ALMA MATER STUDIORUM – UNIVERSITA' DI BOLOGNA
CAMPUS DI CESENA

DIPARTIMENTO DI INFORMATICA – SCIENZA E INGEGNERIA
CORSO DI LAUREA IN INGEGNERIA E SCIENZE INFORMATICHE

ANALISI DELLE PROCEDURE DI MOBILITA' IN UNA RETE 4G

Elaborato in
Reti di Telecomunicazione

Relatore
Prof. Franco Callegati

Presentata da
Lorenzo Campanelli

Anno Accademico 2020/2021

Indice

Abstract

Sebbene sia in atto un cambiamento per certi versi epocale con l'introduzione delle reti 5G, l'architettura di rete 4G rimane comunque la più diffusa attualmente in Italia in termini di copertura del territorio nazionale, considerando anche che molti utenti possiedono ancora dispositivi non predisposti per il collegamento alle reti 5G.

L'obiettivo del presente elaborato, dopo aver fornito informazioni sull'architettura di una rete 4G, è quello di esaminare le procedure eseguite dal dispositivo e dalla rete mediante le quali viene fornito il supporto necessario per garantire non solo l'inoltro dei pacchetti verso la destinazione corretta ma anche un'esperienza d'uso soddisfacente dei servizi richiesti.

In conclusione, poi, vengono evidenziati alcuni limiti dell'architettura 4G analizzata mostrando come questi abbiano portato a cambiamenti architetturali nel design delle reti 5G.

Introduzione

Dalla loro comparsa sul finire degli anni ’70 del secolo scorso le reti cellulari hanno subito una costante evoluzione. Le reti di prima generazione apparse negli anni ’80 col nome di 1G, interamente basate su trasmissione analogica, consentivano solamente di effettuare chiamate vocali. Al di là della dimensione voluminosa dei telefoni cellulari dell’epoca la qualità audio della comunicazione era decisamente scadente e soggetta ad interferenze e frequenti interruzioni. Nonostante questi difetti, le reti 1G non sono state soppiantate fino al 1991 quando le reti 2G hanno fatto la loro comparsa sul mercato. Allo scopo di migliorare la qualità di trasmissione, la capacità del sistema e la copertura del segnale la seconda generazione di reti mobili (2G) ha segnato un punto di rottura rispetto al passato puntando tutto sul passaggio al digitale anche delle chiamate vocali in base allo standard GSM (Global System for Mobile Communication). Le reti 2G hanno introdotto un cambiamento che è andato ben oltre il settore delle telecomunicazioni ponendo le basi per una rivoluzione culturale; per la prima volta le persone hanno potuto inviare messaggi di testo (SMS) o messaggi multimediali (MMS). Inoltre, vi è stato anche un aumento della sicurezza delle trasmissioni con l’uso della crittografia.

L’evoluzione continua dello standard GSM ha portato poi alla creazione di reti 2.5G (GPRS/EDGE) in cui ha fatto la sua comparsa il metodo di trasmissione a commutazione di pacchetto affiancato alla commutazione di circuito già esistente. Dopodiché, con l’introduzione nei primi anni 2000 delle reti 3G si è assistito ad un notevole incremento in termini di data-rate, passando dai 144 kbps massimi del 2.5G che consentivano la ricezione e l’invio di e-mail e un web browsing limitato ad un data rate fino a 14 Mbps che ha aperto la strada a nuovi servizi come video conferencing, Voice over IP (e.g. Skype), video streaming ed online gaming. Al contempo, si è iniziato ad assistere alla sempre maggior diffusione degli smartphone (si veda ad esempio il lancio di Apple iPhone nel 2007), dei veri e propri computer in miniatura in cui quello delle chiamate vocali è diventato solo uno dei possibili utilizzi.

Il 2009 ha visto il lancio sul mercato delle reti 4G che hanno portato velocità teoriche di download comprese tra 10Mbps e 1Gbps offrendo anche una minor latenza. Oltre a ciò, le reti 4G hanno segnato un punto di rottura col passato poiché si è transitati ad un’architettura di tipo packet-switching completamente IP-based che ha comportato una reingegnerizzazione anche della parte della rete deputata alle comunicazioni vocali che vengono quindi ad essere trattate come un qualsiasi altro servizio. Ciò ha richiesto quindi lo sviluppo di una tecnologia che tenesse conto dei requisiti in termini di Quality of Service richiesti dai vari servizi (VoIP, video streaming, ecc.).

Con la diffusione sempre maggiore di Augmented Reality, veicoli autonomi e la crescita esponenziale dei device IoT è risultato ben presto evidente che le reti 4G faticavano a soddisfare le richieste in termini sia di ampiezza di banda che soprattutto di latenza (compresa in media tra i 40 ed i 60 ms)

troppo elevata per servizi in real-time. Ciò ha portato all'introduzione delle reti 5G tenendo conto del fatto che con i device IoT i dati non sono più contenuti solo all'interno di data center ma prodotti anche in real-time dai cosiddetti "edge devices", che si trovano ai margini della rete, quali veicoli ed elettrodomestici di vario tipo.

L'obiettivo di questo elaborato è quindi quello di analizzare l'architettura di una rete 4G nonché le procedure di supporto della mobilità eseguite dai dispositivi mobili e dagli apparati di rete affinché un utente possa usufruire del servizio desiderato in qualunque posto egli si trovi ed in qualunque momento lo desideri.

Nel Capitolo 1 verrà analizzata l'architettura di una rete 4G esaminando nel dettaglio le entità che compongono sia la core network che la parte di accesso radio nonché gli identificatori e i meccanismi necessari per il trasporto delle informazioni attraverso la rete secondo i requisiti di qualità del servizio richiesti.

Nel Capitolo 2 verrà presentata una spiegazione di massima delle procedure messe in atto dalla rete e dal dispositivo per consentire la creazione e il mantenimento di un canale di comunicazione che interconnette il dispositivo dell'utente alla rete esterna che offre il servizio desiderato.

Nel Capitolo 3 verranno quindi analizzate in dettaglio le suddette procedure.

In conclusione infine, verranno trattate alcune criticità che emergono dall'analisi dell'architettura di rete 4G presentata fornendo qualche piccolo accenno a come si sia cercato di porvi rimedio nel design della nuova architettura di rete 5G.

Capitolo I

Architettura di una rete mobile 4G LTE

La EPC (Evolved Packet Core) è la core network che è stata progettata per le reti mobili di quarta generazione (4G). La sua standardizzazione è portata a termine dal 3rd Generation Partnership Project (3GPP) group, di cui fanno parte molti degli organismi di standardizzazione del settore delle comunicazioni a livello globale. La standardizzazione dell'architettura della EPC è iniziata col progetto System Architecture Evolution (SAE), che si è concentrato maggiormente sull'evoluzione della core network mentre il progetto Long Term Evolution (LTE) ha riguardato maggiormente l'evoluzione della rete di accesso radio.

L'intero sistema che comprende gli User Equipments (UE), la Radio Access Network (RAN) e la EPC viene denominato Evolved Packet System (EPS). La rete di accesso radio è detta Evolved Universal Terrestrial Radio Access Network (E-UTRAN) ed include gli Evolved NodeBs (eNodeBs), cioè le base stations LTE che l'UE utilizza per connettersi alla rete ed eseguire tutte le operazioni per stabilire una connessione.

Le caratteristiche principali che distinguono la EPC dalle core network delle generazioni precedenti sono:

- **Supporto a tecnologie di accesso differenti,** così da poter sfruttare un'unica core network per fornire servizi ad access network eterogenee. Di conseguenza, la EPC fornisce supporto per svariate Radio Access Technologies (RATs) 3GPP ivi incluse la E-UTRAN (LTE ed LTE-Advanced), la GERAN (RAN della GSM/GPRS) ed UTRAN (RAN della UMTS), così come tecnologie di accesso non 3GPP quali WiMAX, WLAN o reti fisse. Gli accesi non 3GPP possono essere ulteriormente suddivisi in:
  - Accessi trusted, che interagiscono direttamente con le entità della EPC
  - Accessi untrusted, che sono connessi alla EPC attraverso un'entità intermedia chiamata Evolved Packet Data Gateway (ePDG) che fornisce principalmente funzionalità di sicurezza.
- **Architettura "flat",** poiché viene evitata il più possibile la conversione tra protocolli e viene utilizzata la minor quantità possibile di entità per il processing del traffico dati utente, il che conduce ad una miglior performance e uno scaling più efficiente in termini di costi dell'infrastruttura
- **Separazione di Control Plane e User Plane,** per ottenere un migliore scalabilità e flessibilità. Una gestione separata del traffico di signalling e di user plane permette agli operatori di ottimizzare il deployment delle funzionalità di control e user plane potendo scalarle indipendentemente. Oltre a ciò, la separazione delle funzionalità in diverse entità consente, ad

esempio, di collocare le entità che gestiscono lo user plane più ai margini della rete, vicino all'access network al fine di ridurre le latenze mantenendo però quelle con pure funzionalità di controllo centralizzate. In realtà l'architettura originaria della EPC prevede comunque che alcune entità eseguano il processing sia di messaggi di signalling che del traffico dati utente ed una netta separazione tra i due piani è stata implementata solo a partire dalla Release 14 in avanti.

- **Infrastruttura puramente IP-based:** la EPC si basa solo su una tecnologia a commutazione di pacchetto per trasportare sia la voce che i dati, a differenza di quanto fatto dalle precedenti generazioni che utilizzavano una tecnologia a commutazione di circuito per il trasporto di voce ed SMS ed una commutazione di pacchetto per il trasporto di dati.

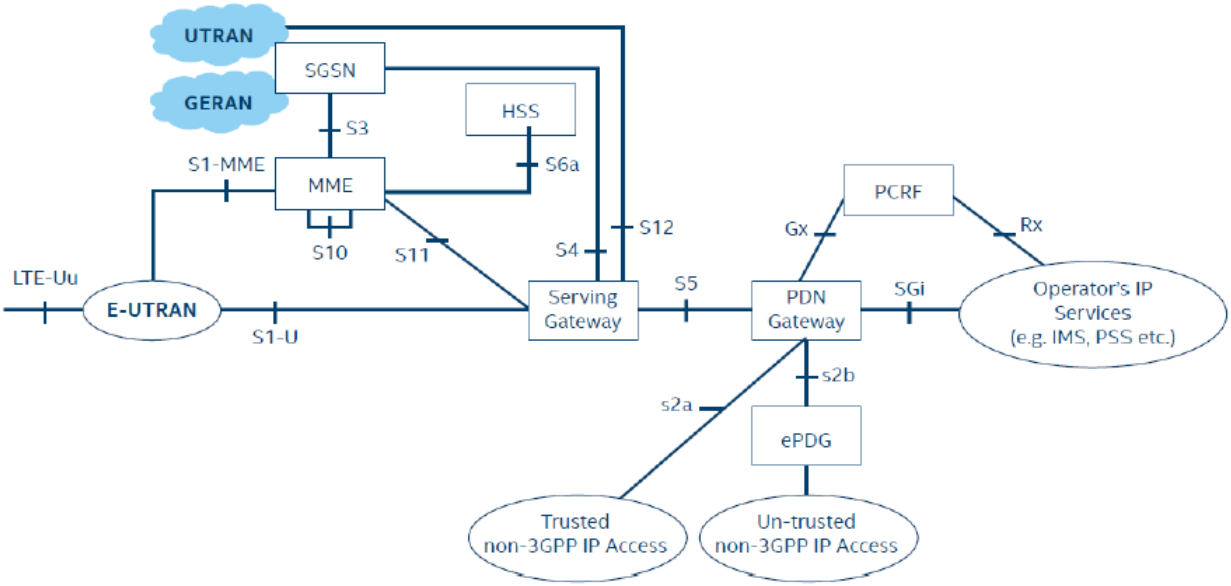


Figura 1 Architettura EPS semplificata

1.1 Entità della Core Network

HOME SUBSCRIBER SERVER (HSS)

L'HSS rappresenta il database centrale dove sono memorizzati i profili degli utenti. Fornisce le informazioni di autenticazione e i profili degli utenti all'MME.

L'HSS contiene le identità degli utenti (dati relativi al contratto sottoscritto), parametri relativi alla posizione del terminale (in termini di quale MME sta servendo attualmente lo User Equipment), parametri crittografici ed anche informazioni relative ai servizi disponibili per l'utente (e.g. profili di QoS sottoscritti o restrizioni concernenti il roaming).

Ad esempio, l'HSS memorizza l'IMSI, un numero univoco che identifica un utente di una rete mobile a livello globale. Oltre all'IMSI vengono memorizzate anche le chiavi crittografiche utilizzate per l'autenticazione degli utenti nonché per la cifratura dei messaggi scambiati.
Ricapitolando quindi, le funzionalità offerte da un HSS sono quelle di seguito riportate:

- **Identificazione dell'utente**, che avviene associando ogni UE con il corrispondente IMSI
- **Autenticazione dell'utente e setup delle procedure di sicurezza**, fornendo credenziali e chiavi crittografiche all'MME ed alle altre entità della Core Network
- **Gestione della mobilità.** l'HSS mantiene l'identità dell'MME al quale un utente è attualmente collegato o registrato.
- **Autorizzazione all'accesso** che avviene verificando se l'utente è autorizzato a collegarsi alla rete visitata in caso di roaming su una rete differente dalla home network con la quale un utente ha sottoscritto un contratto per la fornitura del servizio.
- **Supporto alla fornitura del servizio:** L'HSS mantiene informazioni circa le reti esterne (Packet Data Networks, PDNs) alle quali è consentito l'accesso da parte dell'utente. Queste informazioni sono mantenute sotto forma di Access Point Name o PDN Address (indirizzo IP della PDN).

MOBILITY MANAGEMENT ENTITY (MME)

Il MME è un nodo puramente di controllo, cioè non viene attraversato da traffico dati dell'utente per cui non fornisce nessun servizio allo user plane.
Rappresenta l'elemento chiave che processa il traffico di signalling tra un UE e la CN.
Comunica con un HSS per l'autenticazione dell'utente e il download delle informazioni relative al profilo utente contenute nell'HSS nonché svolge con l'UE le funzionalità di EPS Mobility Management (EMM) e di EPS Session Management (ESM) per mezzo di messaggi di signalling NAS.

L'MME quindi:

- Controlla il signalling con gli eNodeB
- Fornisce funzionalità di gestione della mobilità (paging, Tracking Area List (TAI) e gestione dell'handover)
- Seleziona i gateway appropriati (PGW ed SGW) per servire il terminale
- Effettua l'autenticazione dell'utente e fornisce supporto al roaming interagendo con l'HSS, ovvero si assicura che l'UE abbia l'autorizzazione per agganciarsi alla PLMN di un operatore

ed applica le restrizioni di roaming che l'UE potrebbe avere (in base al contratto sottoscritto dall'utente)

- Si occupa di tutte le procedure relative alla sicurezza. Infatti, rappresenta il punto terminale per il signalling NAS con l'UE e di conseguenza, si occupa di negoziare con quest'ultimo gli algoritmi supportati per eseguire il controllo di integrità dei messaggi scambiati nonché la cifratura degli stessi.

SERVING GATEWAY (SGW)

Il Serving Gateway è uno dei due gateway che si occupano di processare il traffico dati utente. Ogni UE è, di norma, servito da un solo SGW che rappresenta il punto terminale della core network verso la rete di accesso (E-UTRAN) relativamente allo user plane.

Quando un UE è associato con un SGW, quest'ultimo gestisce l'inoltro dei pacchetti dati utente ma rappresenta anche un punto di ancoraggio per le connessioni (data bearers) durante handover sia di tipo inter-eNB che inter-3GPP (cioè un handover tra tecnologie di accesso 3GPP differenti).

Quando un UE si trova in Idle mode (cioè non sta utilizzando alcun servizio) l'SGW mantiene informazioni circa i bearers attivati ed effettua il buffering temporaneo dei pacchetti diretti dalla rete esterna verso l'UE mentre l'MME inizia la procedura di paging verso l'UE per risvegliarlo e ristabilire i bearer rilasciati quando l'UE è transitato in idle mode.

PACKET DATA NETWORK GATEWAY (PGW)

Il Packet Data Network Gateway si occupa anzitutto di allocare un indirizzo IP al terminale scegliendolo tra quelli disponibili nello spazio degli indirizzi della PDN a cui l'UE intende collegarsi ed agisce come punto di entrata ed uscita dalla core network per il traffico dati dell'UE.

Ricapitolando quindi le funzioni svolte da un PGW sono:

- Routing e forwarding IP
- Packet filtering per SDF/ per utente
- Assegnazione dell'indirizzo IP al terminale
- Punto di contatto per la mobilità tra tecnologie di accesso 3GPP e non-3GPP.
- Funzioni PCEF (Policy Charging Enforcement Function)
- Charging per SDF / per-utente in base alle policy determinate dal PCRF.

POLICY AND CHARGING RULES FUNCTION (PCRF)

Il Policy and Charging Rules Function (PCRF) è l'elemento chiave del Policy and Charging Control Framework (PCC). È sua responsabilità determinare le policy di Quality of Service e addebitamento

dei costi che verranno applicate dal Policy and Charging Enforcement Function (PCEF), implementato nel PGW.

Il PCRF fornisce il profilo QoS autorizzato (QoS class identifier e bit rates) che decide in quale modo un particolare flusso dati verrà trattato dal PCEF, assicurandosi che ciò venga fatto in accordo col profilo sottoscritto dall'utente.

Le funzionalità principali dell'architettura PCC includono:

- **Gating control:** Il PCRF decide se i pacchetti appartenenti ad un determinato flusso associato ad un servizio (Service Data Flow) debbono essere bloccati oppure no.

  Le decisioni prese dal PCRF vengono inviate al PCEF in un formato particolare detto PCC Rule.
- **QoS control:** Il PCRF fornisce al PCEF il livello di QoS definito per ogni flusso di dati IP relativo ad un servizio. Il livello di autorizzazione QoS definito include, ad esempio, la QoS class stabilita (QCI) e il bit rate autorizzato.

  Il PCEF provvede poi ad attuare quanto definito dal PCRF instaurando i bearer appropriati.
- **Charging control:** Il PCRF decide se applicare online oppure offline charging per una determinata sessione di servizio. Il PCEF esegue di conseguenza le misurazioni appropriate sul traffico IP che lo attraversa ed applica le policy determinate dal PCRF.

  L'addebitamento dei costi avviene secondo due modalità *online charging* o *oflline charging*.

  Con il sistema di online charging, le informazioni di addebito possono influenzare, in tempo reale, i servizi utilizzati e di conseguenza è richiesta un'interazione diretta del meccanismo di addebitamento con il controllo dell'utilizzo delle risorse di rete.

  La gestione on-line del credito consente ad un operatore di controllare l'accesso ai servizi sulla base del credito attuale dell'utente. Ad esempio, l'utente deve avere abbastanza credito residuo per poter iniziare una nuova sessione di un certo servizio oppure proseguire con una già esistente. L'OCS può autorizzare l'accesso a singoli servizi oppure gruppi di servizi garantendo crediti per i flussi IP autorizzati. L'uso delle risorse è garantito in diverse forme di credito quali un certo ammontare di tempo, una certa quantità di traffico dati oppure sotto forma di eventi addebitabili.

  Se un utente non può accedere ad un determinato servizio perché, ad esempio, non possiede il credito necessario, l'OCS può negare le richieste di credito ed istruire il PCEF affinché dirotti l'utente verso una specifica destinazione che gli consenta di ricaricare il suo credito.

  Il PCC incorpora anche un sistema di *service-based offline charging.* Con l'offline charging, le informazioni per l'addebitamento vengono raccolte dalla rete per poter essere successivamente processate e fatturate.

Le informazioni per l'addebitamento non influiscono, in questo caso, sul servizio utilizzato in tempo reale.

Siccome la fatturazione avviene una volta che la sessione è stata completata, ad esempio con cadenza mensile, la funzionalità di offline charging non fornisce nessun tipo di controllo per l'accesso al servizio.

