Università degli Studi di Cagliari

Corso di Laurea Magistrale in Ingegneria delle Tecnologie per Internet

GSM

Storia e architettura

Cenni Storici

- ✓ **1982**: la CEPT (Conférence des Administrations des Postes et des Télécomunication) 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 tre Working Parties (WP1-3) per la definizione di servizi da offrire in GSM - protocolli di segnalazione, le interfacce, e la architettura di rete
- ✓ **1985**: la definizione della lista di raccomandazioni che il GSM deve produrre (finiranno per essere circa 130: 1500 pagine in 12 volumi!… più tutti quelli relativi all'evoluzione, cioè le fasi 2+ e 3 di GSM, rilasciati in anni successivi)

Cenni Storici

- ✓ **1986**: viene istituito il cosiddetto nucleo permanente con lo scopo di coordinare il lavoro del GSM visto il forte interesse da parte della industria
- ✓ **1987**: viene formato 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
  - ➢ Coordinare politiche di instradamento e la tariffazione (modalità e prezzi)

Cenni Storici

- ✓ **1988**: con l'istituzione dell'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 (?!?).
- ✓ **1992**: viene rilasciato lo standard definitivo relativo al GSM, che a questo punto diventa l'acronimo di Global System for Mobile Communications.
- ✓ **1992**: introduzione ufficiale dei sistemi GSM commerciali.

Cenni Storici

- ✓ **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.
- ✓ **1994-95**: introduzione degli SMS;
- ✓ **1995-97**: introduzione dei servizi a 1800 MHz;
- ✓ **1996**: standardizzazione dei codificatori enhanced sia full- che half-rate;
- ✓ **1997**: terminali dual-band con codificatore enhanced;
- ✓ **1999**: standard GPRS per la trasmissione a pacchetto; primi terminali WAP (Wireless Access Protocol) su circuito commutato;
- ✓ **2000-2001**: introduzione dei servizi GPRS

Cenni Storici

- ✓ **1993-2001**: GSM diventa la rete cellulare più diffusa al mondo con quasi 80M di utenti in Europa e 200M a livello mondiale (quasi 40M solo in Cina), una penetrazione non marginale anche in USA, con quasi 10 operatori, che hanno una quota di mercato seconda solo a AMPS/D-AMPS.

  Di fatto è diventato uno standard mondiale, influenzando in modo significativo l'evoluzione verso le reti di successiva generazione.

Servizi Offerti dal GSM

- ✓ 1 - Servizi di trasporto:
  - Trasmissione dati (non strutturata) sincrona e asincrona tra 300 bit/s e 9.6 kbit/s ;
  - Accesso PAD (Packet Assembly/Disassembly) asincrono 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 multiplexing di canali (HSCSD) fino a 76.8 Kbit/s;

Servizi Offerti dal GSM

- ✓ 2 - Teleservizi:
  - Telefonia sia full rate (13 Kbit/s, 12.6 Enhanced coder) sia half rate (6.5 Kbit/s)
  - Telefax di Gruppo 3;
  - Messaggeria sia unicast che multicast;
  - Messaggi brevi (SMS).

- ✓ 3 - Servizi supplementari: praticamente tutti quelli della rete PSTN (inoltro di chiamata, richiamata su occupato, gruppi di utenti chiusi, ...).

Caratteristiche

- ✓ La possibilità di effettuare il *roaming*, cioè di potersi spostare liberamente sul territorio servito dal proprio gestore e su quello servito dagli altri gestori delle nazioni che aderiscono al GSM, richiede di memorizzare in un database la posizione degli utenti ed aggiornarla man mano che questi si spostano.

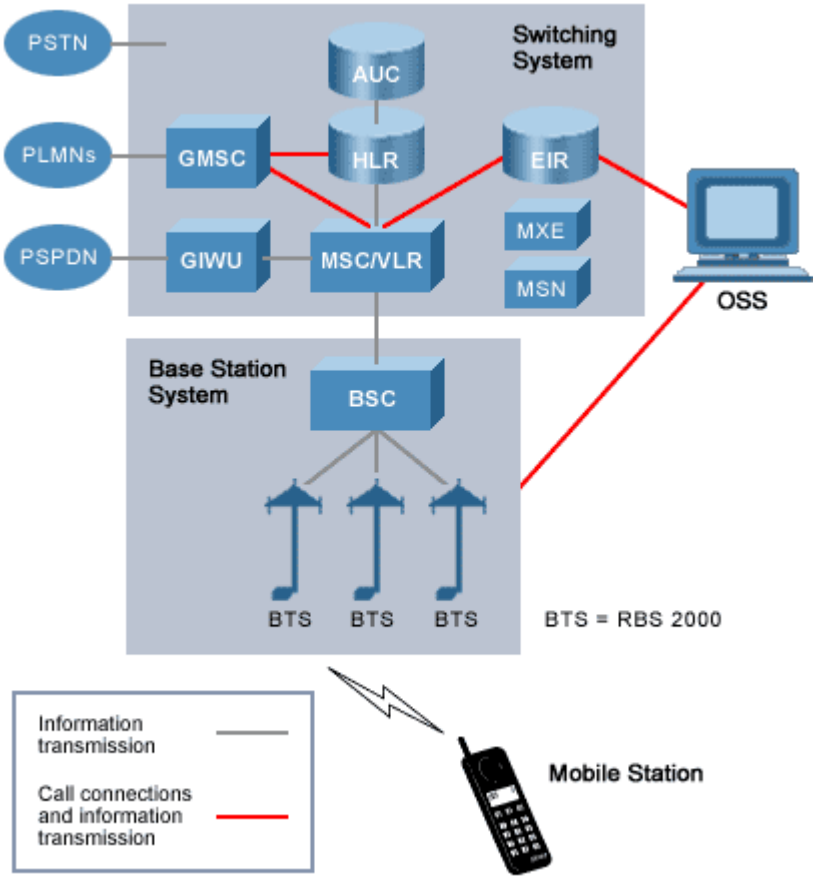
- ✓ A tal scopo l'area geografica di servizio del sistema GSM è suddivisa gerarchicamente in diverse aree:

Network Service Area

- ✓ Un operatore GSM è quindi sempre in grado di conoscere la posizione di ciascun suo abbonato.

