



LTE

Long Term Evolution (4G)

Fulvio Babich (babich@units.it)

DIA – Università di Trieste



LTE: motivazioni

- Mantenere la competitività dei sistemi xG
- Incrementare il tasso di trasmissione
- Migliorare la qualità del servizio
- Realizzare un sistema completamente a commutazione di pacchetto
- Ridurre i tempi di latenza
- Diminuzione del costo
- Diminuzione della complessità
- Unificazione della tecnologia, indipendentemente dal tipo di servizio

- Elemento chiave: **an all IP network.**

- LTE Advanced: 3 Gbit/s DL, 1.5 Gbit/s UL.
- Efficienza spettrale fino a 30 bit/s/Hz

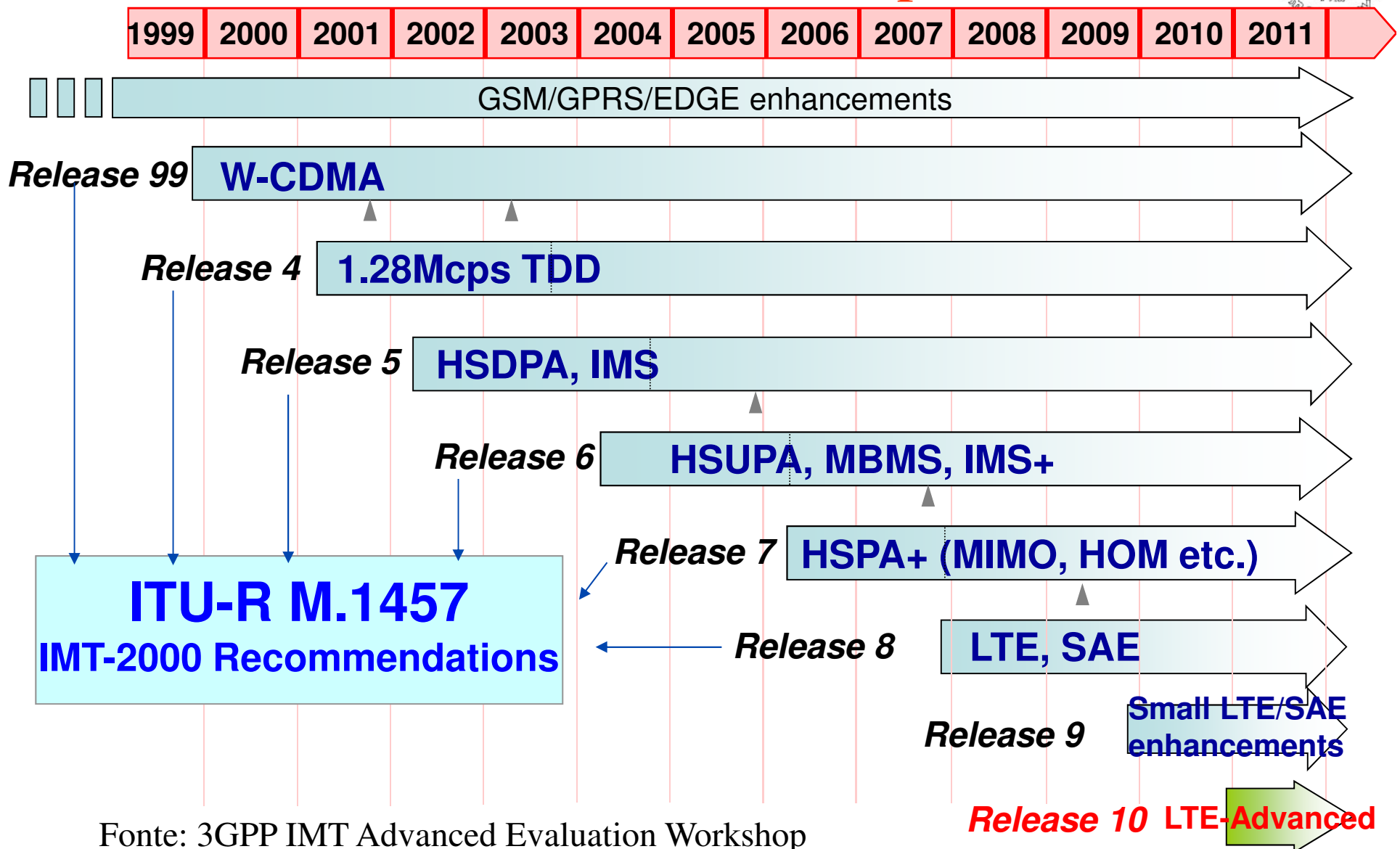


Da GSM a LTE

- **GSM (2G)**: trasmissione di voce, a commutazione di circuito, con moltiplicazione di tipo TDMA ($N=8$ canali di traffico per canale radio; banda del canale radio $W=200$ kHz)
- **GPRS (2.5G)**: trasmissione di dati, a commutazione di pacchetto, utilizzando lo stesso schema di moltiplicazione del GSM (il flusso dati può utilizzare un gruppo di canali di traffico, per incrementare la bit rate).
- **EDGE (2.5G)**: miglioramento dell'interfaccia radio (modulazioni di ordine più elevato 8PSK invece di GMSK) consentono un incremento della bit rate (48 kbit/s per slot). Complessivamente 384 kbit/s nel canale di 200 kHz.
- **UMTS (3G)**: moltiplicazione WCDMA (Wideband Code Division Multiple Access). La commutazione è a circuito per i servizi vocali, e a pacchetto (mediante GPRS) per i servizi dati. L'indirizzo IP viene assegnato utilizzando il *paging* a commutazione di circuito, in fase di apertura del trasferimento dati, e rilasciato quando la connessione termina.
- **LTE (4G)**: moltiplicazione OFDMA. L'accesso EPS (Evolved Packet System) utilizza sia per i servizi in tempo reale che per la trasmissione dati il protocollo IP. L'indirizzo IP viene assegnato quando il terminale viene acceso, e rilasciato quando il terminale viene spento. La connessione avviene entro 100 ms.



Dal 2G al 4G: Release of 3GPP specifications





Un confronto

	UMTS	HSPA	HSPA+	LTE	LTE Adv.
Max DL bit/s	384 k	14.4 M	28 M	300 M	1 G
Max UL bit/s	128 k	5.7 M	11 M	75 M	500 M
Banda (FDD)	5 MHz	5 MHz	5 MHz	20 MHz	100 MHz
ES DL bit/s/Hz	0.077	2.88	5.6	15	10
ES UL bit/s/Hz	0.025	1.14	2.2	3.75	5
Round trip	150 ms	100 ms	50 ms	10 ms	10 ms
Standard 3GPP	99/4	5/6	7	8/9	10
Multiplicazione	W-CDMA	W-CDMA	W-CDMA	OFDMA SC-FDMA	OFDMA SC-FDMA



Release 8: caratteristiche (1)

- Elevata efficienza spettrale
 - OFDM (Downlink)
 - Protezione contro gli effetti del multipath
 - Compatibile con tecniche avanzate per incrementare le prestazioni
 - Water filling
 - MIMO
 - DFTS-OFDM(“Single-Carrier FDMA”) (Uplink)
 - Basso PAPR (Peak to Average Power Ratio)
 - Ortogonalità tra utenti nel dominio della frequenza
 - Tecniche Multi-antenna
- Bassa latenza
 - Connessione & trasferimento
 - Basso ritardo di Handover
 - TTI (*Transmission Time Interval*) breve
 - Gestito da RRC
 - Macchina a stati RRC semplificata
- Banda variabile
 - 1.4, 3, 5, 10, 15 e 20 MHz (LTE Advanced)



Release 8: caratteristiche (2)

- Architettura protocollare semplificata
 - Canali condivisi
 - Commutazione di pacchetto con Voice over IP
- Architettura semplice
 - eNodeB unico nodo E-UTRAN
 - Limitato numero di interfacce RAN
 - eNodeB ↔ MME/SAE-Gateway (S1)
 - eNodeB ↔ eNodeB (X2)
- Piena compatibilità con le versioni precedenti 3GPP
- Interoperabilità con gli altri standard (cdma2000)
- In grado di operare sia in modalità FDD che in modalità TDD con una sola tecnica di accesso radio
- Supporto Multicast/Broadcast
- Supporto alla modalità Self-Organising Network (SON)



Criticità

- I servizi vocali delle generazioni precedenti operano a commutazione di circuito, mentre nella rete fissa, la transizione verso Voice over IP è a uno stadio più avanzato.
- Nella Core Network si sta diffondendo l'architettura Bearer Independent Core Network (BICN), con interfacce spesso basate sulla tecnologia IP.



LTE: elementi principali

- *User Equipment* (UE): una volta acceso è sempre connesso alla rete (ha un indirizzo IP), ed è connesso al *Serving Gateway* (SGW) e al *Data Network Gateway* (PGW).
- *Evolved Universal Terrestrial Radio Access* (E-UTRA): l'interfaccia radio LTE.
- *Evolved Universal Terrestrial Radio Access Network* (E-UTRAN): generalmente indicata come *Enhanced Node B*.
- *Evolved Packet Core* (EPC) il nucleo della rete LTE.
- Non LTE application servers, Internet, legacy network (UMTS).



eNodeB

- Le stazioni base (eNodeB, eNB), gestiscono il traffico e garantiscono il conseguimento della QoS.
- Gestiscono le operazioni di handover (è previsto solo la modalità hard), dialogando direttamente fra loro (interfaccia X2).
- L'interfaccia S1 che pone in comunicazione l'eNodeB e il gateway con cui si accede alla core network è interamente basato sul protocollo IP.
- Le stazioni base sono dotate di port Ethernet a 100 Mbit/s o 1Gbit/s, oppure con porte gigabit Ethernet in fibra ottica.



Interfaccia Core Network – Radio Access Network

- Suddivisa in due elementi (eventualmente implementati nello stesso dispositivo)
 - Serving Gateway (Serving-GW)
 - Mobility Management Entity (MME).
- MME: control plane.
 - Gestione mobilità. Autenticazione, assegnazione dei canali radio, gestione handover (fra eNodeB diversi o fra reti diverse).
 - Gestione posizione terminali mobili nello stato di idle (Location tracking).
 - Selezione del gateway per l'access a Internet.
- Serving-GW: user plane.
 - Trasferimento dei pacchetti IP in rete, mediante l' Encapsulated IP packet, per gestire le fasi di handover.



Internet – User plane

- L'interazione con Internet avviene mediante il Packet Data Network (PDN)-Gateway, che assegna l'indirizzo IP.
- L'interfaccia tra il PDN-GW e l'MME/Serving-GWs è indicata con S5. In analogia con l'interfaccia tra l'SGSN e il GGSN delle generazioni precedenti, si adotta il tunneling (protocolli GTP-U (user) e GTP-S (signaling)) per la gestione della mobilità in caso di cambio del Serving-GWs.
- L'HLR è ridenominato Home Subscriber Server (HSS), e contiene informazioni sugli utenti GSM, GPRS, UMTS, LTE, e IMS (IP Multimedia Subsystem, basato su SIP).
- La comunicazione con HSS non usa il protocollo MAP (basato su SS7) ma il protocollo Diameter basato su IP.

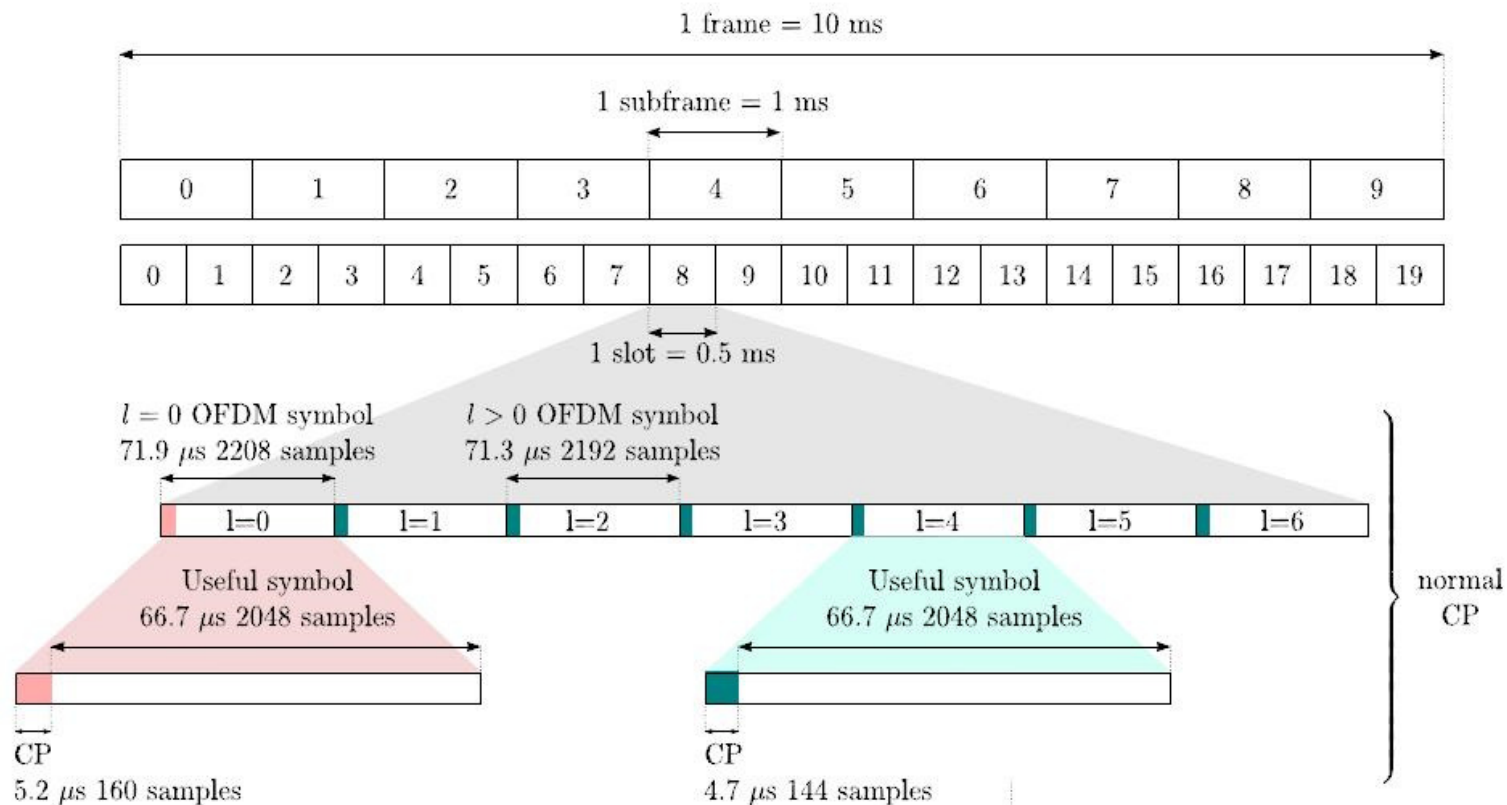


Banda e canali

Banda [Mhz]	1.25	2.5	5	10	15	20	
Durata slot	0.5 ms						
Spaziatura canali Δf	15 kHz						
N_{FFT}	128	256	512	1024	1536	2048	
Frequenza campionamento: $N_{\text{FFT}}\Delta f$ [MHz]	1.92	3.84	7.68	15.36	23.04	30.72	
Canali	75	150	300	600	900	1200	
Simboli/slot (short/long CP)	7/6						
CP ($\mu\text{sec/ campioni}$)	short	4.69 /9	4.69 /18	4.69 /36	4.69 /72	4.69 /108	4.69 /144
	long	16.67 /32	16.67 /64	16.67 /128	16.67 /256	16.67 /384	16.67 /512