Come già menzionato in precedenza il PCRF comunica le decisioni prese sotto forma di "PCC rules" che contengono le informazioni utilizzate dal PCEF e dai sistemi di addebitamento. Il PCEF una volta ricevute le regole dal PCRF, le utilizza per individuare il SDF a cui ogni pacchetto appartiene ed applicando poi quando descritto nella PCC rule relativa a quel determinato SDF.

1.2 Architettura dell'Access Network E-UTRAN

La rete di accesso dell'LTE, E-UTRAN consta semplicemente di una rete di eNodeBs (come illustrato nella Figura 2 sotto). Per il normale traffico utente (non broadcast) non esiste un controller centralizzato in E-UTRAN, motivo per cui l'architettura viene definita "flat".

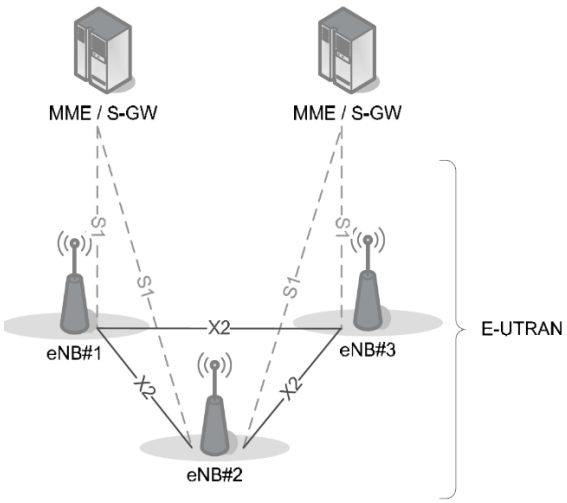


Figura 2 Architettura E-UTRAN in generale

La rete E-UTRAN è responsabile di tutte le funzioni relative alla parte radio della rete che possono essere così riassunte:

- **Gestione delle risorse radio**: Funzioni relative ai radio bearers come radio bearer control, radio admission control, radio mobility control, scheduling e allocazione dinamica delle risorse agli UE (sia in downlink che in uplink).
- **Compressione degli header**: La compressione dell'header aiuta a massimizzare lo sfruttamento dell'interfaccia radio comprimendo l'header del pacchetto IP che può altrimenti

rappresentare un overhead significativo (specialmente per pacchetti piccoli come quelli VoIP).

- **Sicurezza**: Tutti i dati inviati attraverso l'interfaccia radio vengono criptati
- **Connessione con l'EPC**: Gli eNB sono normalmente interconnessi tra loro attraverso l'interfaccia X2 ma sono anche connessi alla core network con l'MME (attraverso l'interfaccia S1-MME) e con il SGW (attraverso l'interfaccia S1-U). Ciò permette il transito delle informazioni di signalling verso l'MME nonché del traffico dati utente verso l'EPC (SGW).

Dalla parte della rete tutte queste funzionalità risiedono negli eNodeB, ognuno dei quali può essere responsabile di più celle. Al contrario di quanto accadeva con le generazioni precedenti, LTE integra le funzioni del controller radio negli eNodeB, riducendo la latenza, migliorando l'efficienza ed anche eliminando la necessità di un singolo controller molto potente che poteva risultare un "single point of failure".

L'aspetto negativo che deriva dalla mancanza di un unico controller centralizzato si nota quando l'UE si sposta costringendo la rete a trasferire tutte le informazioni relative all'UE (c.d. *UE context),* insieme a tutti i dati bufferizzati da un eNodeB ad un altro.

Un eNodeB può essere servito da più nodi della CN (MME/SGW). L'insieme dei nodi MME/SGW che serve un'area comune è denominato *MME/SGW pool* e l'area coperta da un pool è denominata *pool area*.

La creazione di questi pool fa sì che gli UE che si trovano nelle celle controllate da un certo eNodeB possono essere condivisi da più nodi della CN andando di conseguenza a bilanciare il carico ed evitando "single points of failure" dei nodi della CN.

Quando l'UE si trova all'interno di una determinata pool area di norma l'UE context rimane nello stesso MME.

1.3 Architettura di Roaming

Una rete gestita da un operatore in una determinata nazione viene definita Public Land Mobile Network (PLMN).

Il Roaming, in cui gli utenti sono autorizzati a connettersi ad altre PLMN diverse da quella dell'operatore col quale hanno sottoscritto un contratto, è una potente funzionalità fornita anche dall'LTE.

Un roaming user è connesso all'E-UTRAN, MME ed SGW della *visited network*, ma l'LTE consente di utilizzare sia il PGW della *visited network* che quello della *home network.*

L'utilizzo di un PGW della home network consente di accedere a determinati servizi forniti dall'home operator anche mentre ci si trova in una rete diversa dalla home network.
Al contrario, l'utilizzo di un PGW nella visited network permette di avere un "local breakout" alla rete Internet all'interno della visited network.

1.4 Principali interfacce tra i nodi di una rete LTE

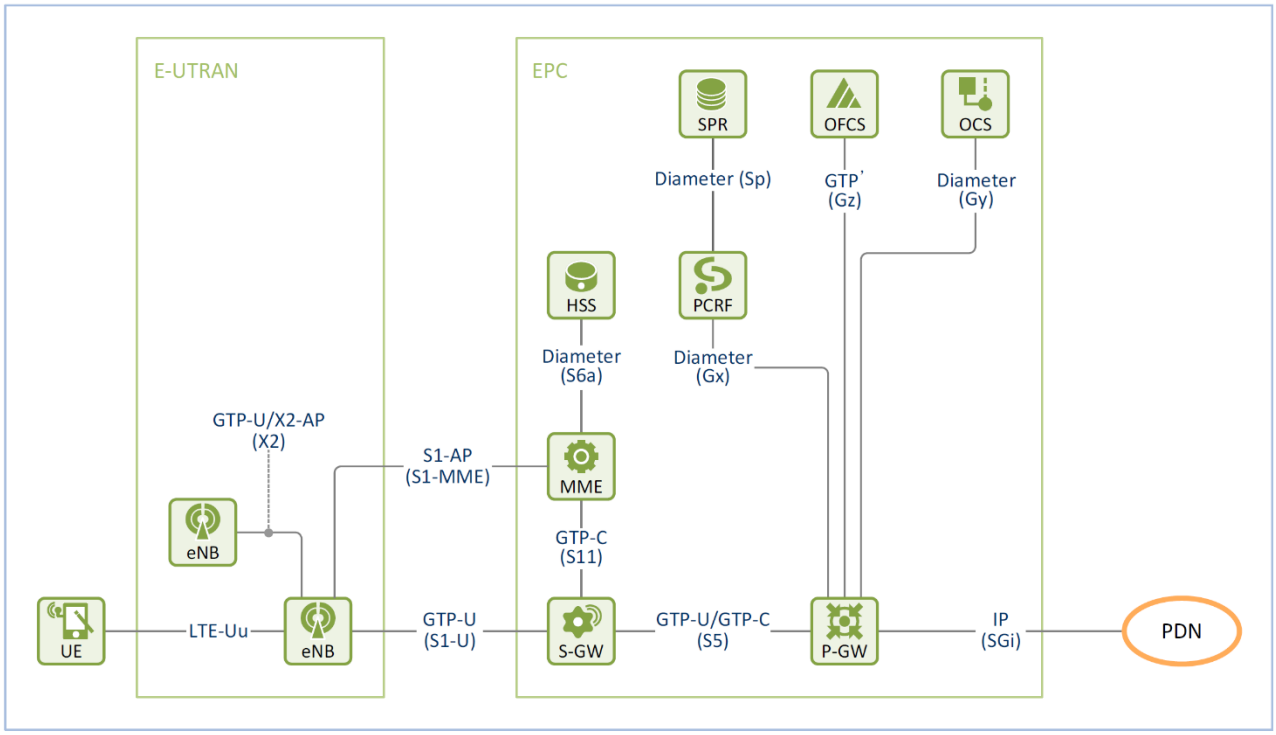


Figura 3 Modello di riferimento di una rete LTE

Di seguito vengono presentate alcune delle principali interfacce (detti anche *reference points*) che forniscono la connettività tra i vari nodi della EPC:

REFERENCE POINT	PROTOCOLLO	DESCRIZIONE
LTE-Uu	E-UTRA (control plane e user plane)	Interfaccia per il piano di controllo tra un terminale e una access network E-UTRAN
X2	X2-AP (control plane) GTP-U (user plane)	Interfaccia utilizzata sia per il control plane che per lo user plane tra due eNB durante l'X2 handover. Il protocollo X2-AP è utilizzato nel control plane mentre un tunnel GTP-U per bearer viene creato per l'inoltro

		dei dati in user plane dal source eNB al target e NB.
S1-U	GTP-U	Interfaccia utilizzata per incanalare il traffico dati utente tra un eNB e un SGW. Fornisce un tunnel GTP per bearer e può essere opzionalmente utlizzata per effettuare l'handover tra due eNB
S1-MME	S1-AP	Interfaccia utilizzata per lo scambio di informazioni di signalling di control plane tra un eNodeB ed un MME.
S11	GTP-C	Interfaccia per il signalling di control plane tra un MME ed un SGW.
S5	GTP-C (control plane) GTP-U (user plane)	Interfaccia definita tra un SGW ed un PGW utilizzata per il tunnelling di traffico dati utente ma anche per lo scambio di informazioni di signalling per la gestione delle sessioni (creazione, modifica, cancellazione di tunnel GTP in user plane). In caso di roaming viene utilizzata la variante S8.
S6a	Diameter	Interfaccia che connette un MME ad un HSS ed è utilizzata per lo scambio delle informazioni richieste per l'autorizzazione di accesso alla rete ed autenticazione dell'utente

SGi		Interfaccia che interconnette un PGW con una PDN esterna.
Gx	Diameter	Interfaccia utilizzata per l'invio delle "PCC rules" e delle "charging rules" da parte del PCRF al PCEF che risiede nel PGW, necessarie per la gestione della Quality of Service e dell'addebitamento.
S10	GTPv2-C	Interfaccia che interconnette gli MME tra di loro per permettere lo scambio di informazioni (ad esempio quando l'MME a cui è collegato un UE cambia)

1.5 Session management e controllo della Quality of Service

1.5.1 Session Management

Lo scopo principale di una rete EPC è quello di stabilire una connessione tra un terminale ed una rete IP esterna (anche detta *Packet Data Network, PDN*).

Uno stesso operatore può fornire l'accesso a diverse PDN ognuna delle quali offre un determinato servizio. Ad esempio, Internet è una PDN in cui l'utente può visitare vari siti web ed usufruire dei servizi offerti da essa, ma possono esistere anche altre PDN; si pensi ad esempio ad una PDN specifica di un determinato operatore che offre servizi dedicati agli utenti della sua rete.

La connettività viene fornita creando una PDN connection (anche chiamata EPS session) che attraversa la parte RAN (Radio Access Network) della rete e la EPC (core network) andando da un terminale fino ad un PGW, che è l'ultima entità della core network ad essere attraversata dal flusso di dati prima che questo raggiunga la rete esterna.

Un terminale può essere connesso in un determinato momento ad una o più PDN simultaneamente: nel caso in cui un abbia più connessioni PDN attive nello stesso momento avrà più indirizzi IP assegnati (uno per ogni connessione PDN).

Una connessione PDN di default viene sempre stabilita quando un terminale si collega alla EPS.

Durante la procedura di collegamento (attachment procedure), il terminale può fornire informazioni circa la PDN con la quale vuole stabilire una connessione provocando a sua volta la selezione di un PGW attraverso il quale l'UE viene connesso con la PDN.
Se il terminale non fornisce un APN durante la procedura di collegamento iniziale, l'MME utilizza l'APN di default memorizzato nel profilo utente richiesto dall'MME all'HSS nel momento del collegamento.
Possono essere stabilite più connessioni a PDN differenti oltre a quella di default. In questo caso occorre però che quando il terminale invia la richiesta alla rete di aprire una nuova connessione includa anche il parametro APN così da informare la rete circa la PDN alla quale vuole accedere.

1.5.2 Quality of Service

Fornire una connettività PDN non è solo una questione di assegnare un indirizzo IP ma significa anche trasportare i pacchetti in maniera che l'utente possa fruire del servizio richiesto con una buona esperienza di utilizzo.
A seconda del tipo di servizio, sia esso una chiamata VoIP, un servizio di video in streaming, un download di file o altro, i requisiti di QoS per il trasporto dei pacchetti IP sono differenti in termini di bit rate, delay, jitter ecc. Ad esempio, una chiamata VoIP ha requisiti più stringenti in termini di Jitter e delay mentre un download di file richiede un tasso di perdita di pacchetti più basso.
La rete deve garantire che tutti i differenti requisiti siano rispettati e che i vari servizi ricevano il trattamento appropriato in termini di QoS così da garantire un'esperienza utente positiva.
Le funzionalità di session management controllano la creazione di percorsi logici di trasmissione dei dati che rispettino i target QoS definiti.
In primo luogo, il traffico dati viene classificato logicamente in Service Data Flows (SDF) in base al tipo di servizio. A loro volta i SDF sono mappati in canali logici di trasporto tra l'UE e il PGW detti *EPS bearers.*
Il signalling di control plane supporta tutte le procedure di attivazione, modifica e cancellazione dei bearers creati nonché l'assegnazione ai bearers dei parametri QoS e dei packet filters.
La EPS garantisce il rispetto dei requisiti di QoS definiti finché il traffico si trova all'interno del sistema (core network ed access network). Infatti, ogni bearer è associato ad un insieme di parametri QoS che descrivono le proprietà del canale di trasporto in termini di bit rate, delay, error rate, scheduling policy ecc. e tutti i flussi dati mappati in un bearer vengono trattati e inoltrati allo stesso modo.

Ogni connessione PDN ha almeno un bearer associato che viene creato quando la connessione viene stabilita e distrutto solo quando l'utente si disconnette da un PDN ma possono essere instaurati ulteriori bearer per ottemperare alle richieste differenti in termini di QoS dei vari servizi.
Oltre al meccanismo di QoS definito attraverso i bearer EPS, il framework PCC, mediante le PCC rules, può effettuare anche un controllo QoS aggiuntivo a livello di servizio (SDF), completamente scorrelato rispetto al mapping dei flussi IP in bearers, poiché i parametri QoS definiti a livello di SDF hanno uno scopo totalmente differente rispetto a quelli definiti per un EPS bearer. Ciò comporta che un singolo bearer EPS possa essere utilizzato per trasportare traffico appartenente a differenti SDF a patto che il bearer garantisca il livello di QoS appropriato per i SDF definite dalle PCC rules.
Per quanto concerne i bearer EPS, questi possono essere di due tipi: default bearer o dedicated bearer. Un default bearer viene sempre creato nel momento in cui un UE si connette per la prima volta ad una PDN. Questo bearer viene mantenuto per l'intera durata della connessione al fine di garantire sempre una connettività con la PDN scelta. Di norma il default bearer è associato con un QoS di default e viene utilizzato per il trasporto di traffico IP che non richiede alcun trattamento QoS in particolare. Quando viene distrutto, la connessione PDN a cui è associato viene chiusa.
Qualora invece l'utente abbia necessità di utilizzare un servizio che richiede un QoS maggiore che il default bearer non può garantire, viene istanziato un *dedicated bearer* con i parametri QoS richiesti dal servizio che si vuole utilizzare che può essere disattivato quando non è più necessario.
L'UE e il PGW utilizzano un insieme di packet filters detti *Traffic Flow Templates (TFT)* per effettuare il mapping dei flussi di pacchetti in uplink o in downlink appartenenti alle varie SDF nei diversi bearer EPS.
I TFT possono contenere filtri sia per il traffico in uplink (UL TFT) che per quello in downlink (DL TFT) che vengono applicati in uno specifico ordine alla ricerca di pacchetti che rispettino i parametri definiti dal filtro. I filtri vengono creati quando viene creato un instaurato un nuovo bearer EPS ma possono essere modificati durante la vita dello stesso.
I packet filters di un TFT contengono informazioni che consentono all'UE o al PGW di identificare i pacchetti appartenenti ai diversi aggregati di flussi IP. L'informazione tipicamente contenuta nei packet filters è rappresentata da una "5-tuple" che definisce l'indirizzo IP sorgente e di destinazione, la porta sorgente e di destinazione nonché il protocollo utilizzato (TCP o UDP).
I parametri di QoS iniziali coi quali viene creato il default bearer all'atto dell'instaurazione di una connessione PDN vengono assegnati in base al subscribed QoS profile presente tra le informazioni di sottoscrizione memorizzate nell'HSS ma il PCEF può cambiare i parametri inviati dall'MME per dare esecuzione ad una "PCC rule" ricevuta dal PCRF.

Un bearer è composto da tre segmenti:

- *Radio Bearer* che copre la parte radio della rete tra l'UE e l'eNodeB
- *S1 Bearer* stabilito tra l'eNodeB e il SGW attraverso l'interfaccia S1-U
- *S5/S8 Bearer (basato su protocollo GTP)* che è attivato tra il SGW e il PGW lungo il reference point S5/S8.

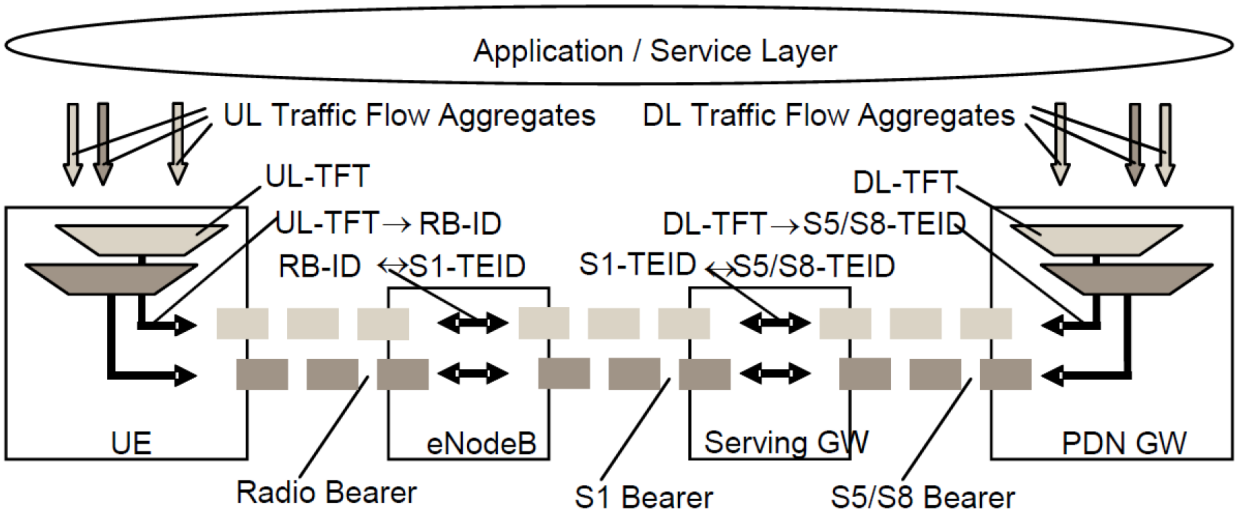


Figura 4 Mapping dei flussi dati in bearer EPS

I principali parametri QoS relativi ad un bearer sono:

- **QoS class identifier (QCI)**: un parametro intero che varia da 1 a 9 e sta a rappresentare in maniera sintetica alcuni parametri specifici di un nodo che definiscono il livello QoS di un bearer e di conseguenza il trattamento di inoltro di un pacchetto
- **Allocation and Retention Priority (ARP)**: specifica un valore di prorità di un bearer che viene utilizzato per decidere se la richiesta di creazione di un nuovo bearer o di modifica di uno già esistente può essere accolta o deve essere rigettata per mancanza di risorse di rete disponibili
- **Guaranteed Bit Rate (GBR):** indica l'ampiezza di banda minima (bit rate) che deve essere garantita per un determinato bearer
- **Maximum Bit Rate (MBR):** indica l'ampiezza di banda (bit rate) massima concessa per un determinato bearer

Come indicato dagli ultimi due parametri elencati sopra esistono quindi due principali tipologie di classificazione di un bearer in base al fatto che si abbia o meno un'ampiezza di banda garantita:

- (Minimum) GBR Bearers: utilizzati in applicazioni quali il VoIP. Hanno un valore GBR associato per cui hanno risorse di rete permanentemente allocate per essi (cioè un'ampiezza

di banda in quantità pari al GBR specificato è garantita loro). Se sono disponibili risorse di rete, ad un GBR bearer possono essere consentiti bit rates superiori al valore GBR specificato. In alcuni casi, per un GBR bearer può essere impostato anche un valore di Maximum Bit Rate (MBR) che stabilisce un limite superiore al bit rate consentito.