Architettura del GSM

- ✓ Il sistema è diviso in gruppi:
  - MS: Mobile Station
    - ME: Mobile Equipment
    - SIM: Subscriber Identity Module
  - BSS: Base Station Subsystem
    - BTS: Base Transceiver Station
    - BSC: Base Station Controller
  - IN: Intelligent Network
    - MSC: Mobile Services Switching Center
    - EIR: Equipment Identity Register
    - AUC: Authentication Center
    - HLR: Home Location Register
    - VLR: Visitor Location Register
  - OSS: Operation Support Subsystem



Mobile Station MS

- ✓ E' il terminale di proprietà dell'utente
- ✓ Ne esistono molti tipi diversi a seconda delle applicazioni e dei luoghi di installazione
- ✓ Esistono varie categorie (classi) a seconda della potenza nominale: veicolari, portatili (es. PC Portatili, Fax, ecc.) e personali (hand–terminal)

Classi di potenza ME

Classe	Potenza di picco	Potenza media	Impiego
I eliminata	20 W (43 dBm)	2.5 W	veicolare o trasportabile
II	8 W (39 dBm)	1 W	veicolare o trasportabile
III	5 W (37 dBm)	0.625 W	hand held
IV	2 W (33 dBm)	0.25 W	hand-held
V	0.8 W (29 dBm)	0.1W	hand-held

ME

- ✓ Codici:
  - **IMEI** (*International Mobile Equipment Identity*)
  - **IMEISV** (*International Mobile Equipment Identity Software Version*)
- ✓ Identificano in modo univoco l'utenza
- ✓ ME è soltanto hardware, per poter funzionare e collegarsi alla rete ha bisogno di una scheda di abilitazione: la **SIM**
- ✓ Nei Paesi dove i numeri di emergenza (Ospedali, Polizia, Vigili del fuoco, ecc.) sono considerati un bene primario (Europa, USA, Giappone etc.) ME è abilitato a chiamare questi numeri anche senza la SIM

Modulo di Identificazione Utente

- ✓ È la SIM (Subscriber Identity Module)
- ✓ E' una scheda intelligente (con processore e memoria) di tipo smart card che rende "operativo" un qualunque terminale MS;
- ✓ Deve essere inserita nell'apposito lettore;
- ✓ Sono ammessi 4 possibili formati:
  - tipo carta di credito (ormai abbandonato)
  - formato ridotto (*plug-in* SIM o mini-SIM)
  - Micro SIM
  - Nano SIM

Modulo di Identificazione Utente

- ✓ Le caratteristiche dell'utente (# telefonico, servizi accessibili, ecc.) sono memorizzate in modo permanente e crittografato nella SIM, che rappresenta, quindi, il vero e proprio servizio offerto dai gestori
- ✓ E' possibile acquistare SIM da gestori diversi e usarle dallo stesso ME a seconda delle esigenze, oppure è possibile recarsi all'estero portando solo la SIM, affittare un ME localmente e connettersi
- ✓ Memorizza messaggi brevi inviati dalla rete (più evolve la tecnologia, maggiori capacità potranno essere associate alla SIM) tra cui gli SMS
  - ➢ 8, 16, 32, 64, 128 e 256K
- ✓ La SIM viene abilitata attraverso un codice di 4 cifre (PIN – Personal Identification Number)
- ✓ Se il PIN viene sbagliato 3 volte consecutive, la SIM si autoblocca e può essere sbloccata solo con un codice di sblocco a 8 cifre (PUK – Personal Unblocking Key)

Stazione Radio Base

- ✓ E' detta BTS (Base Tranceiver Station)
- ✓ E' il punto di accesso alla rete di TLC, o se si vuole, la "controparte" di MS
- ✓ E' collocata in un punto opportuno della cella (es. 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
- ✓ Ciascuna BTS può avere da 1 a 16 interfacce radio, corrispondenti a diversi canali in FDM
- ✓ Ciascuna interfaccia radio corrisponde a 8 canali TDM
- ✓ La BTS è un apparato di livello fisico e non ha praticamente alcuna "intelligenza": nel GSM anche la valutazione e la decisione sugli Handover da effettuare è demandata ad altre entità (MS, BSC e MSC)

Antenne omnidirezionali a basso guadagno

- ✓ La struttura più semplice prevede solo due antenne (una per ricevere e una per trasmettere) di tipo *omnidirezionali* a frusta in grado di "illuminare" uniformemente il segnale in tutte le direzioni
- ✓ La BTS si trova al centro della cella che irradia. Questa soluzione è usata per "coprire" zone a bassa intensità di traffico, ad esempio autostrade o zone rurali vaste e pianeggianti

Antenne omnidirezionali a basso guadagno

Antenna diversity

- ✓ Per migliorare la qualità del segnale ricevuto spesso si utilizzano due antenne riceventi, poste ad una distanza pari ad un multiplo dispari di un quarto di lunghezza d'onda (a 800 MHz la lunghezza d'onda è di 30 cm)
- ✓ Consente di risolvere i problemi connessi al fading. Le antenne possono essere spaziate verticalmente o orizzontalmente