Struttura temporale (20 MHz)



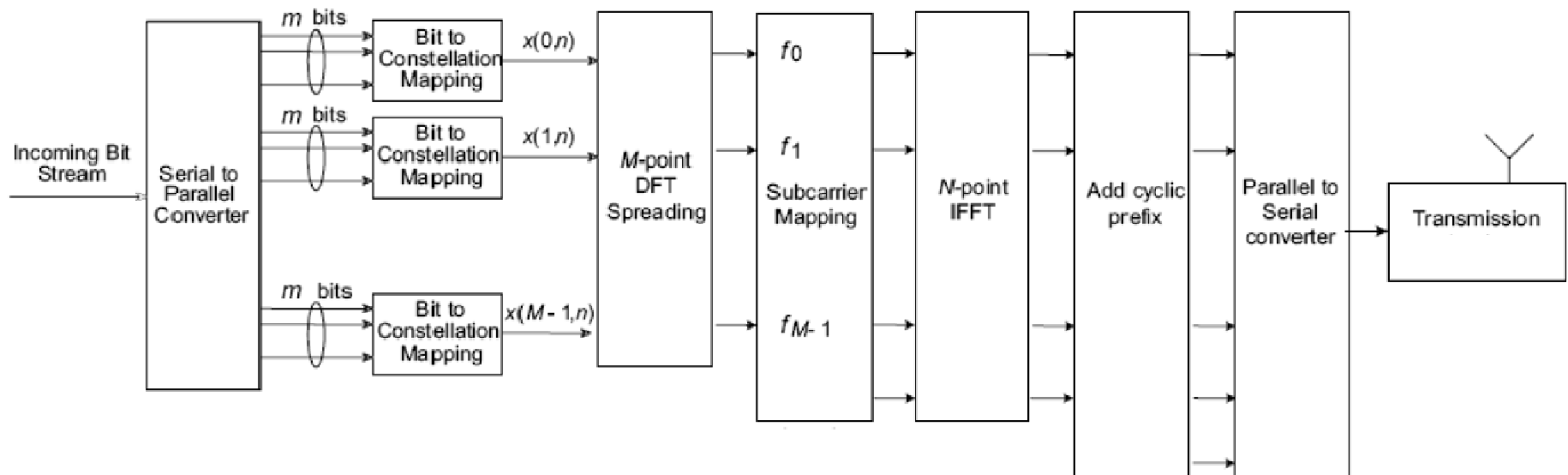


Multiplazione

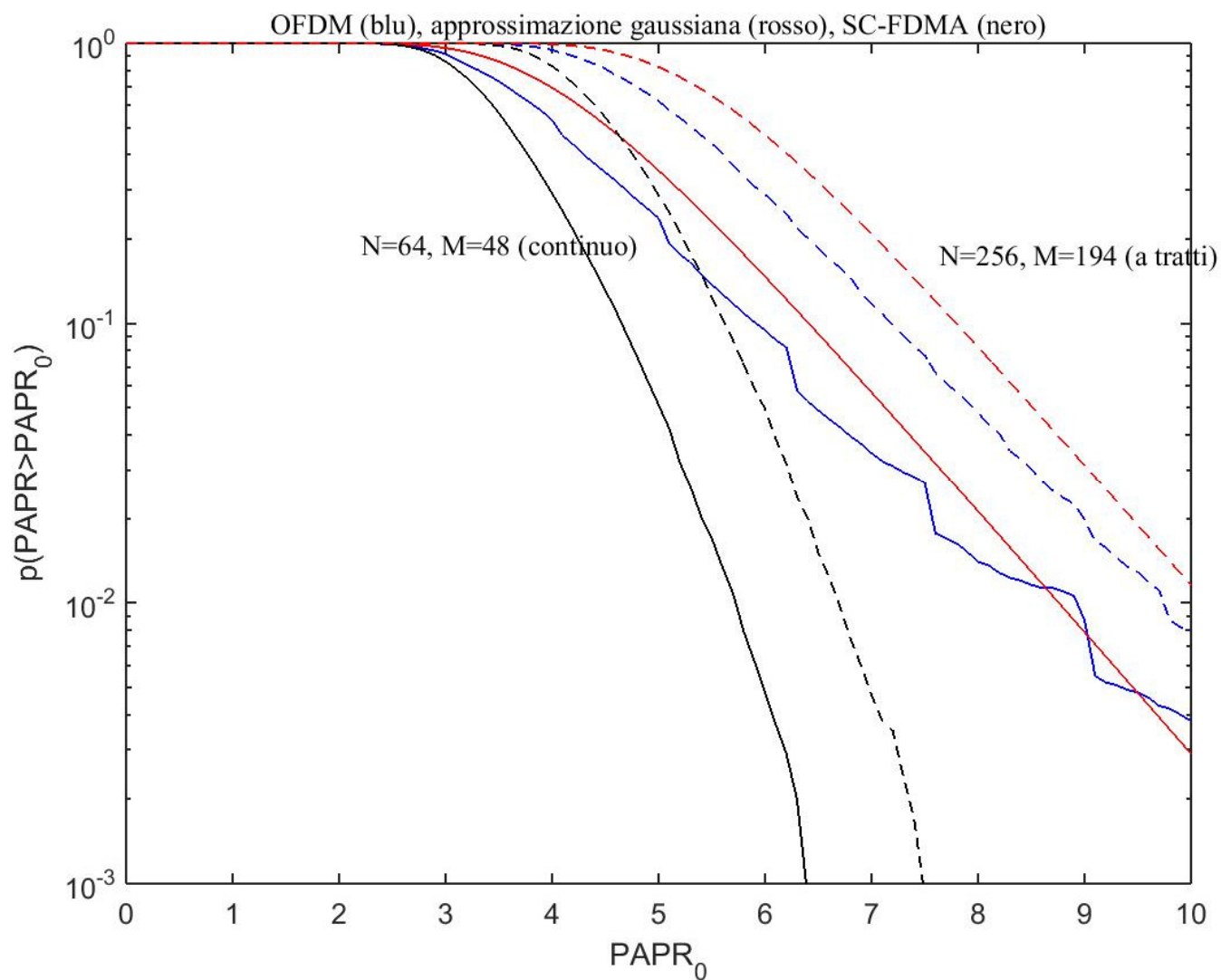
- **Downlink: OFDMA**
 - Elevata efficienza spettrale
 - Protezione contro interferenza selettiva e multipath
 - Utilizzo del prefisso ciclico per evitare interferenza inter simbolica e favorire l'equalizzazione
 - Utilizzo flessibile della banda
 - Scheduling nel dominio della frequenza
 - Compatibile con tecniche MIMO
- **Uplink: SC-FDMA**
 - OFDMA con DFT precoding
 - Compatibile con lo schema Downlink
 - Equalizzazione nel dominio della frequenza
 - Meno sensibile alle distorsioni non lineari (basso valore di Cubic Metric (CM) e Peak to Average Power Ratio (PAPR)).

Uplink: SC-FDMA

- DFT precoding garantisce bassi valori di PAPR / cubic metric
- Il prefisso ciclico (CP) consente un'equalizzazione agevole al NodeB



Peak to Average Power Ratio (PAPR)





Physical Resource Block

Segnale trasmesso

(matrice tempo/frequenza)

Tempo

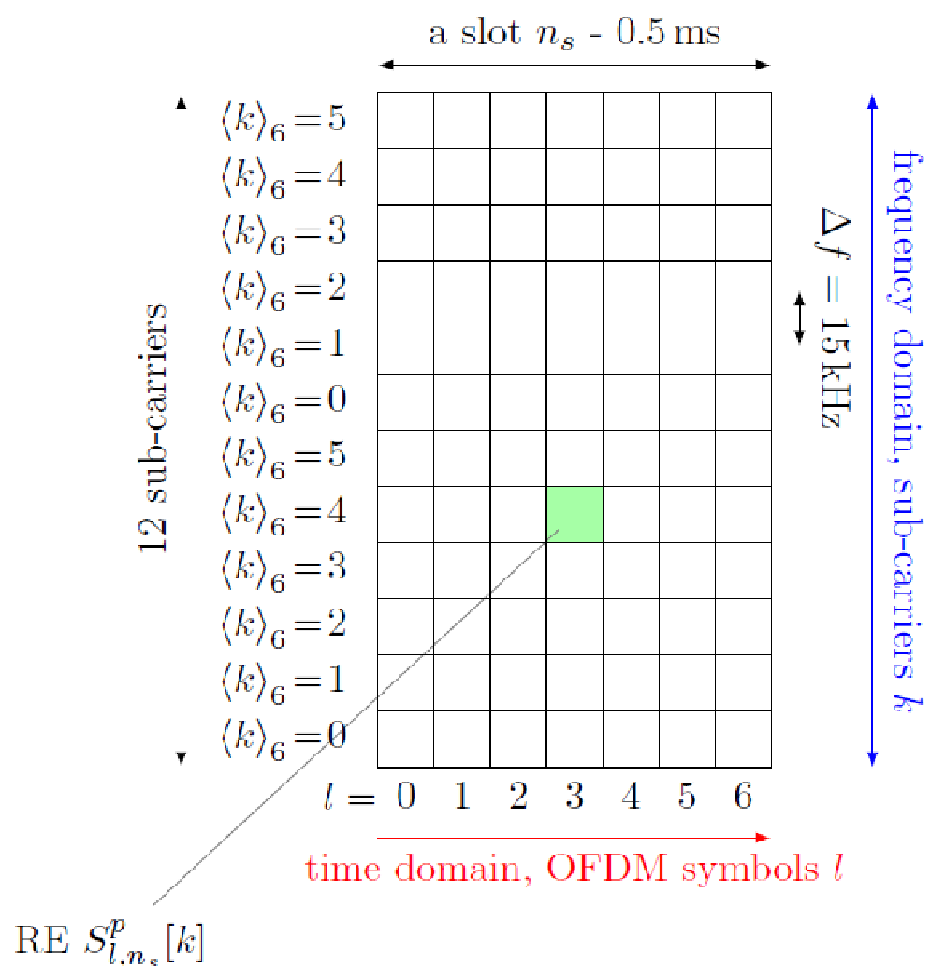
Slot (0.5 ms)

6/7 simboli (long/short CP)

Frequenza

12 sottoportanti

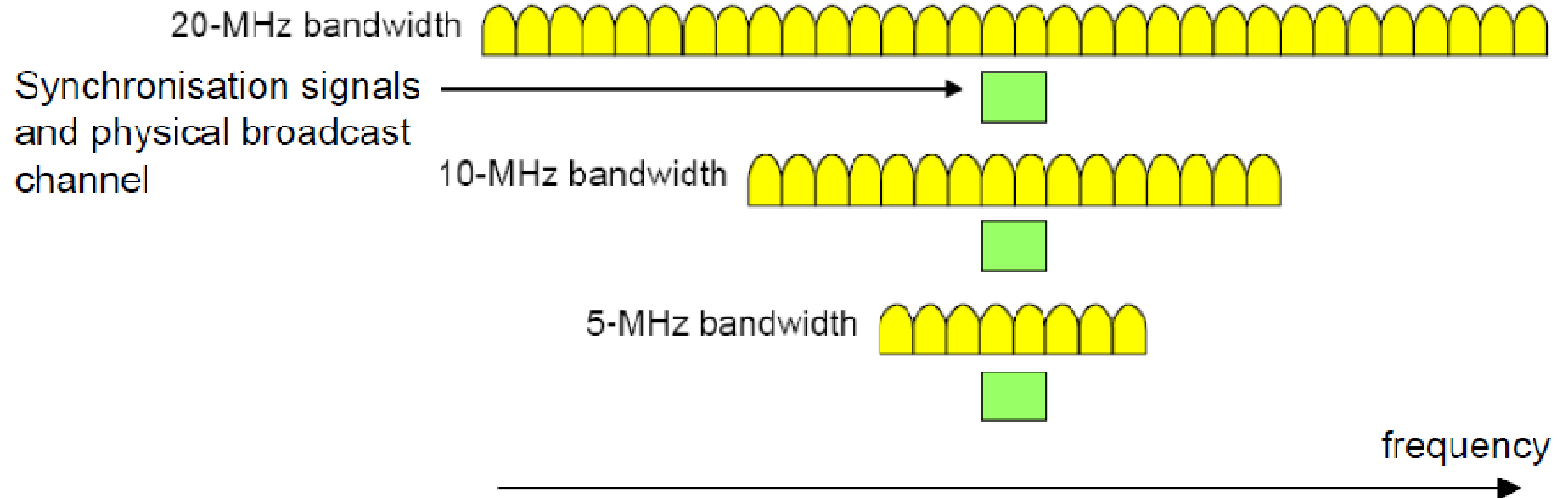
Il generico elemento della matrice rappresenta la risorsa base (Resource Block): 180 kHz



Canali di sincronizzazione e broadcast



- Banda fissa
- Collocati in posizione centrale (indipendentemente dalla banda totale)