- Non GBR Bearers: non hanno un bit rate garantito; quindi non vengono allocate permanentemente risorse in termini di banda per questo tipo di bearer. I default bearers sono sempre di tipo Non GBR poiché devono sempre garantire la connettività con le PDN fornendo un servizio di tipo best-effort.

Per i bearers Non-GBR sono previsti due parametri che limitano il bit rate complessivo di tutti i bearer non-GBR:

- **APN-AMBR (UL/DL)**: indica la massima ampiezza di banda che può essere utilizzata complessivamente da tutti i bearer non-GBR associati ad un APN.
- **UE-AMBR (UL/DL):** indica il bit rate massimo che può essere utilizzato complessivamente da tutti i bearer non-GBR associati ad un UE, considerando tutte le connessioni PDN attive. Il valore reale del parametro UE-AMBR imposto dalla rete corrisponde al minimo tra il parametro UE-AMBR presente nel profilo sottoscritto dall'utente e la somma degli APN-AMBR di tutti gli APN attivi (i.e. tutti gli APN coi quali l'UE ha una connessione PDN attiva).

All'interno della rete EPC, il traffico user-plane viene trasportato utilizzando il protocollo di incapsulamento *GPRS Tunnelling Protocol (GTP)* aggiungendo al pacchetto IP in un header che identifica il bearer a cui il pacchetto appartiene.

1.6 Protocolli

La Figura 5 illustra i protocolli che vengono utilizzati per lo scambio di traffico di signalling o traffico dati lungo le principali interfacce.

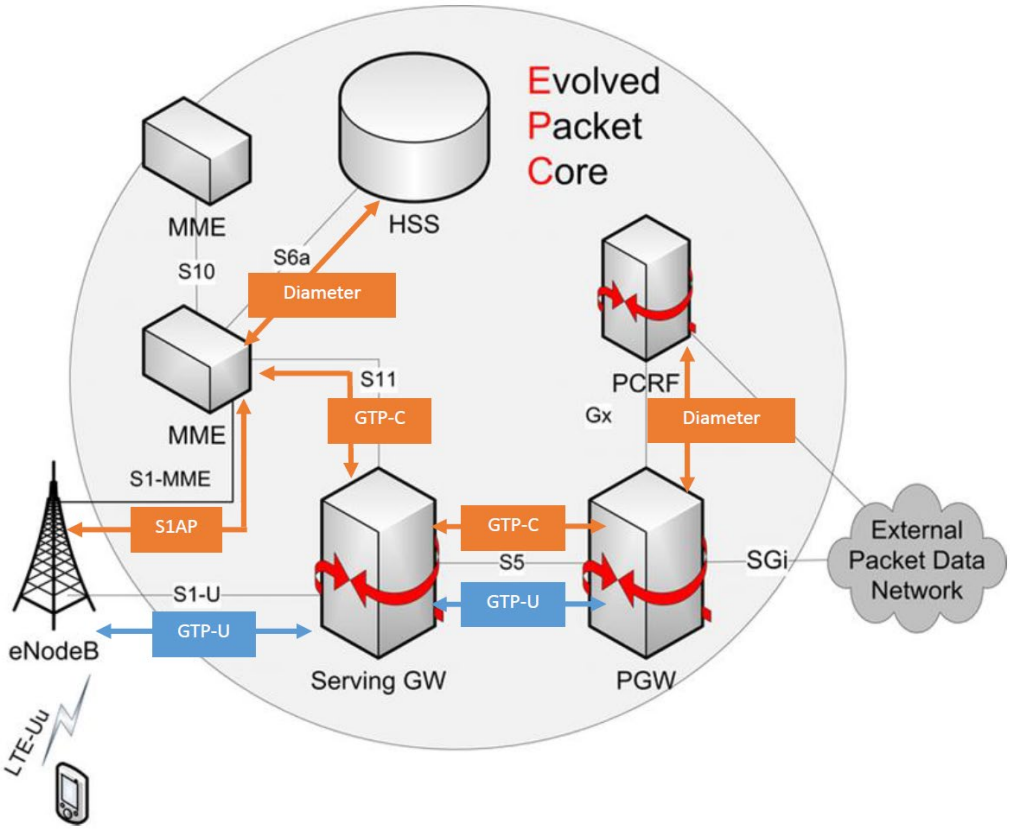


Figura 5 Protocolli utilizzati lungo i principali reference points della EPC

GPRS Tunnelling Protocol (GTP)

Il protocollo GTP è un protocollo di incapsulamento basato su UDP (o TCP) / IP che viene utilizzato per il trasporto di flussi di traffico separati tra due nodi GTP. Nella rete EPS il protocollo GTP è utilizzato per far viaggiare i pacchetti IP attraverso la core network e trasportare i messaggi di controllo tra le varie entità della core network.

Esistono diverse versioni del protocollo GTP che operano sia nel control plane che nel data plane:

- Il protocollo GTP-C (GTPv2-C) è utilizzato nel piano di controllo per supportare le funzionalità di gestione dei bearer.
- Il protocollo GTP-U (GTPv1-U) è la versione user plane del protocollo GTP che implementa il meccanismo di tunnelling per trasportare i pacchetti IP lungo la rete.

  I pacchetti sono incapsulati e poi inoltrati lungo le interfacce S1-U e S5/S8 sulla base dei bearer associati.

I tunnel GTP-C e GTP-U creati sono correlati per ogni utente poiché i primi sono impiegati per scambiare messaggi di controllo al fine di instaurare e gestire i secondi e attivare le connessioni attraverso la rete cosicché lo UE possa inviare/ricevere dati.

In ogni nodo, un endpoint di un tunnel GTP è univocamente identificato da:

- Un Tunnel Endpoint ID locale (TEID)
- Un indirizzo IP
- Un numero di porta UDP.

L'entità ricevente assegna il TEID che deve essere utilizzato per distinguere i vari tunnel GTP che possono essere stabiliti tra due nodi. Ciò significa che un tunnel GTP avrà due TEID differenti, uno assegnato dall'entità ricevente in uplink che identifica il tunnel GTP in uplink ed uno assegnato dall'entità ricevente del traffico in downlink che identifica il tunnel GTP in downlink.

Per quanto concerne in particolar modo il data plane, viene utilizzato il protocollo GTP-U per incapsulare ed inoltrare il traffico dati utente. Come è possibile notare dalla Figura 6 e dalla Figura 7, quando un UE invia pacchetti IP verso una rete PDN esterna (e.g Internet) questi raggiungono l'eNodeB che sta servendo in quel momento l'UE, e ad essi viene aggiunto un header GTP prima di essere spediti lungo il tunnel GTP-U attraverso la core network.

Per instradare i pacchetti lungo la core network verso la loro destinazione finale, i pacchetti GTP vengono incapsulati in pacchetti IP esterni che hanno come indirizzi sorgente e destinazione gli indirizzi IP dei nodi intermedi (i.e. il SGW e il PGW).

L'header GTP contiene il TEID che identifica il bearer lungo il quale devono essere spediti i pacchetti. Quando i pacchetti arrivano al PGW e devono essere inviati al di fuori della EPC esso estrae i pacchetti IP originari e li trasmette verso la destinazione.

La stessa cosa avviene nel verso contrario per i pacchetti inviati dalla PDN esterna verso l'UE.

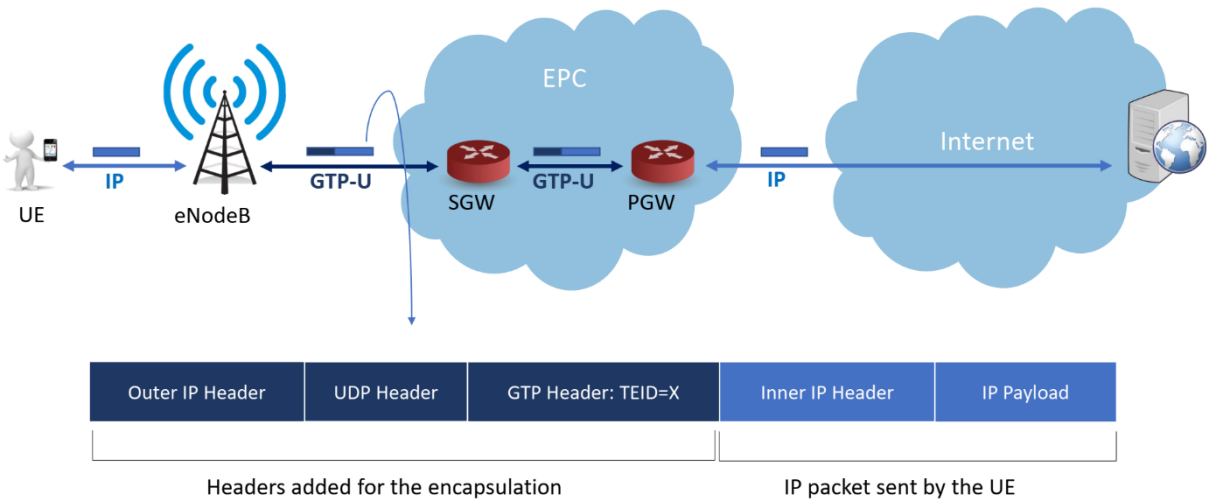
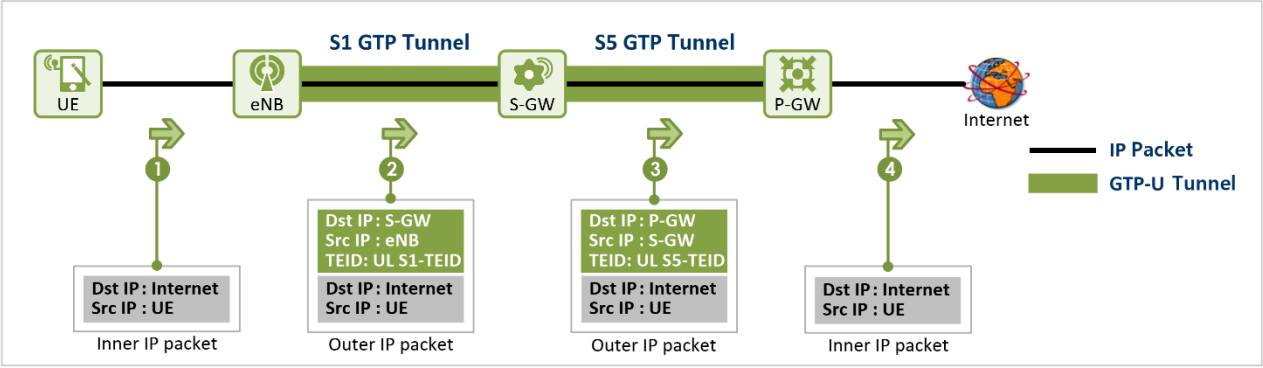
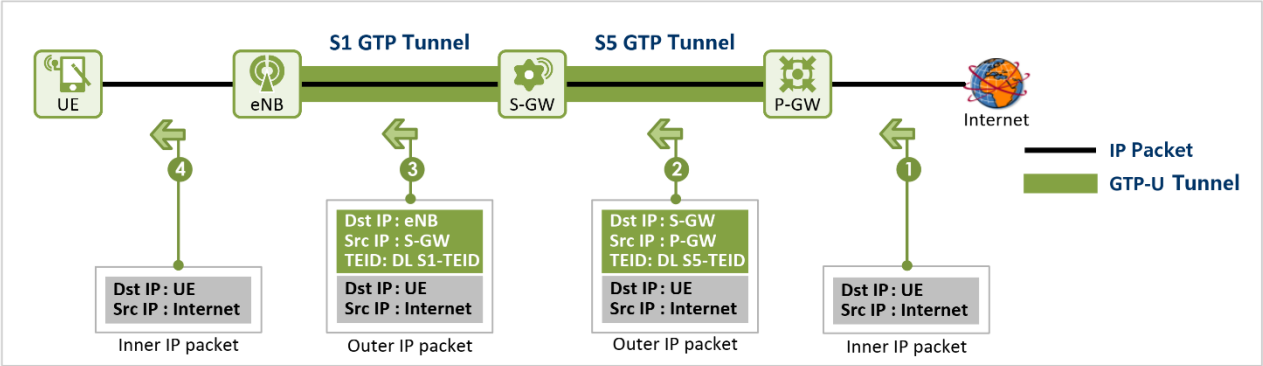


Figura 6 Un esempio di incapsulamento GTP-U



(a) From UE to the Internet



(b) From the Internet to UE

Figura 7 Un altro esempio di incapsulamento GTP-U

Diameter

Il protocollo Diameter supporta le procedure di autenticazione, autorizzazione e accounting (AAA) ed è standardizzato nell'IETF RFC 3588.

Nella rete EPS supporta la trasmissione, attraverso l'interfaccia S6a, delle informazioni di sottoscrizione di un utente nonché lo scambio di dati per l'esecuzione delle procedure di autenticazione dell'utente e autorizzazione di accesso ai servizi.

Questo protocollo è implementato inoltre nell'interfaccia Gx tra il PCRF e il PGW (che agisce in qualità di PCEF) per l'installazione, la modifica o la rimozione delle PCC rules definite.

Diameter si appoggia sul protocollo TCP o Stream Control Transport Protocol (SCTP) per trasportare messaggi tra due peer diameter.

Poiché i due protocolli di livello trasporto sopra citati sono di tipo connection-oriented, deve essere necessariamente stabilita una connessione tra i due peer prima di poter iniziare ad inviare messaggi.

S1 Application Protocol (S1AP)

Il protocollo S1AP è un protocollo specificatamente progettato per l'interfaccia S1-MME al fine di supportare tutti i meccanismi necessari per le procedure tra un MME ed un eNodeB nonché, in

maniera trasparente, le procedure che intercorrono tra un UE ed un MME od altri nodi della core network (e.g. NAS signaling tra l'UE e l'MME).
Questo protocollo consta di Elementary Procedures ognuna delle quali rappresenta un'unità di interazione tra un eNodeB ed un MME.
Un'Elementary Procedure è caratterizzata da un messaggio iniziale al quale può far seguito uno di risposta.
Il protocollo S1AP si basa sul protocollo di livello trasporto SCTP.

X2 Appliction Protocol (X2AP)

Il protocollo X2AP supporta la mobilità dell'UE all'interno della access network E-UTRAN. Per fare ciò fornisce funzioni per l'inoltro dei dati tra due eNB, il trasferimento del sequence number dei pacchetti da inviare/ricevere e funzioni per rilasciare l'UE context.
Il protocollo X2AP si basa sul protocollo di livello trasporto SCTP.

RRC

Il protocollo RRC supporta il trasferimento del signaling NAS. Inoltre, esegue le funzioni richieste per la gestione efficiente delle risorse radio. Le sue funzioni principali sono:

- Broadcasting delle System Information
- Setup, riconfigurazione e rilascio della connessione RRC
- Setup, modifica e rilascio del radio bearer.

Packet Data Convergence Protocol (PDCP)

Il protocollo PDCP processa i messaggi RRC di control plane e i pacchetti IP di user plane. Esegue funzioni di compressione degli header, sicurezza dell'Access Stratum (cifratura e protezione di integrità) e riordino/ritrasmissione dei pacchetti durante l'handover.

Radio Link Control (RLC)

Le funzioni principali del protocollo RLC sono la segmentazione e il riassemblaggio dei pacchetti del layer superiore (PDCP PDU) per adattarli ad una dimensione consona alla trasmissione attraverso il canale radio. Il protocollo RLC può operare in tre modi (transparent mode, acknowledged mode e unacknowledged mode), ognuno dei quali offre differenti livelli di affidabilità. Esegue inoltre il riordino e la ritrasmissione dei pacchetti (RLC PDU)

Medium Access Control (MAC)

Il layer MAC è posizionato tra il livello RLC superiore e il livello fisico (PHY) inferiore. È connesso al layer RLC mediante *logical channels* e al livello PHY attraverso *transport channels.* Supporta quindi le funzioni di multiplexing e demultiplexing tra canali logici e canali di trasporto I layer superiori utilizzano i canali logici per ottenere differenti livellli di QoS. Il protocollo MAC supporta la QoS dando priorità differenti a dati che provengono da canali logici differenti. Lo scheduler eNB si assicura che le risorse radio siano allocate dinamicamente ai vari UE ed esegue il controllo QoS per assicurarsi che ad ogni bearer sia garantito il QoS negoziato.

Non-Access Stratum (NAS)

Il Non-Access Stratum rappresenta un insieme di protocolli tra l'UE e l'MME che implementano funzionalità di gestione della mobilità e gestione delle sessioni. I protocolli NAS denominati EPS Mobility Management (EMM) ed EPS Session Management (ESM) sono stati appositamente progettati per il trasporto di informazioni di signalling non-radio attraverso una rete di accesso LTE/E-UTRAN.

Se si guarda il protocol stack, il NAS rappresenta lo strato più alto del control plane stack.

Ogni messaggio NAS contiene un campo *Protocol Discriminator* ed un campo *Message Identity*. ll primo indica il protocollo utilizzato (EMM o ESM) mentre il secondo indica lo specifico messaggio che viene inviato.

Inoltre, i messaggi NAS possono essere protetti con dei meccanismi di scurezza per il controllo di integrità e/o la cifratura.