Antenna diversity

Splitting

- ✓ Consiste nel suddividere una cella di dimensioni relativamente grandi in un certo numero di celle più piccole

- ✓ Aumenta la capacità di traffico in aree densamente popolate, mantenendo nel contempo la copertura radio con celle grandi nelle aree a bassa densità di traffico

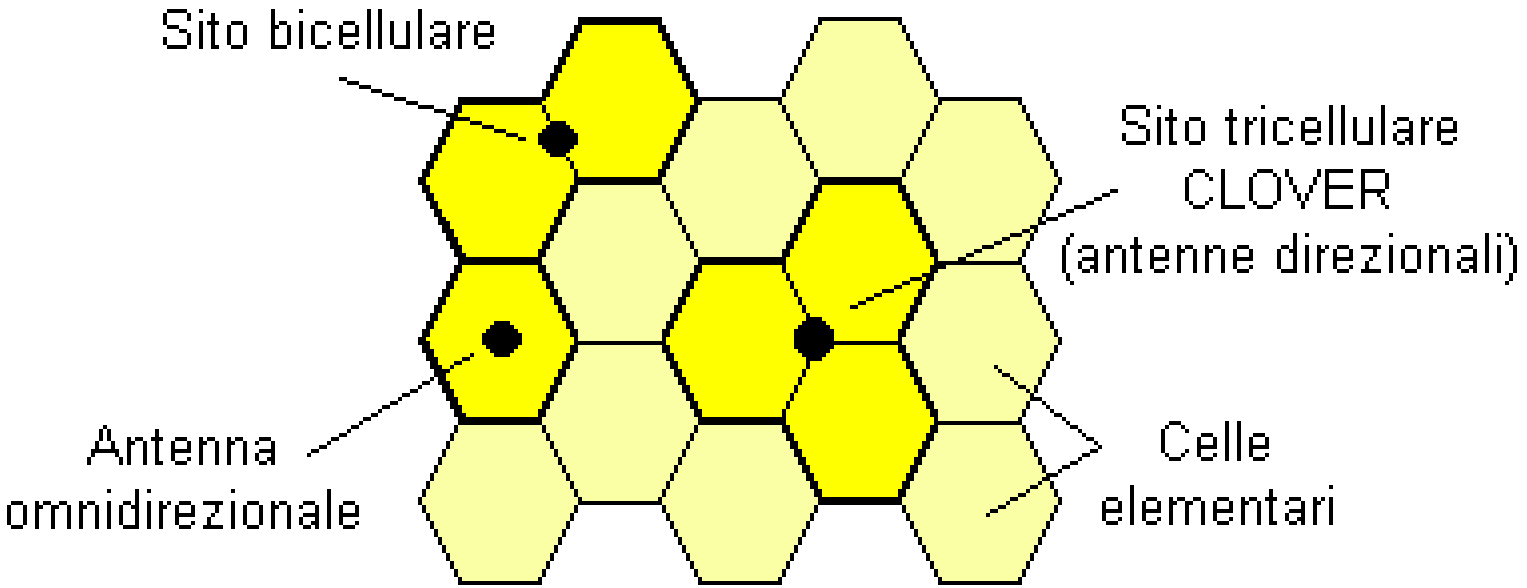
Sectoring

- ✓ Utilizzando antenne omnidirezionali, lo splitting richiede l'installazione di nuove BTS con un aumento dei costi e dell'interferenza di cocanale
- ✓ Una possibile alternativa è quella di suddividere una cella in un certo numero di settori, ognuno dei quali è "illuminato" da una antenna *direttiva* (o pannello)
- ✓ Ogni settore può così essere considerato come una nuova cella
- ✓ Consente ad uno stesso sito cellulare di illuminare più celle (o settori)

Clover

- ✓ È una struttura tipica: sito tri-cellulare
- ✓ Si hanno 3 celle per sito, ognuna servita da un'antenna trasmittente e due antenne riceventi direttive (una sola se l'antenna diversity non è implementata)
- ✓ ogni settore ha direzione di puntamento separata di 120° rispetto agli adiacenti

Possibili disposizioni



Esempio

Impatto visivo

- ✓ L'impatto visivo è uno dei problemi più sentiti per le BTS soprattutto in un paese pieno di edifici storici e paesaggi naturali come l'Italia
- ✓ Viene perciò cercata la tecnica del "mimetismo"
- ✓ Si utilizzano antenne nascoste, o in posti già di per se deturpati da altre strutture

Tree antennas

Chiese e ciminiere

Lampioni

Pico o micro BTS

- ✓ Sono celle di alcune centinaia di metri di raggio, perfette per coprire le piazze delle città, i supermercati o le stazioni della metropolitana
- ✓ Aumentano la capacità di traffico oppure servono per migliorare la qualità del segnale in determinate zone circoscritte del territorio
- ✓ Sono quasi impossibili da individuare ad occhio nudo
- ✓ Potenza di emissione ridotta

