "tace" durante gli altri 7 intervalli dedicati agli altri canali.
- La velocità di cifra al trasmettitore è di circa 271 kbit/s



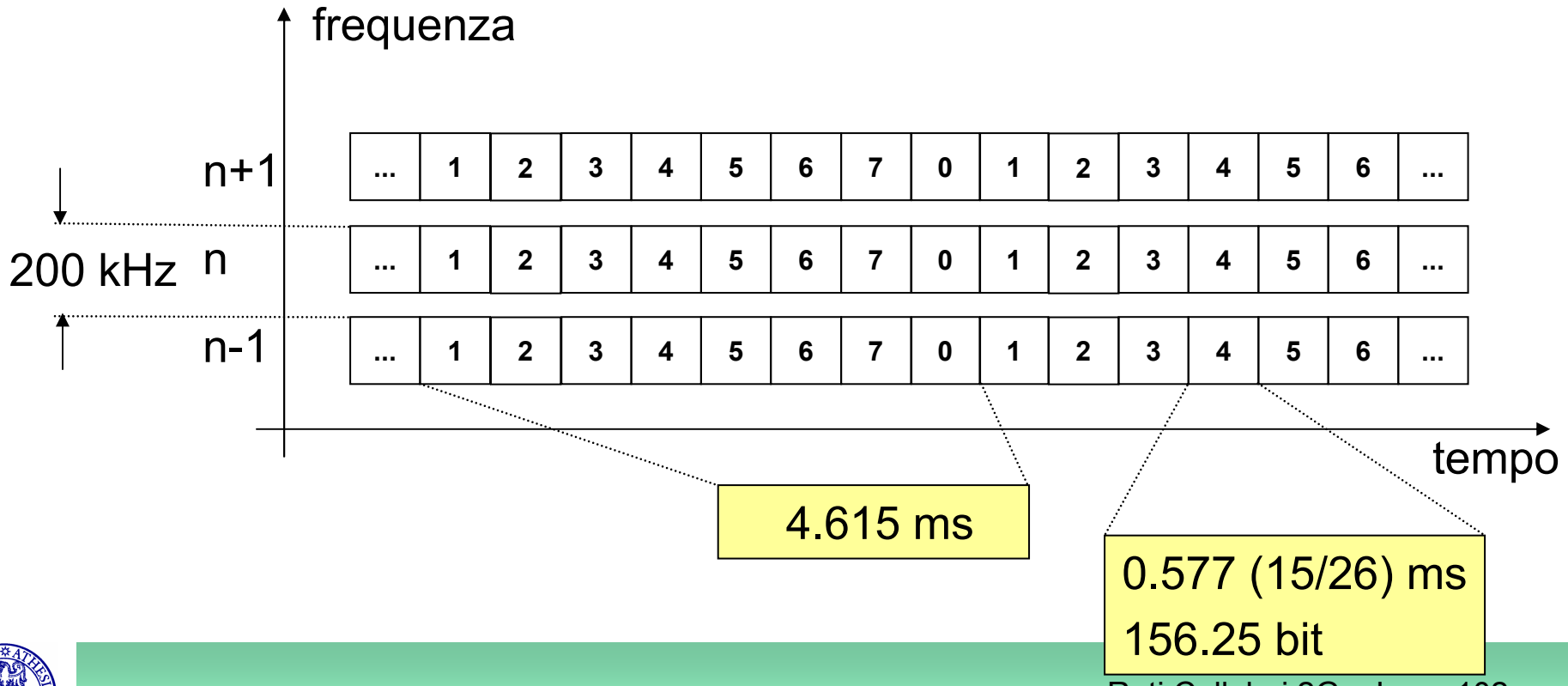
Struttura della trama GSM

- Ogni canale FDM è diviso in 8 canali TDM; la durata della trama TDM è di 4.615 ms (8x156.25 bit)
- La trasmissione bidirezionale in GSM è ottenuta mediante separazione sia in frequenza sia in tempo; in questo modo serve una sola interfaccia radio!
- Le trame sui canali uplink e downlink sono sincronizzate e sfalsate di 3 slot, in modo da consentire la separazione tra trasmissione e ricezione

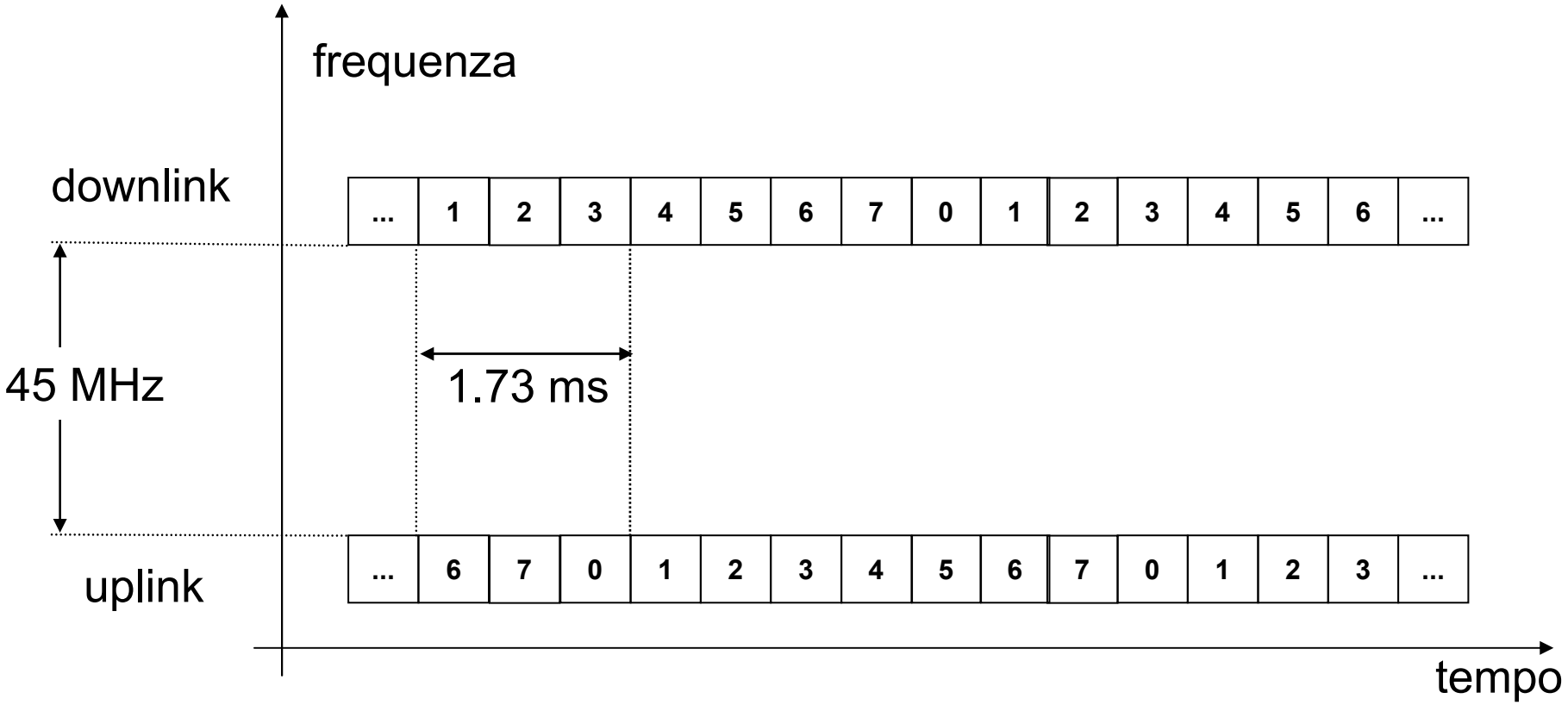


FDM/TDM

- Frequenza + time slot = canale
- Time slot adattati ai burst di trasmissione



FDM/TDM

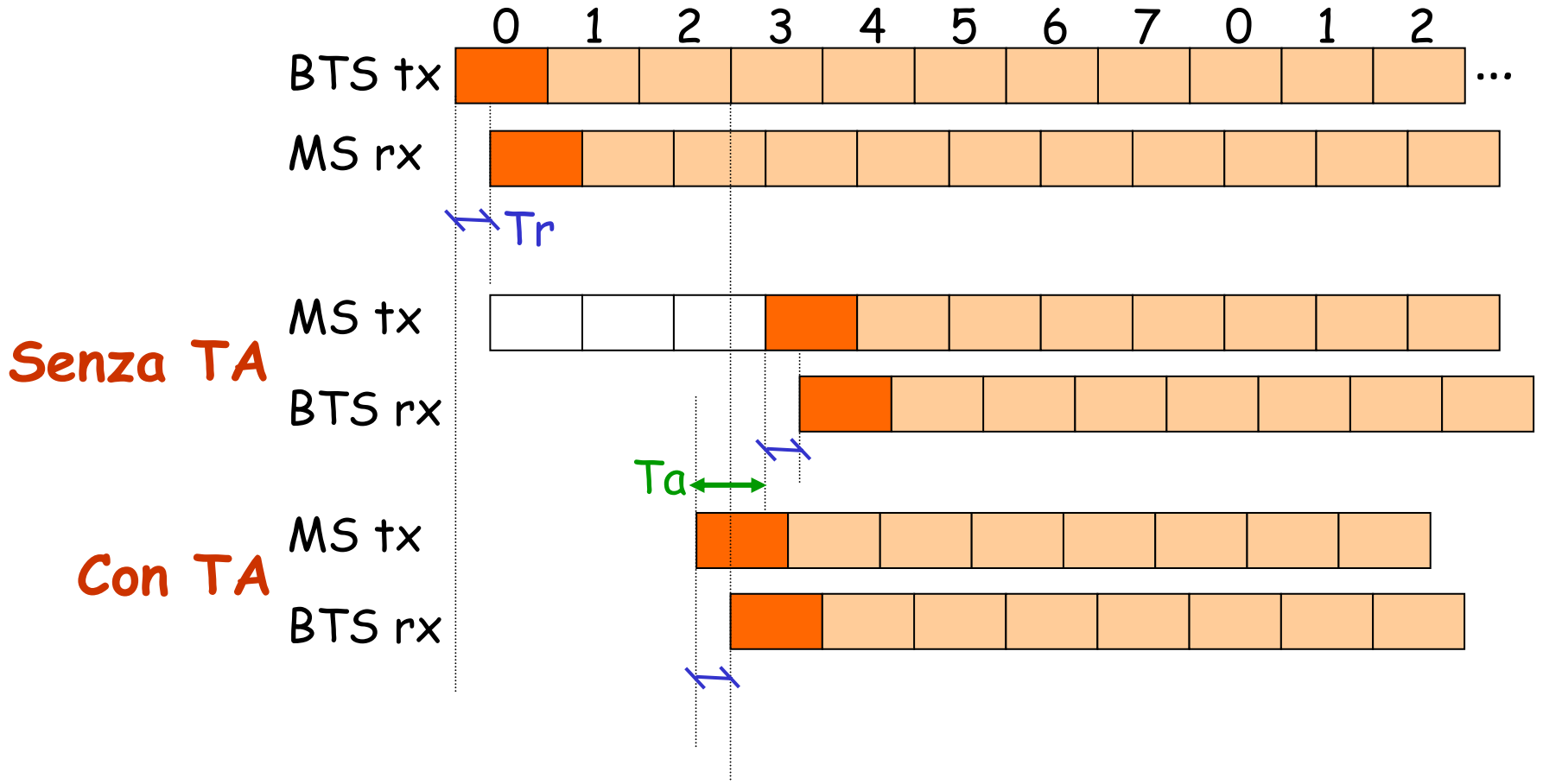

frequenza
downlink
... 1 2 3 4 5 6 7 0 1 2 3 4 5 6 ...
45 MHz
1.73 ms
uplink
... 6 7 0 1 2 3 4 5 6 7 0 1 2 3 ...
tempo

Avanzamento temporale (timing advance)

- Il non perfetto sincronismo tra MS produce interferenza tra timeslot vicini
- I terminali a distanza diversa dalla BTS subiscono ritardi di propagazione diversi
- La BTS ordina al terminale di anticipare la trasmissione di una quantità di tempo che compensa il ritardo di propagazione
- Nei timeslot si devono prevedere opportuni tempi di guardia



Avanzamento temporale (timing advance)



Tecnica di Accesso e Struttura dei Canali

- Per risparmiare le batterie e ridurre l'interferenza il trasmettitore RF viene spento quando non in conversazione e anche quando non vi è informazione da trasmettere durante una conversazione (soppressione dei silenzi)
- Spegnimento e accensione del trasmettitore RF pongono notevoli problemi di "ramping", cioè di transitorio per portare l'amplificatore a regime prima di cominciare la modulazione dei dati