Le procedure EMM riguardanti la gestione della mobilità verranno dettagliate più approfonditamente nel Capitolo 2.1.1. Per quanto concerne invece le procedure ESM, che riguardano la gestione delle sessioni, queste possono essere suddivise in due categorie a seconda di quale sia l'entità che da avvio alla procedura:

1. Procedure iniziate dalla rete: volte alla creazione, modifica e cancellazione di default o dedicated bearers
    - Default EPS Bearer Context Activation
    - Dedicated EPS Bearer Context Activation
    - EPS bearer context modification
    - EPS bearer context deactivation
2. Procedure iniziate dall'UE: eseguite dall'UE per richiedere la creazione o l'eliminazione di una connessione PDN alla rete oppure l'allocazione, modifica o il rilascio di un bearer
    - UE requested PDN connectivity procedure

- UE requested PDN disconnect procedure
- UE requested bearer resource modification procedure

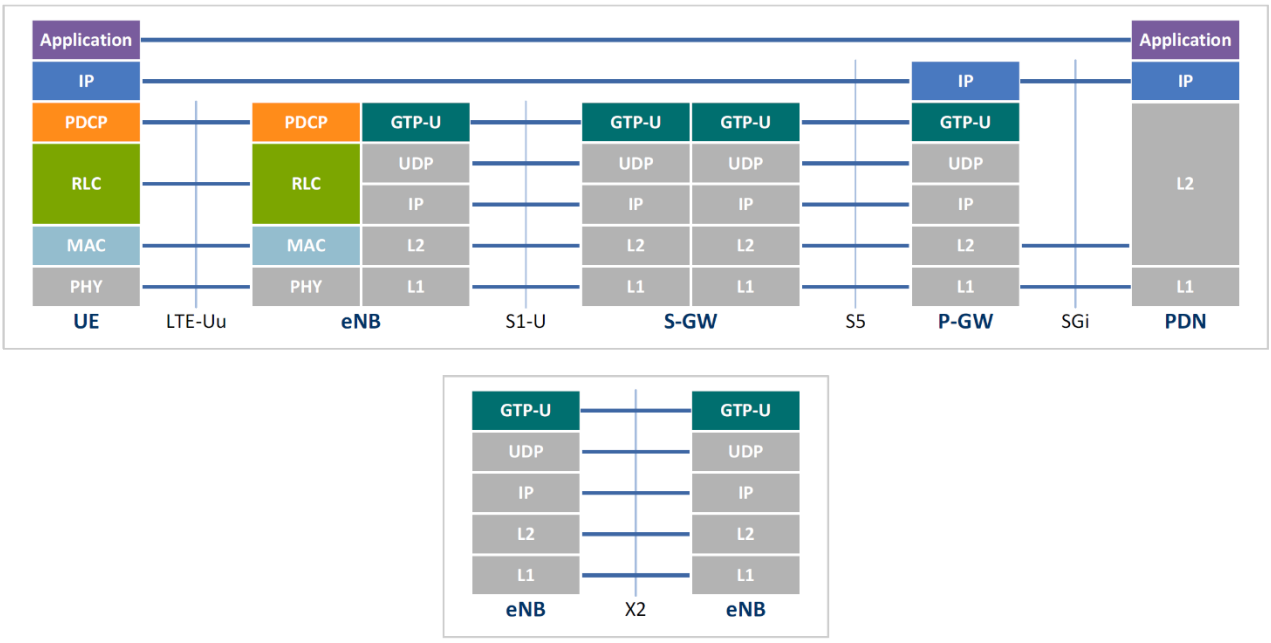


Figura 8 LTE user plane protocol stacks

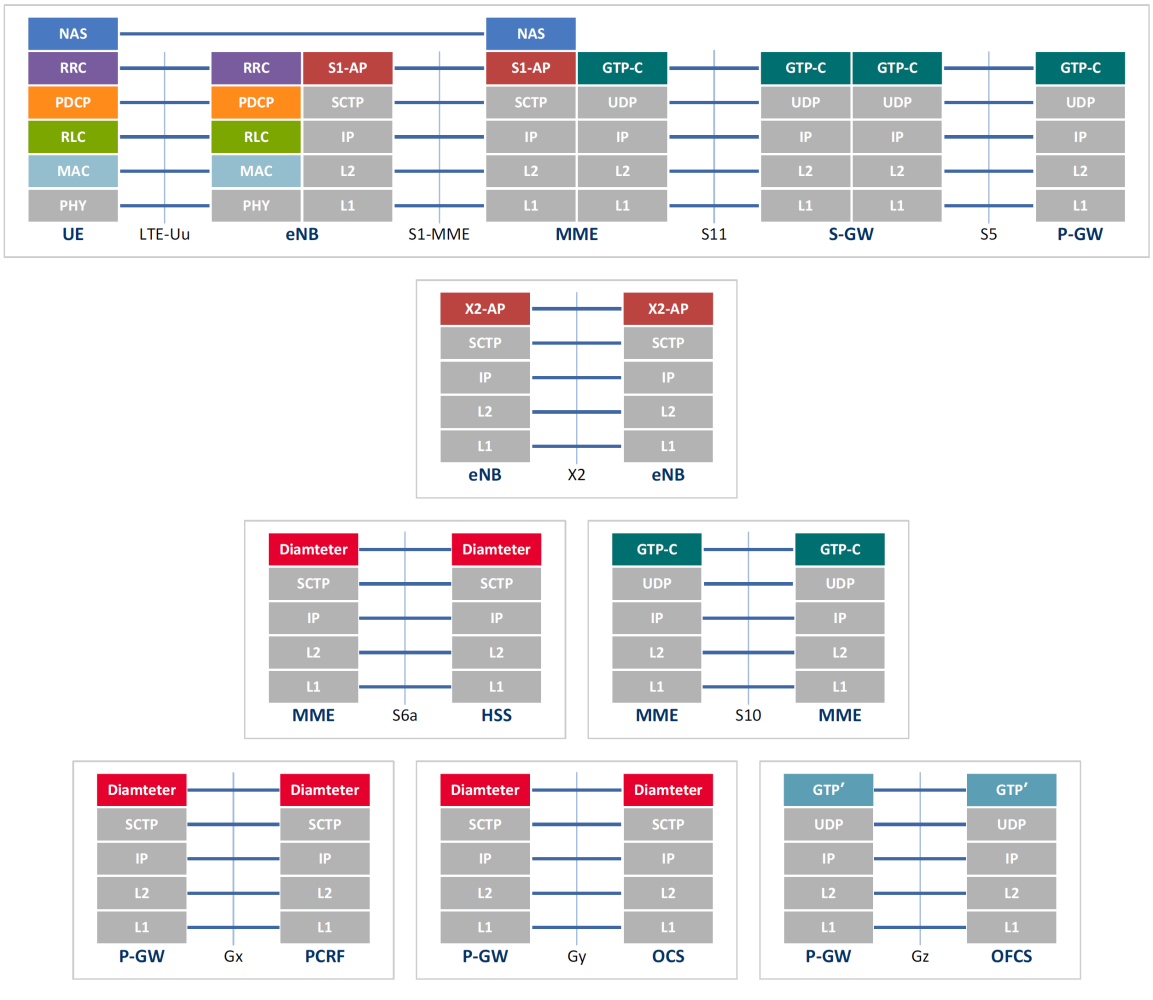


Figura 9 LTE control plane protocol stacks

1.7 Identificatori in una rete LTE

In questo capitolo verranno trattati una serie di identificativi utilizzati all'interno di una rete LTE nelle varie entità e lungo le varie interfacce in termini di tempo di creazione, il tipo di attributo (permanente/temporaneo) e range all'interno del quale sono univocamente definiti.

Tempo di creazione: Un identificativo LTE può essere:

- Assegnato all'atto dell'installazione dell'apparecchiatura
- Assegnato dall'operatore prima o durante le operazioni di servizio
- Creato on-demand quando un utente accede alla rete o utilizza un servizio

Gli ID assegnati all'atto dell'installazione dell'apparecchiatura o dall'operatore durante le operazioni di servizio sono contenuti all'interno dei box blu in corrispondenza delle entità EPS a cui fanno riferimento nella Figura 10

Durata: Un ID LTE può avere sia un valore permanente che rimane fisso una volta assegnato oppure un valore temporaneo. Gli ID assegnati all'atto dell'installazione dell'apparecchiatura oppure quelli inseriti dall'operatore durante le operazioni di servizio hanno valori permanenti mentre quelli allocati on-demand quando un utente accede alla rete o utilizza un servizio sono temporanei.

Range (all'interno del quale un ID è univocamente definito): Ogni ID può essere univocamente definito in tutto il mondo, in una singola rete o anche in una singola entità o canale.

La Figura 10 mostra i vari identificativi presenti all'interno di una rete LTE associati all'interfaccia o all'area geografica per la quale assumono significato.

Per comodità di trattamento gli ID vengono raggruppati in User Equipment ID (UE ID), che identificano un UE, Network Equipment ID (NE ID) che identificano un apparato della core network e Location ID che identificano l'area in cui un utente si trova in un determinato momento.

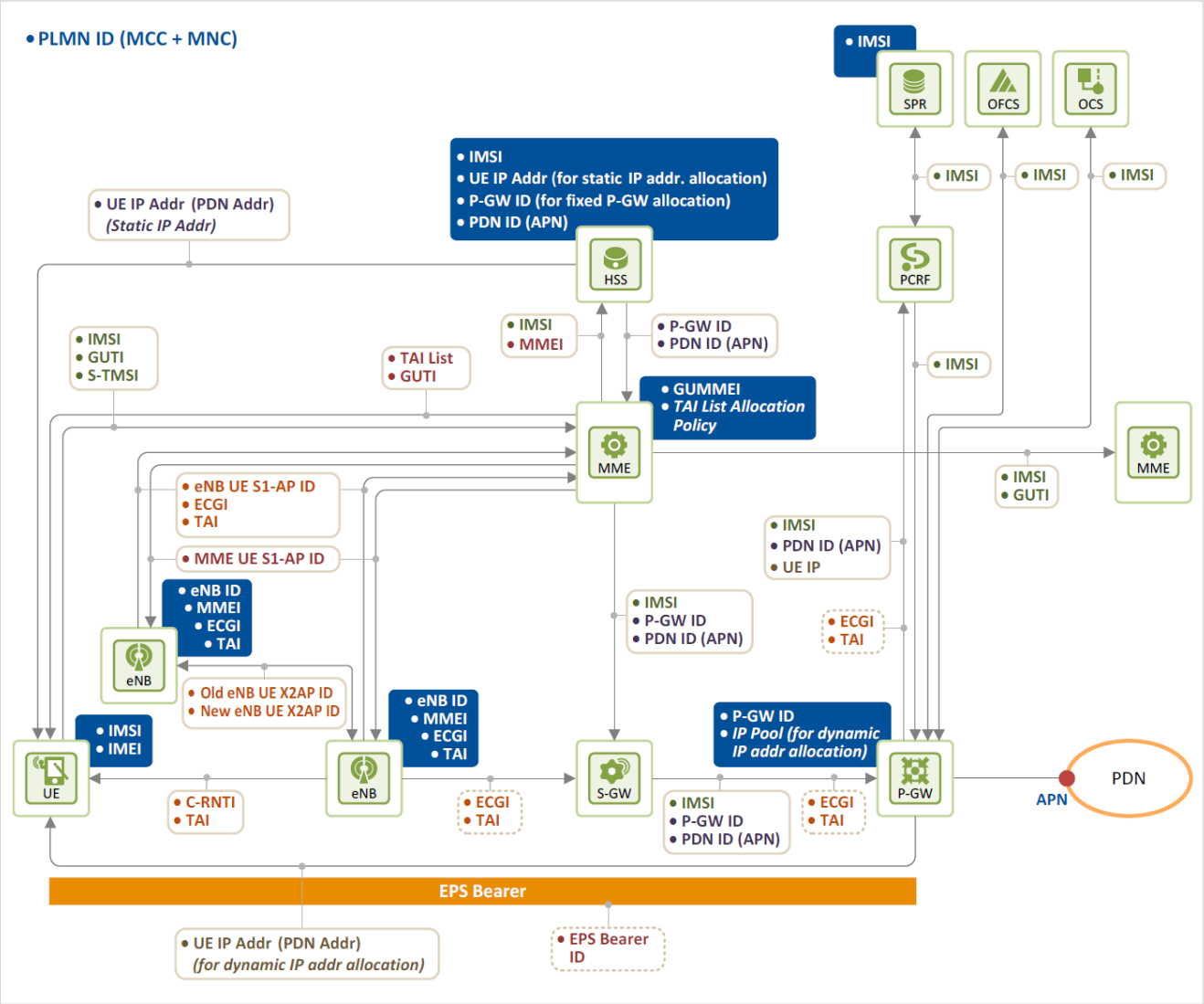


Figura 10 Identificatori in una rete LTE

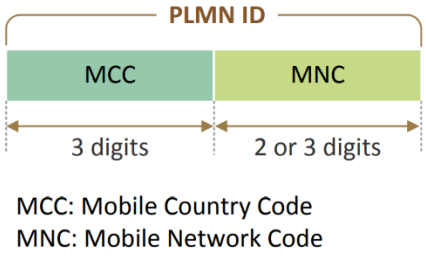
1.7.1 Identificatori di User Equipment (UE ID)

Le reti LTE sono reti IP. In conseguenza di ciò, in una rete LTE gli UE condividono tra loro risorse radio e risorse di rete per cui le entità EPS necessitano di allocare un ID ad ogni UE per poterlo identificare.

PLMN ID

Le reti mobili, dette appunto PLMN (*Public Land Mobile Network)* sono create e mantenute da degli operatori con lo scopo di fornire servizi alla collettività. Un PLMN ID identifica in modo univoco a livello globale la rete mobile con la quale un utente ha sottoscritto un contratto. È composto da un MCC (*Mobile Country Code*) e da un MNC (*Mobile Network Code*) come mostrato in Figura 11. Il MCC, composto da 3 cifre, identifica la nazione dove è collocata la rete mobile. La sua allocazione è

a cura dell'ITU-T. L'MNC, invece, identifica l'operatore di una determinata rete mobile ed è allocato da ogni paese. L'esempio mostrato in Figura 11 fa riferimento agli operatori presenti in Sud Corea.



MCC	MNC	Brand Name	Mobile Network Operator
450	02	KT	KT
450	04	KT	KT
450	05	SKT	SK Telecom
450	06	LG U+	LG Telecom
450	08	Olleh	KT

Figura 11 Formato del PLMN ID ed esempio

IMSI

L'International Mobile Subscriber Identity (IMSI) è un numero che identifica univocamente un utente di una rete mobile a livello globale. In Figura 12 è mostrato il processo di allocazione di un IMSI ed il suo formato. L'IMSI è composto dal PLMN ID che identifica, come già detto sopra, la rete con la quale l'utente ha sottoscritto un contratto e dal Mobile Subscriber Identification Number (MSIN) che viene assegnato dall'operatore ed identifica un utente all'interno di una PLMN. L'IMSI ha una lunghezza massima di 15 cifre.

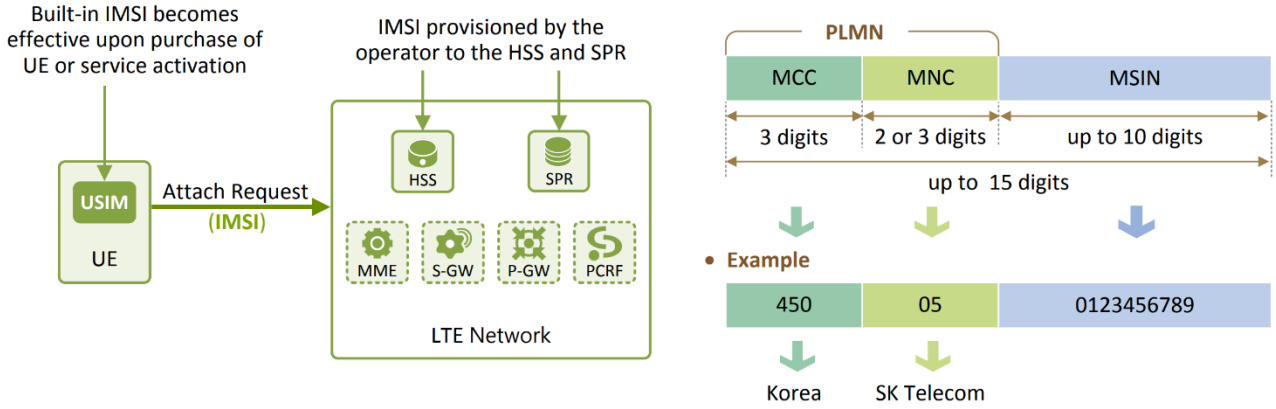


Figura 12 Allocazione dell'IMSI e formato

Quando un utente compra una USIM sottoscrivendo quindi un contratto con un operatore di rete mobile, l'IMSI inserito nella SIM all'atto della sua fabbricazione diventa attivo e viene associato con l'utente. Al contempo, le informazioni relative al contratto sottoscritto e l'IMSI vengono inseriti nell'HSS dell'operatore.

L'IMSI viene inviato dall'UE alla rete quando esegue la procedura di collegamento alla rete (Initial Attach). L'IMSI, per costruzione, permette ad ogni rete mobile del mondo di identificare la home

network dell'utente ed ancor più nello specifico, consente di individuare l'HSS all'interno della home network che mantiene le informazioni relative al contratto sottoscritto.

ID utilizzati dall'MME per identificare l'UE: GUTI, S-TMSI ed M-TMSI

Un IMSI, come detto in precedenza, identifica univocamente e permanentemente un utente di una rete mobile a livello globale e ciò potrebbe comportare problemi di sicurezza se l'IMSI viene inviato frequentemente lungo il canale radio.

Per motivi di sicurezza quindi, all'atto del collegamento iniziale alla rete, l'UE utilizza l'IMSI per richiedere l'accesso alla rete ed ottiene in risposta un identificativo temporaneo univoco a livello globale detto Globally Unique Temporary Identifier (GUTI) allocato dall'MME che potrà essere utilizzato al posto dell'IMSI per identificare l'UE nel caso di un nuovo collegamento o di un TA Update. L'utilizzo o meno del GUTI come identificativo da parte dell'UE nei successivi collegamenti o TA Updates dipende da quale valore viene impostato come TIN (Temporary Identifier used in Next update).

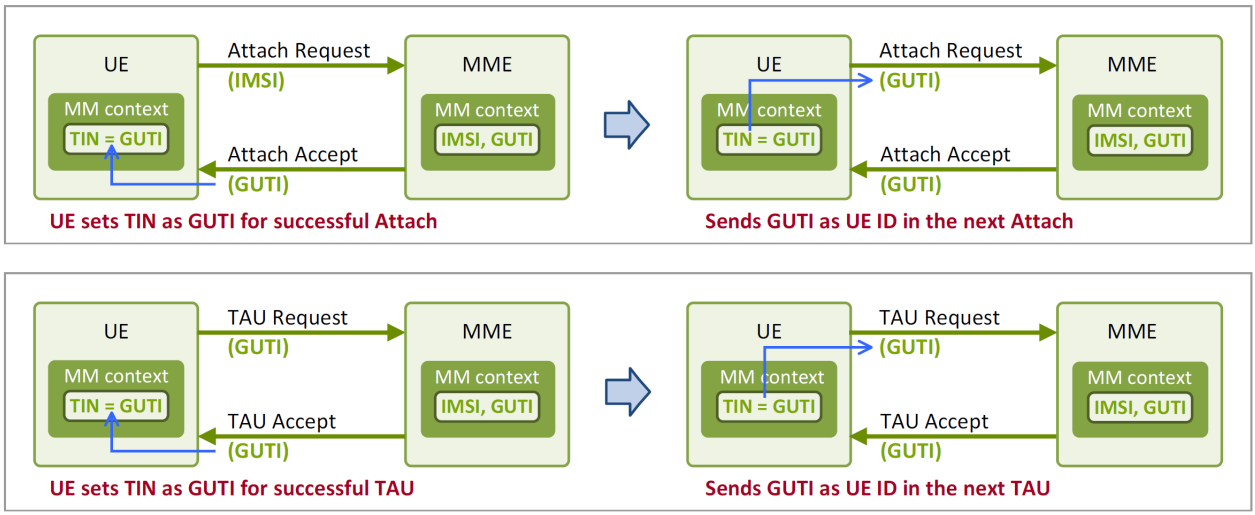
In ragione della sua natura temporanea il GUTI può essere utilizzato in sicurezza anche quando viene esposto di frequente lungo il canale radio.

Per quanto concerne il formato del GUTI, bisogna tenere presente che un operatore può avere uno o più gruppi di MME formati ciascuno da più MME, per far fronte, ad esempio, ad esigenze di load balancing. Il GUTI è formato dal GUMMEI (Globally Unique MME Identifier) che identifica a livello globale l'MME che alloca il GUTI e dall'M-TMSI (MME Temporary Subscriber Identity), allocato dall'MME, che individua in maniera univoca un utente all'interno dello stesso.

Il GUMMEI è composto dall'MME Identifier (MMEI) che rappresenta univocamente un MME all'interno della rete e dal PLMN ID che identifica a livello globale la rete mobile alla quale un MME appartiene. L'MMEI, a sua volta è formato dall'MMEGI (MME Group Identifier) che rappresenta un MME group e dall'MMEC (MME Code) che identifica un MME all'interno di un determinato MME group.

Il GUTI è un identificatore piuttosto lungo, perciò, per migliorare l'efficienza di trasmissione lungo il canale radio, in presenza di un unico MME group, viene utilizzata una versione accorciata detta S-TMSI. L'S-TMSI, formato dall'MMEC e dal M-TMSI, identifica univocamente un UE all'interno di un MME group e viene utilizzato, ad esempio, durante le procedure di Paging e di Service Request.