Pico BTS

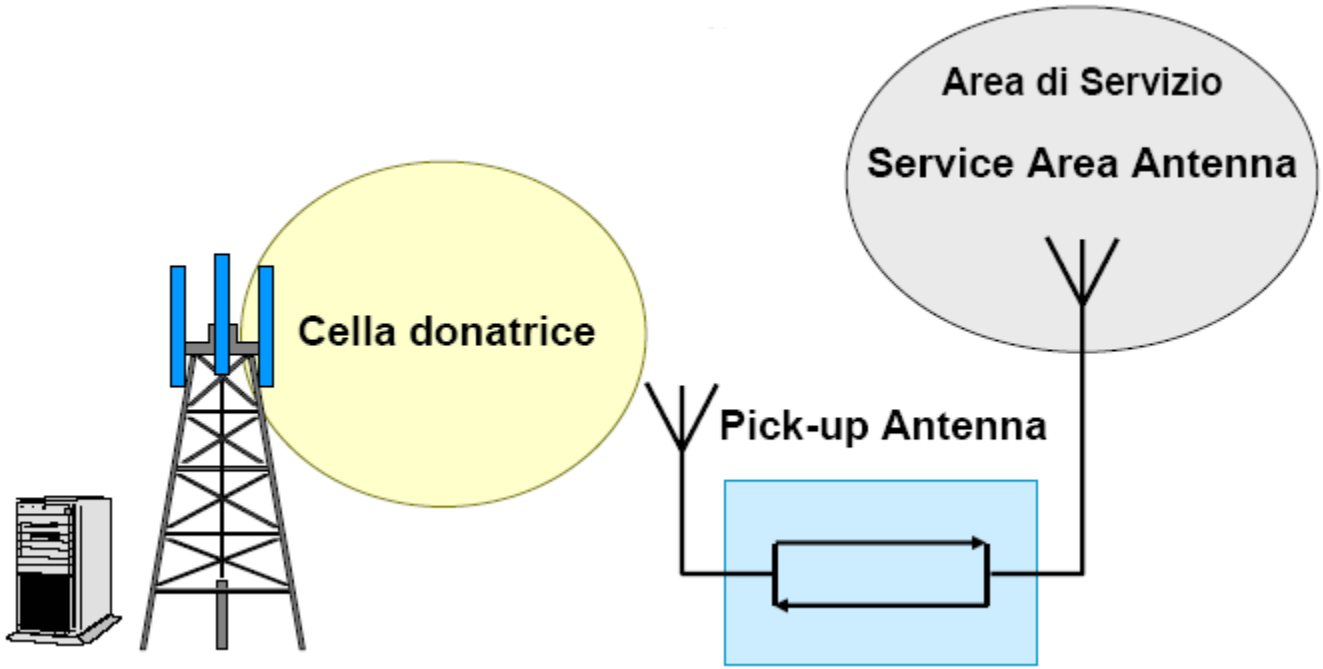
BTS trasportabili

- ✓ Spesso per manifestazioni o eventi sportivi, gli operatori di telefonia mobile utilizzano BTS trasportabili e effettuano uno splitting temporaneo delle celle

BTS trasportabili

Ripetitori

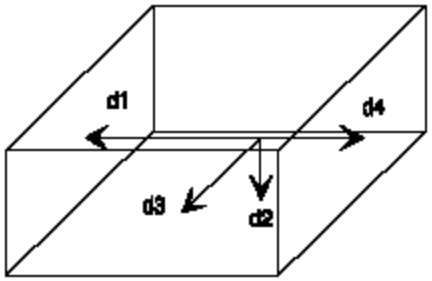
- ✓ **Sono utilizzati per migliorare la copertura in zone d'ombra nelle aree a basso traffico, poiché si aggiungono canali addizionali**

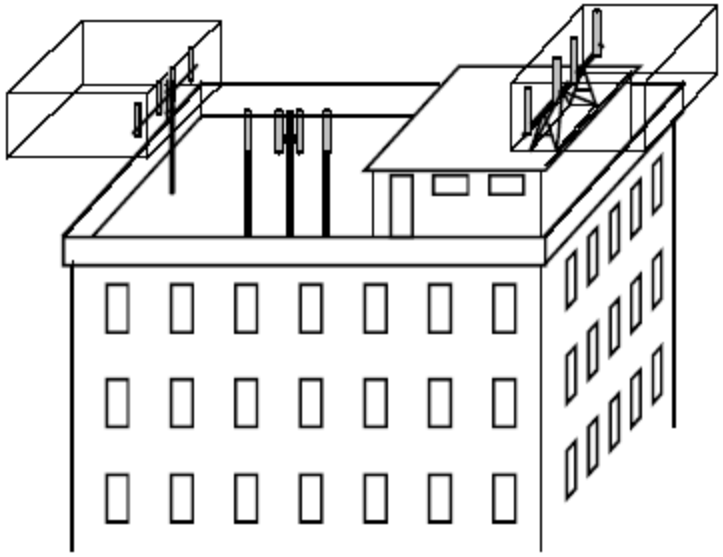


Ripetitori

Volume di rispetto

- ✓ Il volume di rispetto è la porzione di spazio al di fuori della quale sono rispettati i limiti di esposizione ai campi elettromagnetici
- ✓ Il volume di rispetto non deve pertanto essere accessibile alla popolazione





Classi di potenza BTS

Classe (BTS normali)	Potenza di picco (all'ingresso del combinatore TX)
I	320 - 640W (55-58 dBm)
II	160 - 320 W (52-55 dBm)
III	80 - 160 W (49-52 dBm)
IV	40 - 80 W (46-49 dBm)
V	20 - 40 W (43-46 dBm)
VI	10 - 20 W (40-43 dBm)
VII	5 - 10 W (37-40 dBm)
VIII	2.5 - 5 W (34-37 dBm)
(Micro BTS)	
M1	0.08 - 0.25 W (19-24 dBm)
M2	0.03 - 0.08 W (14-19 dBm)
M3	0.01 - 0.03 W (9-14 dBm)