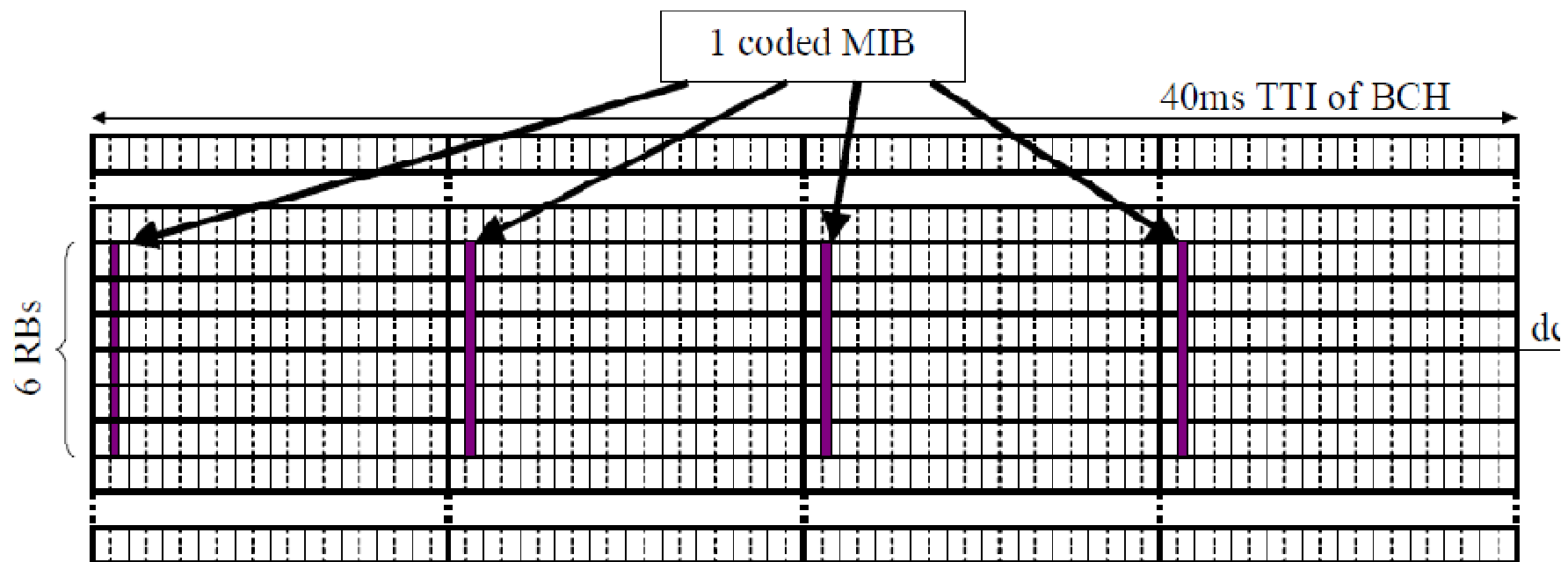




Banda e Resource Blocks

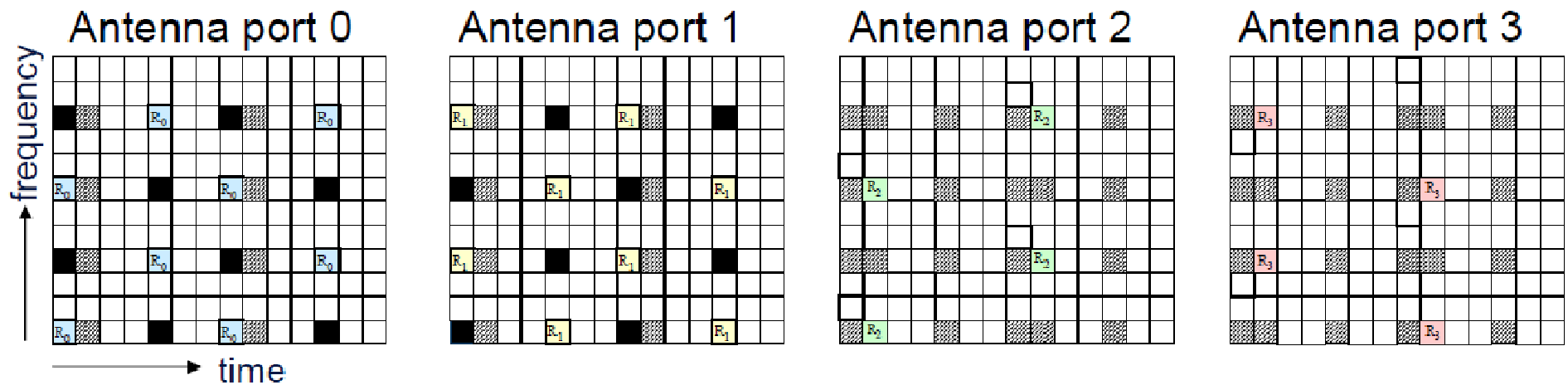
Banda	MHz	1.4	3	5	10	15	20
Configurazione di trasmissione	N_{RB}	6	15	25	50	75	100
	MHz	1.08	2.70	4.5	9.0	13.5	18.0

- Physical broadcast channel (PBCH) nel subframe 0 di ogni radio frame
 - Master Information Block (MIB)
 - Specifica la banda utilizzata
 - Ricevibile correttamente anche a bordo cella
 - Basso tasso di trasmissione, QPSK, codice convoluzionale di tasso 1/3 con ripetizione, TTI=40 ms
 - Indicazione del numero di antenne

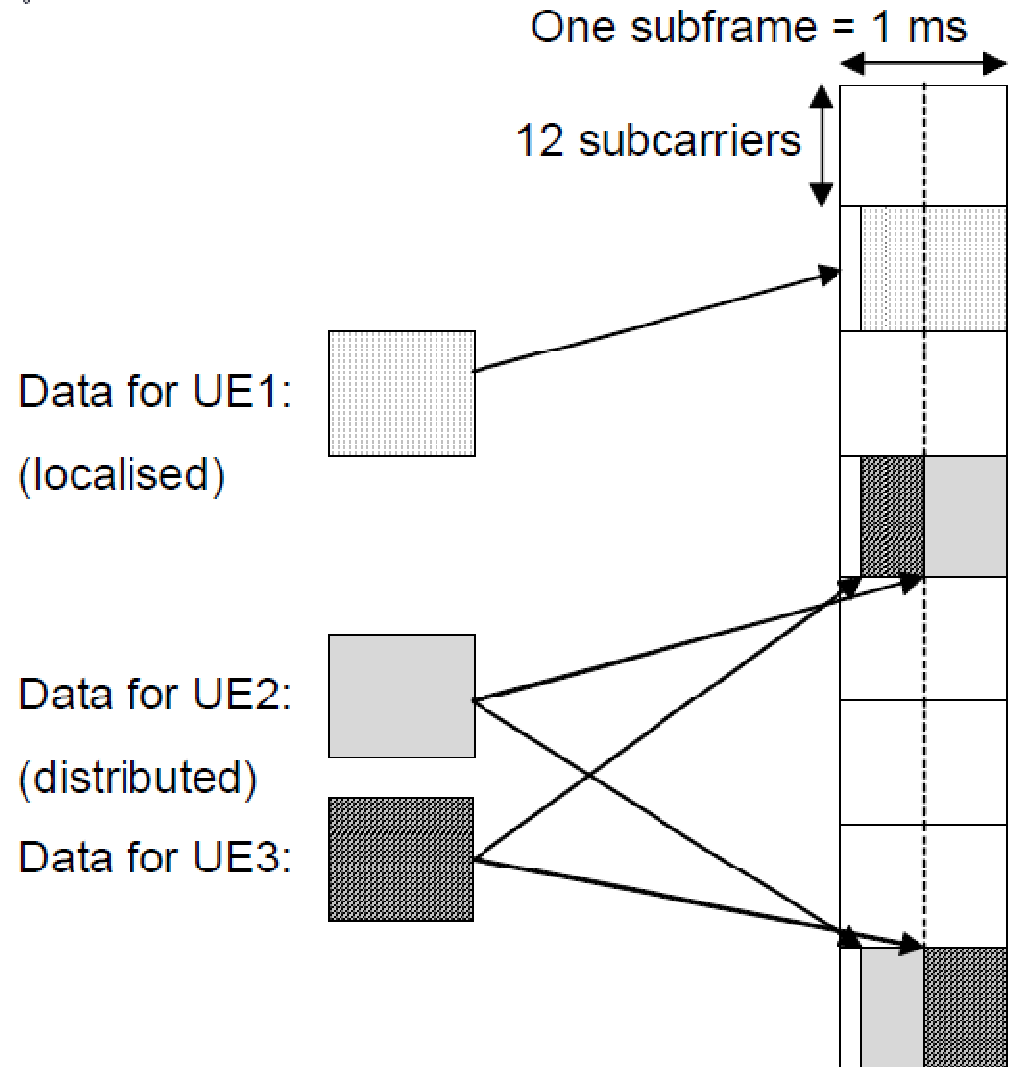


Segnali di riferimento

- Previsti per 1, 2, 4 antenne (Rel. 8)
 - Stima del canale
 - Disposizione sparsa, a rombo, per canali selettivi in frequenza a compatibile con elevata mobilità.
 - Limitato overhead
 - QPSK con basso valore PAPR

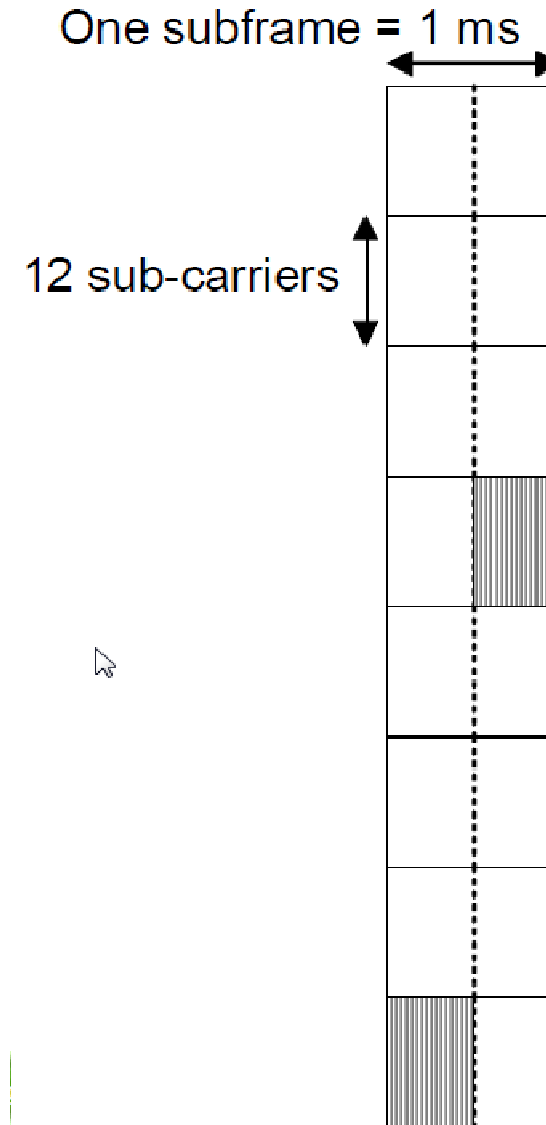


- Trasportano dati utente, informazioni broadcast di sistema, messaggi di paging
- Risorse assegnate dinamicamente mediante i canali di controllo (PDCCH)
- Risorse localizzate (trasmesse in unico blocco di sottoportanti)
- Risorse distribuite (diversità)



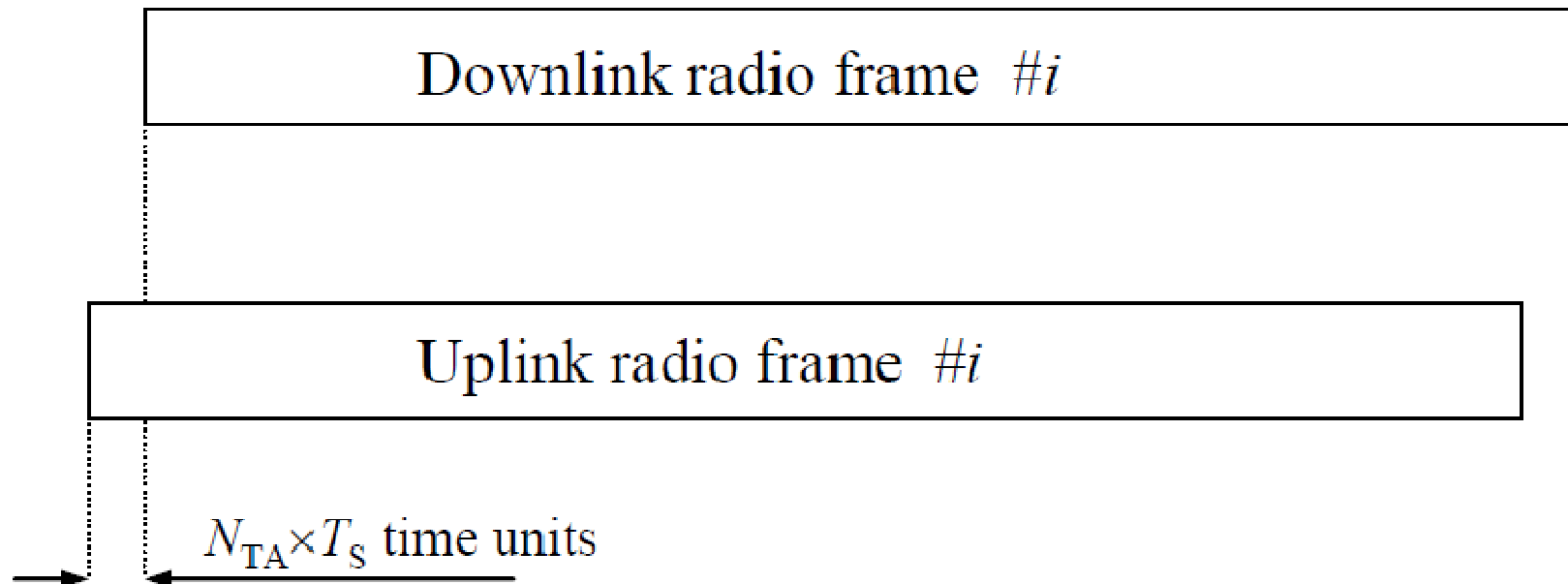
Uplink Resource allocation

- Stessa struttura del downlink basata sui PRB.
- Allocazione contigua di PRB
- Frequency hopping facoltativo
- In un subframe i PRB allocabili sono multipli di 2, 3 o 5.



Timing advance

- L'ortogonalità delle trasmissioni in uplink viene ottenuta utilizzando il *Timing Advance*
- Il valore viene impostato in fase di Random Access
- In seguito il valore viene continuamente aggiornato
- Dimensione massima: 100 km





Struttura canali uplink

- In presenza di dati utente la trasmissione avviene sul Physical Uplink Shared Channel (PUSCH)
- Vengono utilizzate le sottoportanti centrali per limitare le emissioni fuori banda.
- Si utilizzano gli stessi tassi di codifica e le stesse tecniche adattative del PDSCH
- Modulazioni QPSK, 16QAM, 64QAM
- Le informazioni di controllo vengono multiplexate con i dati, per garantire la struttura single carrier
- In assenza di dati utente, le informazioni di controllo vengono inviate utilizzando il Physical Uplink Control Channel (PUCCH), posizionato in uno dei due estremi della banda (per diversità, l'estremo utilizzato cambia nel tempo)