- GUTI Allocation



- GUTI Format

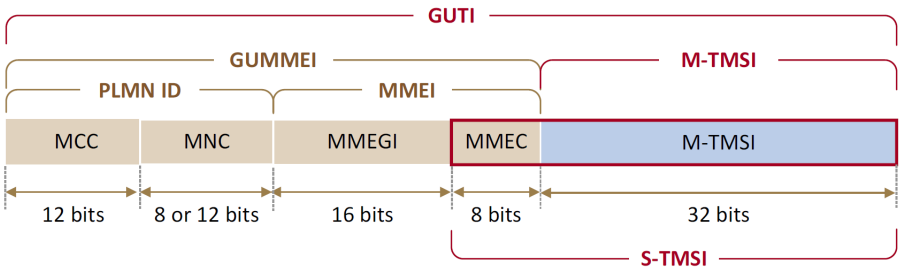


Figura 13 Procedura di allocazione del GUTI e formato

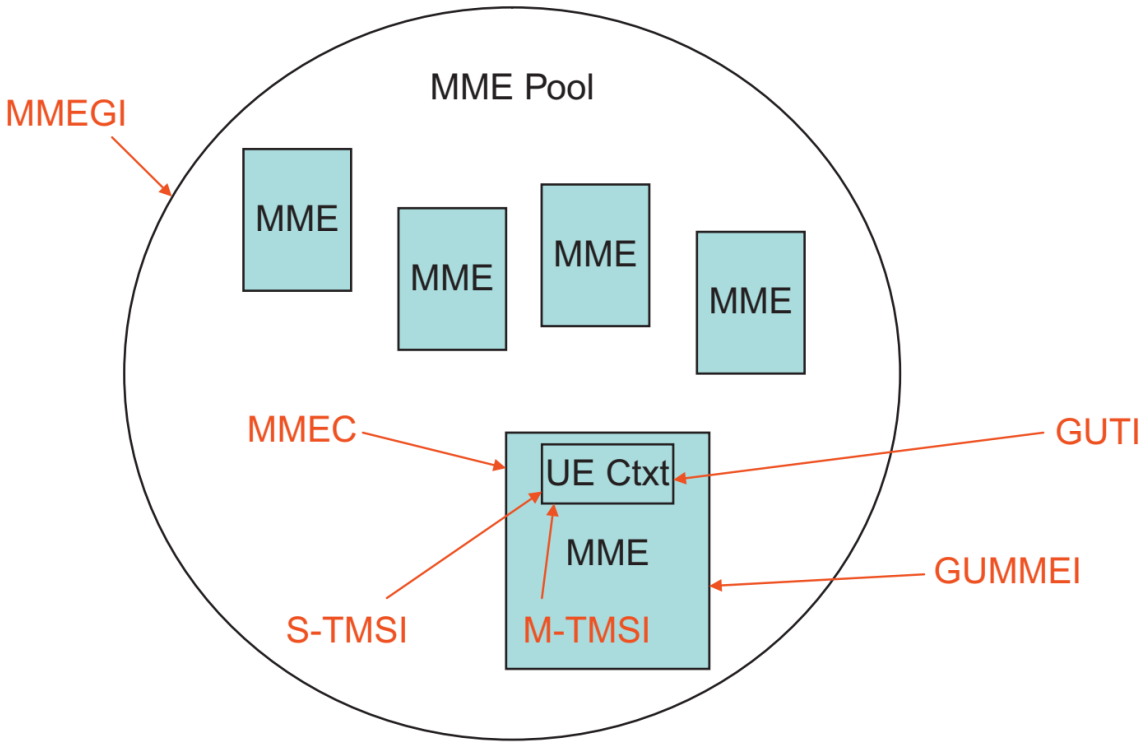


Figura 14 Visione degli identificatori come puntatori

Indirizzo IP

Un indirizzo IP, detto anche "PDN address", viene allocato dalla rete LTE ad un UE all'atto del collegamento iniziale affinché quest'ultimo possa connettersi ad una PDN. Poiché un UE può essere connesso a più di una PDN attraverso una rete LTE (a seconda dei servizi che sta utilizzando), la rete alloca ad ogni UE un indirizzo IP differente per ogni PDN a cui è connesso. Questi indirizzi IP sono utilizzati per identificare l'UE di provenienza/destinazione dei pacchetti IP in arrivo dalla o diretti verso la PDN.

Un indirizzo IP può essere allocato dinamicamente o staticamente. Nel caso di allocazione statica, l'operatore assegna un indirizzo IP permanente all'UE all'atto della sottoscrizione del contratto. Così facendo, l'UE avrà sempre lo stesso indirizzo all'atto del collegamento ad una determinata PDN a prescindere dal luogo e dal momento in cui si collega.

Nel caso di allocazione dinamica, invece, un PGW ha un IP pool dal quale attinge, per assegnare all'UE un indirizzo IP disponibile al momento in cui questo esegue la procedura di collegamento alla rete. Di conseguenza, un UE potrebbe ricevere un indirizzo IP diverso ogni volta in cui si collega ad una determinata PDN.

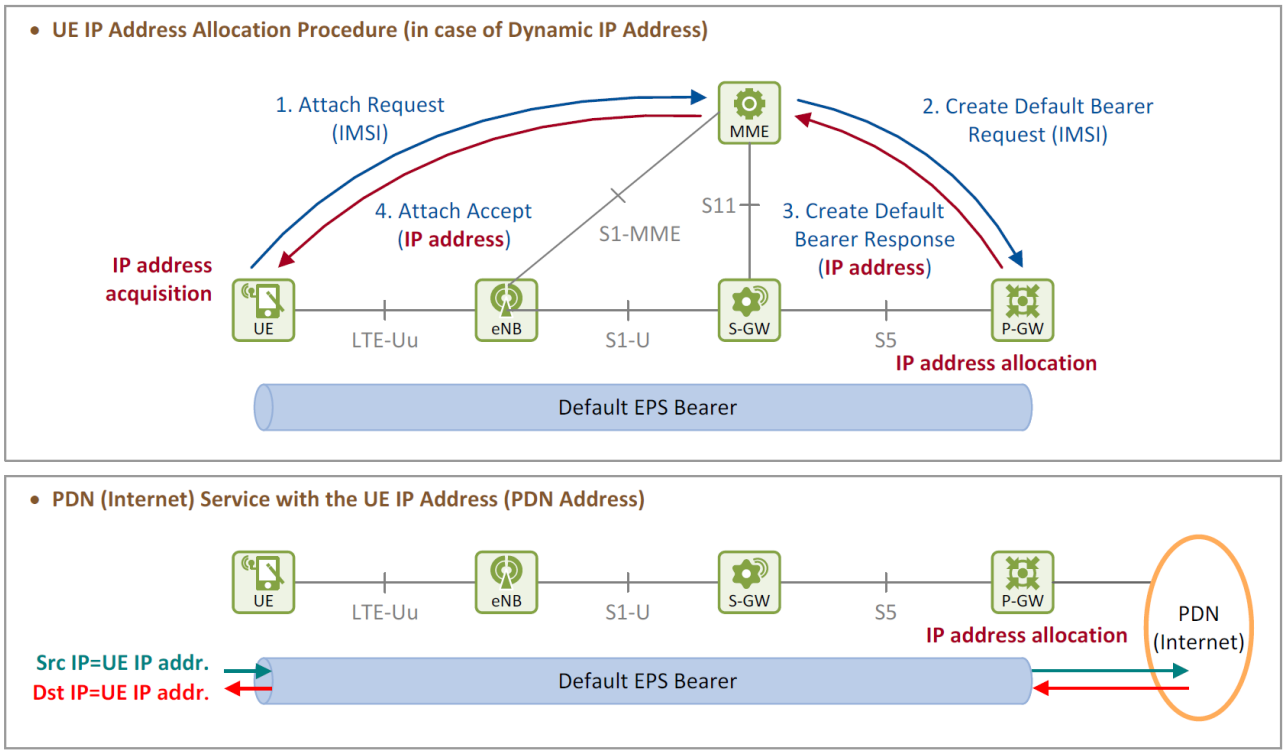


Figura 15 Procedura di allocazione dell'indirizzo IP

C-RNTI

Il Cell Radio Network Temporary Identifier (C-RNTI) è un identificativo allocato ad un UE da un eNB attraverso una "random access procedure" in una cella controllata dall'eNB ed è valido solo all'interno della serving cell. Gli UE agganciati ad una determinata cella sono identificati univocamente dal loro C-RNTI. Quando un UE si sposta lasciando una determinata cella ed agganciandosi ad un'altra, la nuova serving cell provvede ad allocargli un C-RNTI attraverso la "random access procedure".

Il C-RNTI viene utilizzato, ad esempio, dall'eNB per indicare ad un UE che nel prossimo Transmission Time Interval in downlink o uplink potrà utilizzare le risorse radio.

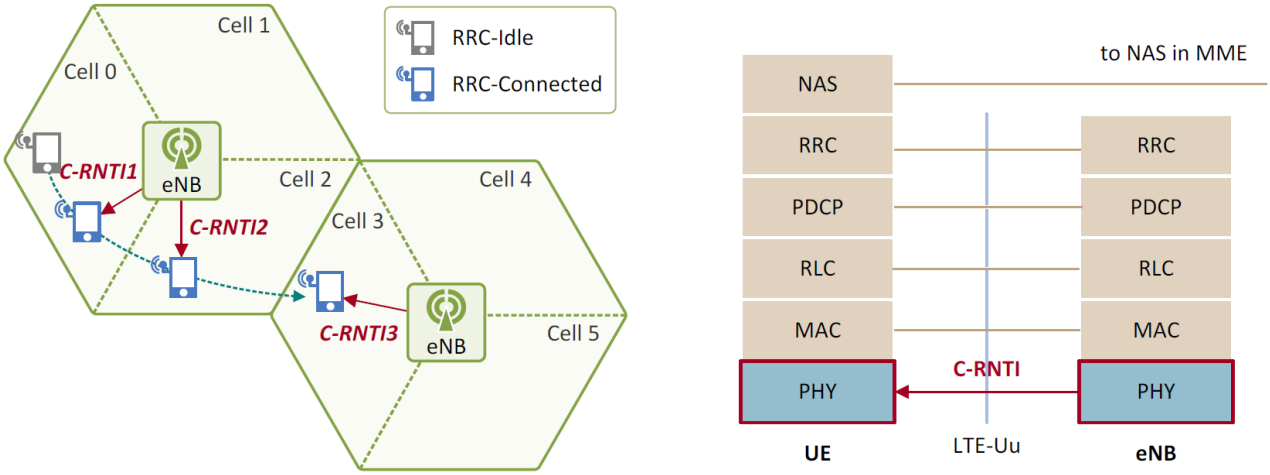


Figura 16 Allocazione del C-RNTI

Coppia di ID UE S1AP

Il layer S1AP gestisce i messaggi di controllo scambiati tra un eNB ed un MME attraverso l'interfaccia S1-MME. In un determinato momento, ad ogni eNB possono essere connessi più UE ed un eNB utilizza sempre lo stesso collegamento S1 per scambiare con un MME tutti gli S1AP control messages relativi ai diversi UE. Quindi, per poter sapere a quale UE è relativo un determinato messaggio S1AP, un eNB alloca un ID (eNB UE S1AP ID) ad ogni UE quando invia ad un MME il primo messaggio S1AP relativo ad un UE. Similmente, un MME scambia messaggi S1AP con più di un eNB attraverso vari collegamenti S1 simultaneamente. Allora, per poter determinare a quale UE è rivolto un messaggio S1AP, l'MME alloca un ID (MME UE S1AP ID) ad ogni UE quando invia ad un eNB il primo messaggio relativo ad un determinato UE.

Dopo questo primo scambio iniziale di messaggi S1AP, tutti i successivi messaggi S1AP scambiati lungo l'interfaccia S1-MME vengono inviati con una coppia di UE S1AP ID (eNB UE S1AP ID, MME UE S1AP ID) cosicché entrambe le parti (MME ed eNB) possano sapere a quale UE un messaggio S1AP fa riferimento.

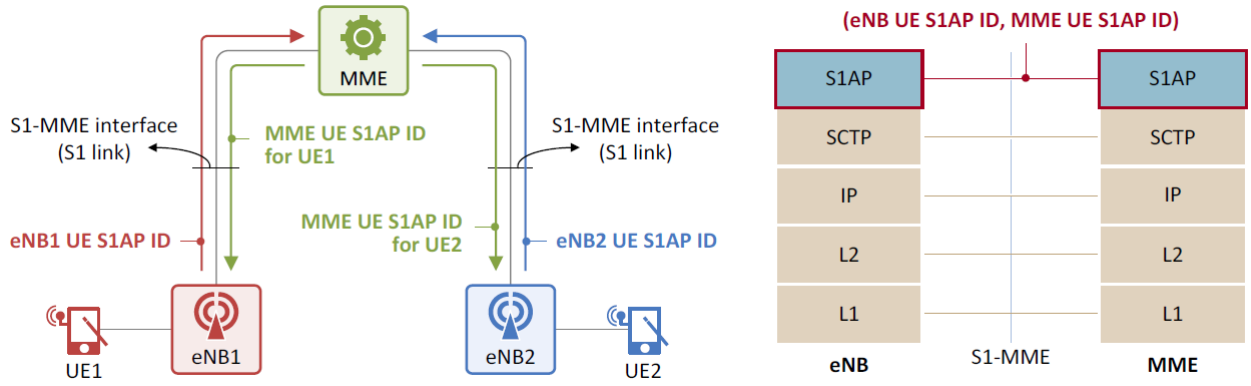


Figura 17 Allocazione dell'UE S1AP ID e layer S1AP

Coppia di UE X2AP ID

Il layer X2AP gestisce i messaggi di controllo scambiati tra due eNB lungo un'interfaccia X2. Durante ogni handover di UE tra due eNB vicini, i messaggi X2AP relativi ad UE differenti, vengono scambiati tra due peer eNB utilizzando lo stesso link X2. La prima volta che un eNB (source o target) invia un messaggio X2AP ad un peer eNB relativamente ad un determinato UE in handover assegna a quest'ultimo un ID che identifica l'UE a cui è relativo il messaggio inviato. Un source eNB alloca un Old eNB UE X2AP ID al primo messaggio che invia al target eNB (Handover Request). Il target eNB a sua volta, alloca un New eNB UE X2AP ID al primo messaggio di risposta inviato al source eNB (Handover Request Acknowledge).

Dopo questo round-trip iniziale, tutti i messaggi X2AP relativi all'handover inviati lungo l'interfaccia X2 sono scambiati utilizzando una coppia di ID (Old eNB UE X2AP ID, New eNB UE X2AP ID) affinché il source eNB ed il target eNB possano associare l'UE corretto al messaggio appena ricevuto o inviato.

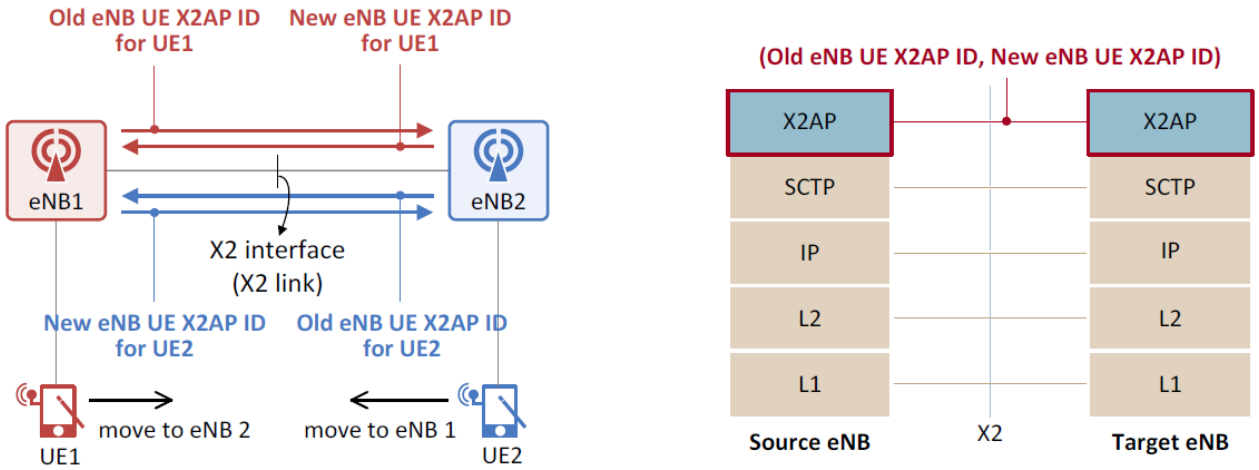


Figura 18 Allocazione dell'UE X2AP ID e layer X2AP

1.7.2 Identificatori di Mobile Equipment (ME ID)

Un UE consta di un ME e di un UMTS Subscriber Identity Module (USIM). Un ME a sua volta può essere suddiviso in Terminal Equipment (TE) e Mobile Terminal (MT). Un MT è dove i protocolli di accesso radio lavorano mentre TE è dove operano le funzioni di controllo del MT.

In un cellulare le funzioni di MT e TE sono integrate insieme.

La Figura 19 mostra un paio di esempi in cui si hanno diverse combinazioni di MT e TE.

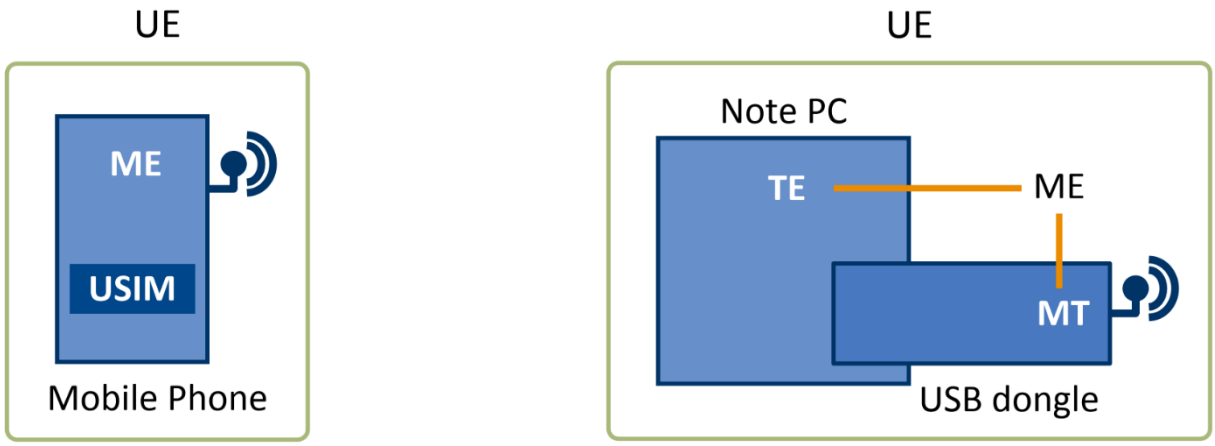


Figura 19 Relazione tra UE ed ME

IMEI

L'International Mobile Equipment Identity è un numero univoco allocato ad ogni mobile equipment (ME). Un IMEI viene assegnato all'atto della costruzione di un ME e contiene le informazioni circa il produttore, il modello ed il numero di serie dell'ME. La Figura 20 illustra il formato dell'IMEI ed un esempio di utilizzo. L'IMEI è composto da un Type Allocation Code (TAC), un Serial Number (SNR) ed un Check Digit (CD). Un IMEI/SV è composto invece da un TAC, un SNR ed un Software Version Number (SVN).

Un TAC a sua volta è composto da un Reporting Body Identifier (RBID) che indica un reporting body ed un ME Type ID che rappresenta il nome del produttore e del modello. I serial numbers sono assegnati dal produttore. Nell'Esempio in Figura 20 l'RBID "35" indica che l'ME è stato approvato dal British Approvals Board for Telecommunications (BABT) e l'ME Type ID "643205" indica che l'ME è uno smartphone prodotto da Samsung.

Un operatore mantiene un DB detto Equipment Identity Register (EIR) che memorizza le informazioni sugli IMEI e di conseguenza può negare l'accesso alla rete ad ME che risultano smarriti o rubati.