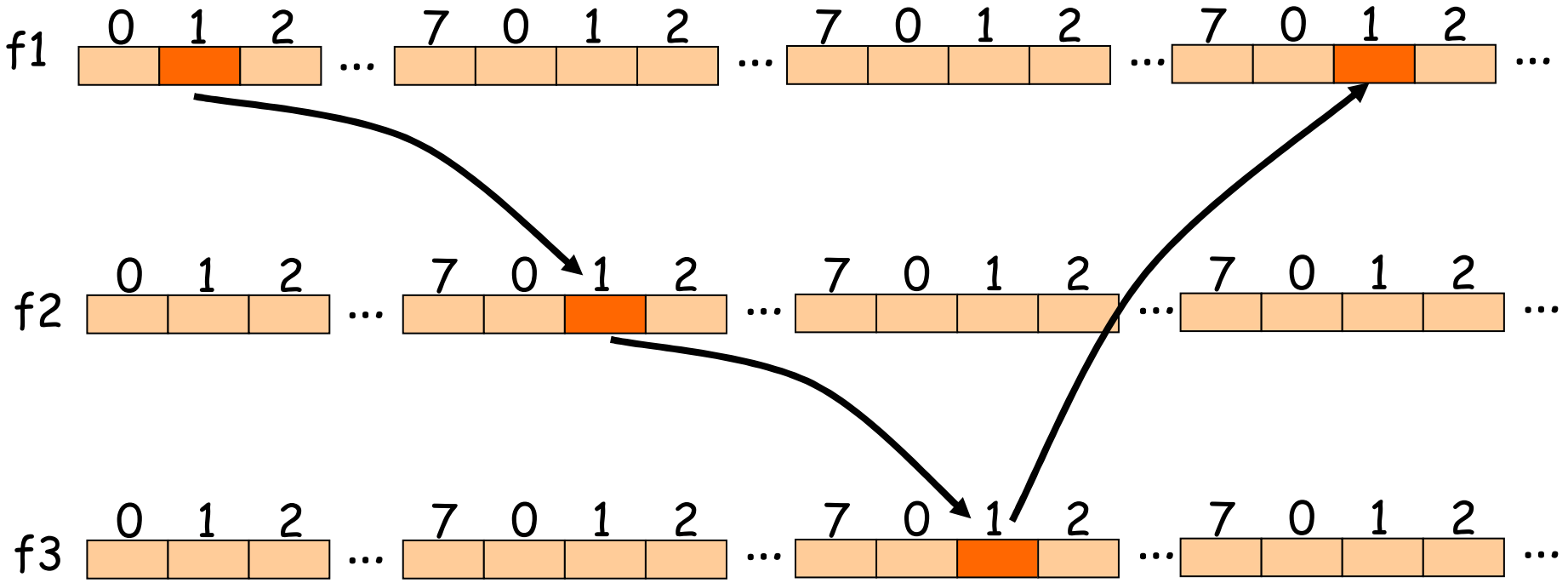


Frequency hopping

- In GSM è previsto di poter trasmettere messaggi consecutivi della stessa comunicazione su frequenze diverse (Frequency Hopping – FH)
- FH serve a ridurre gli effetti del fading da percorsi multipli: si guadagnano circa 2dB
- Il FH usato in GSM è "lento" perchè il cambio di frequenza avviene con cadenza di trama (8 slot - 4.615 ms) e non di pochi bit come in altri sistemi
- MS deve essere in grado di re-sintonizzare Tx ed Rx in circa 1 ms



Frequency hopping



FH - Modalità

- L'uso o meno di FH è una scelta dell'operatore
- Se la rete indica a MS di andare in modalità FH questo deve essere in grado di farlo
- Le sequenze di Hopping sono calcolate da BTS ed MS in base ad algoritmi di generazione di sequenze pseudo-casuali; in alternativa si può seguire un più semplice hopping ciclico
- Le modalità e la sequenza di hopping sono decise da BTS e trasmesse ad MS

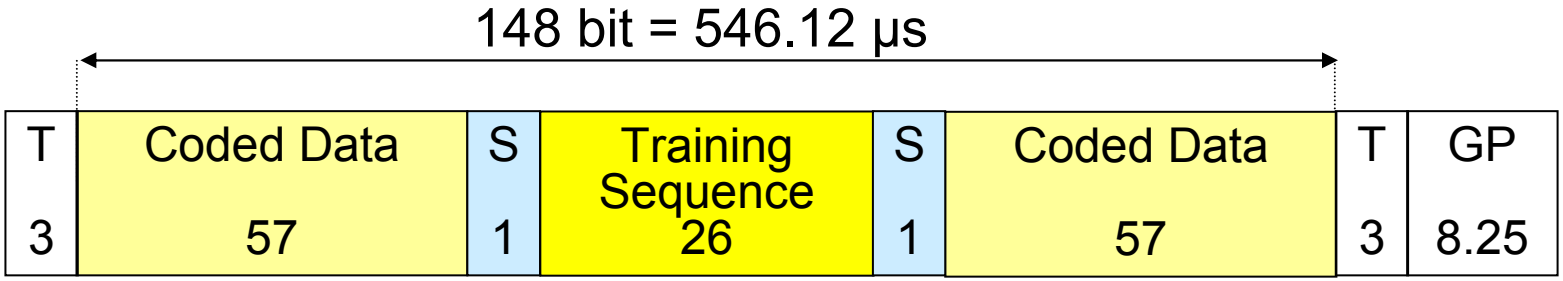


5 tipi di burst

- **normale:** per la trasmissione di messaggi sia sui canali di traffico che su quelli di controllo
- **accesso:** usati nelle fasi di setup quando MS non è ancora sincronizzato con BTS (solo uplink)
- **sincronizzazione:** inviati da BTS per la sincronizzazione dei MS (solo downlink)
- **correzione della frequenza:** inviati periodicamente da BTS per consentire la correzione degli oscillatori dei MS (solo downlink)
- **dummy:** inviati negli slot vuoti se è necessario tenere alta la potenza della portante



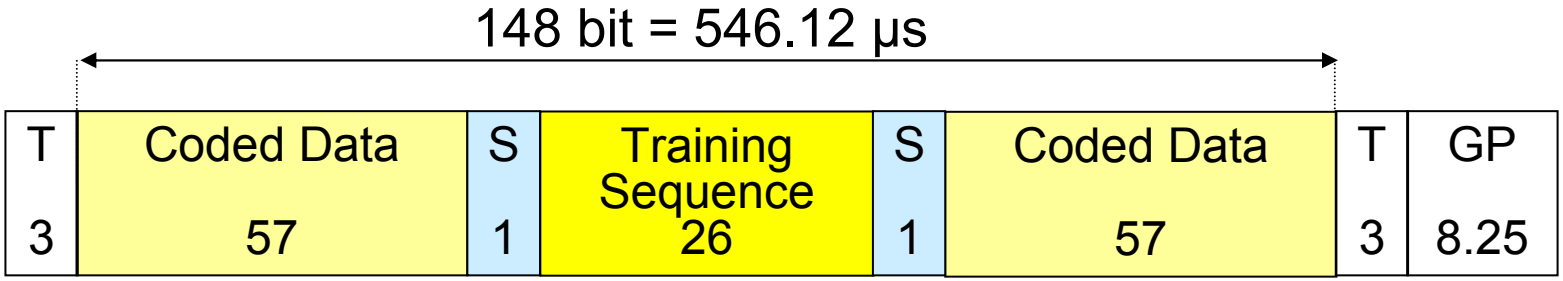
Struttura dei burst normali



- **Coded Data**: bit di utente (voce, dati etc.), 114 bit dopo la codifica di canale, che corrispondono a 13 kbit/s netti per la voce, a 9.6 kbit/s o meno per i dati (che usano una codifica di canale più ridondante)
- **Training Sequence**: bit di controllo usati per la sincronizzazione e per l'aggancio dei trasmettitori



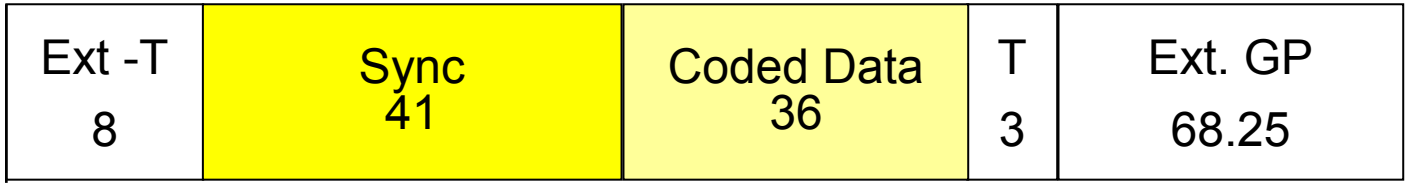
Struttura dei burst normali



- **T-bits**: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore
- **S-bits**: segnalano se il burst contiene dati utente (0) o segnalazione (1)
- **GP**: periodo di guardia per consentire l'accensione e lo spegnimento dei trasmettitori (pari a 30.46 µs, corrispondenti a circa 9 Km)



Struttura dei burst di accesso



- **T-bits**: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore (8 bit all'inizio del burst)
- **Sync-bits**: sequenza nota; consente l'aggancio del ricevitore alla BTS e il calcolo del timing advance
- **Coded Data**: bit di utente (dati),
- **Extended GP**: periodo di guardia allungato per garantire che il burst, trasmesso come se ci si trovasse alla massima distanza da BTS, non interferisca con lo slot successivo

  (68.25 bit $\cong$ 0.2525 ms)



Sincronizzazione e Dimensione delle celle

- La dimensione massima delle celle deve essere tale per cui il burst di accesso giunga alla BTS senza pericolo di interferenza con lo slot successivo
- In mancanza di altre informazioni MS si comporta come se il ritardo di propagazione tra MS e BTS fosse il massimo ammesso trasmettendo per un tempo ridotto
- Ne consegue (con un po' di approssimazione):

$$R_{max} = (c \times GP)/2 = 37.5 \text{ km}$$

- in realtà, per convenzione si assume come raggio massimo 35 km



Struttura dei burst di sincronizzazione

T 3	Coded Data 39	Ext. Training Sequence 64	Coded Data 39	T 3	GP 8.25

- **T-bits**: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore
- **Extended training sequence-bits**: sequenza nota; consente l'aggancio del ricevitore alla BTS
- **Coded Data**: bit di segnalazione per la trasmissione dei dati relativi alla sincronizzazione globale. Contengono anche informazioni per identificare la rete (operatore) cui appartiene la cella e la cella stessa (Location Area e codice di cella)
- **GP**: periodo di guardia



Struttura dei burst di correzione di frequenza

- **T-bits**: posti sempre a 0, usati come tempi di guardia e per l'inizializzazione del demodulatore
- **GP**: periodo di guardia

- La sequenza di tutti zero, data la modulazione GMSK, equivale a trasmettere una sinusoide pura per tutta la durata del burst

T 3	Sequenza di tutti 0 142	T 3	GP 8.25



Struttura dei burst dummy

- Sono burst normali in cui al posto dei dati vengono trasmessi tutti zero
- I bit di stealing sono eliminati
- Vengono usati solo dalle BTS per consentire ai MS le misure di potenza

T	All zero	Training Sequence	All zero	T	GP
3	58	26	58	3	8.25



Assegnazione delle risorse alle celle

- Ciascuna cella GSM può avere da 1 a 16 portanti
- Lo slot '0' di una delle portanti è usato per un canale broadcast downstream su cui vengono trasmessi i burst di correzione della frequenza e di sincronizzazione. Questa frequenza è chiamata **C0** ed è la "portante principale" della cella
- Su C0 la BTS trasmette in modo continuo, usando burst dummy se non ha dati da trasmettere
- Se ci sono più di tre portanti in una cella è possibile abilitare la funzione di Frequency Hopping (FH) per ridurre gli effetti del fading veloce



Canali fisici GSM

- Un canale fisico è definito da un time-slot ogni trama
- La velocità di trasmissione (lorda) è

  148bit/4.615ms ≅ 32kbit/s
- Nei burst normali i bit utili (a valle della codifica) sono 114 per time-slot ≅ 24.7kbit/s
- I dati utente sono protetti da codici, la velocità di trasmissione per l'utente dipende dallo schema di codifica, 13kbit/s + codifica = ~ 22.8 kbit/s
- I restanti 24.7-22.8=1.9 kbit/s sono usati per la segnalazione



Canali fisici GSM

- Sui canali fisici sono mappati i canali logici
- Lo schema di codifica dipende dal canale logico
- La mappatura dei canali logici sui canali fisici fa riferimento ad uno schema di temporizzazione assoluto che definisce trame, supertrame (di traffico e controllo) e ipertrame