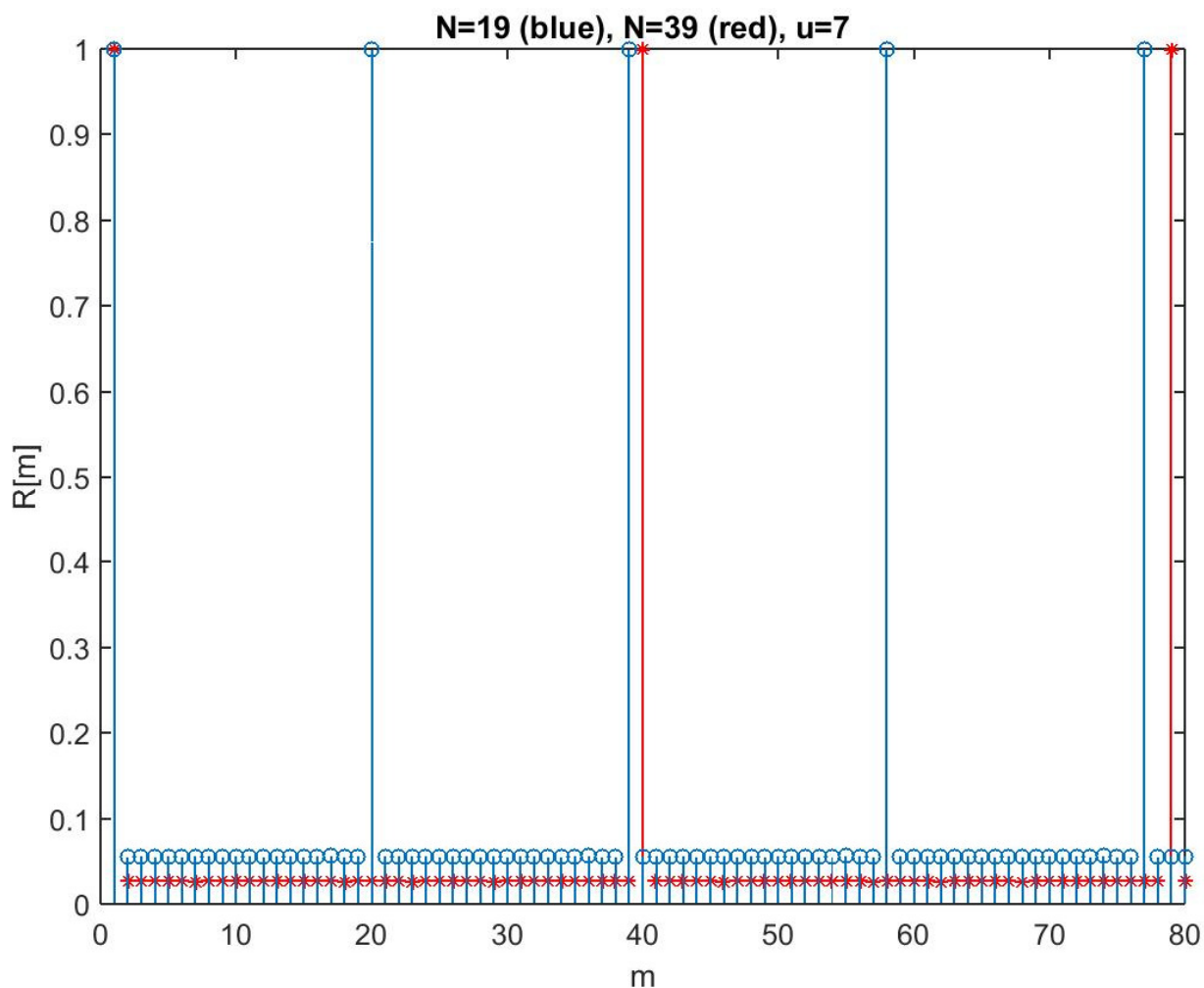


Random Access Channel (RACH)

- La procedura di accesso inizia con un preambolo (PRACH).
- La posizione del preambolo, assegnata dall'eNB, è interna alla regione PUSCH.
- Il PRACH preamble occupa 6 PRB
 - Stima temporizzazione
 - Indipendente dalla banda
 - Sequenze Zadoff Chu
 - $x[n]=\exp(-j\pi un(n+1+2q)/N)$, u , N , q interi, N dispari e primo con $u < N$.
 - Periodica di periodo N .
 - Eccellenti caratteristiche in termini di correlazione (autocorrelazione nulla per valori diversi dal periodo)
 - Spettro piatto
 - Disponibili sequenze distinte, ottenute mediante shift ciclici oppure radici (valori u_1, u_2 tali che $u_1 - u_2$ è primo con N) diverse.

Sequenze Zadoff Chu

- Autocorrelazione









Categorie UE LTE

Categoria	Banda (MHz)	MIMO	Duplex	Modulation		Bit rate Mbit/s	
				UL	DL	UL	DL
1	1.4,	2x2	FDD	QPSK	QPSK	5	10
2	3.5,10,		H-FDD	16QAM	16QAM	25	51
3	15, 20		TDD	64QAM	64QAM	51	100
4					64QAM	51	150
5			2x2 4x4		QPSK 16QAM 64QAM		75



Bande utilizzate in Europa

N	Duplex	f MHz	Nome	UL MHz	DL MHz	Spacing MHz	B MHz	A	C	I	S
											
1	FDD	2100	IMT	1920 – 1980	2110 – 2170	190	5, 10, 15, 20				X
3	FDD	1800	DCS	1710 – 1785	1805 – 1880	95	1.4, 3, 5, 10, 15, 20	X	X	X	X
7	FDD	2600	IMT-E	2500 – 2570	2620 – 2690	120	5, 10, 15, 20	X		X	X
8	FDD	900	E-GSM	880 – 915	925 – 960	45	1.4, 3, 5, 10				X
20	FDD	800	EU Digital Dividend	832 – 862	791 – 821	-41	5, 10, 15, 20	X	X	X	X



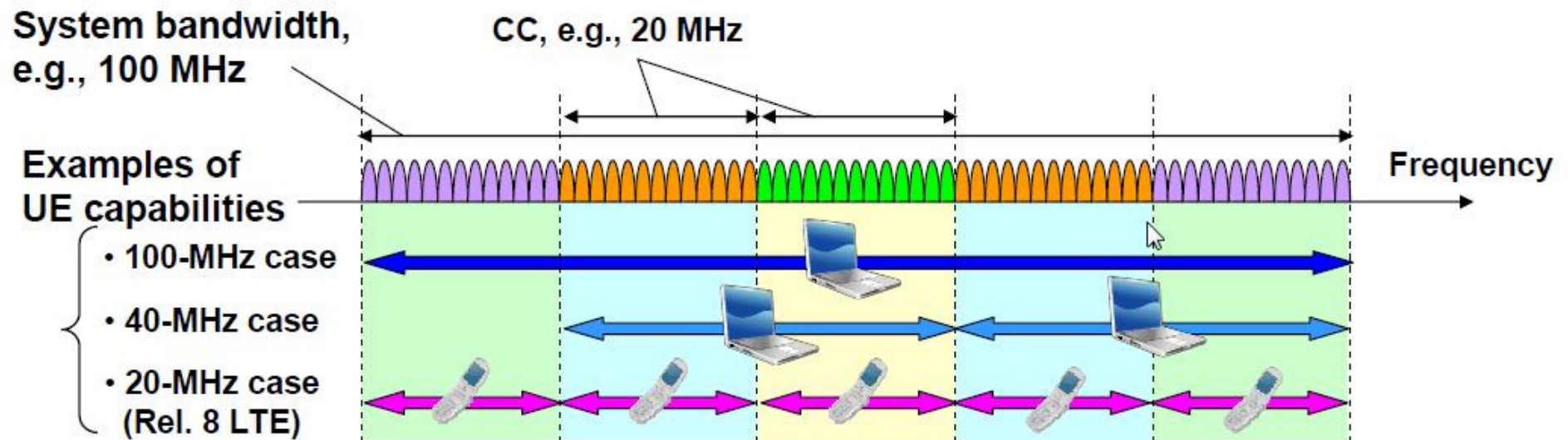
Release 10 (LTE Advanced)

- Tasso massimo di trasmissione
 - 1 Gbps utilizzando 4-by-4 MIMO e una banda maggiore di 70 MHz
- Efficienza spettrale
 - Raddoppio dell'efficienza spettrale in UL

		Rel. 8 LTE	LTE advanced	IMT-Advanced
Tasso massimo di trasmissione	DL	300 Mbps	1 Gbps	1 Gbps
	UL	75 Mbps	500 Mbps	
Efficienza spettrale massima [bps/Hz]	DL	15	30	15
	UL	3.75	15	6.75

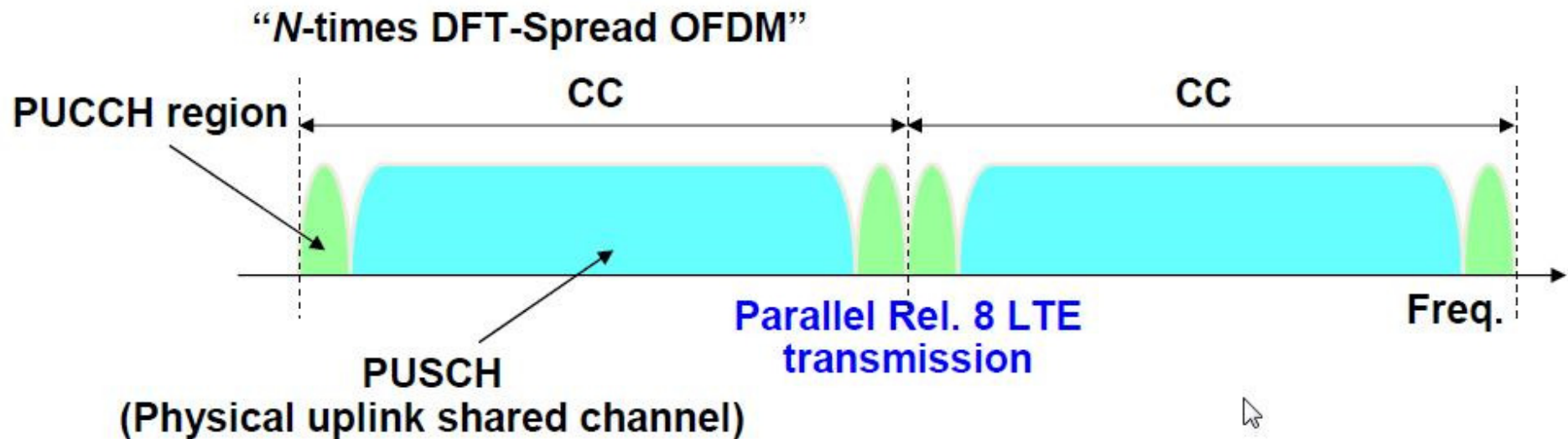
Aggregazione di portanti

- Incremento della banda aggregando portanti.
- L'aggregazione si ottiene combinando i Frequency Blocks (tipicamente da 20 MHz).
- L'aggregazione può avvenire in modo non continuo e asimmetrico fra UL e DL.



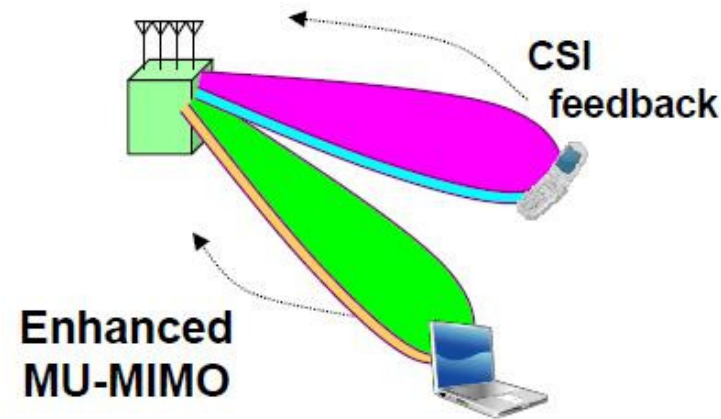
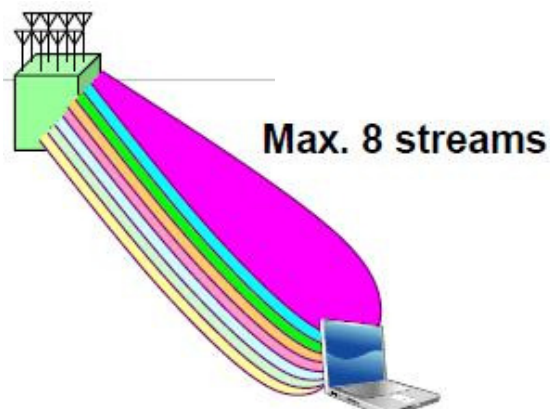
Uplink Multiple Access Scheme

- Trasmissione multi CC (Carrier Component) in parallelo.
- Allocazione non contigua
- Trasmissione simultanea PUSCH – PUCCH
- Controllo di potenza indipendente fra CC distinti

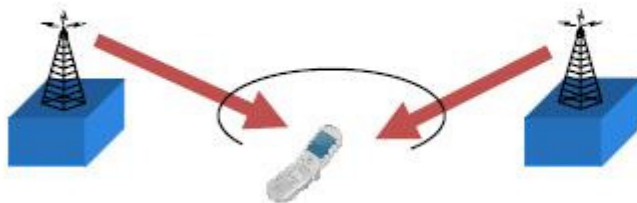


Enhanced Downlink Multi-antenna Transmission

- Trasmissione fino a 8 flussi indipendenti al singolo utente.
- Incremento dei simboli di riferimento per la stima del canale.
- Trasmissione multi-utente.
- Scheduling/beamforming coordinato fra le celle.



Coherent combining or dynamic cell selection



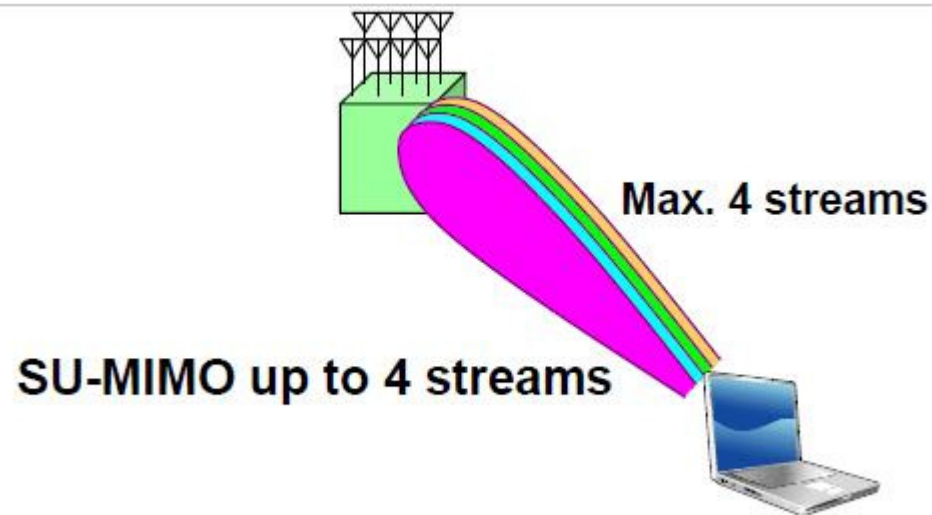
Joint transmission/dynamic cell selection