Controller della BTS

- ✓ È la BSC (Base Station Controller)
- ✓ Una BSC controlla un numero elevato di BTS: da alcune decine ad alcune centinaia
- ✓ I compiti principali del BSC sono:
  - la gestione delle frequenze, che possono essere assegnate in modo dinamico alle varie BTS
  - la concentrazione del traffico verso un MSC e lo smistamento del traffico verso le BTS
  - la gestione degli Handover tra BTS adiacenti

Base Station Controller – BSC

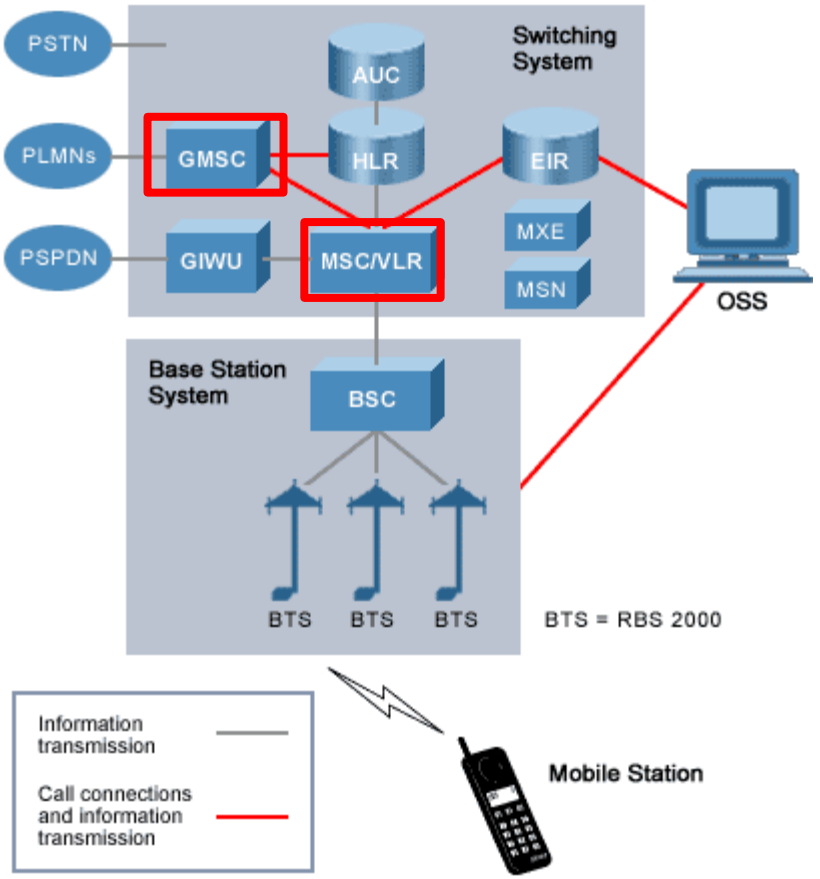
- ✓ I BSC possono essere collocate nel sito di un MSC (Mobile Switching Center) o essere autonome, o ancora essere posizionate vicino (o insieme) ad alcune BTS. Normalmente vengono collocate con MSC per questioni di controllo e manutenzione
- ✓ La connessione BTS-BSC avviene mediante linea dedicata PCM a 2.048 Mbit/s (32 canali a 64 kbit/s)
- ✓ Poiché la codifica vocale utilizzata dal GSM è diversa da quella PCM viene utilizzato il **TRAU** (*Transcoder Rate Adapter Unit*), che realizza un *adattamento* o transcodifica dalla codifica GSM alla codifica PCM

Base Station Controller – BSC

- ✓ L'interfaccia di comunicazione tra le BTS e BSC è detta ***A-bis***

Centro di Commutazione dei Servizi Mobili

- ✓ È il MSC (Mobile Switching Center)
- ✓ Sono "normali" commutatori PCM (commutatori a circuito) a cui sono state aggiunte funzionalità di segnalazione per la gestione della mobilità
- ✓ Consentono l'instradamento delle chiamate da un MS ad un altro
- ✓ Un caso particolare di MSC è il GMSC (Gateway-MSC), che è l'interfaccia tra la rete GSM e le reti fisse (PSTN) e altri reti mobili (PLMN)