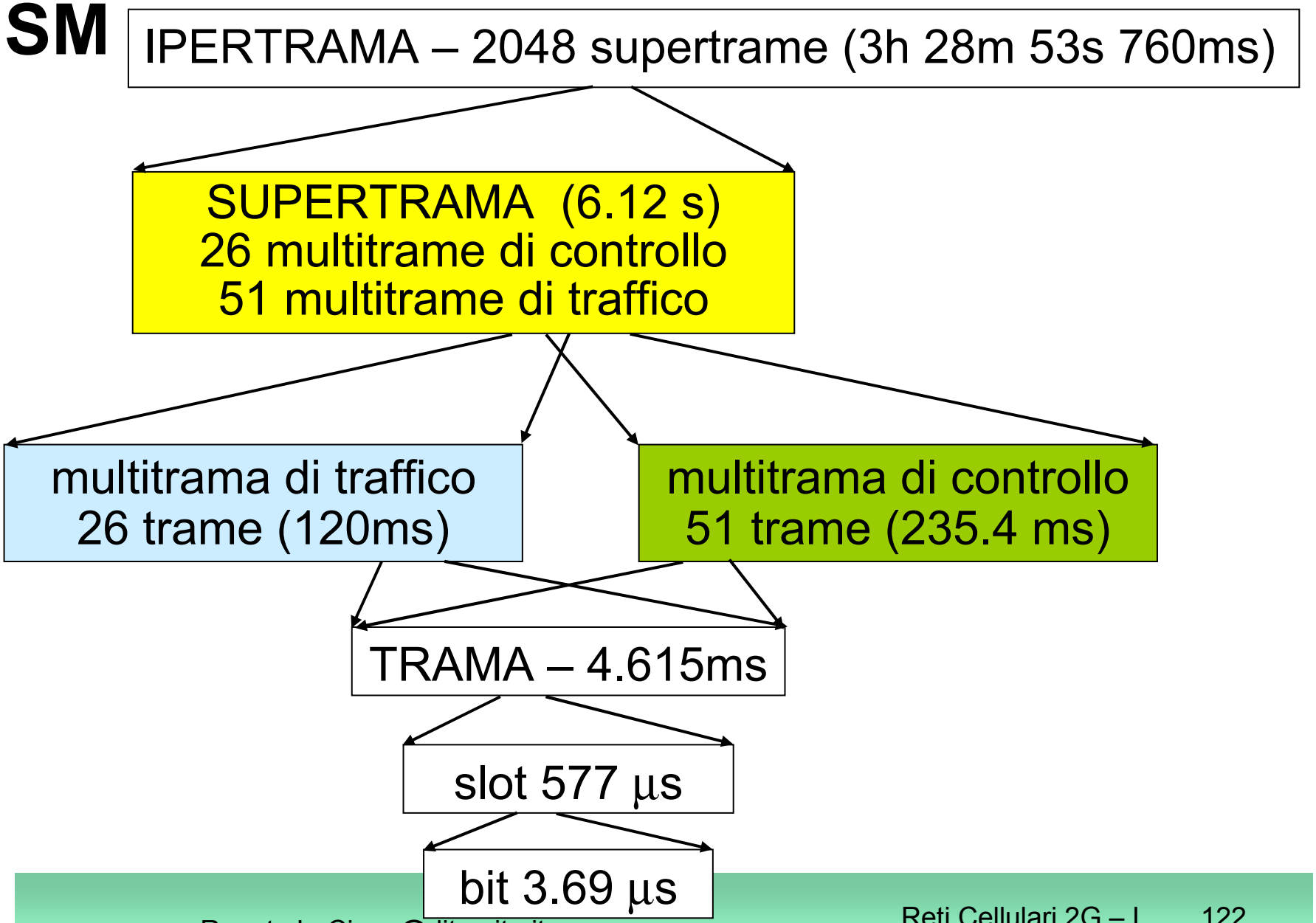


Tramatura GSM

- TRAMA – 8 slot TDMA (4.615ms)
- MULTITRAMA DI TRAFFICO – 26 trame (120ms)
- MULTITRAMA DI CONTROLLO – 51 trame (235.4 ms)
- SUPERTRAMA – 26 multirame di controllo, ovvero 51 multitrame di traffico (6.12 s)
- IPERTRAMA – 2048 supertrame (3h 28m 53s 760ms)



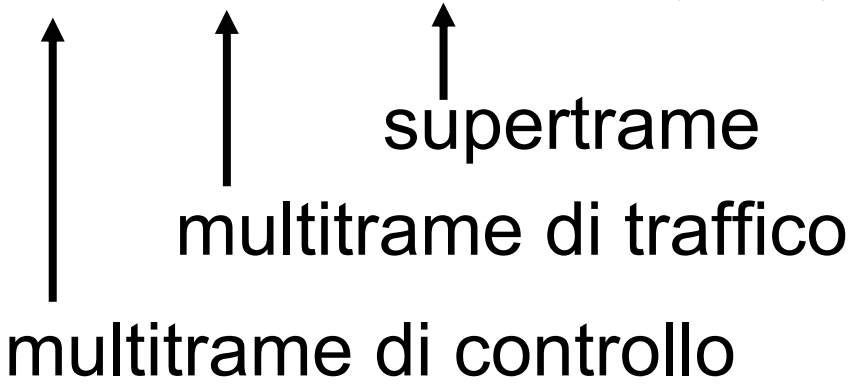
Tramatura GSM



Temporizzazione GSM

- Il modulo di frame number (FN) è

  26 * 51 * 2048 = 2.715.647



- FN viene trasmesso da BSC nei burst di sincronizzazione

Temporizzazione GSM

- Il "quanto" di tempo in GSM è un quarto del tempo di bit
- Il tempo e` misurato in:
  - Quarter-bit number QN 0-624
  - Bit Number BN 0-156
  - Time slot Number TN 0-7
  - Frame Number FN 0-2,715,647

- QN, BN e TN sono calcolati localmente da MS, inizializzandoli sugli slot in cui viene trasmesso FN



GSM: I canali logici

Renato Lo Cigno
www.dit.unitn.it/locigno/didattica/wn/



I canali del GSM

- I **canali fisici:**
  - Sono la combinazione di un timeslot e una frequenza portante
  - 8 canali fisici per portante: timeslot 0 - 7
- I **canali logici** portano le informazioni utili e sono mappati sui canali fisici secondo opportuni criteri



Canali logici

I canali logici si dividono in

- **Canali di controllo:**

portano le informazioni di segnalazione (di rete e di utente)

- **Canali di traffico:**

portano le informazioni utili degli utenti



Canali di controllo

- **Segnalazione di rete:**
  - Parametri della cella
  - Sincronizzazione
  - Sintonizzazione del ricevitore
- **Segnalazione di utente:**
  - Controllo delle chiamate
  - Controllo della qualità del segnale (distribuzione delle misure)



Canali di controllo

Segnalazione di rete:

- **Broadcast CHannels, BCH o canali di distribuzione**: Canali per informazioni di interesse generale
  - Frequency Correction CHannel, FCCH
  - Synchronization CHannel, SCH
  - Broadcast Control CHannel, BCCH



Canali di controllo

Segnalazione di utente:

- **Common Control CHannels, CCCH o canali di controllo comuni**: Per la fase preliminare in cui non è ancora stato assegnato un canale di segnalazione alla connessione
- **Dedicated Control CHannels, DCCH o canali di controllo dedicati**: Per la segnalazione di una specifica connessione



Frequency Correction CHannel (FCCH)

- Permette la correzione di frequenza al MS
- E' una sequenza di 148 bit che specifica la frequenza dalla portante
- E' un canale monodirezionale down-link



Synchronization CHannel (SCH)

Trasporta in 25 bit le seguenti informazioni:

- Base Station Identity Code (BSIC): 6 bit che identificano la stazione base, l'operatore e il colour code
- Reduced TDMA Frame Number (RFN): 19 bit che identificano il numero di trama
- E' un canale monodirezionale down-link



Broadcast Control CHannel (BCCH)

Trasporta in 184 bit informazioni generali sulla cella e sulla rete:

- Numero di canali di controllo comuni
- Numero di blocchi riservati al canale AGCH nei canali di controllo comuni
- Distanza dei messaggi di paging verso lo stesso terminale (in multipli di 51 trame)



Broadcast Control CHannel (BCCH)

- Parametri dell'algoritmo di frequency hopping:
  - CA: Cell Allocation
  - MA: Mobile Allocation
  - MAIO: MA Index Offset
  - HSN: Hopping Sequence generator Number
- E' un canale monodirezionale down-link



Uso dei canali di controllo di tipo broadcast

1. MS si accende
2. MS scandisce l'intera banda GSM cercando un segnale (in alternativa, cerca tra alcune frequenze memorizzate nella SIM)
3. Quando trova il segnale più forte (C0), il MS cerca il **Broadcast Control Channel (BCCH)**
   - BCCH porta l'informazione di controllo
   - BCCH è diverso in ogni cella



Uso dei canali di controllo di tipo broadcast

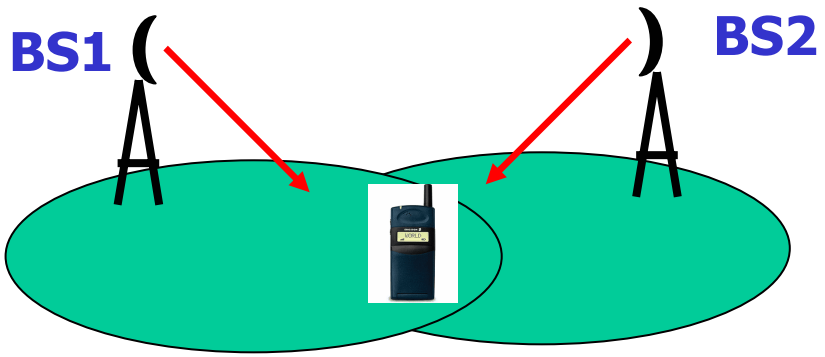
Per essere in grado di leggere l'informazione del BCCH, il MS deve prima:

1. Sintonizzarsi sulla frequenza della cella, tramite il canale FCCH
2. Sincronizzarsi con i dati trasmessi nella cella, tramite il SCH



Aggiornamento delle informazioni di controllo

- Le stazioni base non sono sincronizzate tra loro
- Ogni volta che la MS cambia cella deve nuovamente ricevere le informazioni su FCCH, SCH, BCCH, relative a quella cella



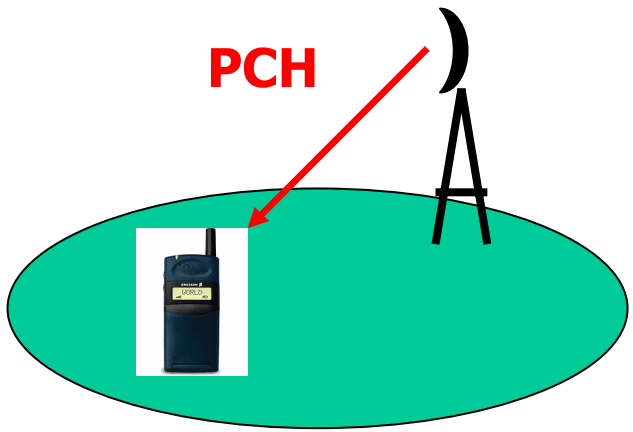
Canali di controllo comuni

- Servono per la fase di inoltro di una richiesta di connessione
- Sono unidirezionali
  - Paging CHannel (PCH)
  - Random Access CHannel (RACH)
  - Access Grant CHannel (AGCH)



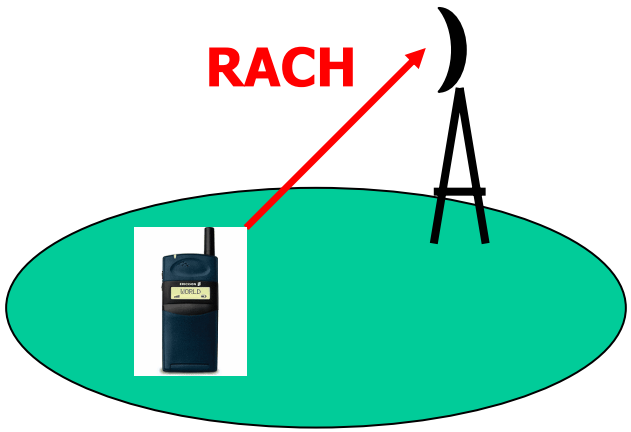
Paging CHannel (PCH)

- E' unidirezionale downlink
- E' utilizzato per notificare a un terminale una chiamata entrante
- E' trasmesso in tutte le celle della stessa Location Area



Random Access CHannel (RACH)