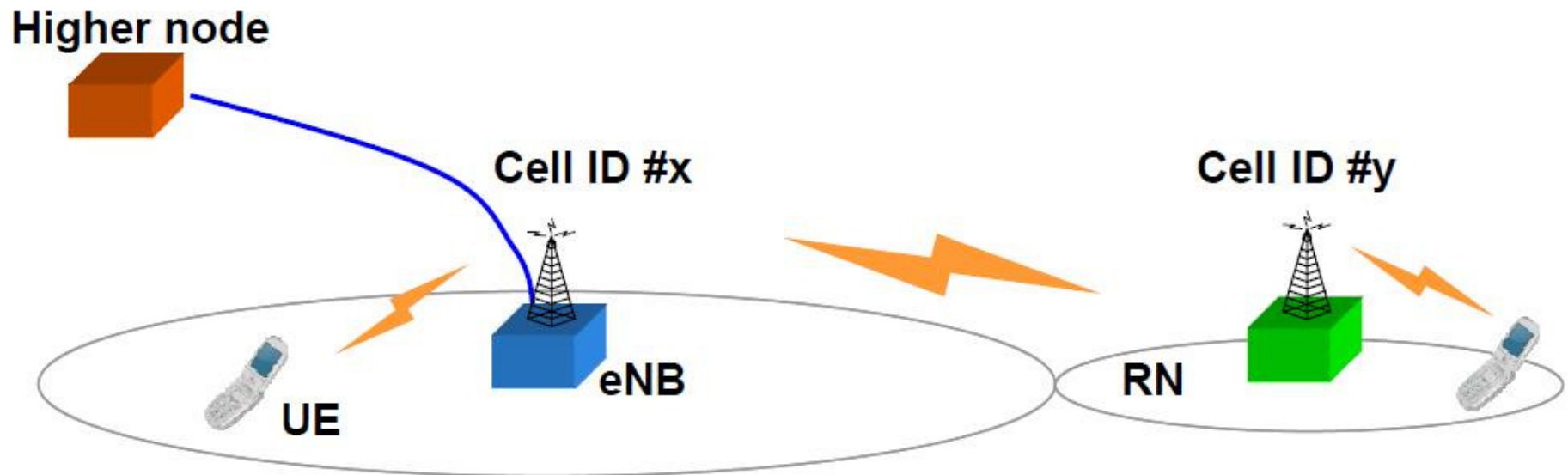
Coordinated scheduling/beamforming

Enhanced Uplink Multi-antenna Transmission

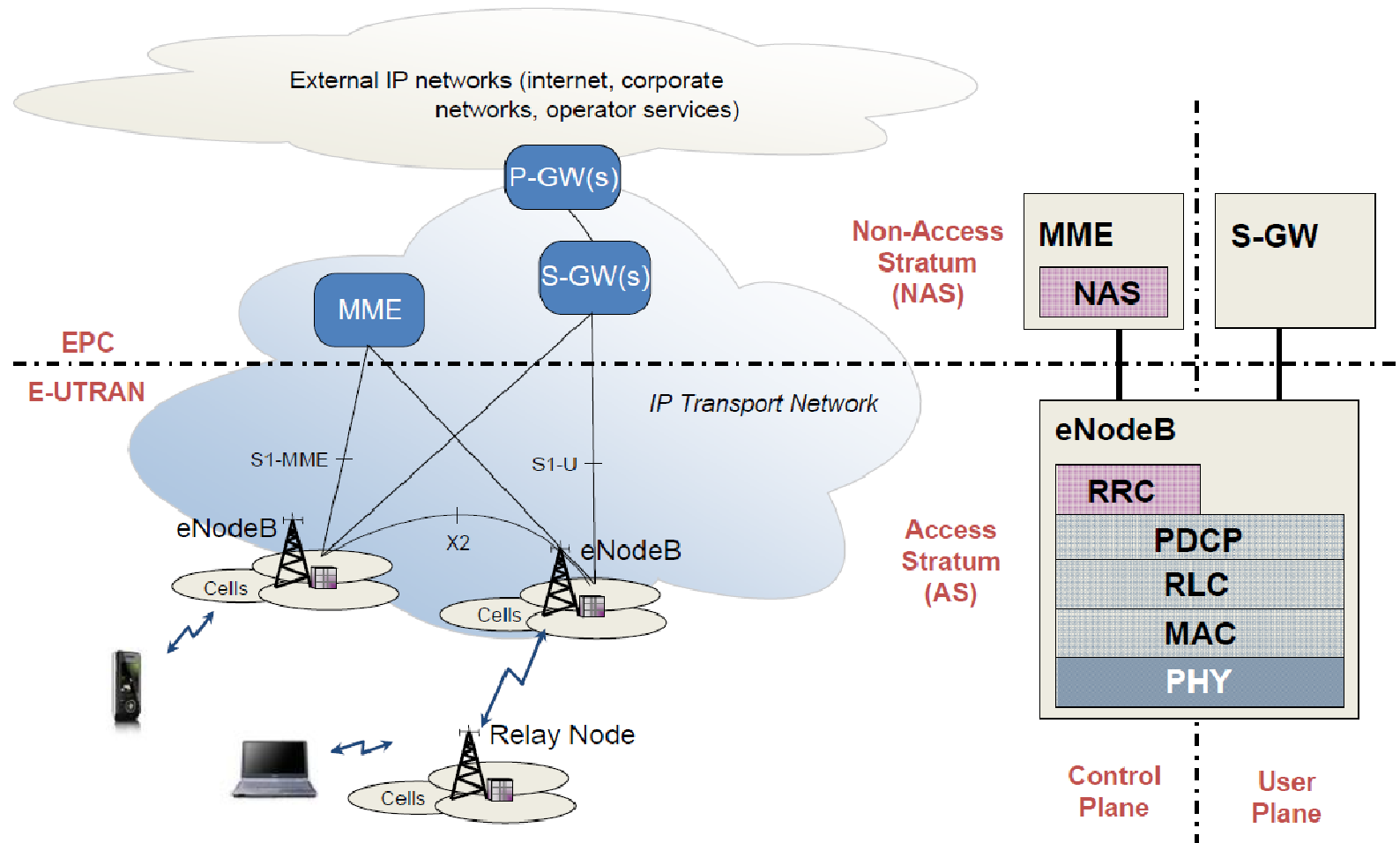
- Diversità in trasmissione per il PUCCH
- SU MIMO con 4 flussi trasmissivi
- Cancellazione dell'interferenza iterativa per incremento del throughput.



- Utilizzo di Relay
 - Il Relay forma una cella distinta da quella presso cui l'utente è registrato
 - Il Relay coopera nella trasmissione di segnali di controllo e nell'esecuzione di hybrid ARQ
 - Il Relay è visto come un Node B dai mobili compatibili con la Rel. 8



Architettura E-UTRAN





User Plane Protocol Stack (1)

- Livelli comunicazione Ue-NodeB
 - PDCP (*Packet Data Convergence Protocol*)
 - Compressione Header
 - Consegna ordinata
 - Gestione Radio Bearers AM (Ack Mode) in fase di handover
 - Rivelazione pacchetti duplicati
 - Cifratura
 - Protezione integrità (Control Plane)
 - RLC (Radio Link Control)
 - Trasmissione PDU dei livelli superiori AM, UM, TM (Transparent)
 - Gestione ARQ
 - Segmentazione
 - Ri-segmentazione in caso di ripetizione
 - Concatenazione SDU per lo stesso radio bearer
 - Rivelazione a recupero errori
 - Consegna ordinata



User Plane Protocol Stack (2)

- MAC (Media Access Control)
 - Multiplexing/demultiplexing RLC PDU
 - Scheduling Information reporting
 - Correzione d'errore mediante HARQ
 - Gestione priorità
 - Padding



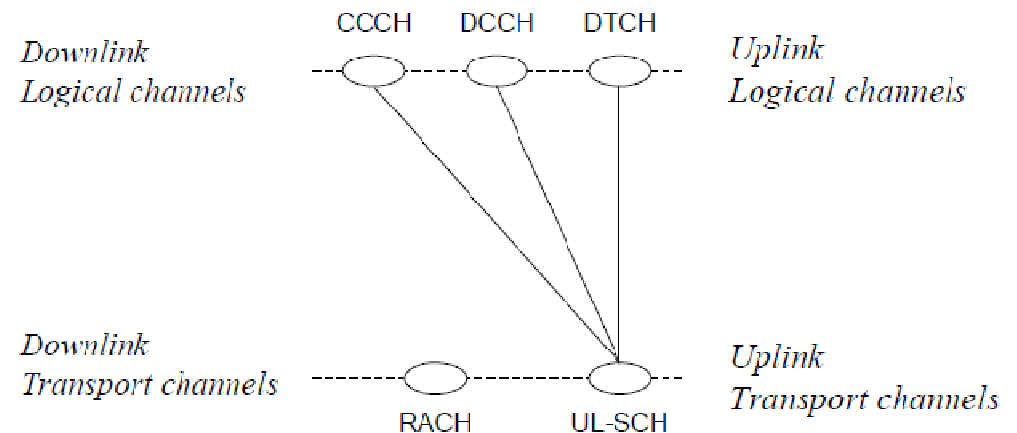
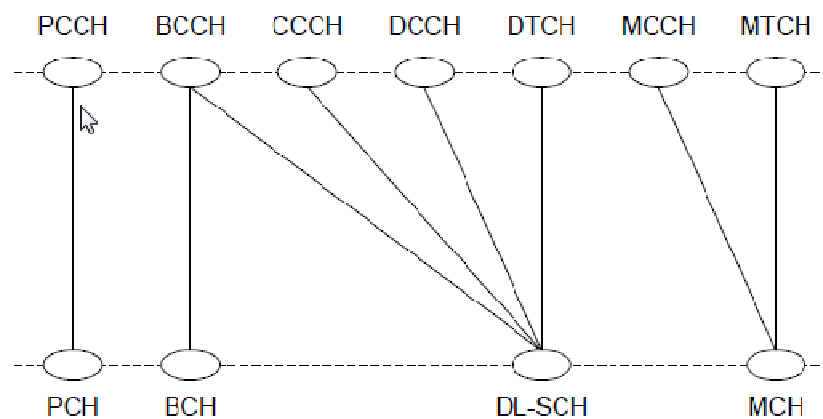
RLC: modalità operative

- Transparent Mode
 - Gestisce il flusso di pacchetti senza fare modifiche (senza aggiungere header, senza compiere suddivisioni o assemblaggi), svolgendo solo la funzione di buffer, con timeout.
- Unacknowledged Mode
 - Gestisce il flusso di pacchetti fornendo le funzioni di buffering, segmentazione e ri-assemblaggio.
- Acknowledged Mode
 - Gestisce il flusso di pacchetti fornendo le funzioni di buffering, segmentazione e ri-assemblaggio. Memorizza i pacchetti per procedere a eventuali ritrasmissioni.

Canali logici e canali di trasporto

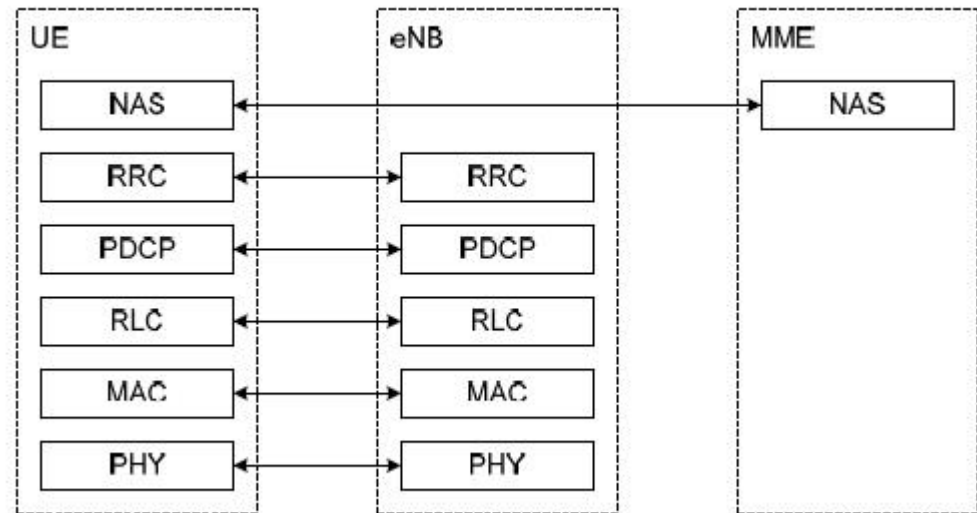
- Canali di trasporto:
 - PCH: Paging Channel
 - BCH: Broadcast Channel
 - MCH: Multicast Channel
 - DL-SCH: DL Shared Channel
 - UL-SCH: UL Shared Channel

- Canali logici:
 - PCCH: Paging Control Channel.
 - BCCH: Broadcast Control Channel
 - CCCH: Common Control Channel
 - DCCH: Dedicated Control Channel
 - DTCH: Dedicated Traffic Channel
 - MCCH: Multicast Control Channel
 - MTCH: Multicast Traffic Channel



Control plane protocol stack

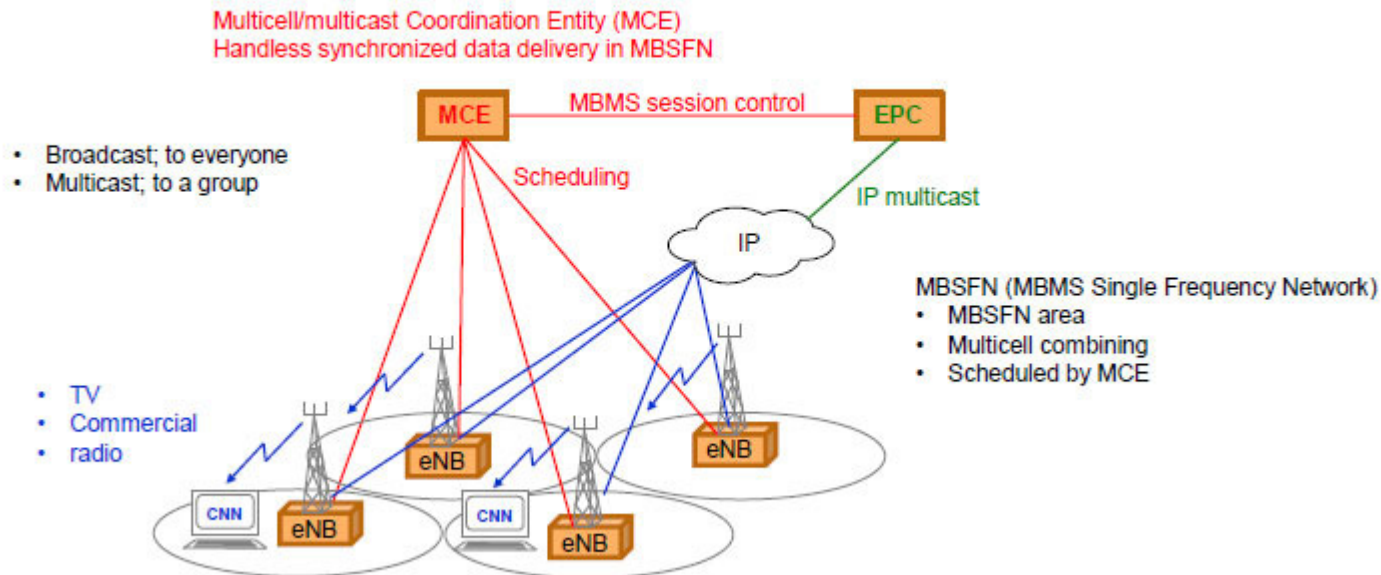
- RLC e MAC come nell'User Plane
- PDCP gestisce cifratura e integrità
- Funzioni RRC
 - Invio di Informazioni Broadcast e di sistema associate al NAS (Non Access Stratum) e all' AS (Access Stratum)
 - Stabilire, mantenere e rilasciare connessioni RRC
 - Stabilire, mantenere e rilasciare Signalling e Data Radio Bearers (SRBs and DRBs)
 - Funzioni associate alla sicurezza (gestione della chiave)
 - Funzioni di mobilità
 - Selezione cella
 - Paging
 - Misure e rapporti UE
 - Handover
 - QoS management
 - Notifiche per ETWS (Earthquake e Tsunami Warning System), CMAS (Commercial Mobile Alert System) e MBMS (Multimedia Broadcast/Multicast Service)



MBMS

- E-UTRAN (Evolved Universal Terrestrial Access Network)
- Requisiti: elevata efficienza spettrale, flessibilità, basso ritardo.