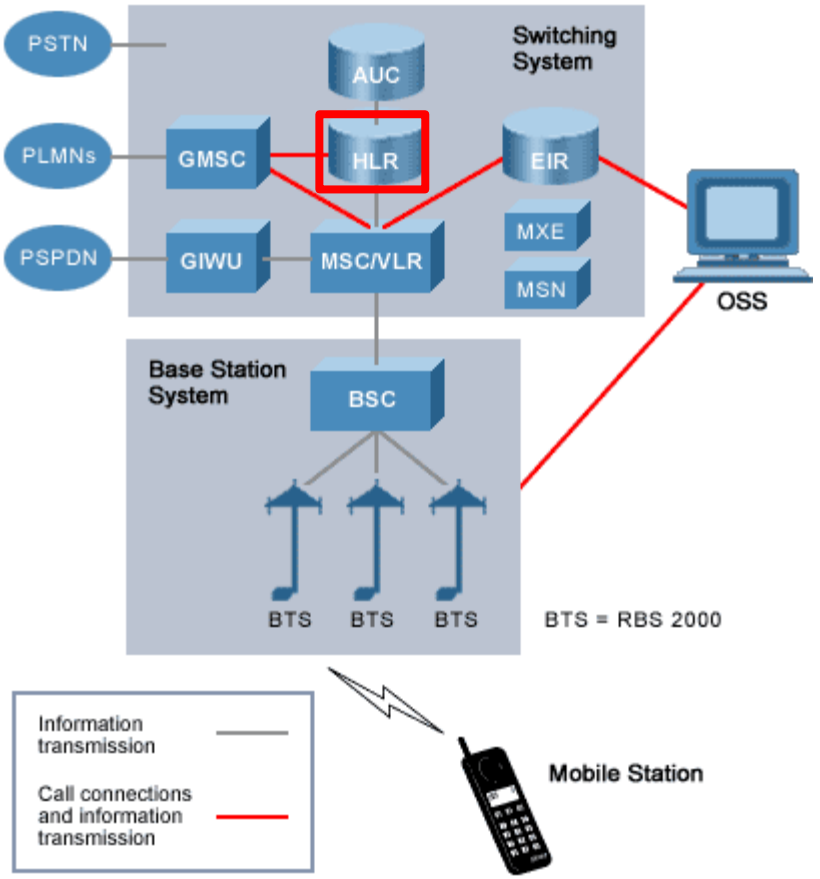


Mobile Switching Center

- ✓ GMSC è anche il "punto di partenza" per la ricerca degli MS nella rete cellulare
- ✓ Le funzioni legate alla sicurezza e all'autenticazione sono effettuate solo presso i GMSC
- ✓ 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 gli MS
- ✓ Una chiamata entrante verso un MS passa sempre attraverso il "suo" GMSC

Registro di Localizzazione Principale

- ✓ È l'HLR (Home Location Register)
- ✓ È una base dati permanente associata in modo univoco a un GMSC
- ✓ Memorizza le informazioni relative a tutti gli MS la cui localizzazione di default è presso il GMSC considerato
- ✓ HLR memorizza informazioni permanenti come l'IMSI (International Mobile Subscriber Identity), il numero di telefono della SIM associata e la sua chiave di autenticazione, lo stato dell'MS (acceso o spento), un eventuale numero di telefono per l'inoltro delle chiamate, i servizi supplementari a cui l'utente è abilitato



IMEI e IMEISV

- ✓ International Mobile Station Equipment Identity
- ✓ Numeri di identificazione dell'apparato
- ✓ IMEI (60 bit) identifica l'hardware
- ✓ IMEISV (64 bit) identifica anche eventuali diverse versioni di software/firmware
  - ❖ 24 bit: TAC (Type Approval Code)
  - ❖ 8 bit: FAC (Final Assembly Code) - il produttore
  - ❖ 24 bit: SN (Serial Number)
  - ❖ 4 bit: non usati in IMEI
  - ❖ 8 bit: SVN (Software Version Number) in IMEISV

Registro di Identificazione degli Apparati

- ✓ È il EIR (Equipment Identity Register)
- ✓ È una database il cui uso è a discrezione dell'operatore
- ✓ Contiene l'identificativo e le caratteristiche di tutti gli apparati GSM prodotti, insieme al produttore, al paese di fabbricazione, etc.
- ✓ Può essere usato per proteggere la rete dall'uso di apparecchiature non a norma, rubate, esportate illegalmente

EIR

- ✓ Ha tre liste:
  - **White list:** contiene gli IMEI di tutti i ME di tipo omologato, ed in condizioni operative, presenti nei paesi aderenti al GSM. Sono quindi autorizzati a connettersi alla rete.
  - **Black list:** contiene tutti gli IMEI che sono considerati bloccati (per esempio quelli rubati oppure di tipo non autorizzato) che non sono quindi autorizzati a connettersi con la rete.
  - **Grey list:** contiene tutti gli IMEI marcati come *faulty* oppure quelli relativi ad apparecchi non omologati (a discrezione del gestore). I terminali inseriti in questa lista vengono segnalati agli operatori di sistema mediante un allarme quando richiedono l'accesso, consentendo l'identificazione dell'abbonato che utilizza il terminale e l'area di chiamata in cui si trova.

Handover nel GSM

- ✓ La rete cellulare adotta come visto un'architettura ad albero
- ✓ Ciò implica che il passaggio di un MS (in connessione con la rete) tra celle (stazioni) contigue avvii, oltre all'evidente cambio di frequenza a livello radio, anche una sequenza di azioni e di re-instradamenti
- ✓ Il GSM prevede tre tipi di *handover*:
  - ➢ *intra* BSC
  - ➢ *inter* BSC, *intra* MSC (Mobile Switching Centre)
  - ➢ *inter* BSC, *inter* MSC

Handover nel GSM

- ✓ la necessità di procedere ad un *handover* è stabilita sulla base di specifiche misure che rappresentano sia la qualità della connessione in atto sia quella potenzialmente disponibile, stimata in merito alle celle contigue a quella che ospita la connessione stessa
- ✓ nel caso in cui *l'handover* sia deciso, (la rete assume questa decisione), la stessa sceglie la nuova cella di riferimento per il mobile
- ✓ il nuovo cammino della chiamata è predisposto a livello radio e di rete, ed avviene la creazione di un *ponte* nella rete (il punto in cui vecchio e nuovo cammino convergono)
- ✓ l'*handover* è eseguito attivando il nuovo cammino, mentre quello vecchio viene abbandonato

Parametri per l'handover

- ✓ Livello di potenza sul canale UL (Up-Link) e DL (Down-Link)
- ✓ Livello di qualità (BER) sul canale UL e DL
- ✓ Distanza base-mobile (stimata da BTS)
- ✓ Livello di potenza relativo alle celle adiacenti (valutato dal mobile misurando la potenza ricevuta sui BCCH delle celle adiacenti; i risultati delle misure sono inviati ogni 480 ms alla BTS, sul SACCH)