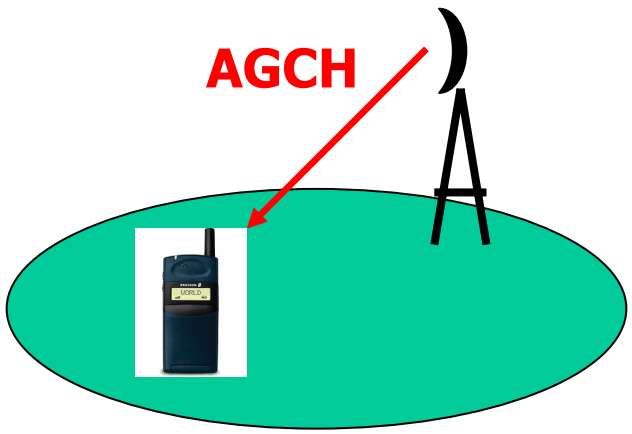
- E' unidirezionale uplink
- E' utilizzato per chiedere l'accesso alla rete:
  - inizio chiamata
  - richiesta di location update
- E' soggetto a collisioni





Access Grant CHannel (AGCH)

- E' unidirezionale downlink
- E' utilizzato per rispondere a una richiesta della MS, ricevuta su RACH
- Alloca un canale di segnalazione detto Stand-alone Dedicated Control CHannel (SDCH)



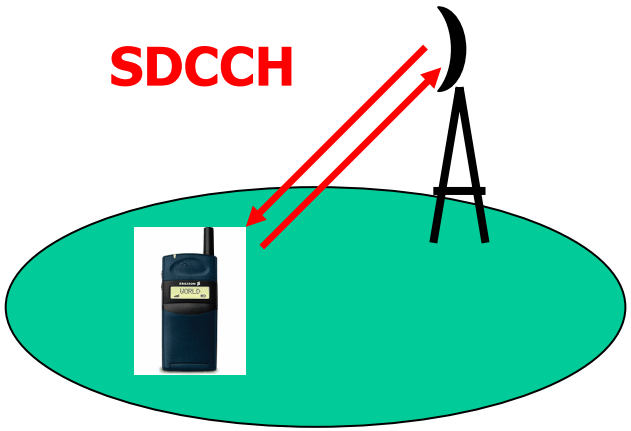
Canali di controllo dedicati Dedicated Control CHannels (DCCH)

- Servono per il controllo di chiamata
- Sono bidirezionali (uplink e downlink)
  - Stand Alone Dedicated Control Channel (SDCCH)
  - Slow Associated Control Channel (SACCH)
  - Fast Associated Control Channel (FACCH)



Stand-alone Dedicated Control CHannel (SDCCH)

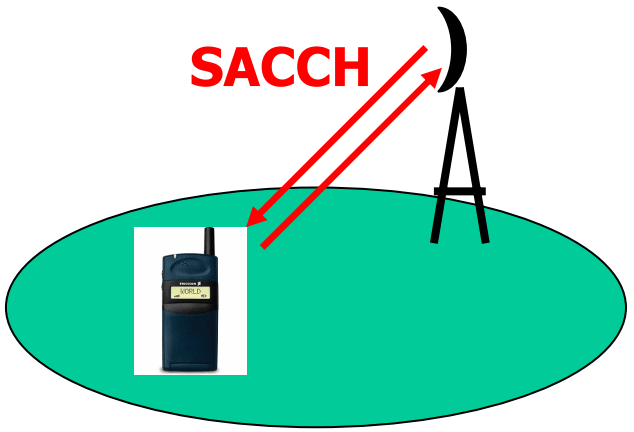
- Assegnato dalla BS tramite il canale AGCH
- Usato per lo scambio di informazioni di autenticazione, identificazione, call set-up
- Usato prima dell'assegnazione di un canale di traffico alla chiamata





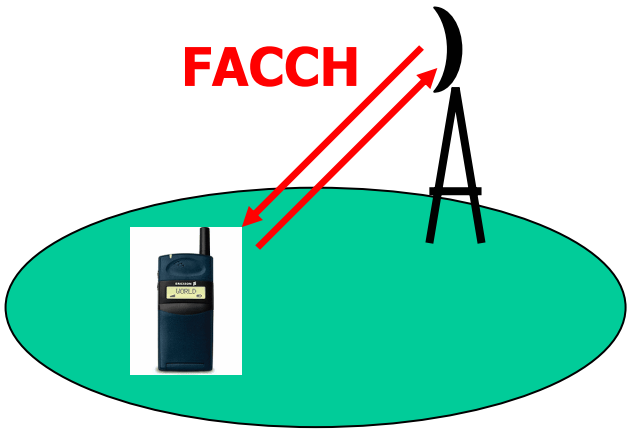
Slow Associated Control CHannel (SACCH)

- In downlink trasporta le informazioni di
  - Misurazioni della BTS
  - Controllo di potenza
  - Informazioni del BCCH che sarebbero perse dal MS cui è stato assegnato un canale di traffico
- In uplink (184 bit ogni 20ms)
  - Misurazioni della MS



Fast Associated Control CHannel (FACCH)

- Per segnalazione immediata di parametri che non possono attendere i tempi del SACCH
  - Tipicamente per handover immediato
- L'informazione è inviata, in *stealing mode*, al posto dell'informazione vocale (20 ms di parlato)



Uso dei canali di controllo Riepilogo

All'accensione del MS

1. MS cerca il segnale più forte
2. Frequency Correction CHannel, FCCH
3. Synchronization CHannel, SCH
4. Broadcast Control CHannel, BCCH
5. Se la rete non è ammessa (p. es. Altro operatore) ripete la procedura per il succesivo canale più forte



Uso dei canali di controllo Riepilogo

Quando la rete deve contattare il MS

1. Usa il Paging CHannel, PCH
2. MS risponde tramite il Random Access CHannel, RACH
3. La rete assegna un canale di segnalazione dedicato (SDCCH) tramite il canale Access Grant Channel, AGCH



Uso dei canali di controllo Riepilogo

Quando il MS deve contattare la rete

1. MS usa il Random Access CHannel, RACH
2. La rete assegna un canale di segnalazione dedicato (SDCCH) tramite il canale Access Grant Channel, AGCH



Canali di traffico

Trasportano voce o dati di utente

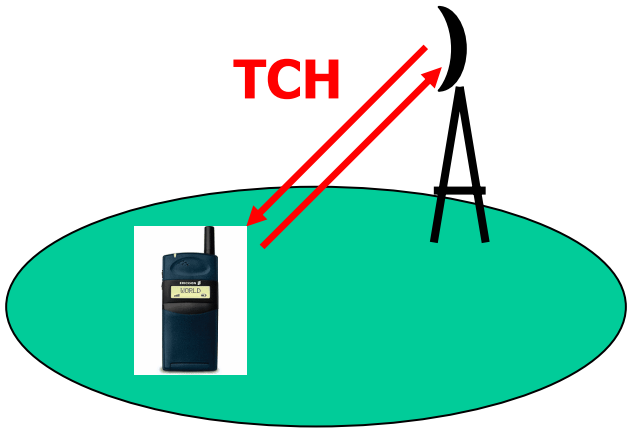
- Canali a velocità piena (Full rate Traffic CHannel: TCH/F) pari a 22.8 Kbit/s
- Canali a velocità dimezzata (Half rate Traffic CHannel: TCH/H) pari a 11.4 Kbit/s
  - 2 TCH/H condividono lo stesso canale fisico in trame alterne

Un canale di traffico viene assegnato a una connessione per tutta la durata della chiamata



Canali di traffico

- La trasmissione di voce avviene a commutazione di circuito
- La voce usa un solo canale di traffico
- Due possibili velocità
  - Full rate: 13 Kbit/s
  - Half rate: 6.5 Kbit/s

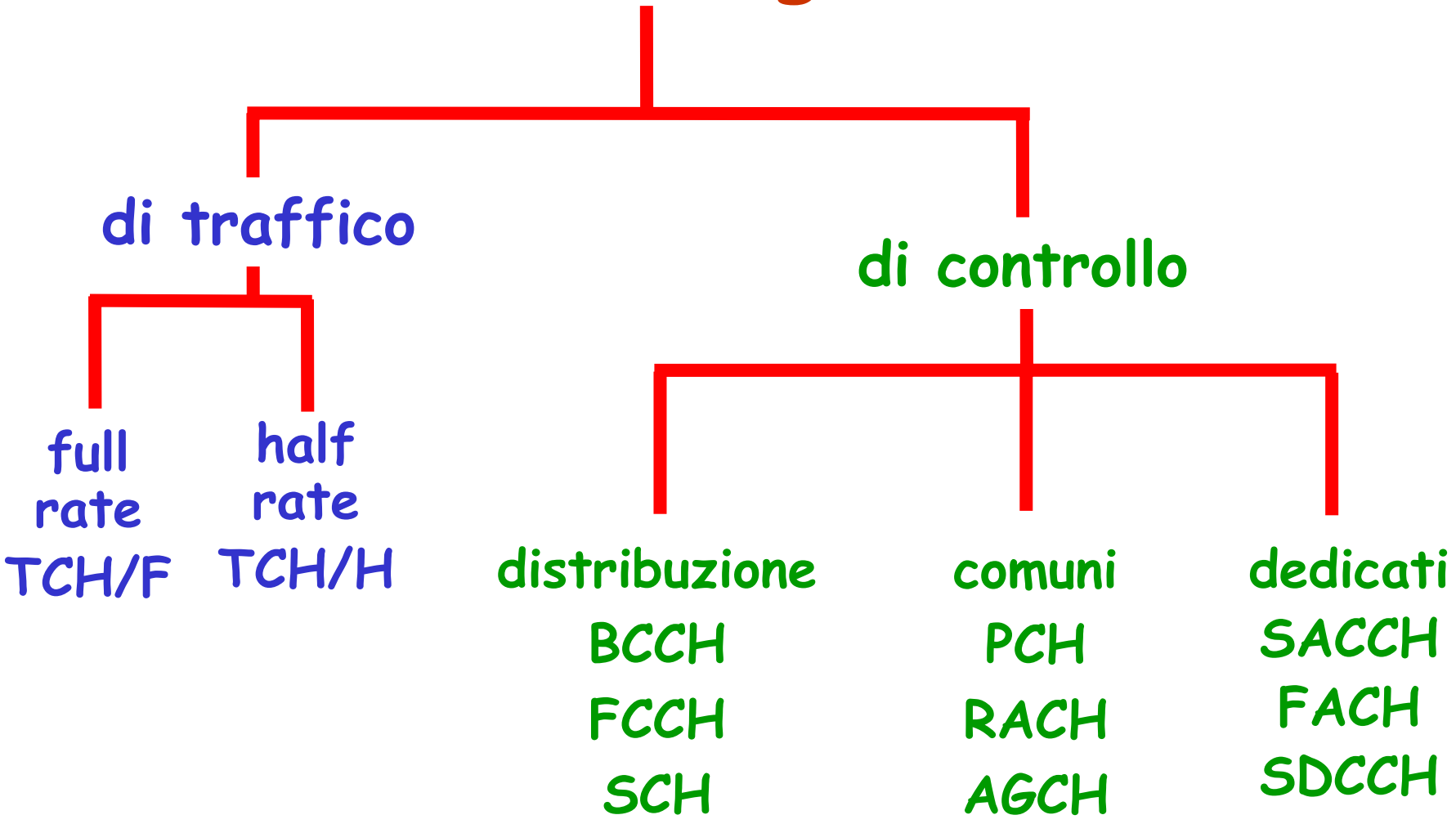


Canali di traffico

- La trasmissione di dati voce avviene a *commutazione di circuito*
- La trasmissione usa un solo canale di traffico
- La velocità di trasmissione dipende dalla codifica FEC impiegata:
  - Full rate: 4.8 o 9.6 o 14.4 Kbit/s
  - Full rate e utenti veloci: 2.4 Kbit/s
  - Half rate: 2.4 o 4.8 Kbit/s



Canali logici





SMS

- Lunghi 160 caratteri
- Scambiati tra un Centro Servizi e il MS
- Se il MS è spento, la rete GSM informa il Centro Servizi che inoltrerà il messaggio all'accensione del MS
- Se il MS è acceso ma idle si usa il SDCCH
- Se il MS è attivo si usa il SACCH
- Il MS notifica la ricezione del SMS
- Al MS il messaggio è memorizzato nella SIM



Canali logici e tipi di burst

Il burst di tipo normale è usato per:

- **TCH** -> canali di traffico utente
- **BCCH**
- **PCH**
- **SACCH**
- **FACCH**
- **SDCCH**

} segnalazione



Canali logici e tipi di burst

Il burst di tipo correzione di frequenza:

- **FCCH**

Il burst di tipo sincronizzazione:

- **SCH**

Il burst di tipo accesso:

- **RACH**



GSM: Le procedure

Renato Lo Cigno
www.dit.unitn.it/locigno/didattica/wn/



Esempi di procedure

- Registrazione all'accensione
- Roaming e location update
  - Nella stessa location area
  - Nella stessa MSC/VLR service area
  - Tra MSC/VLR service area diverse
- Chiamata originata da mobile
- Chiamata diretta a un mobile
- Handover
  - Intra-cella
  - Tra BTS dello stesso BSC
  - Tra BSC diverse ma stesso MSC/VLR
  - Tra BSC diverse e diverso MSC/VLR
- Procedura di detach