a) Multimedia Broadcast Multicast Service (MBMS)



- <http://www.3gpp.org/technologies/keywords-acronyms/98-lte>

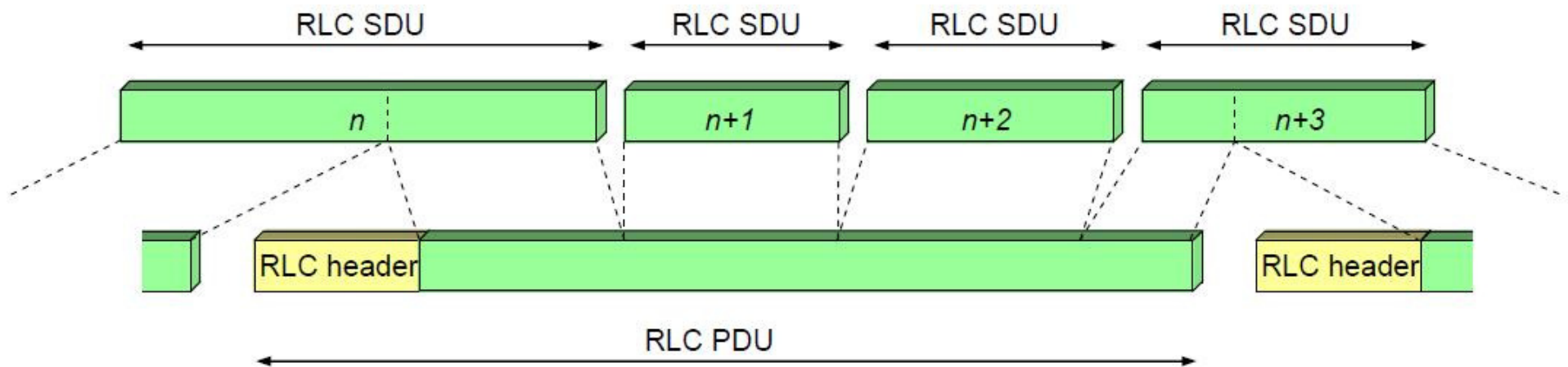


Gestione ritrasmissioni

- A livello MAC si adotta il protocollo Hybrid ARQ, mentre per i servizi confermati (AM) un ulteriore protocollo ARQ è adottato a livello RLC
- Affidabile ed efficiente
 - HARQ feedback trasmesso sul canale di controllo L1/L2
 - Un solo bit, non codificato (basso overhead)
 - Trasmissione a ogni subframe (veloce)
 - Soft-combining (efficiente)
 - Rapporti ARQ trasmessi come MAC data (protetti da CRC a 24 bit) e ripetizioni HARQ
- Sia HARQ che ARQ sono gestiti a livello eNB
 - Gestione veloce di errori residui HARQ
 - Bassa latenza ed elevata affidabilità

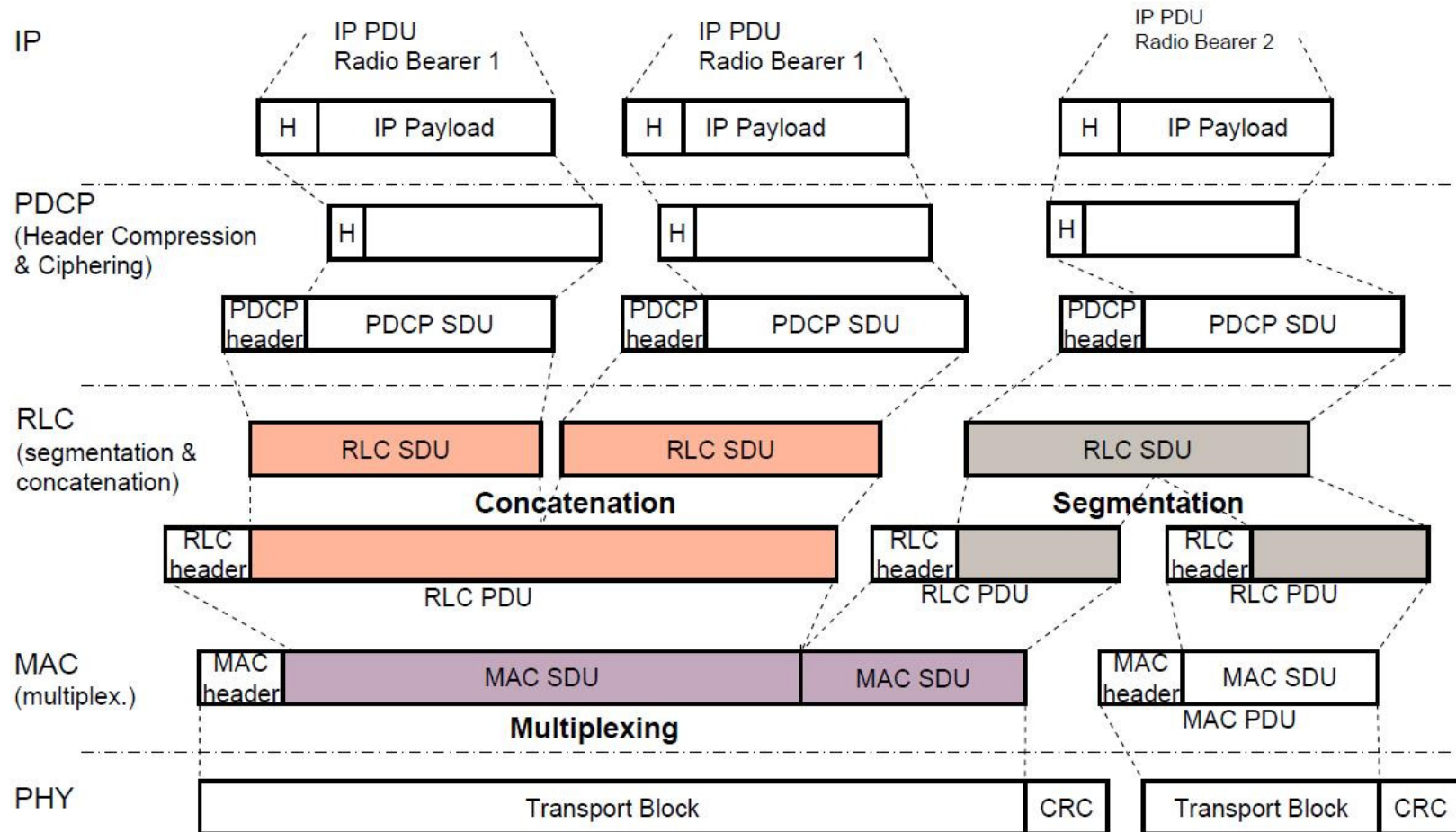
Trasporto affidabile e senza perdite

- Consegna in sequenza e senza perdite garantita dalle ripetizioni RLC (ARQ), utilizzando il Sequence Number (SN) per riordinare
- Il PDCP gestisce il recupero e riordino in caso di handover (radio bearers AM solamente)

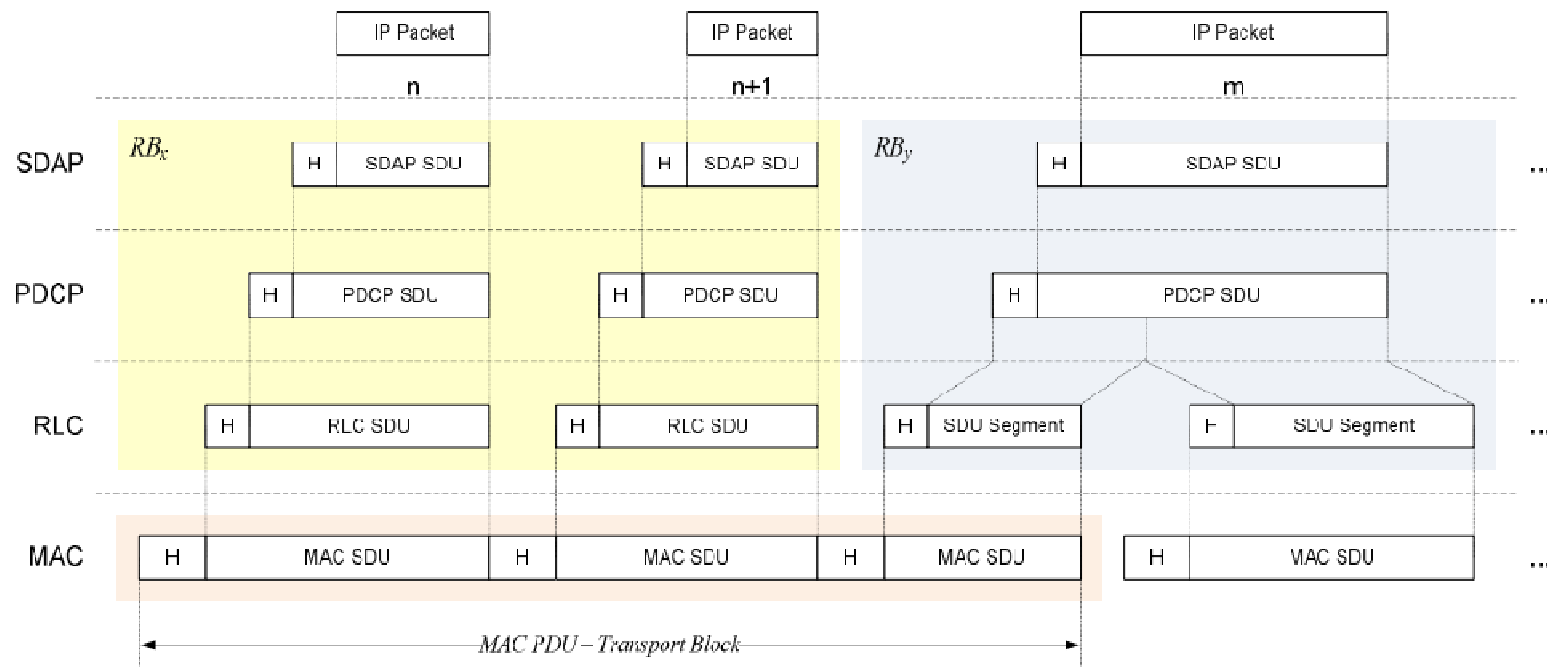


- Il PDCP elimina eventuali duplicati (in base al SN) che creerebbero problemi al TCP.

LTE: Concatenation-Segmentation



5G Concatenation-Segmentation





Scheduling

- Lo Scheduler si trova nell'eNB, con l'obiettivo di:
 - Garantire il rispetto della QoS garantita
 - Massimizzare il throughput della cella
 - Garantire la *fairness*
- Informazioni utili allo Scheduling fornite dall'UE:
 - Channel Quality Indication
 - Buffer Status Report
 - Power Headroom Report
 - Uplink Sounding
- QoS con granularità a livello di bearer (parametri associati ai bearer)
 - QoS Class Identifier (**QCI**); Guaranteed Bit Rate (**GBR**); Allocation and Retention Priority (**ARP**)
 - Logical Channel Priority; Prioritised Bit Rate (**PBR**); Aggregate Maximum Bitrate (**AMBR**)
 - Servizi: Conversazione base, Conversazione avanzata, Scambio interattivo a basso e alto ritardo, streaming live e non-live, background.



Cifratura e protezione d'integrità

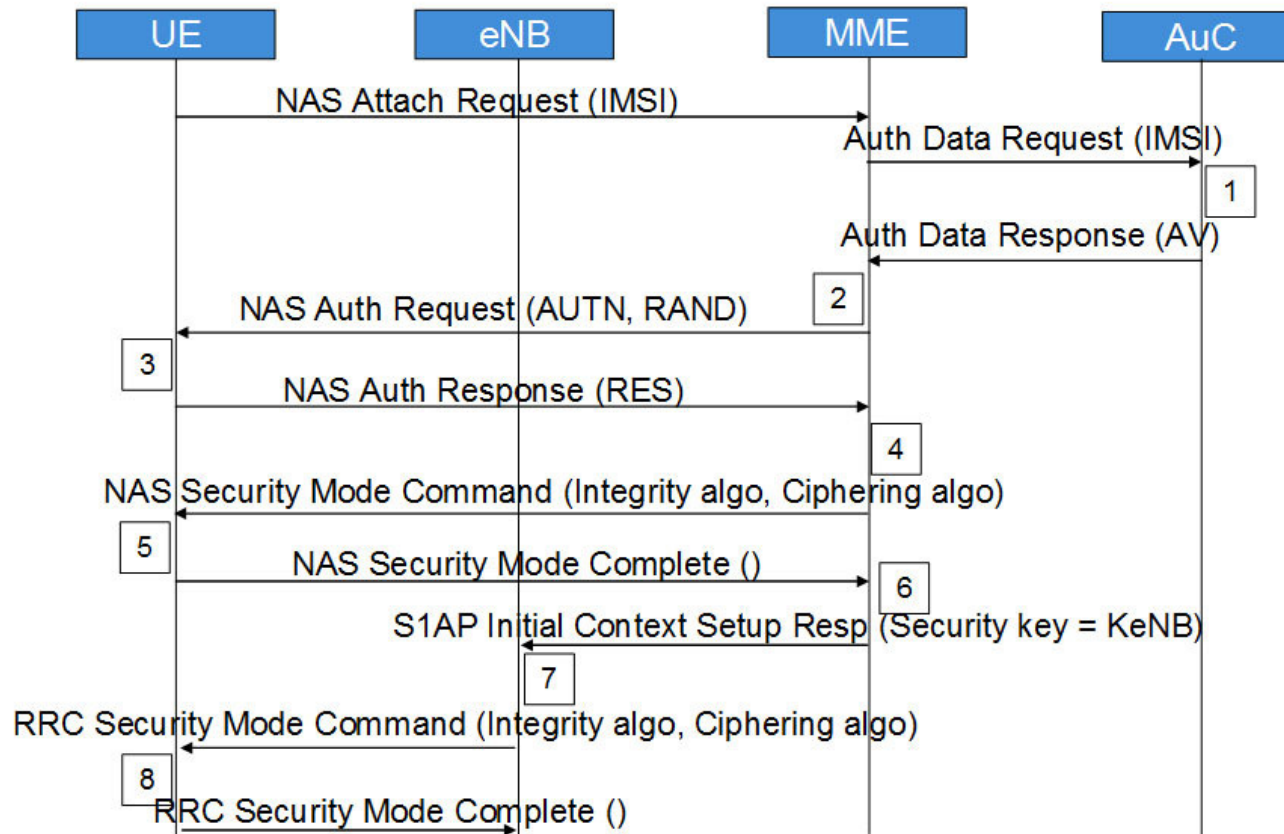
- Funzioni di sicurezza fornite dal PDCP su controllo dell'RRC
 - Attive dall'accensione
 - Basate sugli algoritmi SNOW 3G e AES
 - Chiavi modificate in caso di handover
 - Contatore diviso in due parti
 - Hyper Frame Number (HFN): gestione locale
 - Sequence Number (SN): trasmesso over the air
- Protezione d'integrità
 - Per i C-plane radio bearers (Radio Bearers di segnalazione)
 - 32-bit Message Authentication Code (MAC-I) posto in fondo alla PDU
- Cifratura (confidenzialità)
 - Per i C-plane radio bearers (Radio Bearers di segnalazione)
 - Per gli U-plane radio bearers (Data Radio Bearers)
 - Le PDU di controllo del PDCP (RoHC feedback and PDCP status reports) non sono cifrate