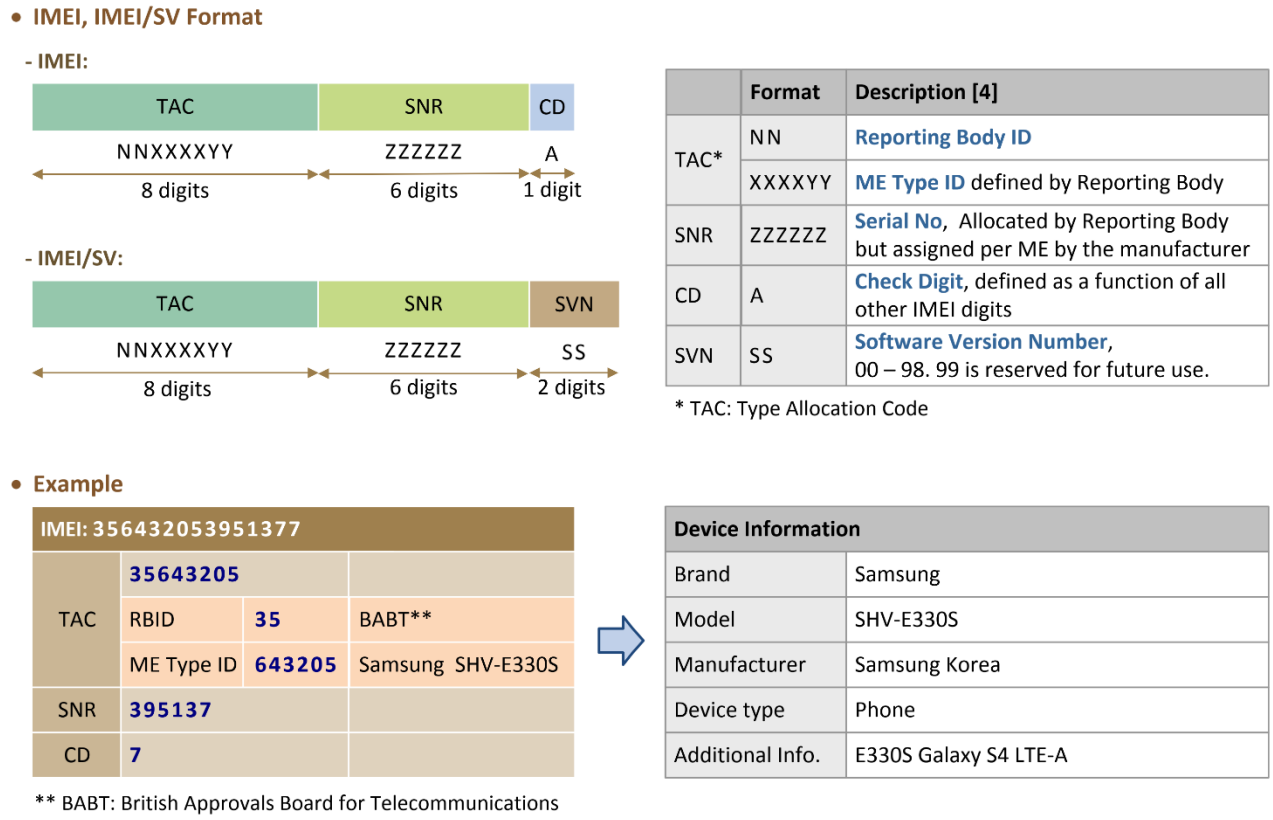


Figura 20 Formato dell'IMEI ed esempio applicato

1.7.3 Identificatori di Network Equipment (NE ID)

Identificatori di eNB

Un eNB ID identifica un eNB all'interno della rete di un operatore. Un Global eNB ID, formato dalla combinazione di un PLMN ID ed un eNB ID, è utilizzato per identificare l'eNB all'esterno della rete di appartenenza. Per identificare una cella appartenente ad un eNB, viene utilizzato un ID formato dall'unione di un Cell ID con un eNB ID (ECI) oppure con un Global eNB ID (ECGI).

Gli eNB ID e i Cell ID vengono assegnati dall'operatore quando l'eNB viene installato. Terminata l'installazione, l'eNB inizia il setup del collegamento S1 tra sé stesso ed un MME. Quando richiede all'MME la creazione del link S1, riporta il suo Global eNB ID, le Tracking Areas (TA) supportate e un CSG (Closed Subscriber Group) ID se i CSG sono supportati. Un CSG è una cella aperta solo ad un determinato gruppo di utenti ed è composta da una singola cella o da un insieme di celle. L'MME, in risposta, invia all'eNB i GUMMEI degli MME appartenenti al suo pool.

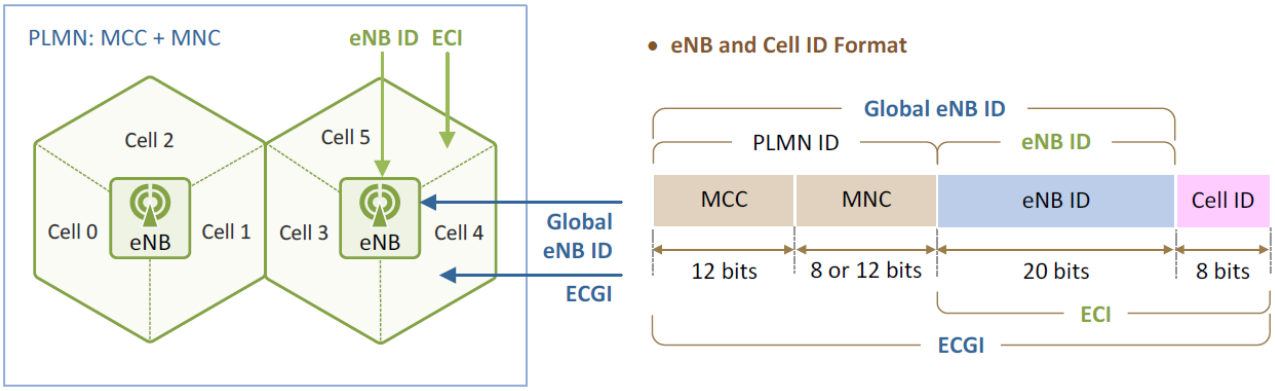


Figura 21 Identificatori di eNB e cella

PGW ID

Quando l'UE si connette ad una rete LTE, la rete gli fornisce il servizio di connessione ad una PDN. Per poter creare un collegamento tra l'UE ed una PDN, l'MME deve conoscere la PDN alla quale connettere l'UE nonché il PGW attraverso il quale far transitare i pacchetti diretti verso quella PDN. La PDN di default per l'UE è già stata inserita nell'HSS come parte del profilo sottoscritto. L'MME può quindi utilizzare semplicemente questa informazione ottenuta dall'HSS. Per quanto riguarda il PGW, può essere allocato in due modi:

- *allocazione fissa* in cui l'operatore di rete inserisce nell'HSS un PGW ID come parte del profilo sottoscritto dall'utente
- *allocazione dinamica* in cui l'MME seleziona un PGW in accordo alle policy di selezione definite dall'operatore.

In caso di allocazione fissa, l'HSS fornisce all'MME il PGW ID, affinché questi possa richiedere al PGW di stabilire una connessione con la PDN scelta.

In caso di allocazione dinamica invece, l'MME ottiene una lista di indirizzi IP di PGW attraverso una query DNS, ne seleziona uno in base alle policy stabilite dall'operatore e richiede a quel PGW di stabilire una connessione con la PDN.

In Figura 22 viene mostrato il caso di un PGW ID assegnato con allocazione statica ed il suo formato. Nel caso in esempio, ci può essere un UE le cui PDN di default sono definite come PDN 1 (Internet) per l'accesso ai servizi Internet e PDN 2 (IMS) per i servizi voce. All'atto del collegamento iniziale dell'UE alla rete, l'MME richiede all'HSS le informazioni relative al profilo sottoscritto dall'utente e dalle informazioni ottenute emerge che: le PDN di default dell'UE sono PDN 1 (Internet) e PDN 2 (IMS) e il PGW collegato alla PDN 1 è PGW 1 mentre quello collegato alla PDN 2 è PGW 3

Sapendo ciò, l'MME provvede a stabilire una connessione tra l'UE ed Internet attraverso il PGW 1 ed una tra l'UE e la rete IMS attraverso il PGW 3.

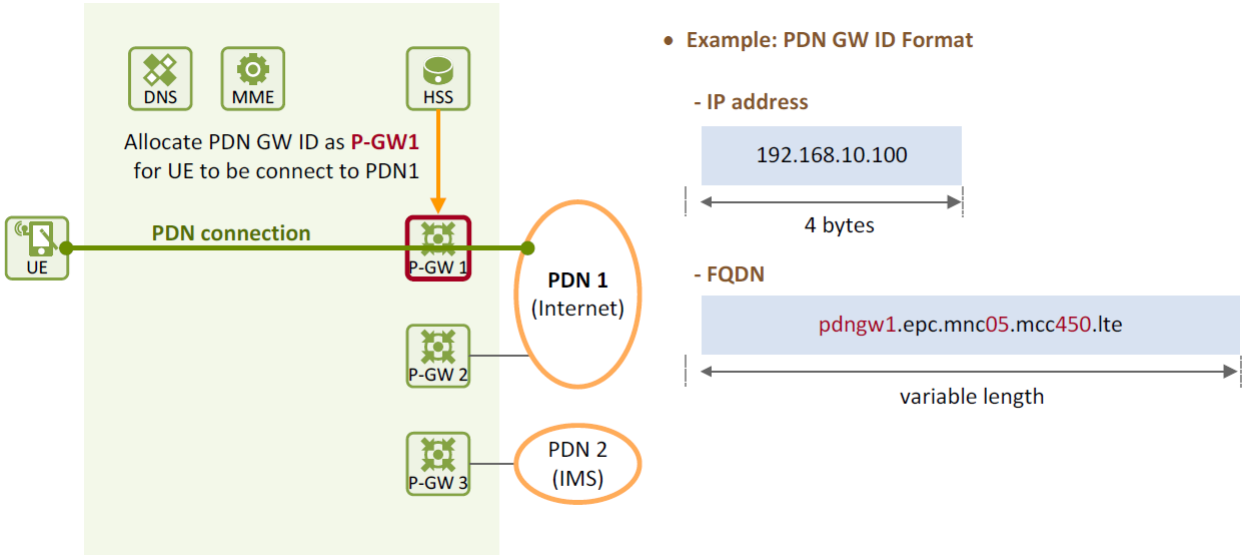


Figura 22 Identificatori di PGW

ID dell'MME: GUMMEI, MMEI, MMEGI e MMEC

Un MMEI (MME Identifier) viene utilizzato per identificare un MME all'interno di una rete di un operatore.

Un GUMMEI (Globally Unique MME Identifier), combinazione di un PLMN ID ed un MMEI identifica univocamente un MME a livello globale anche al di fuori della rete di un operatore.

Nel caso in cui l'operatore decida di raggruppare gli MME in gruppi (MME groups), l'MMEI è composto da un MMEGI che rappresenta un MME group e un MMEC che rappresenta un particolare MME all'interno di un MME group.

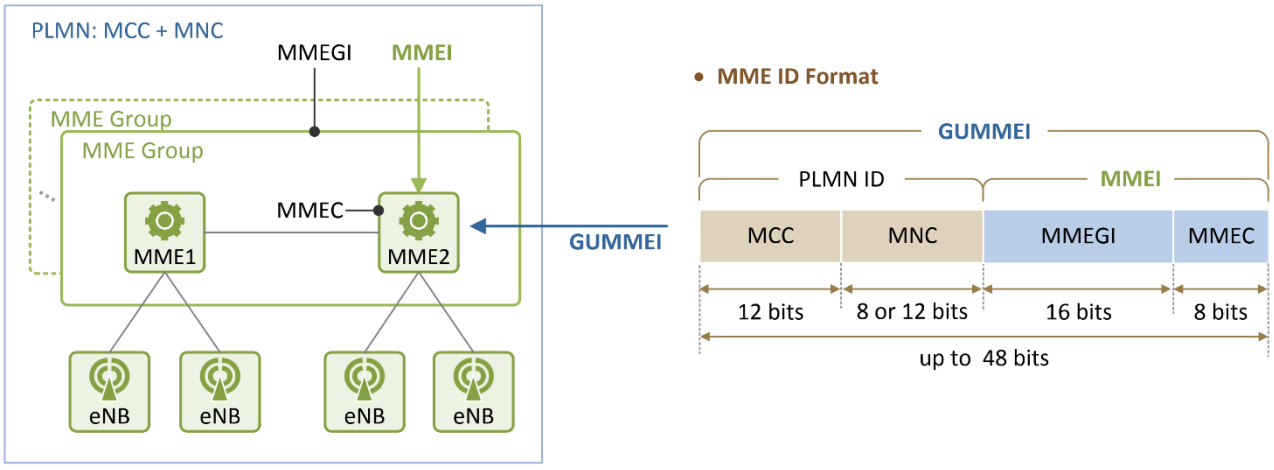


Figura 23 ID di MME e loro formato

1.7.4 Identificatori di posizione dell'UE

TAC e TAI

Dato che un MME si fa carico di gestire la mobilità dell'utente deve poter avere informazioni aggiornate circa la posizione dell'UE. La posizione di un UE è nota alla rete a livello di cella se l'UE si trova in active state e sta utilizzando servizi mentre lo è a livello di Tracking Area (TA) se l'UE si trova in idle state.

Un operatore in fase di initial deployment della rete definisce un gruppo di eNB vicini tra loro come una Tracking Area, configurando ogni eNB con la sua Tracking Area di appartenenza.

Gli identificatori di TA sono il TAC (Tracking Area Code) e il TAI (Tracking Area Identifier). Il TAC è utilizzato per identificare una TA all'interno della rete di un operatore, mentre il TAI, che è composto da PLMN ID e TAC identifica univocamente una TA a livello globale.

Il concetto di Tracking Area è necessario poiché qualora vi sia nuovo traffico in arrivo per un UE che si trova in Idle state la rete deve poter "risvegliarlo" segnalandogli che ci sono dati in arrivo per esso. Questa procedura di "risveglio" detta Paging e avviene a livello di TA poiché quando la rete deve risvegliare un UE in Idle state, invia un messaggio di Paging a tutti gli eNB appartenenti alla TA dove si presume che l'UE sia collocato. Ogni eNB provvede poi a diffondere in broadcast il paging message lungo il canale radio per poter risvegliare l'UE. Un UE in Idle state, si risveglia periodicamente per controllare se ci sono messaggi di paging a lui diretti per segnalare la presenza di nuovi dati in arrivo. Se un UE nota di essere stato oggetto di paging (controllando l'S-TMSI nel Paging mesasge) da parte di un eNB ritorna in stato attivo pronto per ricevere i dati in arrivo.

Per poter far sì che la rete (l'MME in particolare) sappia in quale TA è collocato l'UE, quest'ultimo deve notificare alla rete (MME) la sua posizione corrente inviando un TAU Request Message ogni volta che si sposta in TA diverse.

Ogni eNB diffonde in broadcast il suo Cell ID (ECI, ECGI) e le informazioni circa la sua TA (TAC, TAI). Quando un UE si connette ad una nuova cella scopre, ascoltando le informazioni diffuse in broadcast, se questa si trova in una TA differente da quella in cui si trova attualmente (per cui dovrà effettuare un TAU Request) oppure se la cella è situata nella la TA attuale (per cui non dovrà effettuare una TAU Request).

In realtà, all'atto della procedura di collegamento iniziale, un UE ottiene una TAI list quando si connette ad una rete LTE. Questa lista mostra le TA in cui la rete crede che un UE si sposterà e all'interno delle quali potrà muoversi senza effettuare un TA Update.

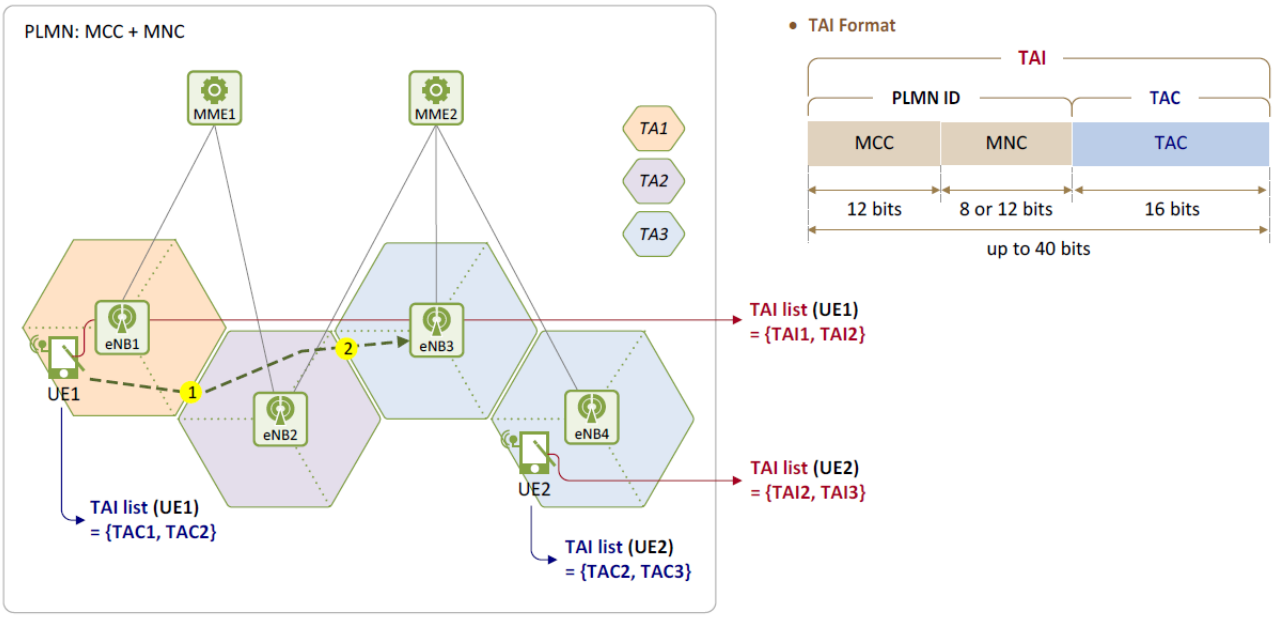


Figura 24 Esempio di TA

Nell'esempio in Figura 24 la TAI list è {TAC1, TAC2}. Ciò significa che un UE non dovrà inviare un TAU message all'MME a patto che rimanga in TA1 o TA2, mentre dovrà effettuare una TAU Request qualora si sposti in una TA non presente nella TAI list allocatagli (e.g. TAI3). L'MME provvederà poi ad assegnargli una nuova TAI list che rifletta al meglio i suoi spostamenti (e.g. nuova posizione, velocità di movimento ecc.) per garantire un paging più efficiente.

Oltre al TAU effettuato per spostamento in una TA non registrata, un UE che si trova in idle state è tenuto ad effettuare TAU periodici attraverso i quali invia periodicamente un TAU message ad un MME anche se si trova all'interno di una TA presente nella sua TAI list.

Questa procedura è richiesta poiché, se un UE in idle state è rimasto nella stessa posizione (o si è spostato tra TA presenti nella sua TAI list) e non ha più notificato all'MME la sua posizione, la rete non può sapere se si trova ancora in idle state oppure se non è più in grado di comunicare. Per questo motivo, anche se l'UE non si sposta invia periodicamente dei messaggi di TAU Request all'MME per informarlo che è in grado di ricevere dati. Qualora questo non avvenga, la rete crederà che l'UE non sia più in grado di ricevere dati e non eseguirà il paging quando ci sarà traffico diretto all'UE.