Accensione di un terminale

- Quando il MS è spento, l'IMSI del MS è marcato come *detached* nell'ultimo VLR visitato
- All'accensione, il MS scandisce le portanti radio alla ricerca del BCCH che sente meglio (il BCCH non è soggetto a frequency hopping)
- Il MS si sintonizza tramite il FCCH
- Il MS acquisisce il sincronismo sul SCH
- Tramite il BCCH, il MS acquisisce informazioni sulla rete, tra cui il LAI

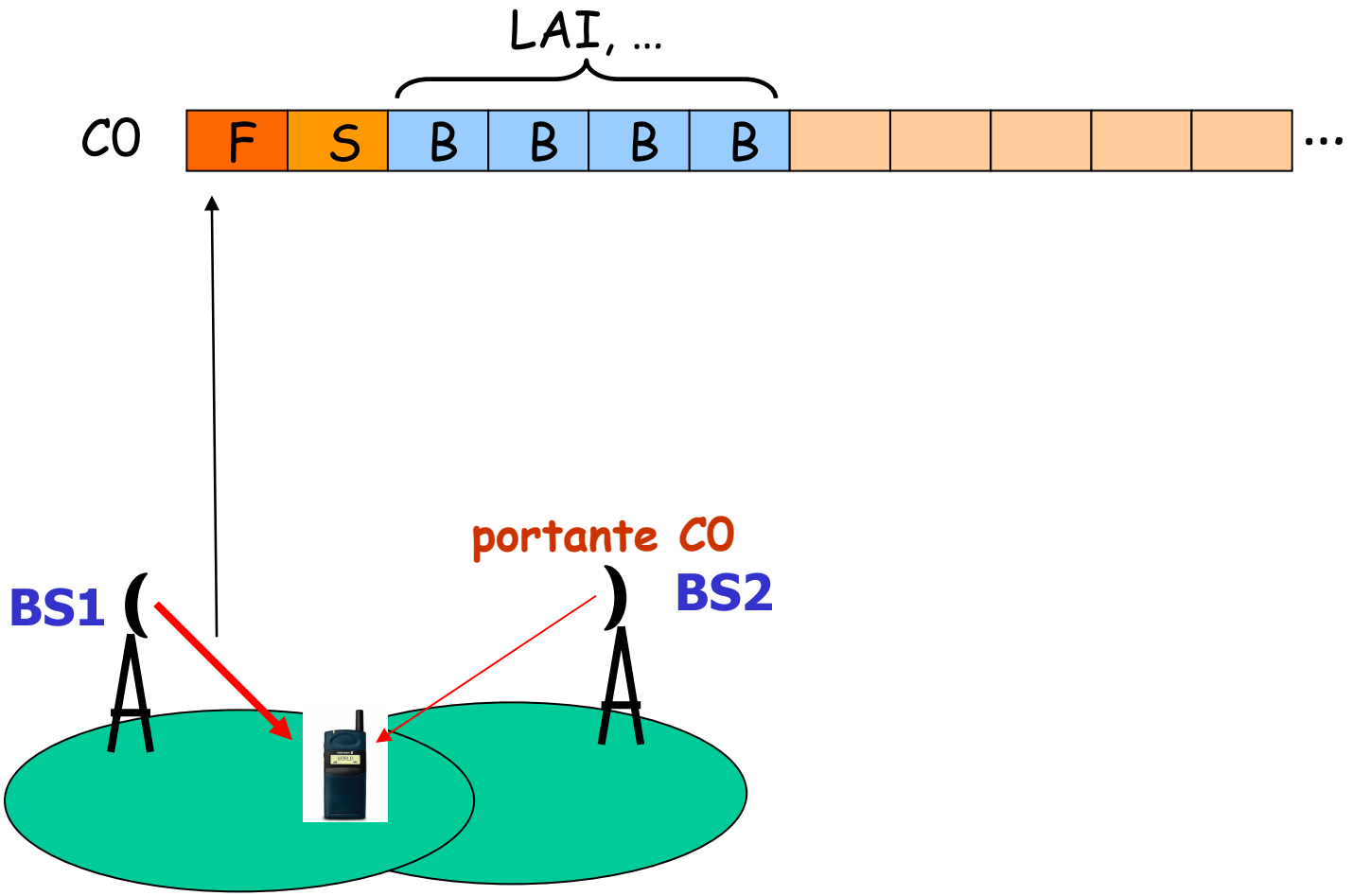


Accensione di un terminale

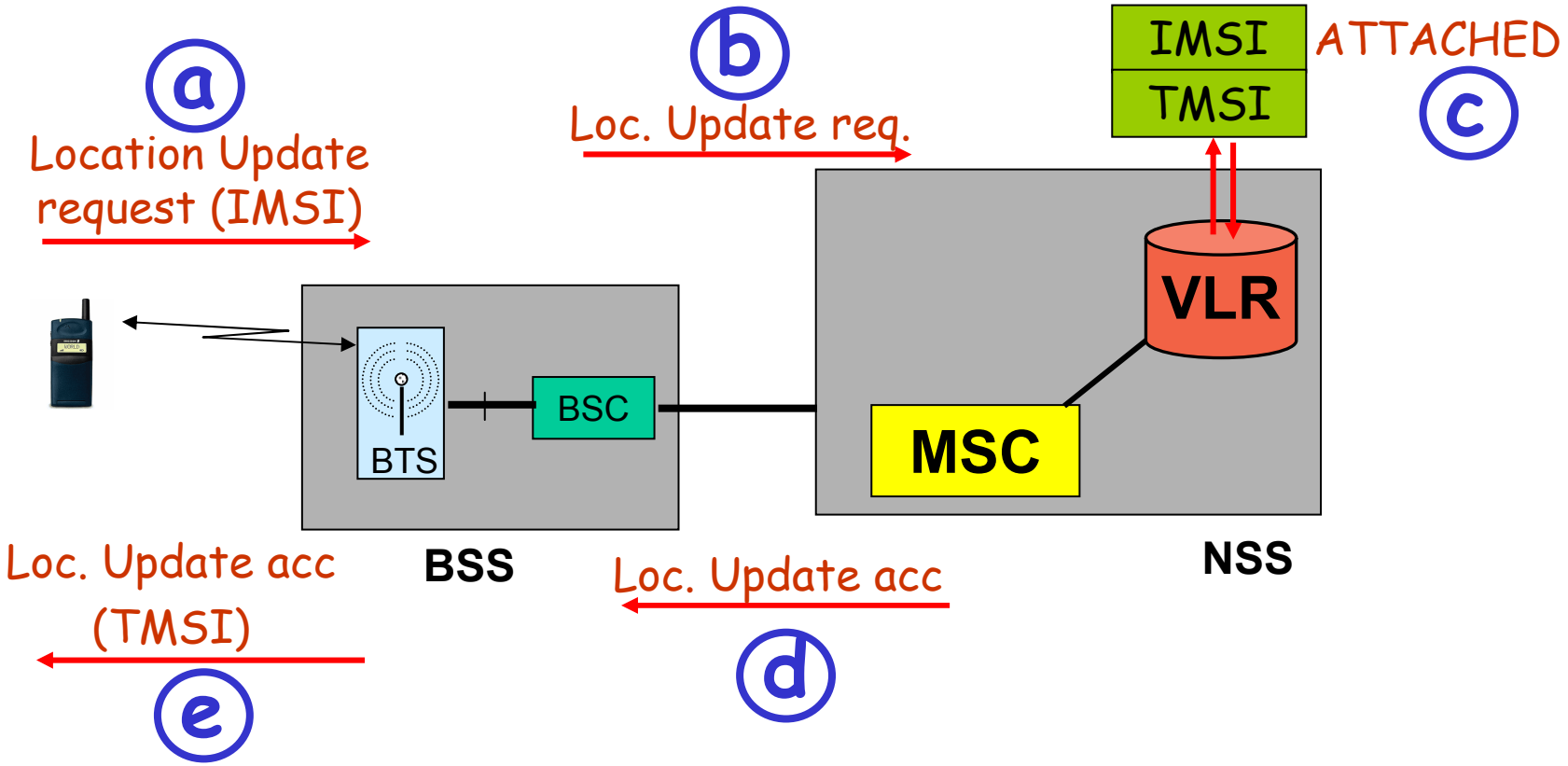
- Se il LAI è uguale a quello memorizzato nel MS si esegue la procedura *IMSI attach*
  - Il VLR registra l' IMSI del MS come *attached*
- Se il LAI è diverso (o se nessun LAI è memorizzato nel MS) si esegue la procedura *first registation*
  - MS richiede Location Updating inviando l' IMSI
  - VLR contatta HLR per aggiornare il puntatore e ottenere dati sul MS, marca il IMSI come attached
  - Il VLR risponde assegnando un TMSI



Accensione di un terminale



Accensione di un terminale

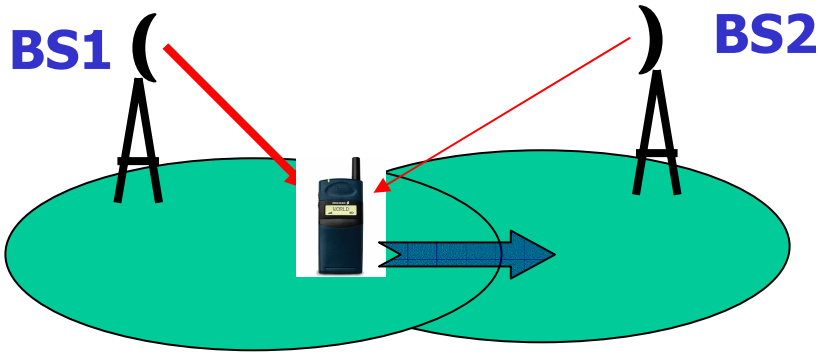


Roaming entro una LA

- Mentre si sposta, il MS misura la potenza ricevuta sul BCCH della BTS cui è agganciato e sui BCCH delle BTS che riesce a sentire
- Il MS si aggancia alla BTS che riceve meglio
- Il cambiamento di BTS (cella) è una decisione autonoma del MS
- Non è necessario avvertire la rete, perché la LA non è cambiata

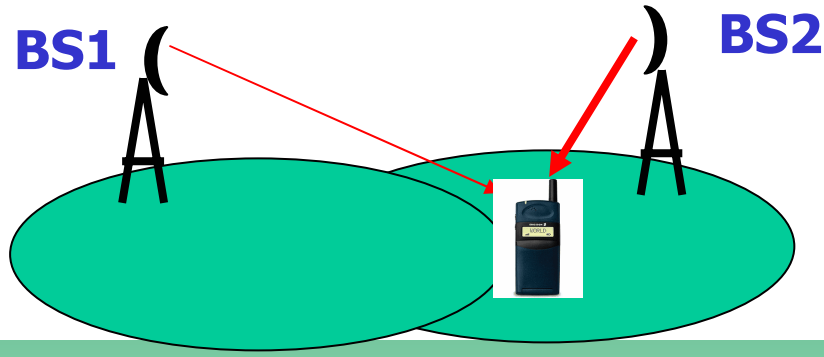


Roaming entro una LA



MS è agganciata
a BS1

MS si aggancia
a BS2



Roaming entro una VLR service area

- Il MS sul nuovo BCCH riceve un LAI diverso dal precedente
- Il MS invia una richiesta di accesso sul RACH
- La BTS assegna un SDCCH al MS tramite AGCH
- Il MS invia una richiesta di Location Update contenente il TMSI e il vecchio LAI
- Procedura di autenticazione
- Procedura di cifratura