SNOW 3G - AES

- **SNOW 3G:**
Cifratura sequenziale basata su un registro a scorrimento, e una macchina a stati
128-bit key, 128-bit IV
Generate Keystream: 10K gates, 1.72 Gbps
- **AES:**
Cifratura a blocchi
128-bit block, 128, 192 and 256-bit keys
Enc/Dec: 5.4K gates, 311Mbps ~ 21K gates, 2.6Gbps @ 0.13 μ m CMOS

Autenticazione



<http://www.3gppinfo.com/wp-content/uploads/2011/03/Security-state-diagram.jpg>



Fasi autenticazione (1)

- 1. Il mobile (UE) inizia la procedura (NAS attach request)
 - MME (VLR del 3G) richiede i vettori di autenticazione (AV) associati all'IMSI richiedente inviando l'Authentication Data Request.
 - AuC/HSS recupera le Pre Shred Keys (PSK) associate all'IMSI e le utilizza per il calcolo dei vettori di autenticazione, che vengono inviati mediante l'Authentication Data Response (Authentication Vector AV).
- 2. MME ricava IK, CK, XRES, RAND e AUTN dall'AV
 - MME trasmette AUTN e RAND a UE (Authentication Request).
- 3. UE autentica NW (la rete) verificando l'AUTN ricevuto
 - Quindi calcola IK, CK, RES, XMAC dalla propria chiave di sicurezza UE AMF, (OP), da AUTN e RAND.
 - UE trasmette RES con l'Authentication response.
- 4. Ricevuto il comando RRC security mode UE
 - Calcola Krrc-int, Krrc-enc, Kup-enc.
 - Invia RRC security mode complete to eNB

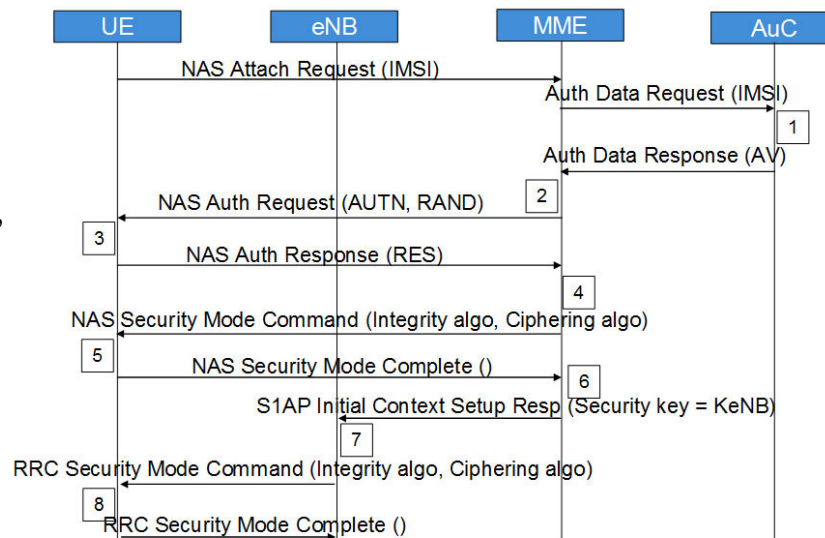


Diagram4: - Security state diagram

Fasi autenticazione (2)

- 5. Ricevuto il NAS Security Mode Command UE
 - Calcola KASME, KeNB, Knas-int, Knas-enc
 - Invia il NAS Security Mode Complete con integrità protetta e cifrato.
- 6. Ricevuto il comando NAS security mode da UE, MME
 - Invia KeNB a eNB con S1AP Initial Context Setup Request (Security key)
- 7. Ricevuta keNB, eNB
 - calcola Krrc-int, Krrc-enc, Kup-enc.
 - Invia RRC Security mode Command con AS integrity algo and AS ciphering algo.
- 8. MME compara RES e XRES. Se uguali l'autenticazione è andata a buon fine, altrimenti MME invia Authentication failure a UE.
 - MME azzera il contatore DL NAS, e calcola KASME, KeNB, Knas-int, Knas-enc. MME invia il NAS Security mode command (integrity algo, ciphering algo, NAS key set ID, UE Security capability) con integrità protetta ma non cifrato, usando Knas-inc.

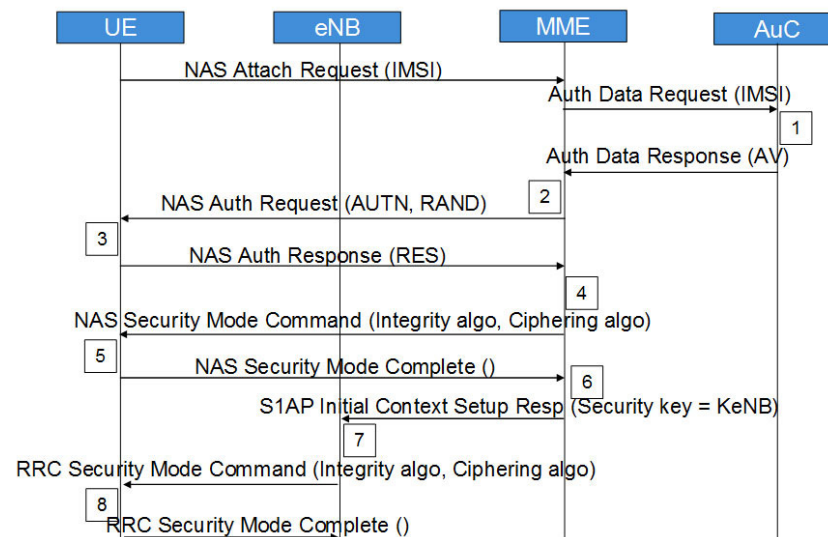


Diagram4: - Security state diagram



Riepilogo chiavi

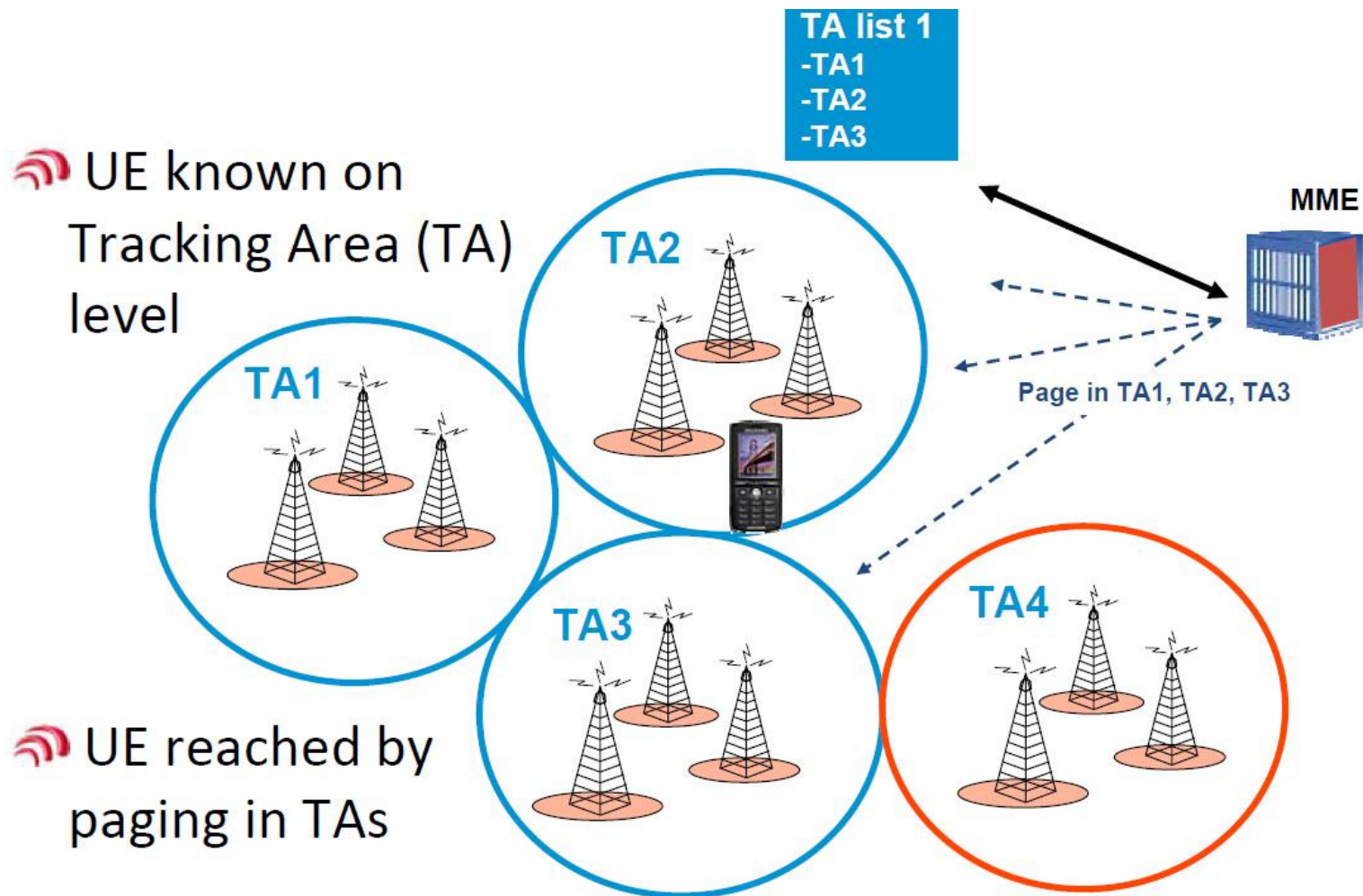
	UE	eNB	MME	HSS/AuC
Chiavi memorizzate	UE Security Key			UE Security Key
	AMF			AMF
	OP			OP
Chiavi generate				SQN
				RAND
Authentication Vectors	IK			IK
	CK			CK
				AK
	RES			XRES
	XMAC			MAC
				AUTN
Chiavi di cifratura	KASME		KASME	
	Knas-int		Knas-int	
	Knas-enc		Knas-enc	
	KeNB	KeNB		
	Krrc-int	Krrc-int		
	Krrc-enc	Krrc-enc		
	Kup-enc	Kup-enc		



Stati RRC

- IDLE:
 - UE noto all'EPC e ha un indirizzo IP
 - UE non noto all'E-UTRAN/eNB
 - La posizione dell'UE è nota a livello Area Tracking
 - La trasmissione di dati Unicast non è possibile
 - UE raggiungibile dal paging nelle aree tracking controllate dall'EPC
 - UE-based cell-selection e tracking area aggiornate dall'EPC
- CONNECTED (Dormant-Active):
 - UE nota all'EPC e all'EUTRAN/eNB; "context" in eNB
 - La posizione UE nota a livello di cella
 - La trasmissione di dati Unicast è possibile
 - Ricezione discontinua (DRX) attiva per risparmio energetico
 - La rete gestisce la mobilità

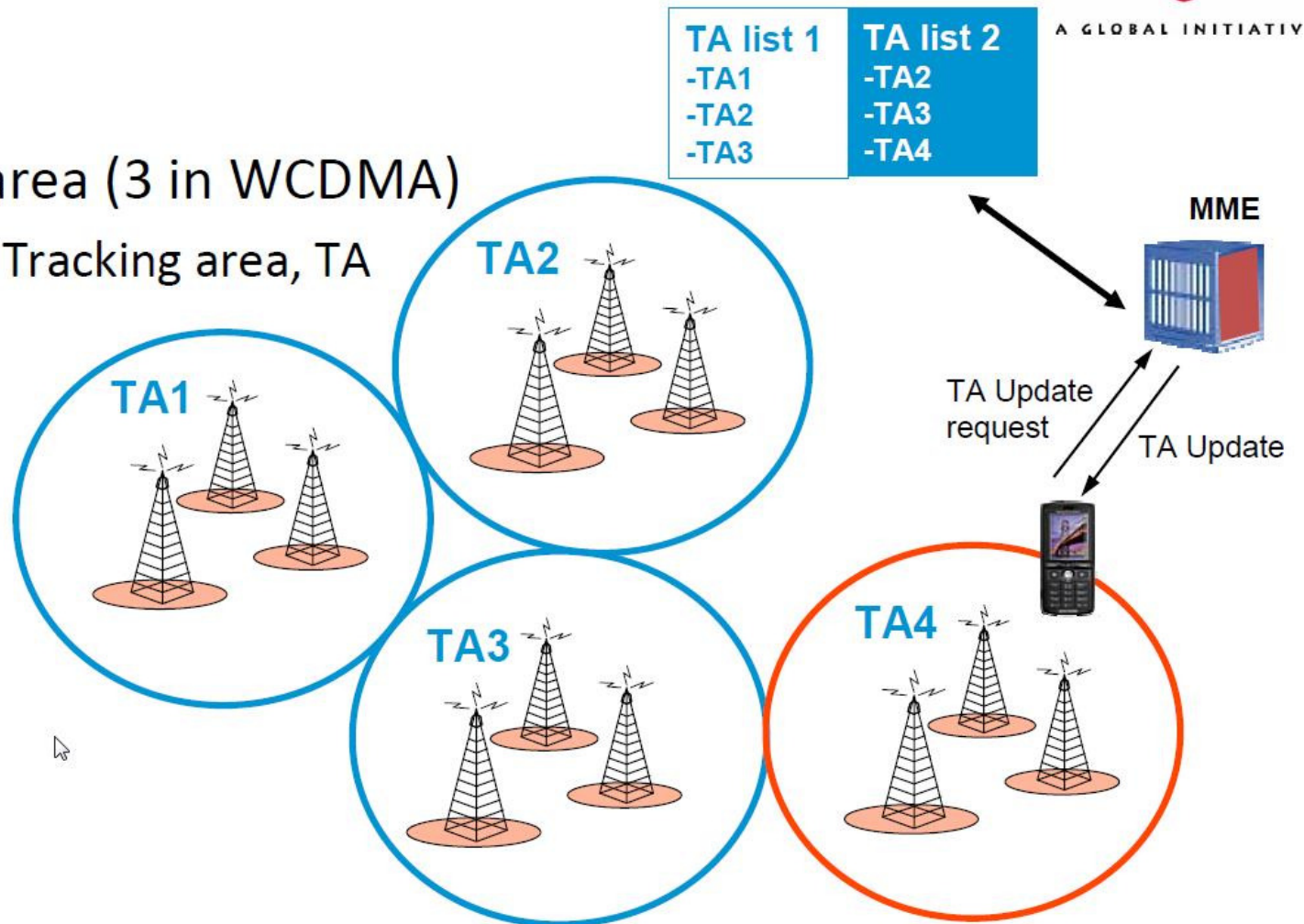
Mobilità in IDLE (1)



Mobilità in IDLE (2)