Le suddette misure sono elaborate e confrontate con le relative soglie di handover e su tale base viene compilata una lista di preferenza delle celle idonee per HO

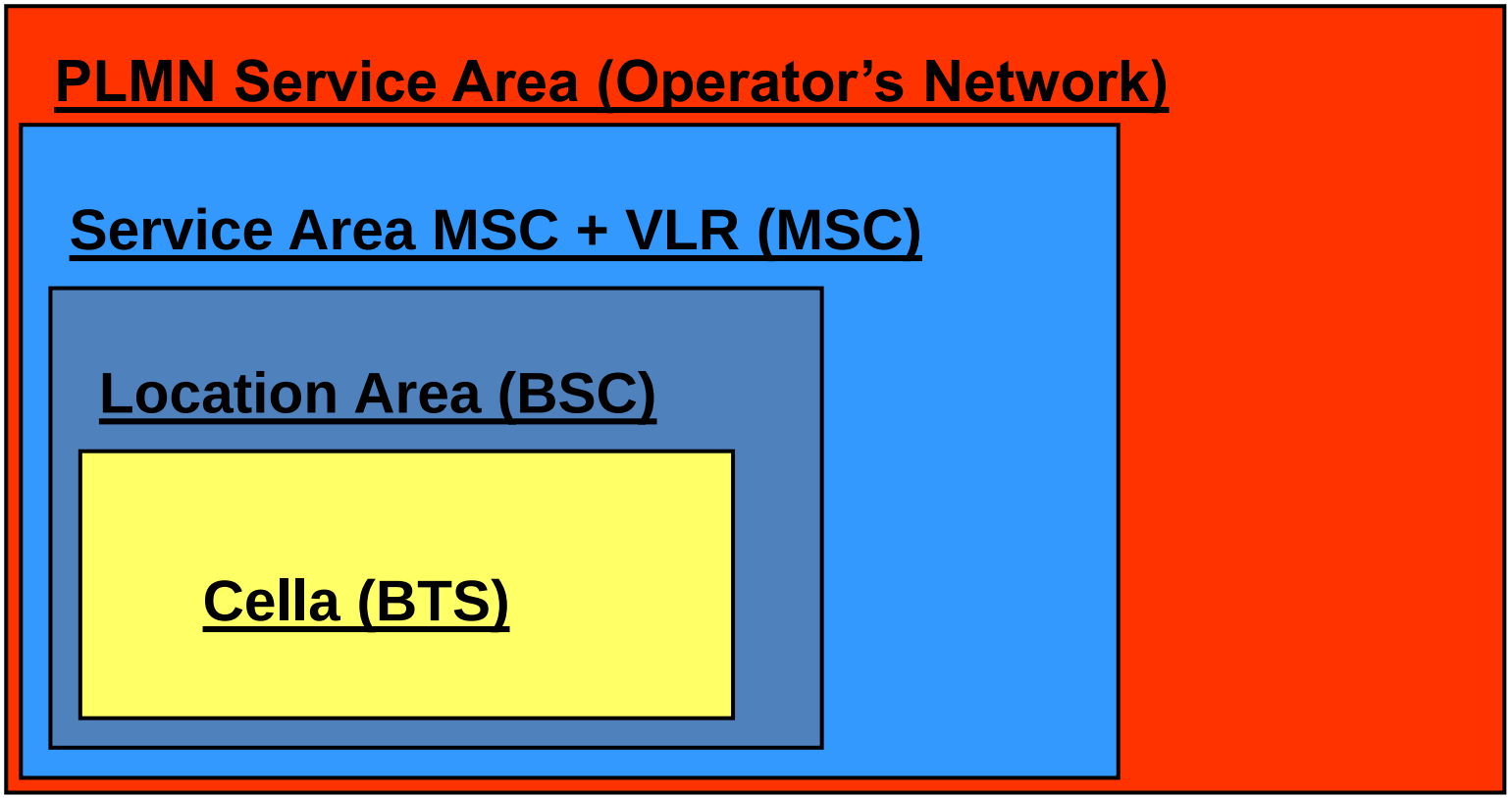
(Authentication Center – AUC)

- ✓ 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
- ✓ Gestisce alcune importanti operazioni per abilitare la cifratura della trasmissione sull'interfaccia radio

Centro Gestione e Controllo

- ✓ OMC (Operation and Maintenance Center)
- ✓ È la sede di tutte le operazioni di gestione (tecnica e non) della rete
- ✓ Effettua la tariffazione, controlla il traffico in rete, gestisce i messaggi di errore provenienti dalla rete, controlla e memorizza il carico delle singole BTS e BSC per operazioni di pianificazione (eventualmente dinamica)
- ✓ L'implementazione del OMC si chiama OSS