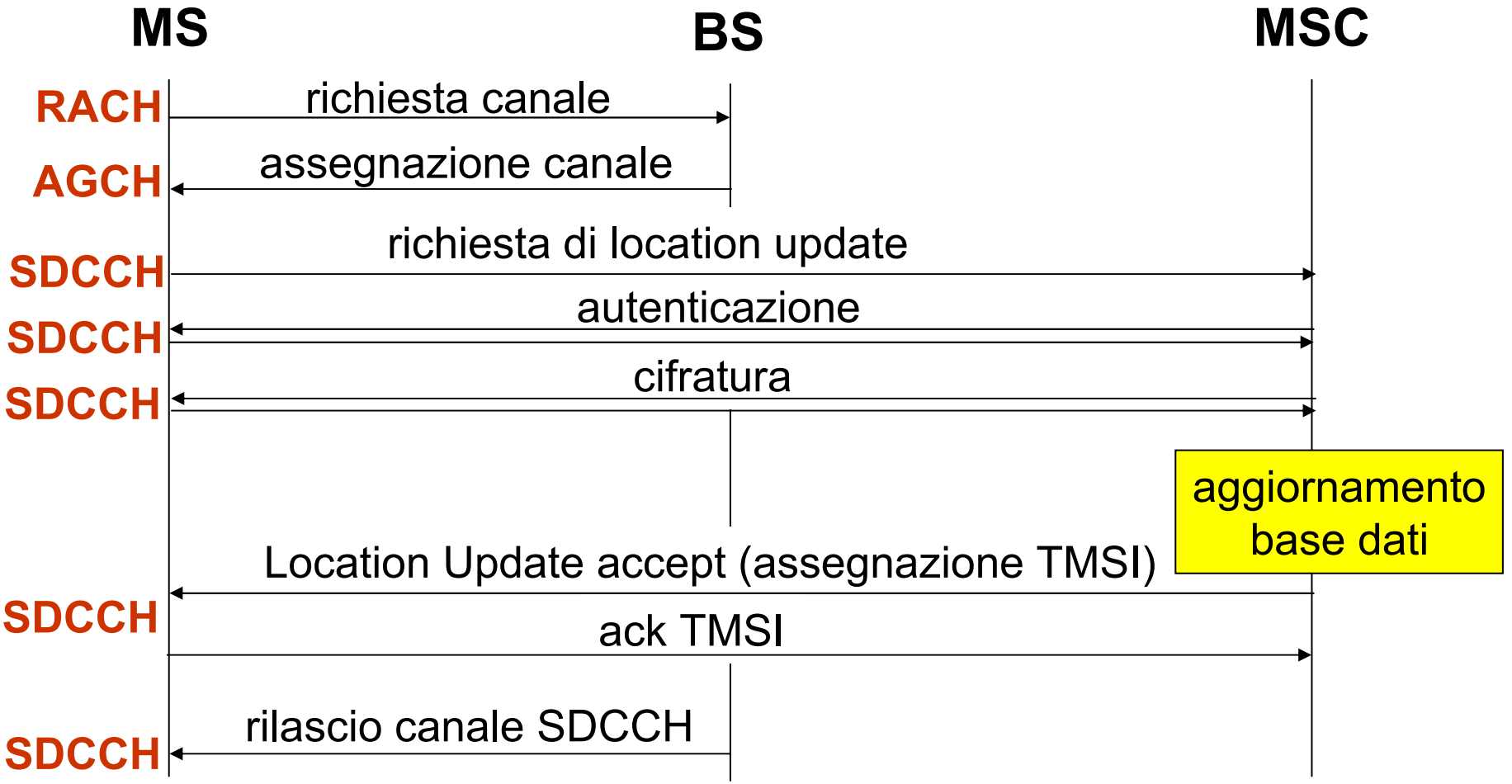
Roaming entro una VLR service area

- L'MSC accetta la nuova localizzazione, aggiorna il VLR e riassegna il TMSI al MS
- Il MS conferma la ricezione del nuovo TMSI
- Il BSC rilascia il SDCCH

(HLR non è informato del cambiamento perché il VLR non è cambiato)



Roaming entro una VLR service area: Procedura di Location Update



Roaming tra MSC service area diverse

La prima parte della procedura è identica:

- Il MS sul nuovo BCCH riceve un LAI diverso dal precedente
- Il MS invia una richiesta di accesso sul RACH
- La BTS assegna un canale al MS tramite AGCH
- Il MS invia una richiesta di Location Update sul SDCCH contenente il TMSI e il vecchio LAI
- Procedura di autenticazione
- Procedura di cifratura



Roaming tra MSC service area diverse

Nella seconda parte si cambia MSC:

- L'MSC contatta il vecchio VLR per ottenere i dati del MS
- L'MSC contatta l' HLR affinché aggiorni il puntatore al VLR
- L'HLR ordina al vecchio VLR di cancellare i dati del MS
- L'MSC accetta la nuova localizzazione e riassegna il TMSI al MS

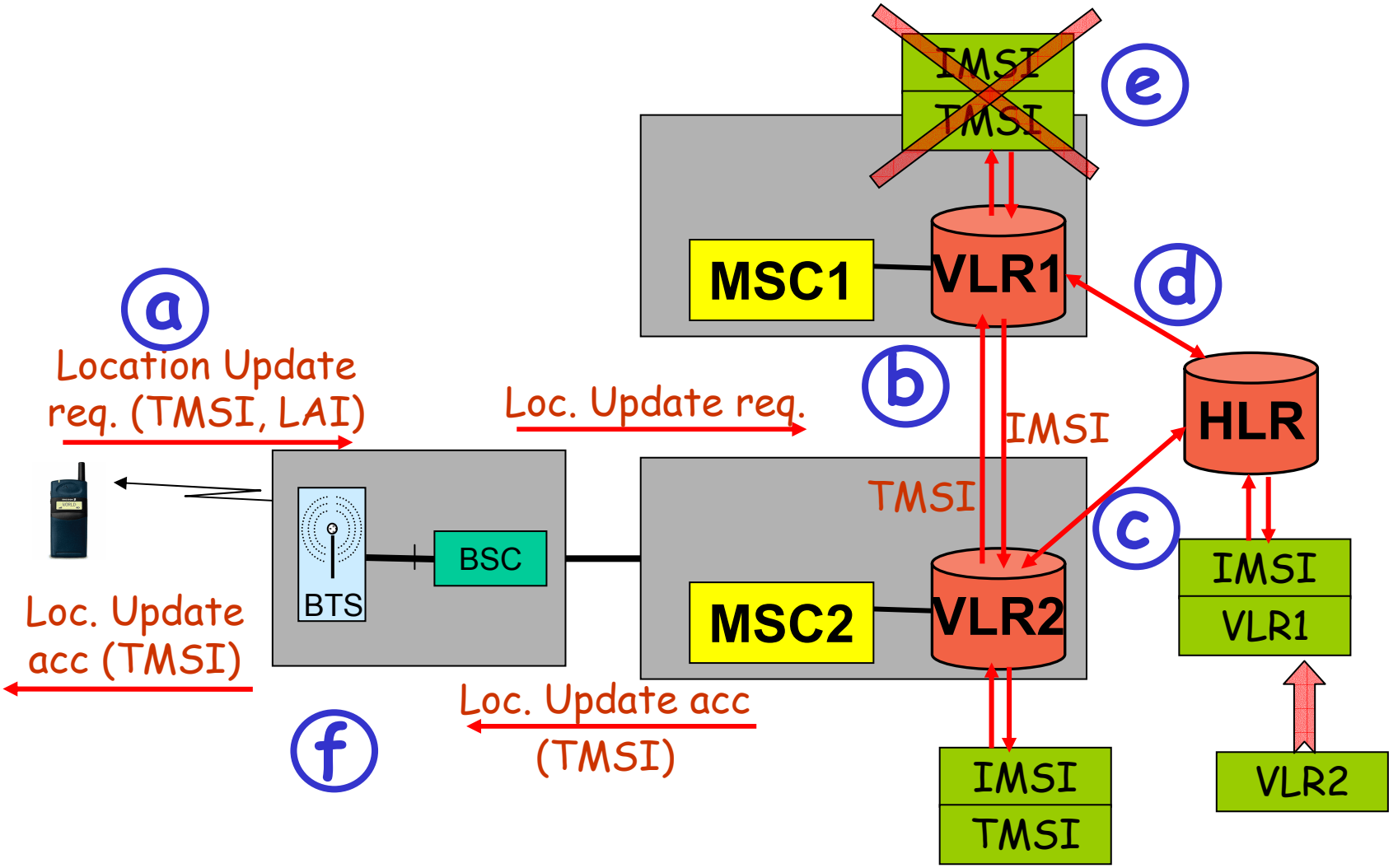


Roaming tra MSC service area diverse

- Il MS conferma la ricezione del nuovo TMSI
- Il BSC rilascia il SDCCH



Roaming tra MSC service area diverse



Chiamata originata dal MS

- L'utente compone il numero
- Il MS invia una richiesta di accesso sul RACH
- La BTS assegna un canale al MS tramite AGCH
- Il MS invia una richiesta di servizio sul SDCCH
- Procedura di autenticazione
- Procedura di cifratura

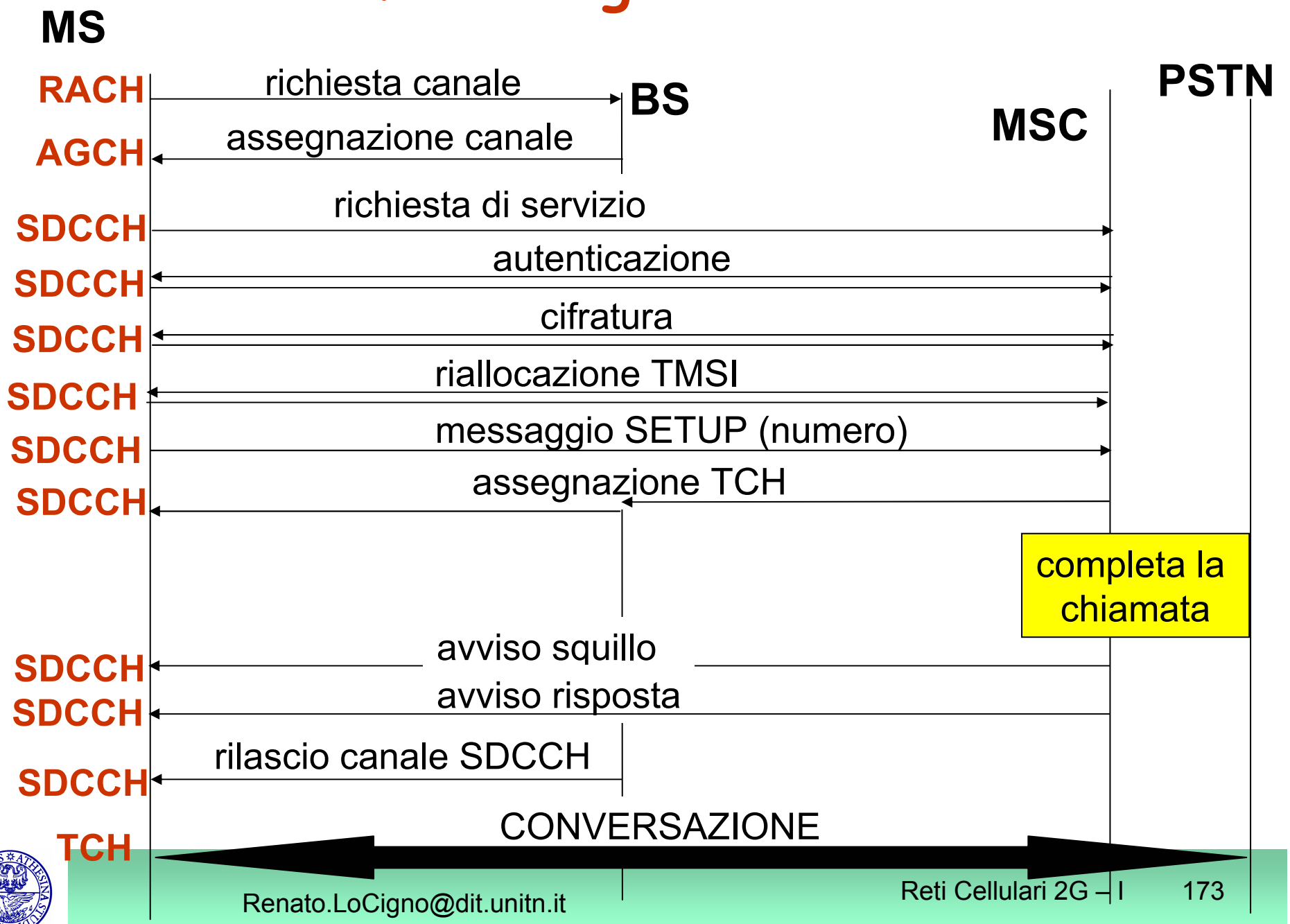


Chiamata originata dal MS

- L'MSC rialloca TMSI
- Il MS inizia la procedura di setup con un messaggio sul SDCCH
- L'MSC e la BTS assegnano un TCH
- L'MSC completa la chiamata verso il chiamato
- L'MSC avvisa il MS che il chiamato sta ricevendo la segnalazione (squilla il telefono)
- L'MSC avvisa il MS che il chiamato ha risposto
- IL MS connette la chiamata sul TCH e conferma



Chiamata originata dal MS



Chiamata destinata a MS

- L'utente compone il MSISDN del MS
- Le centrali della rete fissa tramite il MSISDN instradano la chiamata verso un GMSC
- Il GMSC determina l'HLR del MS
- Il GMSC invia all'HLR un messaggio con il MSISDN
- L'HLR determina l' IMSI del MS e il VLR presso cui il MS è temporaneamente registrato
- L'HLR invia al VLR una richiesta di informazioni di roaming