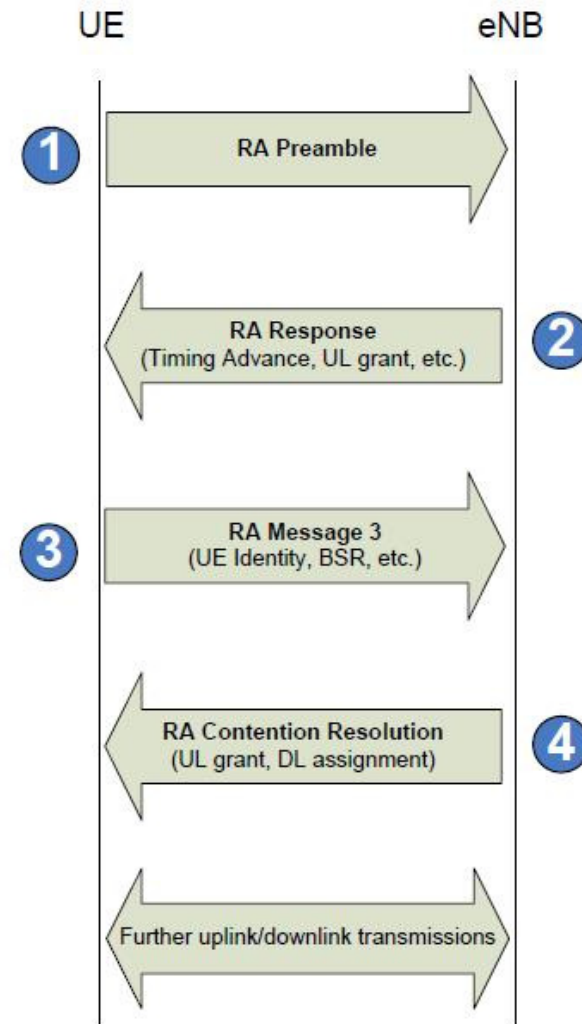
 1 area (3 in WCDMA)

- Tracking area, TA



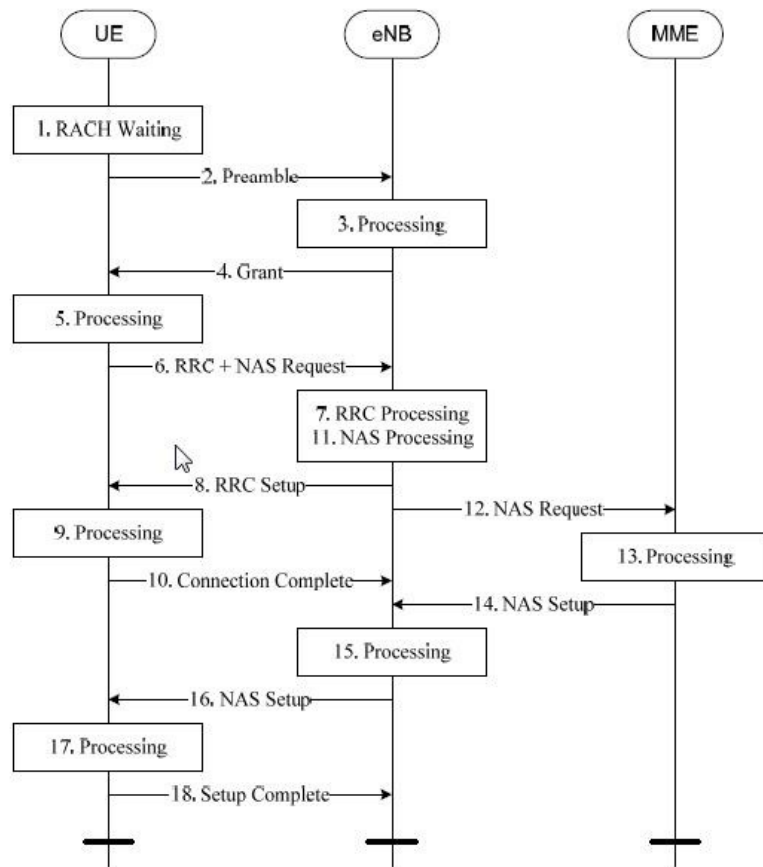
Random Access

- Trasmissione preambolo su PRACH
 - Stima ritardo da parte dell'eNodeB
- 2. Random access response
 - Impostazione Timing Advance
 - Assegnazione risorse UL-SCH
- 3. Risoluzione contesa
 - Trasmissione dati terminale
 - Possibile trasmissione altri dati
- 4. Risoluzione contesa
 - Eco dati terminale (da step 3)
 - Trasmissione altri dati segnalazione



Latenza

- User Plane. Latenza UE-eNB (FDD): TTI=1 ms; latenza=4 ms, quando non serve ripetere (HARQ)
- Control Plane



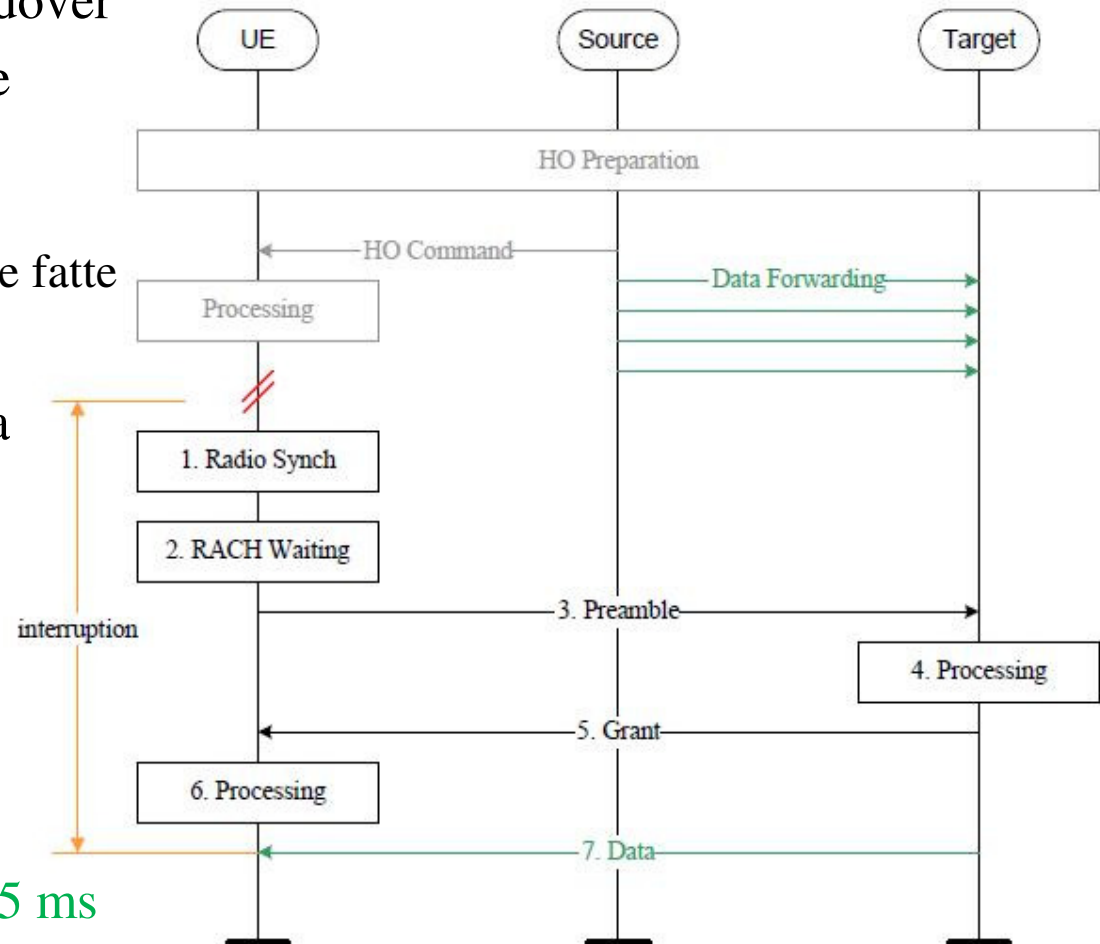
NOTE: LTE Rel-8 supports IDLE→CONNECTED latency of around 80ms and, hence, already meets the ITU requirement on C-plane latency for IDLE→CONNECTED transition

A GLOBAL INITIATIVE

Step	LTE Advanced Description	Time [ms]
1	Average delay due to RACH scheduling period (1ms RACH cycle)	0.5
2	RACH Preamble	1
3-4	Preamble detection and transmission of RA response (Time between the end RACH transmission and UE's reception of scheduling grant and timing adjustment)	3
5	UE Processing Delay (decoding of scheduling grant, timing alignment and C-RNTI assignment + L1 encoding of RRC Connection Request)	5
6	Transmission of RRC and NAS Request	1
7	Processing delay in eNB (L2 and RRC)	4
8	Transmission of RRC Connection Set-up (and UL grant)	1
9	Processing delay in the UE (L2 and RRC)	12
10	Transmission of RRC Connection Set-up complete	1
11	Processing delay in eNB (Uu → S1-C)	
12	S1-C Transfer delay	
13	MME Processing Delay (including UE context retrieval of 10ms)	
14	S1-C Transfer delay	
15	Processing delay in eNB (S1-C → Uu)	4
16	Transmission of RRC Security Mode Command and Connection Reconfiguration (+TTI alignment)	1.5
17	Processing delay in UE (L2 and RRC)	16
	Total delay	50

Tempistica Handover

- Intra-LTE inter-eNB handover
- Cella Target identificata e misurata dall'UE
 - Sincronizzazione radio rapida grazie alle misure fatte
- Inoltro dati iniziato prima della sincronizzazione
 - Dati già disponibili quando UE inizia la ricezione
- Ritardo complessivo: 10.5 ms

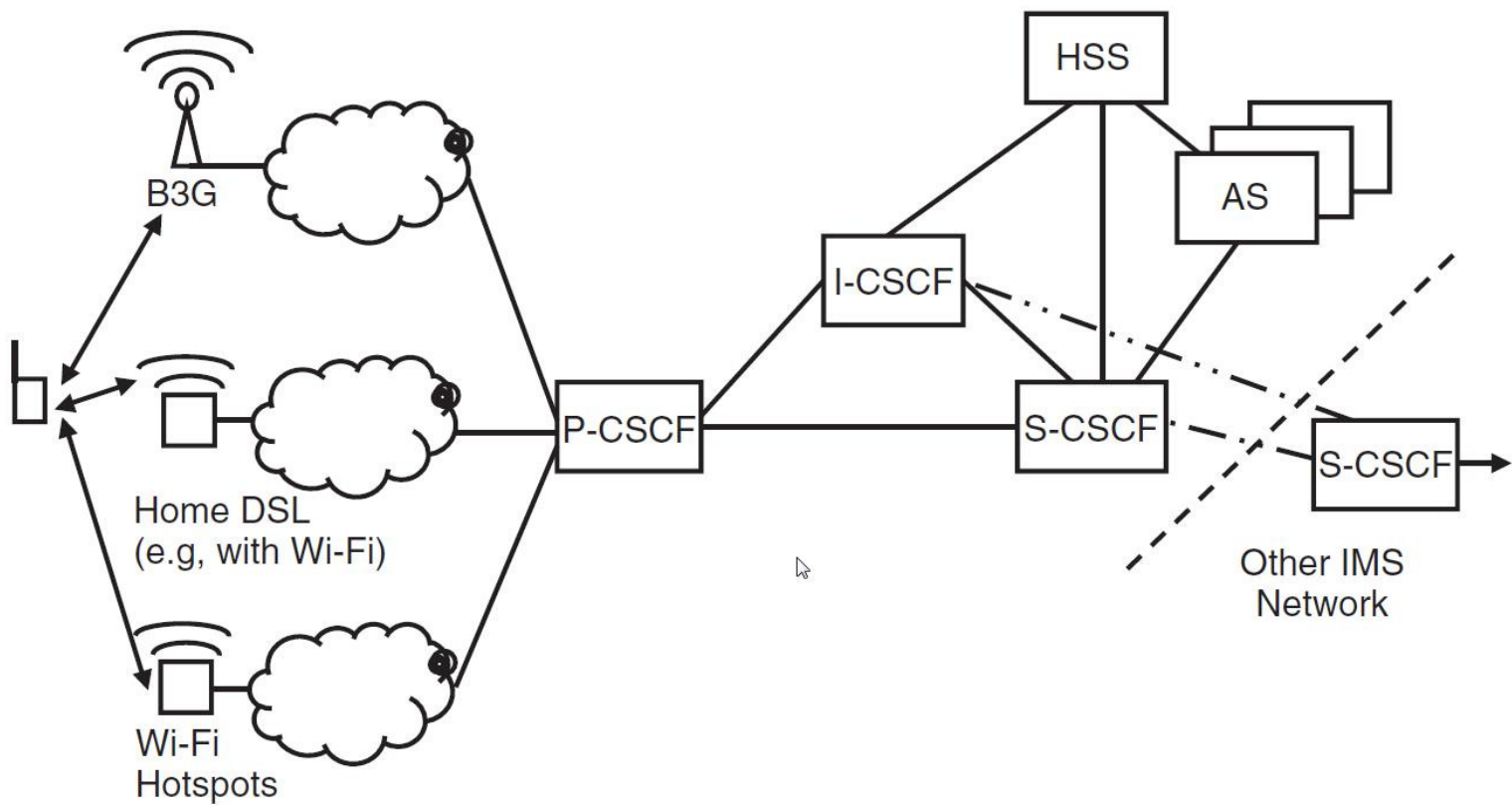




IP Multimedia System (IMS)

- SIP (Session IP) protocol viene comunemente utilizzato in Internet per gestire applicazioni che richiedono l'apertura di una sessione (Voice over IP soprattutto).
- SIP presenta numerose criticità che lo rendono inadatto all'ambiente wireless:
 - Manca gestione della mobilità
 - Insufficiente sicurezza
 - Scalabilità
- Per superare le criticità di SIP, da un'attività che vede cooperare 3GPP e IETF, è stato sviluppato IMS.
 - 3GPP TS 22.228
 - 3GPP TS 23.228

Architettura IMS





Proxy Call Session Control Function (P-CSCF)

- Funge da User Proxy; tutta la segnalazione che coinvolge l'utente transita per lui.
- Sicurezza: le comunicazioni di registrazione fra utente e proxy sono cifrate usando IPSec.
- Efficienza: IMS si avvale dei messaggi SIP che vengono compressi.
- QoS: P-CSCF verifica il rispetto dei requisiti minimali di QoS (ad esempio banda disponibile).
- Tariffazione: P-CSCF gestisce l'acquisizione delle informazioni utili alla tariffazione.



Altri elementi di IMS

- **Serving Call Session Control Function (S-CSCF)**: svolge le funzioni di registrazione SIP, e di proxy SIP.
- **Interrogating-Call Session Control Function (I-CSCF)**: identifica il S-CSCF idoneo a soddisfare le prestazioni dall'utente (sulla base delle indicazioni dell'HSS).
- **Home Subscriber Server (HSS)**: evoluzione dell'HLR; contiene informazioni sugli utenti GSM, GPRS, UMTS, LTE, e IMS
- **Diameter**: protocollo di segnalazione usato da IMS (deve il suo nome al predecessore, RADIUS (Remote Access Dial In User Server)).
- Applicazioni principali
 - Rich Communication Service (RCS-e)
 - Messaggistica e servizi complementari alla telefonia
 - Condivisione immagini e video, file transfer
 - Voice Over LTE (VOLTE)
 - Conversazioni vocali



Verso il 5 G