Network System Area



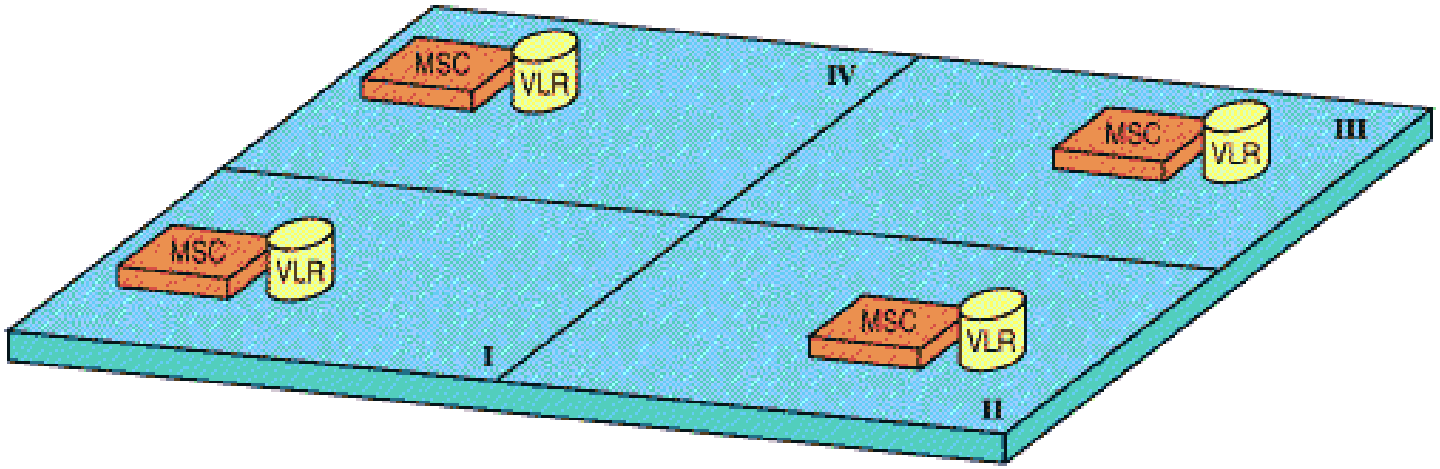
GSM e PLMN Area

- ✓ **GSM Service Area**: è l'area di servizio formata dalle singole reti di tutti gli operatori delle nazioni che partecipano al sistema GSM

- ✓ **PLMN Service Area**: Area di copertura complessiva servita dalla rete di un singolo operatore

MSC/VLR Service Area

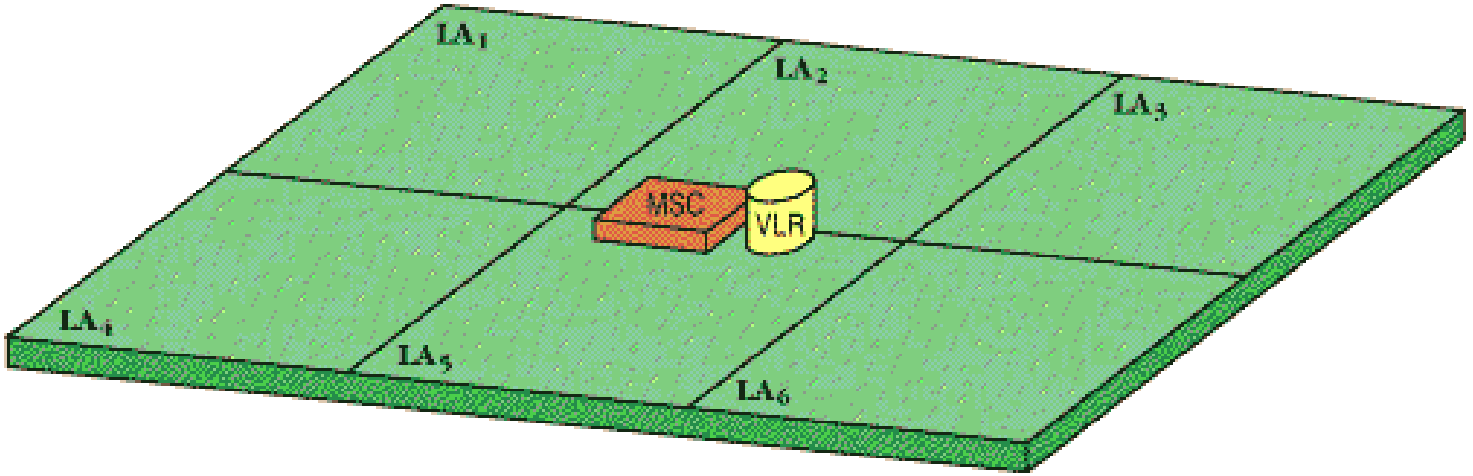
- ✓ Area servita da un solo MSC e dal VLR in esso integrato. Vi è la possibilità che MSC e VLR siano separati e quindi possono essere definite una **MSC Service Area** e una **VLR Service Area** distinte



Location Area

- ✓ È definita come quella zona dentro la quale una MS può muoversi liberamente senza che la sua posizione, memorizzata nel VLR, debba essere aggiornata.
- ✓ I messaggi di paging diretti ad una MS, per notificargli l'arrivo di una chiamata, sono irradiati **solo** nella LA dove è correntemente localizzata la MS.
- ✓ Quando una MS passa da una LA ad un'altra invia un messaggio di *Location updating* alla rete, in modo che questa possa aggiornare le informazioni contenute nel VLR

Location Area



HLR e VLR

- ✓ HLR gioca un ruolo fondamentale nella gestione delle chiamate che provengono dalla rete fissa e sono inoltrate verso un MS
- ✓ Ad ogni HLR viene associato un identificativo (**HLR number**), che viene fornito ai VLR (Visitor Location Register) interessati e permette loro di individuare l'HLR di appartenenza di ogni MS su di essi registrata.
- ✓ Ogni VLR è identificato da un **VLR number**, in modo tale che l'HLR sappia presso quale VLR è registrata correntemente ogni suo MS.
- ✓ È il VLR (Visitor Location Register), gestisce gli aggiornamenti dell'utente all'interno della rete
- ✓ In VLR vengono duplicati tutti i dati permanenti (HLR) di un utente
- ✓ VLR gioca un ruolo fondamentale nella gestione delle chiamate che provengono dagli MS