1.7.5 Identificatori di EPS Session / EPS Bearer

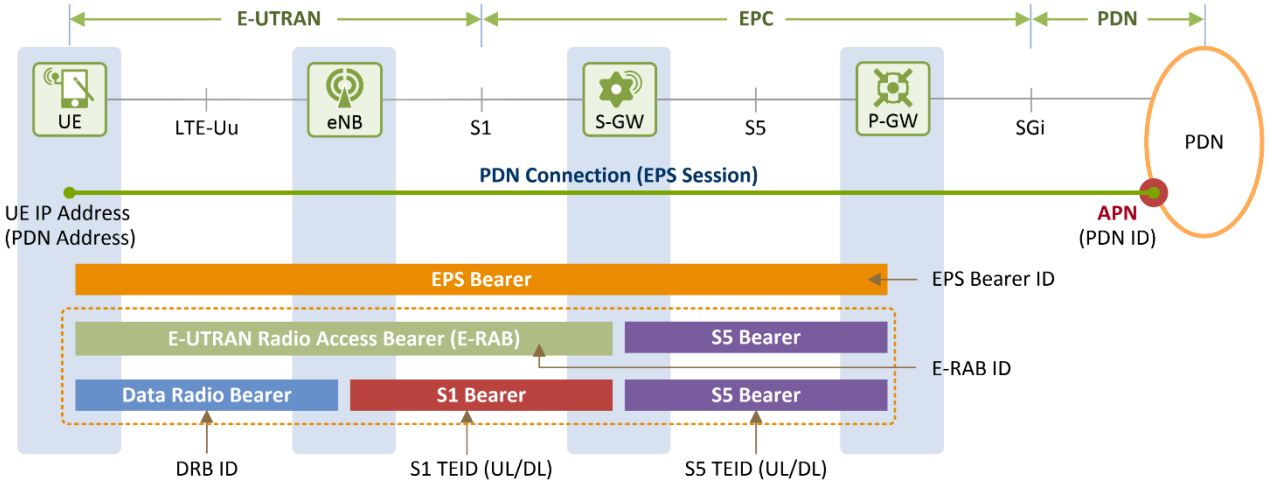


Figura 25 panoramica di Session/Bearer ID

Come già detto in precedenza, un EPS Bearer rappresenta una sorta di tubo attraverso il quale i pacchetti IP vengono spediti attraverso la rete LTE, cioè tra un UE ed un PGW (UE – eNB – SGW – PGW). Un UE può avere più bearers EPS attivi contemporaneamente che vengono distinti da un EPS Bearer ID, allocato da un MME.

Come mostrato in Figura 25, un EPS bearer è in realtà la concatenazione dei seguenti tre bearers (DRB, S1 bearer ed S5 bearer):

- [UE] – [eNB]: Data Radio Bearer (DRB)
  EPS bearer attivo lungo l'interfaccia LTE-Uu. Il traffico dati utente viene spedito attraverso un DRB. I diversi DRB sono identificati da un DRB ID allocato da un eNB.
- [eNB] – [SGW]: S1 bearer
  EPS bearer stabilito lungo l'interfaccia S1-U. Il traffico dati utente viaggia attraverso un tunnel GTP. Differenti bearer S1 sono identificati dal loro Tunnel Endpoint Identifier (TEID) che è allocato dagli endpoint (eNB ed SGW) del tunnel GTP.
- [SGW] – [PGW]: S5 bearer
  EPS bearer stabilito lungo l'interfaccia S5. Il traffico dati utente viene spedito lungo un tunnel GTP. Differenti bearer S5 sono identificati dal loro TEID allocato dagli endpoint (SGW e PGW) del tunnel GTP.

Un E-RAB è un bearer che ha come endpoint un UE ed un SGW, è formato dalla concatenazione di un DRB con un S1 bearer e connette un UE ad un SGW (UE – eNB – SGW). E-RAB differenti sono identificati da un E-RAB ID allocato da un MME. I DRB ID sono in relazione 1:1 con gli EPS Bearer ID.

PDN ID (APN)

Una PDN connection (EPS Session) è rappresentata da un indirizzo IP dell'UE e da un PDN ID (APN).

Una PDN a sua volta è identificata da un PDN ID (o Access Point Name (APN)). Un APN, come è facile intuire, si riferisce ad un access point ad una PDN alla quale l'utente desidera connettersi per usufruire di un servizio/applicazione. In Figura 26 viene illustrato il formato di un APN. Un APN è la combinazione di un network ID e di un operator ID. Il network ID viene utilizzato quando si devono identificare PDN come Internet o servizi come IMS che la PDN fornisce.

Un APN viene inserito in un HSS come parte del profilo di un utente all'atto della sottoscrizione del contratto (come nel Caso 1 in Figura 26)[1]. Quando l'UE effettua la procedura di collegamento iniziale alla rete, l'MME scarica le informazioni di sottoscrizione dell'utente, tra le quali vi è l'APN di default. L'MME seleziona quindi una PDN a cui connettere l'UE sulla base dell'APN e poi individua un PGW attraverso il quale connettere l'UE alla PDN. In Figura 26, l'MME ha selezionato PDN 1 sulla base di APN 1 e poi PGW 1 per connettere l'UE alla PDN 1.

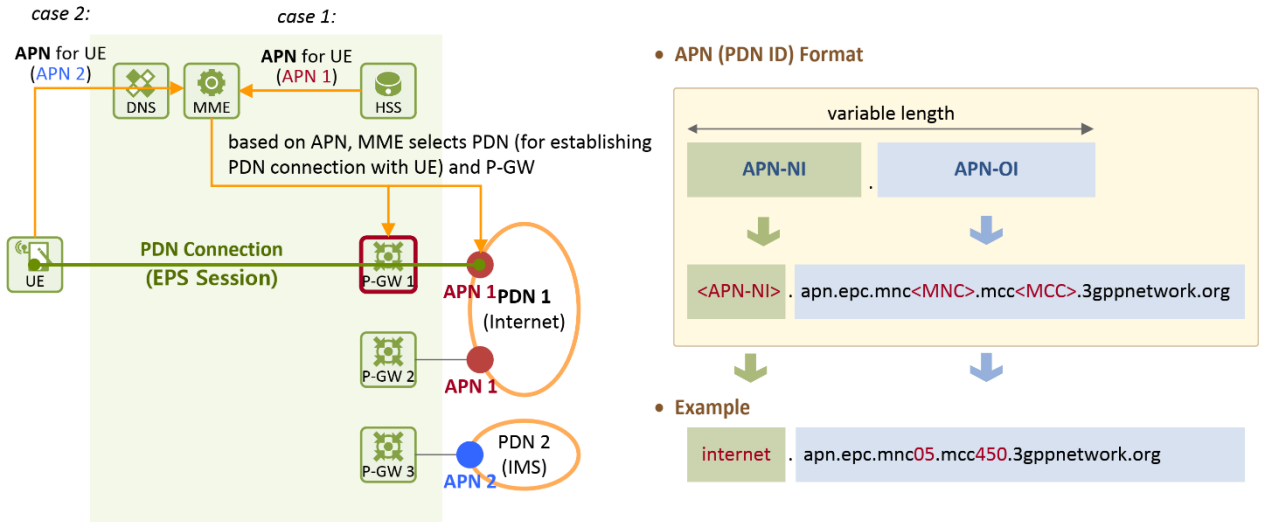


Figura 26 Formato ed esempio di APN ID

EPS Bearer ID

Un EPS Bearer è una connessione virtuale creata tra un UE ed un PGW per consentire il transito del traffico lungo la rete LTE.

EPS Bearer differenti sono identificati da un EPS Bearer ID di 4 bit. La Tabella 1 mostra i valori degli EPS Bearer ID e i loro range di allocazione. Un UE può avere fino a 11 EPS bearer attivi e il range degli ID ad essi assegnabili varia da 5 a 15.

[1] Un APN può anche essere fornito dall'UE (come nel caso 2 in Figura 26)

Tabella 1 Range di assegnazione dell'EPS bearer ID

EPS Bearer ID Value	Assigned/Not assigned
0	Not Assigned
1 ~ 4	Reserved
5 ~ 15	Available values

La Figura 27 mostra gli ID relativi ad un EPS Bearer e le entità che li allocano. Gli ID per gli EPS bearers, default o dedicated che siano, vengono allocati di un MME. Quando un UE si collega inizialmente alla rete, l'MME ottiene il profilo QoS necessario per stabilire und default bearer da un HSS e crea il default bearer con i parametri QoS ricevuti. La procedura di setup di un EPS Bearer inizia proprio con l'allocazione di un EPS Bearer ID da parte dell'MME.

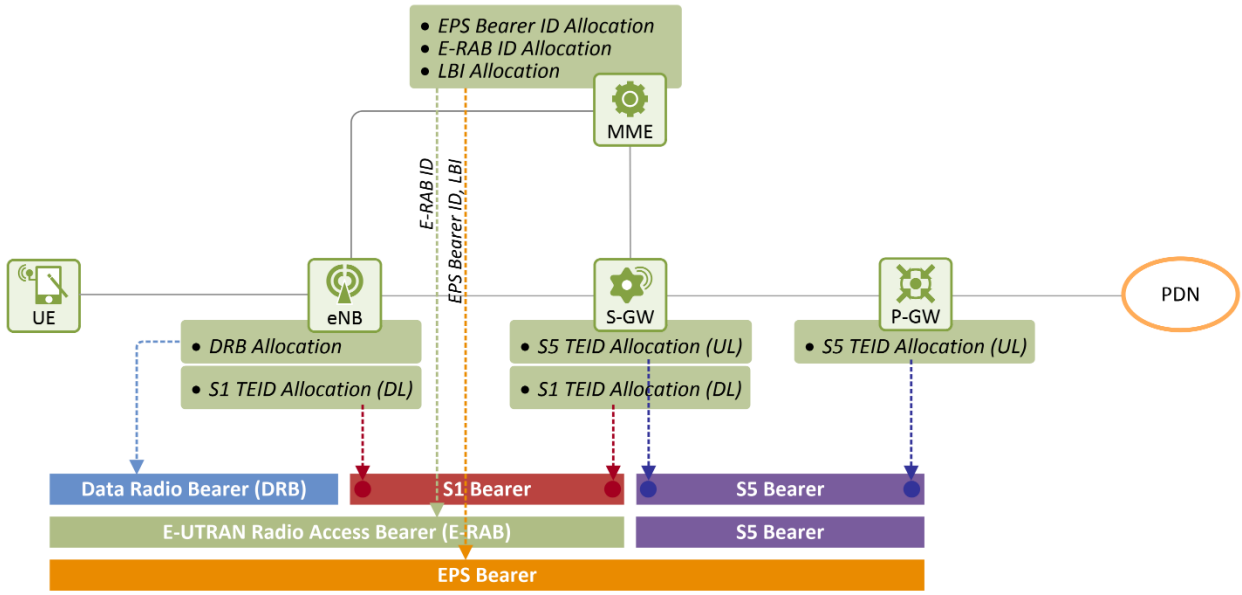


Figura 27 Entità che allocano i Bearer ID

Il flusso di traffico in downlink lungo un EPS Bearer transita attraverso un S5 bearer, un S1 Bearer ed un DRB ed infine arriva all'UE. Il percorso per il traffico in uplink è esattamente identico ma avviene al contrario. Per poter far sì che il traffico fluisca ogni entità deve mappare i bearer ID per ogni bearer come mostrato nella Tabella 2. La Figura 28 mostra un esempio di questo processo di mapping

Tabella 2 Mapping tra EPS bearer ID

Entità che effettua il mapping	**Mapping in Uplink**	**Mapping in Downlink**
UE	UL IP flows → DRB ID	
eNB	DRB ID → S1 Bearer ID (UL S1 TEID)	S1 Bearer ID → DRB ID (DL S1 TEID)
SGW	S1 Bearer ID → S5 Bearer ID (UL S1 TEID) (UL S5 TEID)	S5 Bearer ID → S1 Bearer ID (DL S5 TEID) (DL S1 TEID)
PGW		DL IP flows → S5 Bearer ID (DL S5 TEID)

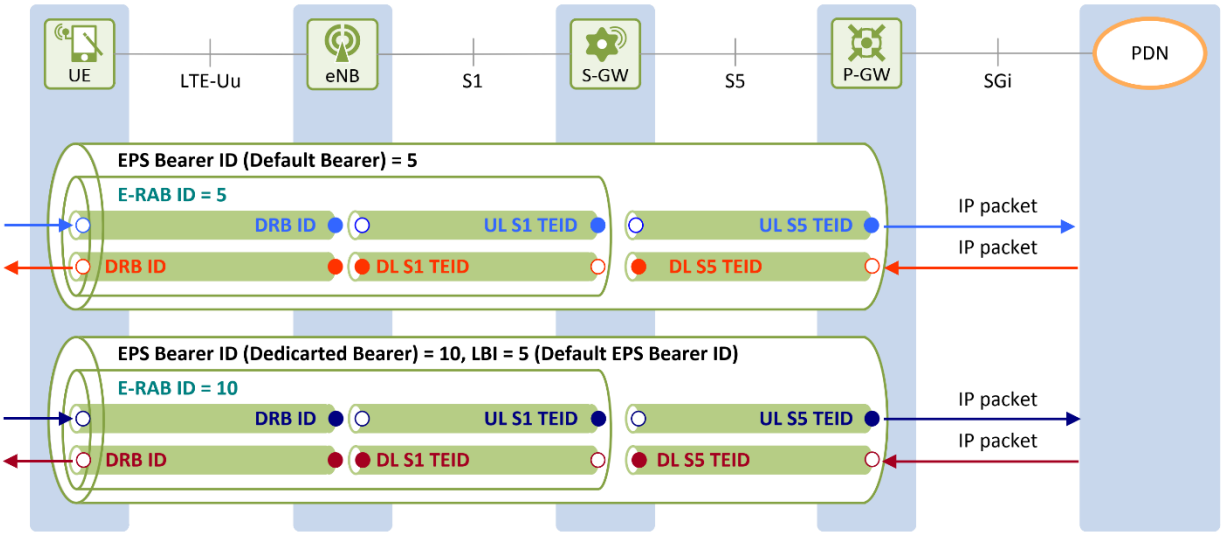


Figura 28 Mapping tra EPS bearer ID

E-RAB ID

Come mostrato nelle figure precedenti, un E-RAB è un EPS Bearer stabilito tra un UE ed un SGW, identificato da un E-RAB ID a 4 bit. L'E-RAB ID è assegnato da un MME, generalmente con lo stesso valore di un EPS Bearer ID all'atto della costruzione dell'EPS bearer ed è in relazione 1:1 con l'EPS bearer ID. Quando, durante le procedure di setup dell'EPS bearer, l'MME richiede all'eNB la creazione dell'E-RAB, l'eNB crea un DRB con l'UE e un S1 bearer col SGW.

Il default EPS bearer mantiene l'UE connesso alla rete. Quando non c'è traffico per cui l'UE cambia stato ad Idle, l'E-RAB viene disattivato e rimane attivo solo l'S5 bearer. Non appena arriva nuovo traffico utente in uplink o downlink l'E-RAB viene ristabilito consentendo al traffico di essere consegnato tra l'UE e il PGW.

DRB ID

Come mostrato nelle figure precedenti un DRB è un EPS bearer instaurato lungo il canale radio tra un UE ed un eNB, identificato da un DRB ID a 4 bit. Il DRB ID è assegnato da un eNB all'atto della creazione dell'EPS bearer ed è mappato con l'EPS bearer ID in rapporto 1:1. Quando durante la procedura di setup dell'EPS bearer l'MME richiede all'eNB la creazione di un E-RAB.

TEID

I bearer S1 ed S5, entrambi bearer EPS, sono stabiliti rispettivamente tra un eNB ed un SGW e tra un SGW ed un PGW in forma di tunnel GTP. I tunnel GTP sono identificati da degli interi a 32 bit detti Tunnel Endpoint Identifiers (TEID) assegnati dagli endpoint in downlink e in uplink. La Figura 27 mostra le entità che allocano i TEID ai berer S1 ed S5. Durante la procedura di setup dei bearer EPS, il SGW alloca il DL S5 TEID e il PGW alloca l'UL S5 TEID per il bearer S5 mentre, per il bearer S1, il SGW assegna l'UL S1 TEID e l'eNB assegna il DL S1 TEID.

LBI

Come già detto in precedenza, una sessione EPS può avere più di un bearer EPS. Il default EPS bearer viene attivato/disattivato quando la EPS session viene creata/distrutta. D'altro canto, un dedicated EPS bearer può essere creato o rimosso in qualsiasi momento una volta che la sessione EPS è stata creata. Siccome entrambi i bearer (il default e i dedicated bearers) appartengono alla sessa PDN per lo stesso utente, è necessario un ID per indicare che i bearer si riferiscono tutti alla stessa PDN.
A questo scopo, viene utilizzato un ID detto LBI che corrisponde al default EPS bearer ID.
Quando un default EPS bearer viene creato, l'MME alloca un bearer ID che è assegnato anche come LBI. Successivamente, quando gli EPS bearer dedicati vengono stabiliti, l'MME assegna loro, oltre al bearer ID, anche un LBI per collegarli al default EPS bearer

Capitolo II

Mobilità nelle reti 4G LTE

Lo scopo principale delle reti mobili è quello di garantire una esperienza d'uso soddisfacente durante l'utilizzo di un servizio offerto.

Un insieme sempre crescente di tecnologie di accesso (sia mobili che da rete fissa) a disposizione degli utenti nonché degli operatori stessi ha reso la mobilità sempre più complessa. Si è avvertita la necessità e il desiderio di trovare un insieme "comune" di strumenti che consentano ai dispositivi degli utenti finali di convergere verso il supporto di un insieme di meccanismi di mobilità.

Con l'EPS, il consorzio 3GPP ha puntato non solo a creare una core network comune per le varie tecnologie di accesso ma anche al garantire mobilità tra tecnologie di accesso eterogenee.

EPS rappresenta infatti la prima realizzazione completa di "multi-access convergence": una packet core network che offre un supporto completo alla gestione della mobilità, funzioni di discovery della rete di accesso e selezione per ogni tipo di access network.

La mobilità rappresenta la principale caratteristica dei sistemi mobili e molte delle decisioni riguardanti la progettazione della core network EPC derivano direttamente dalla necessità di supportare la mobilità.

La funzionalità di gestione della mobilità è richiesta per assicurare le seguenti condizioni:

- Che la rete possa "raggiungere" l'utente, ad esempio per notificare al terminale una chiamata in arrivo
- Che l'utente possa iniziare una comunicazione verso altri utenti o servizi ad es. la rete Internet
- Che le sessioni in atto possano essere mantenute quando l'utente si sposta sia all'interno della stessa rete d'accesso che fra reti d'accesso diverse.

Una funzionalità associata di autenticazione e autorizzazione assicura anche l'autenticità e la validità dell'accesso dell'utente preparando la rete e l'UE con le informazioni di sottoscrizione e le credenziali di sicurezza necessarie.

2.1 Stati EMM ed ECM

Quando un utente si collega ad una rete LTE, viene innanzitutto autenticato e registrato alla rete, poi viene instaurata una EPS session, vengono costruiti i bearer per utilizzare i servizi e vengono eseguite le funzioni di mobility management per supportarne il movimento. La Mobility Management Entity (MME) nella rete si fa carico di eseguire i compiti sopra elencati stabilendo una connessione di signaling attraverso la quale scambiare messaggi di controllo con l'utente. La gestione della mobilità

e delle sessioni avviene secondo i protocolli NAS del layer Non Access Stratum collocato nel control plane di UE ed MME.

Le due entità colloquiano tra loro usando dei messaggi NAS. I protocolli NAS definiti nel documento 3GPP TS 24.301 possono essere classificati sommariamente in procedure di EPS Mobility Management (EMM) e procedure di EPS Session Management (ESM). Le prime sono relative alla mobilità, autenticazione dell'utente e alla sicurezza della comunicazione mentre le seconde supportano la creazione e la gestione di connessioni con le reti esterne che offrono il servizio richiesto.

2.1.1 Tipi di procedure EMM

La Tabella 3 riporta i tipi di procedure EMM supportate dai protocolli NAS e le specifiche procedure appartenenti ad ognuno di essi.