Chiamata destinata a MS

- Il VLR invia all' HLR il MSRN
- L' HLR invia al *GMSC* il MSRN
- Il *GMSC* instrada la chiamata verso il MSC relativo al VLR del MS
- Il MSC riceve l' IMSI del MS, e individua la location area dove si trova il MS
- Il MSC invia un messaggio di *PAGE* ordinando ai BSC di mandare il paging su tutte le BTS della location area del MS



Chiamata destinata a MS

- Ogni BSC fa eseguire dalle BTS il paging sul PCH con TMSI del MS
- Il MS risponde con un access burst sul RACH
- La BTS assegna al MS un SDCCH con AGCH
- Procedura di autenticazione
- Procedura di cifratura
- L'MSC rialloca TMSI
- L'MSC e la BTS assegnano un TCH

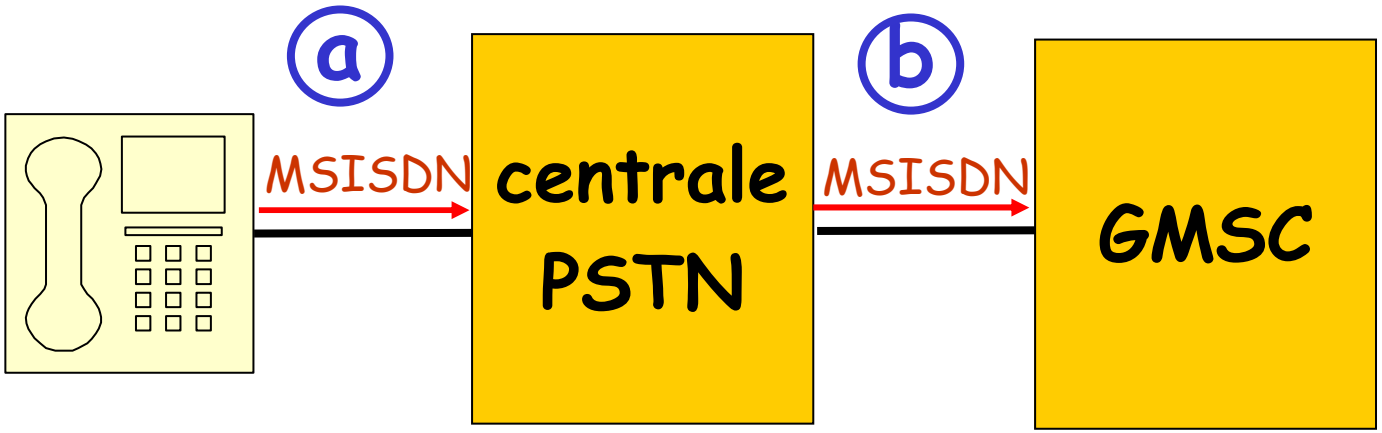


Chiamata destinata a MS

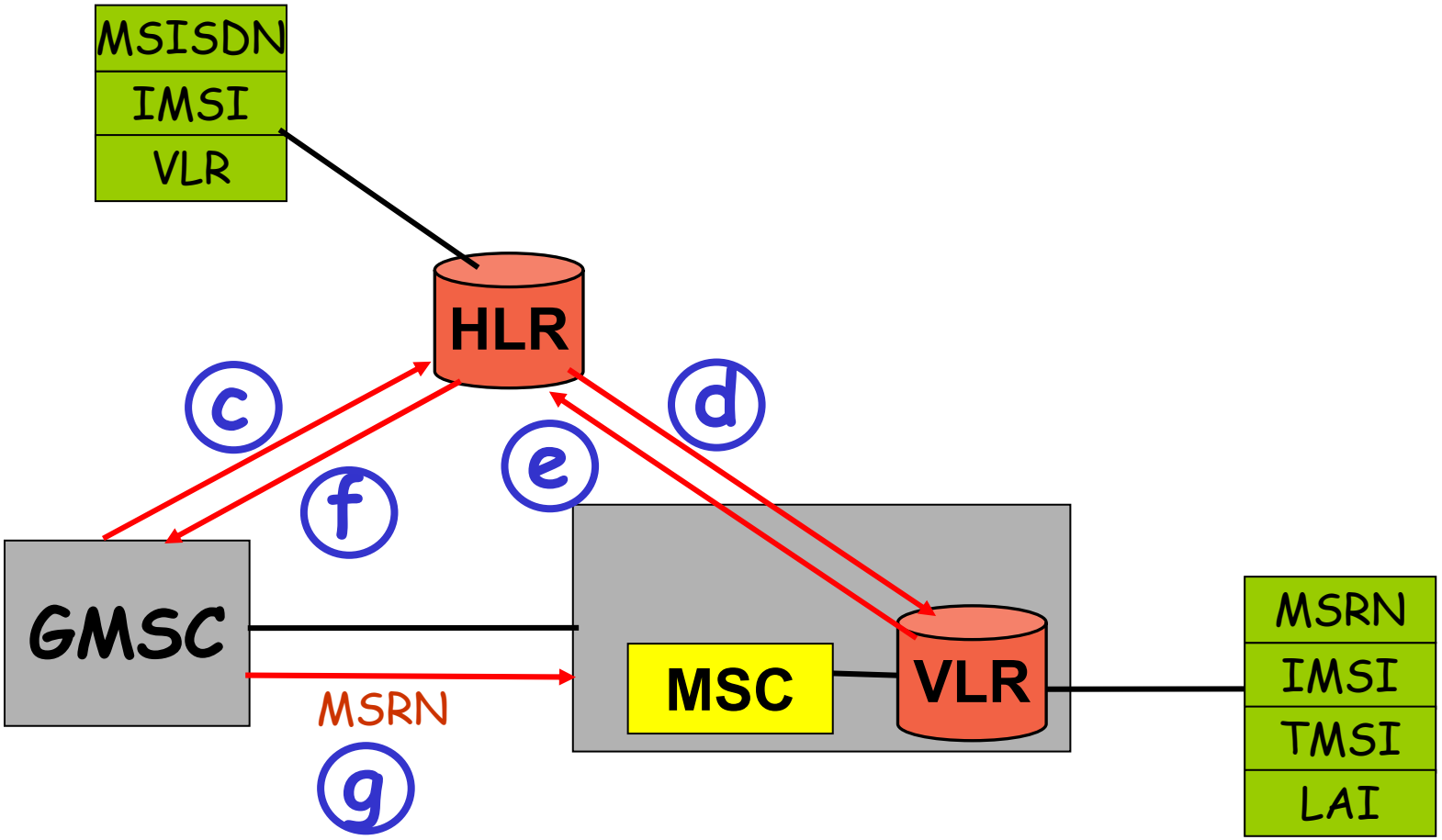
- Il MS avvisa l'MSC che il chiamato sta squillando
- Il MS avvisa l'MSC che il chiamato ha risposto
- L'MSC connette la chiamata sul TCH e conferma



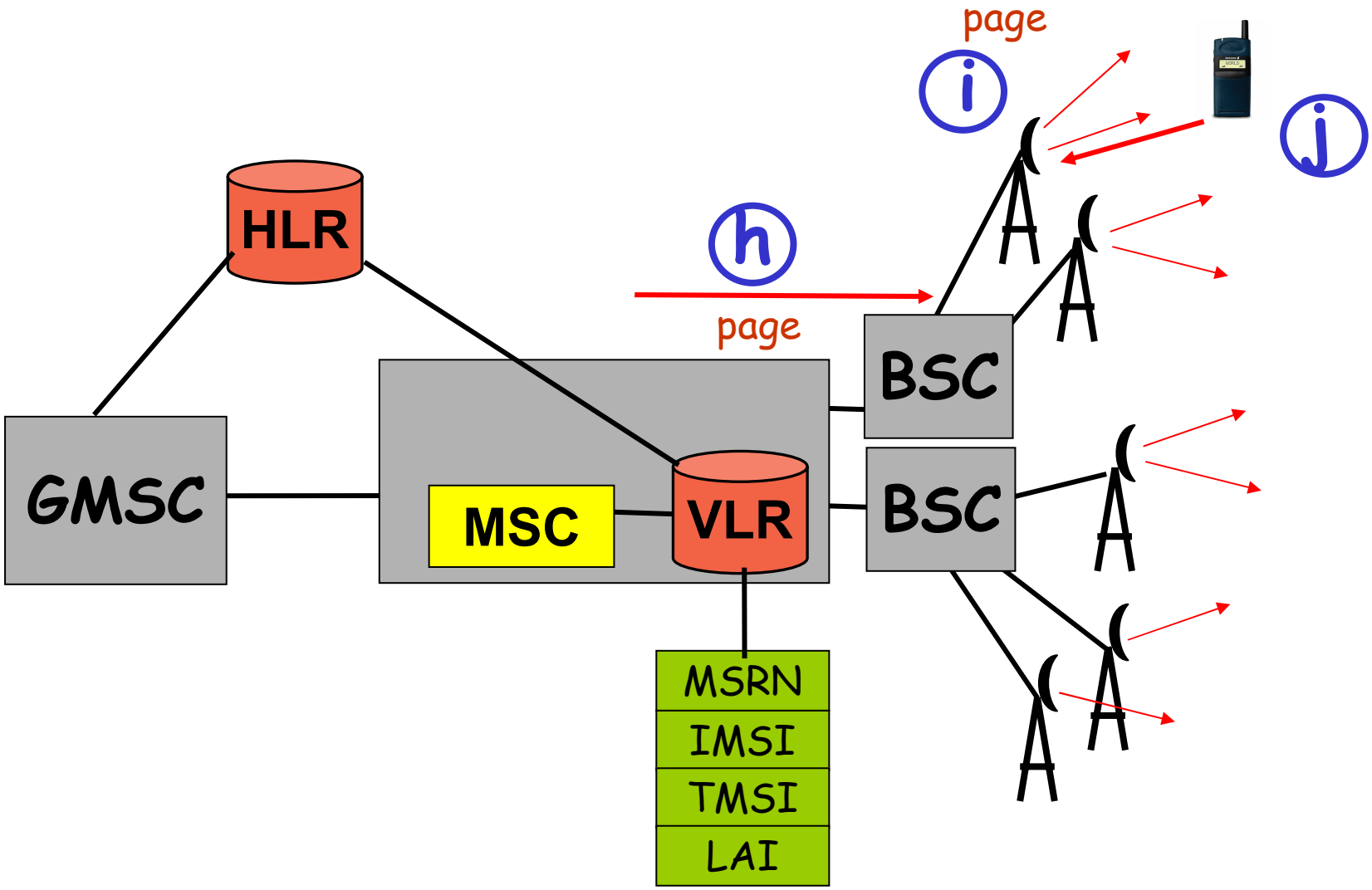
Chiamata destinata a MS



Chiamata destinata a MS



Chiamata destinata a MS



Handover

- Gli handover sono decisi dalla BSC sulla base di misure effettuate da MS e BTS
- Ogni MS comunica le misure con la procedura di *locating*



Handover - procedura di LOCATING

1. La BSC comunica al MS sul SACCH gli identificativi delle 6 BTS su cui fare le misure relative al BCCH
2. MS misura:
   - Intensità del segnale ricevuto su BCCH, RXLEVNCELL
   - Intensità del segnale su TCH, RXLEV
   - Qualità del segnale su TCH, RXQUAL



Handover - procedura di LOCATING

La BTS misura RXLEV, RXQUAL sull'uplink, e valuta la distanza del MS

- A intervalli regolari (p. es., 480ms) il MS comunica alla BTS le misure sul SACCH
- La BTS invia le misure alla BSC
- La BSC crea una lista ordinata di preferenza
- Quando la qualità sul TCH scende sotto una soglia predefinita, la BSC decide l'handover sulla base della lista



Handover

Motivi per effettuare un handover:

- Qualità del segnale sotto una soglia prestabilita
- Distanza del MS dalla BTS superiore a un valore massimo consentito
- Eccessivo traffico nella cella
- Altre esigenze (p. es., manutenzione)



Handover

Tipi di handover:

- Intra-cella
- Tra BTS facenti capo allo stesso BSC
- Tra BTS appartenenti a BSC diversi facenti capo allo stesso MSC/VLR
- Tra BTS appartenti a BSC diversi facenti capo a MSC/VLR diversi

I tempi di un handover devono essere molto brevi (meno di 100ms)



Handover intra-cella

- La BSC comanda al MS di cambiare canale di traffico ma non BTS
- Si verifica solitamente quando
  - la qualità del segnale è bassa (RXQUAL)
  - il livello del segnale è adeguato (RXLEV)
  - nessuna BTS può servire meglio il MS

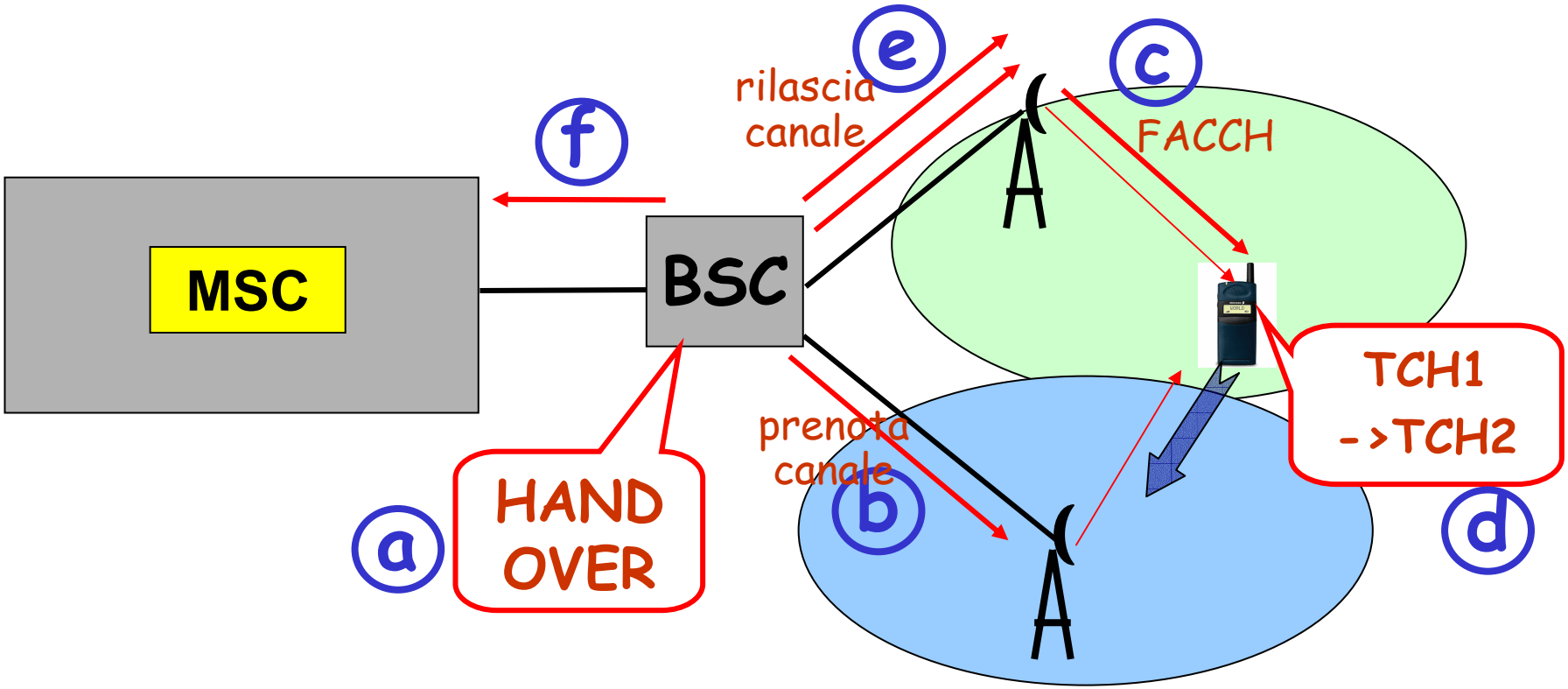


Handover tra BTS dello stesso BSC

- La BSC raccoglie misure effettuate da MS e BTS
  - decide se cambiare BTS
  - sceglie la BTS migliore per il MS
- La BSC apre un circuito con la BTS e prenota un TCH
- La BSC ordina al MS di sintonizzarsi sul nuovo TCH (utilizzando il FACCH)
- Il MS si sintonizza sul nuovo TCH
- La BSC rilascia vecchio circuito
- La BSC avvisa il MSC dell'avvenuto handover



Handover tra BTS dello stesso BSC



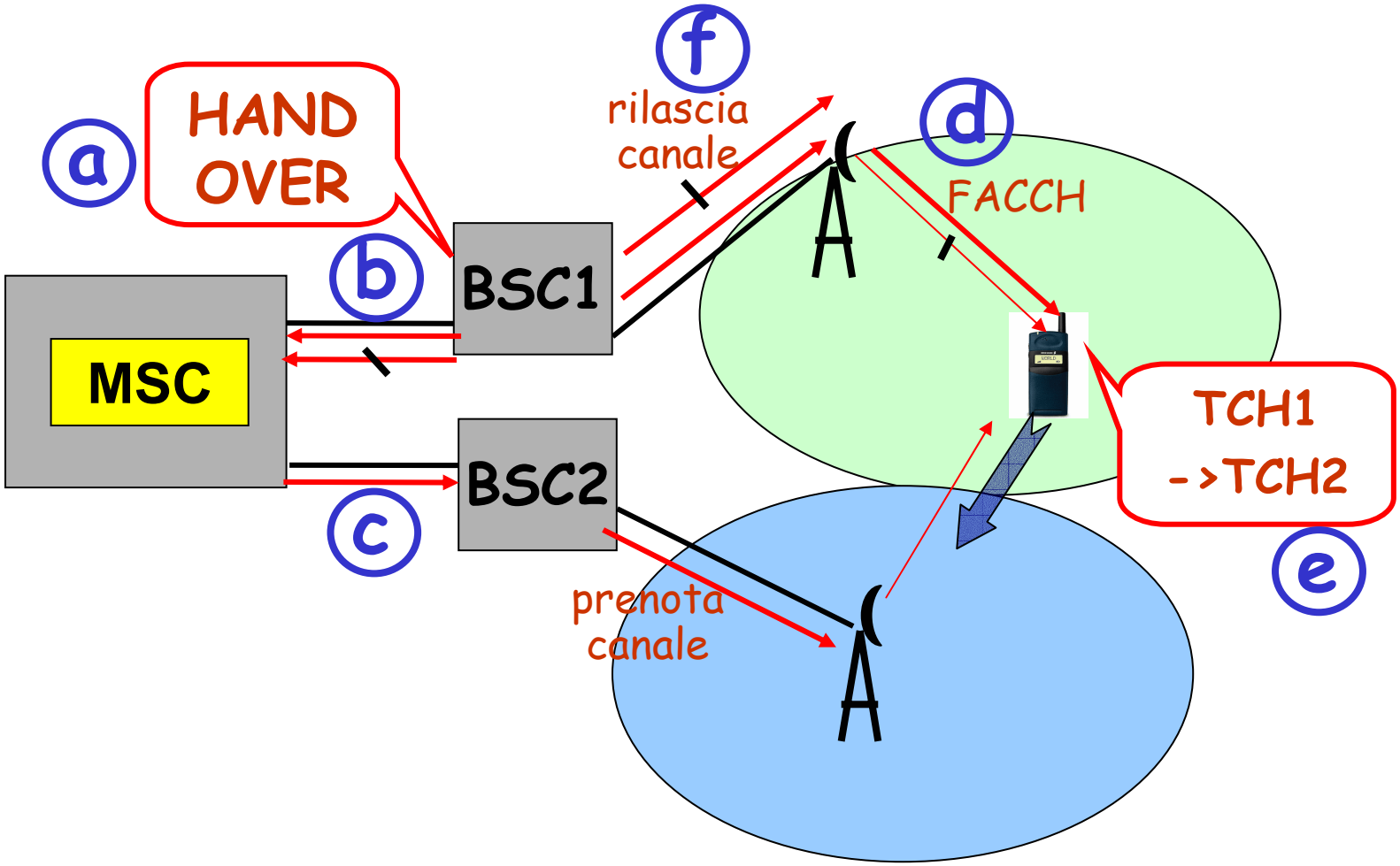
Dopo l'handover il MS riceve sul SACCH nuove informazioni sulle celle adiacenti

Handover tra BSC diversi, ma stesso MSC

- La BSC raccoglie le misure effettuate da MS e BTS
  - decide se cambiare BTS
  - sceglie la BTS migliore per il MS
- La BSC contatta il MSC che apre un circuito verso la nuova BSC che prenota un TCH
- La BSC ordina al MS di sintonizzarsi sul nuovo TCH (tramite il FACCH)
- Il MS cambia TCH
- Il MSC rilascia il vecchio circuito



Handover tra BSC diversi, ma stesso MSC



Handover tra BSC diversi con diverso MSC

- La BSC raccoglie le misure effettuate da MS e BTS
  - decide se cambiare BTS
  - sceglie la BTS migliore per il MS
- La BSC contatta il MSC vecchio, che contatta il nuovo MSC
- Il nuovo MSC alloca un handover number e lo comunica al vecchio MSC che lo usa per instradare la chiamata
- Il nuovo MSC apre un circuito verso la nuova BSC e questa verso la nuova BTS e prenota un TCH

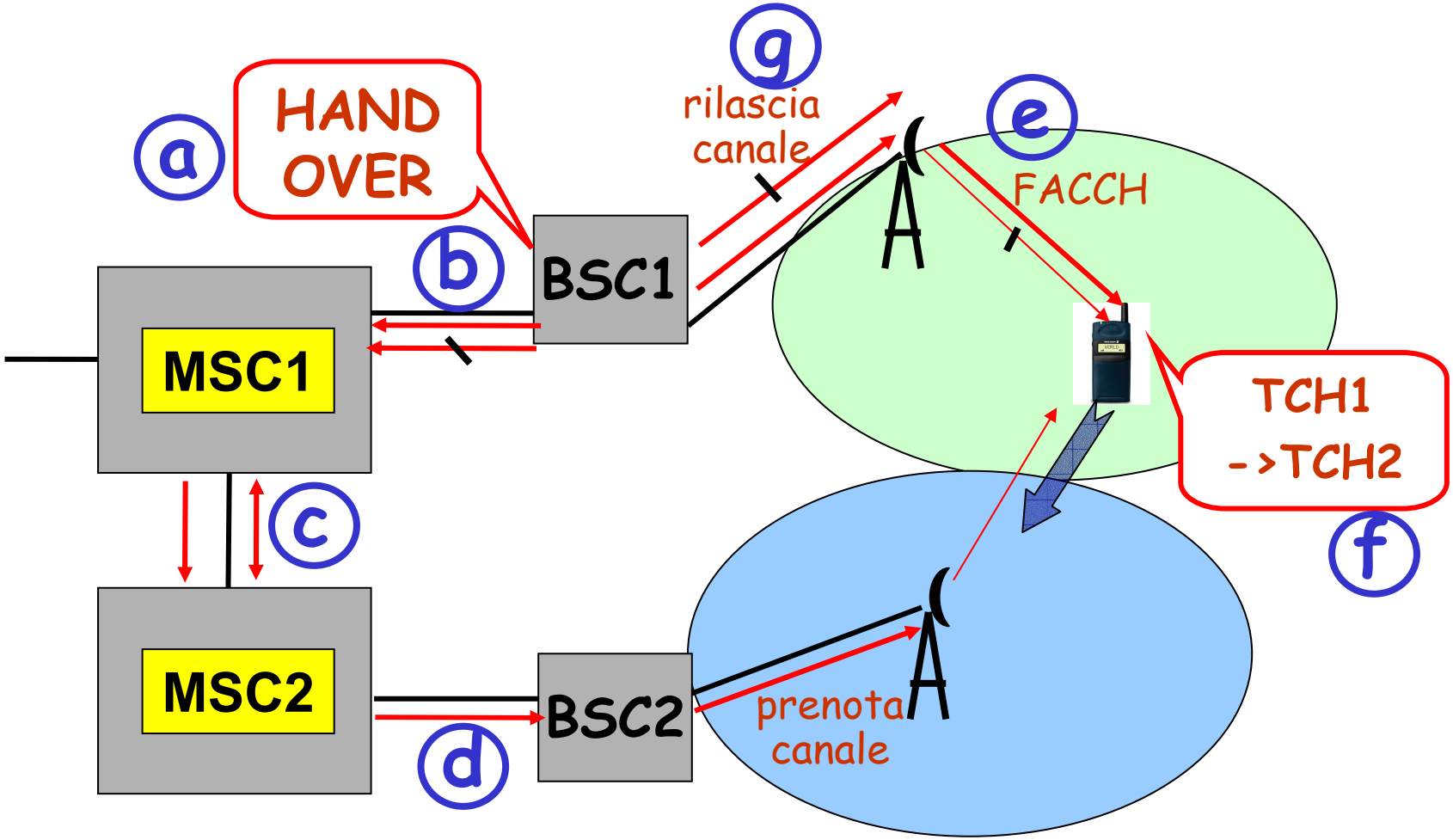


Handover tra BSC diversi con diverso MSC

- La vecchia BSC ordina al MS di sintonizzarsi sul nuovo TCH (tramite il FACCH)
- Il MS cambia TCH
- Il vecchio MSC rilascia il vecchio circuito



Handover tra BSC diversi con diverso MSC



Procedura di detach

E' la procedura eseguita allo spegnimento del MS

- Il MS invia un messaggio *IMSI detached*
- Il MSC marca il MS come *detached* (inattivo)
- Quando è detached un MS non riceve messaggi di paging

La procedura di detach non prevede alcuna conferma, né la comunicazione all' HLR