Tabella 3 Tipi di procedure EMM

Tipo	**Procedura EMM**
EMM Common Procedure	GUTI Allocation Authentication Security Mode Control UE Identification EMM Information
EMM Specific Procedure	Attach Detach Tracking Area Update
EMM Connection Management Procedure	Service Request Paging Transport of NAS Message (usato per SMS)

Esistono tre tipi di Procedure EMM distinte come segue:

i) **EMM common procedure**: Procedura che può essere sempre eseguita purché esista una connessione tra UE ed MME. Questa procedura può essere a sua volta suddivisa in cinque sotto-procedure: globally unique identifier (GUTI) allocation, authentication, identification, security mode control ed EMM information;

ii) **EMM specific procedure**: Procedura collegata alla mobilità dell'utente (registrazione ed aggiornamento della posizione dell'utente). Può essere suddivisa in tre sotto-procedure: attach, detach, TA update (TAU).

iii) **EMM connection management procedure**: Procedura volta alla creazione di una connessione di signaling NAS. Può essere suddivisa ulteriormente in tre sotto-procedure: service request, paging, transport of NAS messages.

2.1.2 Stati EMM/ECM/RRC

EMM è un sub-layer del NAS layer.

Mentre una EMM procedure è in esecuzione, un UE può trovarsi in uno dei sette[2] stati EMM previsti per l'UE mentre un MME può trovarsi in uno dei quattro[3] stati EMM previsti per l'MME. Tra tutti questi stati, quelli di maggior interesse, che sono comuni ad entrambi (UE ed MME), sono "EMM-Registered" ed "EMM-Deregistered".

Affinché un UE ed un MME possano scambiarsi messaggi NAS, deve esistere una connessione di signaling tra loro. Questa connessione è denominata EPS Connection Management (ECM) connection. È una connessione logica formata da una connessione RRC tra un UE ed un eNB ed una connessione di signaling S1 tra un eNB ed un MME come mostrato in Figura 29. Ciò significa che quando una connessione ECM viene creata/terminata le connessioni RRC ed S1 di signaling vengono create/terminate anch'esse.

Per un UE, avere una connessione ECM stabilita significa avere una connessione RRC stabilita con un eNB e per un MME significa avere una connessione S1 di signaling stabilita con un eNB.

La Figura 29 mostra gli stati EMM, ECM ed RRC associati con l'UE e l'MME. EMM può trovarsi in stato "EMM-Registered" o "EMM-Deregistered" a seconda che l'UE sia connesso o meno alla rete. ECM può avere stato "ECM-Connected" o "ECM-Idle" a seconda che una NAS signaling connection (i.e. ECM connection) sia presente oppure no.

Similmente, RRC può trovarsi sia in stato "RRC-Connected" che "RRC-Idle" a seconda che una connessione RRC sia stabilita o meno.

[2] EMM-Null, EMM-Deregistered, EMM-Deregistered-Initiated, EMM-Registered, EMM-Registered-Initiated, EMM-TAU-Initiated ed EMM Service-Request-Initiated.

[3] EMM-Deregistered, EMM-Deregistered-Initiated, EMM-Registered ed EMM-Common-Procedure-Initiated.

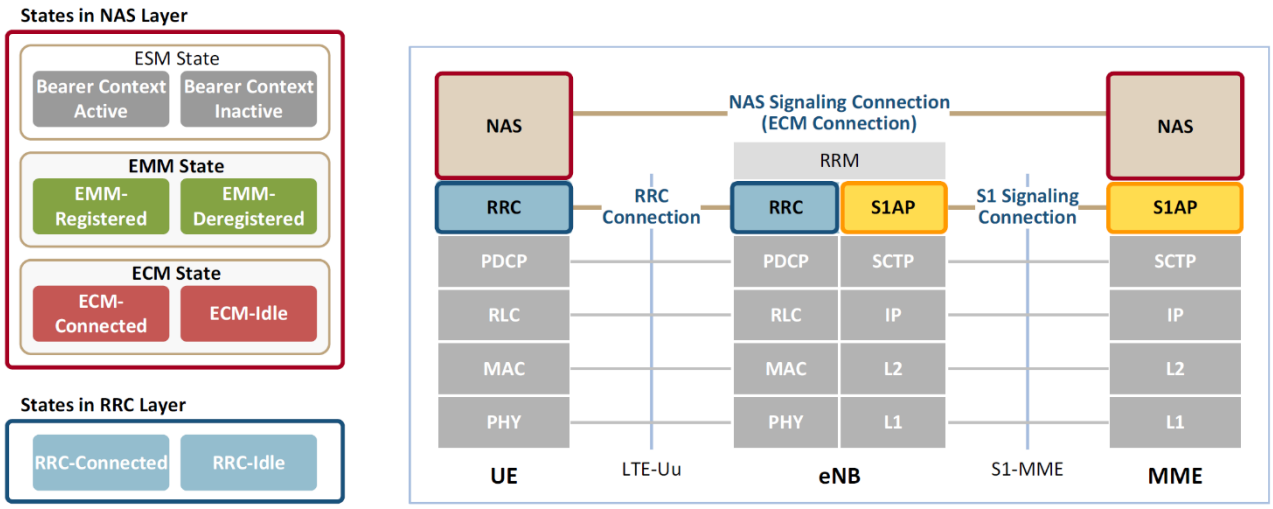


Figura 29 Stati EMM, ECM ed RRC

Tabella 4 Descrizione degli stati EMM, ECM ed RRC

Layer	Stato	Entità	Descrizione
EMM	EMM-Deregistered	UE, MME	L'UE non è collegato a nessuna rete LTE. L'MME non conosce la posizione corrente dell'UE ma può avere informazioni sulla Tracking Area riportate dall'UE all'atto dell'ultima connessione
	EMM-Registered	UE, MME	L'UE è collegato ad una rete LTE e gli è stato assegnato un indirizzo IP. Un EPS bearer è stato creato. L'MME è a conoscenza della posizione corrente dell'UE con accuratezza a livello di cella o almeno a livello di TA.
ECM	ECM-Idle	UE, MME	Non è stata ancora stabilita alcuna connessione di signaling NAS (ECM connection) All'UE non sono ancora state allocate risorse fisiche, i.e. risorse radio (SRB/DRB) e risorse di rete (S1 bearer/ S1 signaling connection).
	ECM-Connected	UE, MME	La connessione di signaling NAS (ECM connection) è stabilita. All'UE sono state assegnate le risorse fisiche, i.e. risorse radio (SRB/DRB) e le risorse di rete (S1 bearer/S1 signaling connection)
RRC	RRC-Idle	UE, eNB	Nessuna connessione RRC è ancora stata stabilita.
	RRC-Connected	UE, eNB	È stata stabilita una connessione RRC.

2.1.3 Transizioni di stato EMM

Gli stati di EMM, ECM ed RRC cambiano con l'avanzare delle procedure EMM. Questo processo è denominato "transizione di stato". Dato che la connessione RRC rappresenta una parte della connessione ECM, ECM ed RRC hanno sempre lo stesso stato dal punto di vista dell'UE.

La Figura 30 mostra le transizioni di stato tra EMM ed ECM/RRC in un UE e gli eventi scatenanti. Nella Figura 30, le combinazioni di stati EMM ed ECM/RRC sono mostrati come A, B, C e D.

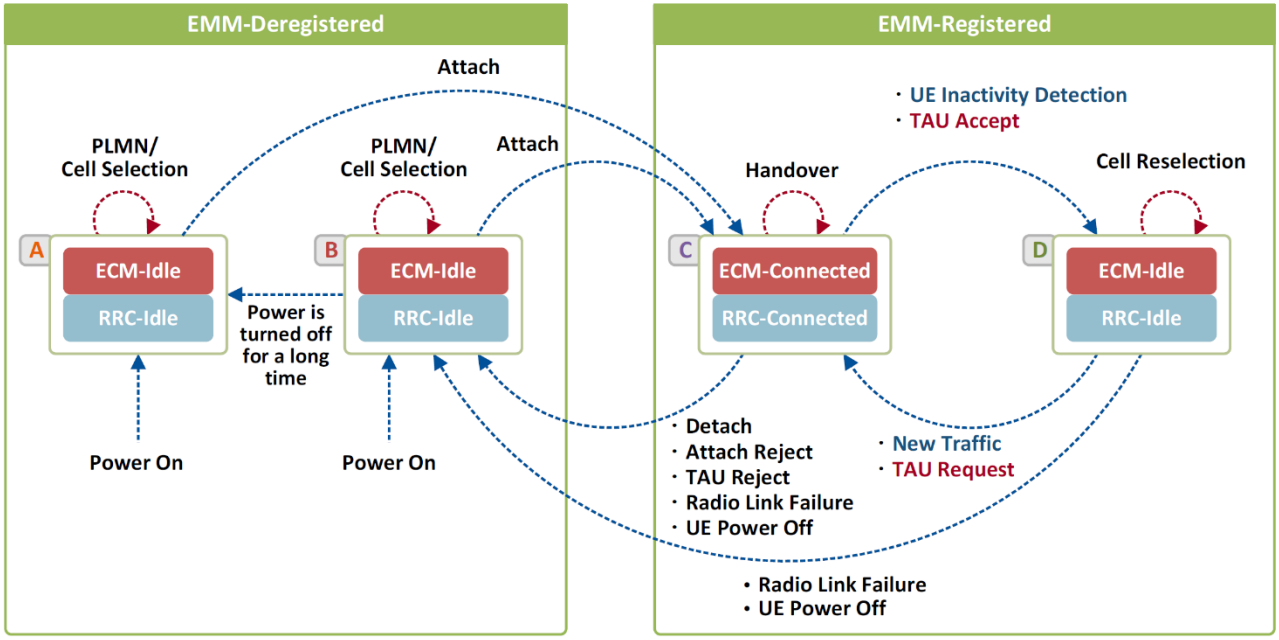


Figura 30 Transizioni di stato EMM

Tabella 5 User Experiences in stati EMM, ECM ed RRC

Caso	Stato	Esempi
A	EMM-Deregistered + ECM-Idle + RRC-Idle	Un UE si trova in questo stato quando viene acceso per la prima volta dopo la sottoscrizione di un contratto oppure quando viene acceso dopo essere stato spento per tanto tempo o ancora quando non esiste un UE context all'interno della rete
B	EMM-Deregistered + ECM-Idle + RRC-Idle	Un UE si trova in questo stato quando viene acceso entro un certo periodo di tempo dopo essere stato spento oppure quando viene persa la connessione ECM durante la comunicazione a causa di un problema del collegamento radio.

		Una parte di UE context derivante dall'ultimo collegamento alla rete può essere ancora memorizzata nella rete (e.g. per evitare di eseguire di nuovo la procedura di autenticazione ad ogni collegamento alla rete)
C	EMM-Registered + ECM-Connected + RRC-Connected	Un UE si trova in questo stato quando è connesso alla rete (ad un MME) e sta utilizzando servizi (e.g. Internet). La mobilità di un UE in questo stato è gestita attraverso una procedura di handover
D	EMM-Registered + ECM-Idle + RRC-Idle	Un UE si trova in questo stato quando è connesso alla rete (ad un MME), ma non sta usando alcun servizio. La mobilità di un UE in questo stato è gestita da una procedura di cell reselection.

2.1.3.1 Stato EMM-Deregistered

In entrambi i casi A e B gli stati sono EMM-Deregistered, ECM-Idle ed RRC-Idle e l'UE è scollegato dalla rete. La differenza risiede però nel fatto che le informazioni che la rete possiede circa l'UE nei due casi sono differenti. Nel caso A non possiede alcuna informazione se non quelle già inserite in fase di provisioning quando è avvenuta la sottoscrizione del contratto. Nel caso B invece mantiene il GUTI e il NAS Security Context ottenuti l'ultima volta che l'UE si è connesso alla rete (posto che siano ancora validi). Quindi la procedura di collegamento alla rete (Initial Attach) può variare, soprattutto per ciò che riguarda la fase di autenticazione dell'utente, a seconda che l'UE si colleghi alla rete trovandosi in stato A o B.

In stato B, la rete mantiene le informazioni necessarie per l'autenticazione dell'utente e il setup della sicurezza del collegamento radio, utili nel caso in cui l'UE si ricolleghi in un secondo momento. Trascorso un certo periodo di tempo, queste informazioni vengono eliminate e la rete transita in stato A (in relazione a quel determinato UE).

Quando l'UE si trova in stato EMM-Deregistered (stati A e B), determina a quale cella in una determinata rete può collegarsi eseguendo la procedura di Public Mobile Land Network (PLMN) / Cell Selection. Successivamente l'UE richiede il permesso di collegarsi alla rete per utilizzare i servizi, eseguendo una procedura di Initial Attach che lo porta a passare nello stato C (EMM-Registered, ECM-Connected ed RRC-Connected).

2.1.3.2 Stato EMM-Registered

In entrambi i casi C e D lo stato è EMM-Registered, e l'UE è connesso alla (o registrato alla) rete. La differenza risiede nello stato in cui si trovano ECM ed RRC, che può essere ECM-Connected/RRC-Connected (C) oppure ECM-Idle/RRC-Idle (D) a seconda dello stato di attività dell'UE. Quando l'UE si collega con successo alla rete transita dallo stato EMM-Deregistered (A o B) nello stato C e vi permane finché utilizza servizi, transitando in stato D quando non utilizza più alcun servizio.

Mentre un UE si trova in stato C, le risorse radio e di rete sono assegnate a connessioni di signaling nel control plane e ad EPS bearers nello user plane. Inoltre, può eseguire un handover ad una cella che risulta avere una migliore qualità di segnale rispetto alla serving cell corrente, qualora ve ne siano le condizioni.

Quando si trova in stato D invece, l'UE è inattivo e di conseguenza la connessione ECM/RRC è rilasciata. Le risorse non sono assegnate né alla connessione ECM nel control plane, né ai bearers EPS (DRB ed S1 bearer) dello user plane, ad eccezione del bearer S5.

In questo stato, non vi può essere traffico (UL/DL) tra l'UE e la rete. Per poter nuovamente consegnare traffico dati in stato D, la connessione ECM deve essere ristabilita, effettuando una transizione allo stato C, nel quale la rete procederà alla ricostruzione di un nuovo DRB ed S1 bearer per poter riattivare anche il bearer EPS. In stato D l'UE seleziona una cella alla quale agganciarsi in accordo ai criteri di cell reselection, eseguendo una misurazione della potenza e qualità del segnale della sua serving cell e delle celle vicine.

La transizione di stato da D a C avviene quando c'è nuovo traffico (UL/DL) oppure l'UE in Idle state effettua una TAU Request a seguito del cambio di TA o alla scadenza del TAU timer. In senso contrario, la transizione di stato da C a D avviene quando l'UE risulta inattivo per un certo periodo di tempo (cioè non c'è traffico UL/DL) oppure al termine della procedura di TA Update periodico scatenata dalla scadenza del TAU timer avvenuta quando l'UE si trovava nello stato D in precedenza.

Se mentre si trova in stato EMM-Registered (C o D), l'UE viene disconnesso dalla rete, transita in stato B (i.e. EMM-Deregistered). Ciò avviene per esempio qualora l'UE venga spento oppure il collegamento radio cada vale a dire quando il packet error rate sul collegamento radio eccede un determinato valore soglia. In aggiunta, la transizione di stato da EMM-Registered ad EMM-Deregistered (stato B) avviene quando un UE in stato C esegue un handover ad una rete non-LTE, oppure quando la sua richiesta di collegamento alla rete è rigettata (Attach Reject) o la sua TA Update Request è rigettata (TAU Reject).

2.1.4 Funzionalità EMM ed informazioni memorizzate nei vari stati EMM/ECM

In questo paragrafo vengono trattati i seguenti argomenti utili per la trattazione successiva:

i) Granularità con la quale la posizione dell'UE è nota per ogni entità EPS in ogni stato
ii) Stati EMM in cui i bearer EPS e la NAS signalling connection sono stabilite
iii) Procedure relative alla mobilità dell'UE in ogni stato
iv) Tipi di identificatori dell'UE memorizzati in ogni entità EPS per ogni stato

2.1.4.1 Informazioni sulla posizione dell'UE memorizzate nelle entità EPS nei vari stati EMM/ECM

La Tabella 6 sottostante mostra la granularità delle informazioni sulla posizione dell'UE riconosciute da ogni entità EPS. In stato EMM-Registered (C e D) l'UE è collegato ad una rete che ne conosce la posizione. In questo stato, la rete conosce la posizione dell'UE a livello di cella se l'UE si trova in stato attivo (C), altrimenti a livello di TA se si trova in stato Idle (D). Per un HSS la posizione dell'UE è nota a livello di MME tranne quando si trova in stato disconnesso (A).

Tabella 6 Informazioni sulla posizione dell'UE memorizzate in ogni entità EPS nei vari stati

Case	State	UE	eNB	S-GW	P-GW	MME	HSS	PCRF	SPR
A	EMM-Deregistered + ECM-Idle + RRC-Idle	-	-	-	-	-	-	-	-
B	EMM-Deregistered + ECM-Idle + RRC-Idle	-	-	-	-	TAI of last TAU	MME	-	-
C	EMM-Registered + ECM-Connected + RRC-Connected	-	Cell/eNB	Cell/eNB	Cell/eNB	Cell/eNB	MME	Cell/eNB	-
D	EMM-Registered + ECM-Idle + RRC-Idle	-	-	TAI of last TAU	TAI of last TAU	TAI of last TAU	MME	TAI of last TAU	-

2.1.4.2 Stato degli EPS Bearer e della NAS Signaling Connection nei vari stati EMM/ECM

La Tabella 5 mostra in quale stato EMM/ECM/RRC un EPS bearer per la consegna del traffico utente e una NAS signaling connection per la consegna dei messaggi di signaling sono attivi. Quando un UE si collega con successo alla rete e passa in stato EMM-Registered, utilizza i servizi forniti mediante gli EPS bearers. Un EPS bearer, come già detto in precedenza, consiste di tre bearer: Data Radio Bearer (DRB), S1 bearer ed S5 bearer concatenati tra loro. Come mostrato in Figura 31, tutti questi bearer vengono creati e rimangono attivi (e di conseguenza le risorse radio sono assegnate) in

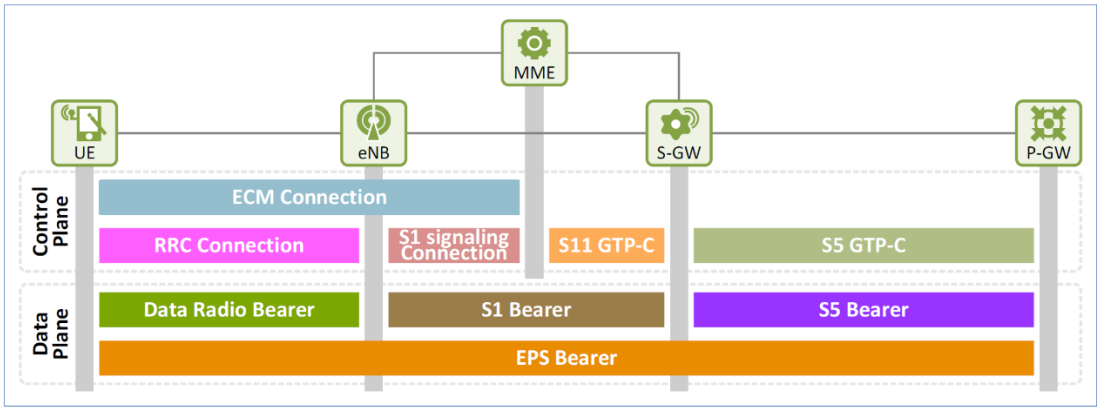
stato ECM-Connected/RRC-Connected (stato C) ed il traffico viene consegnato. D'altra parte, solo il bearer S5 è attivo in stato ECM-Idle/RRC-Idle (stato D) quando non vi è traffico dati utente.

La connessione di signaling NAS (i.e. connessione ECM), che consta di una connessione RRC e di una connessione di signaling S1, è attivata solo quando il traffico utente viene consegnato, i.e. in stato ECM-Connected/RRC-Connected (stato C).

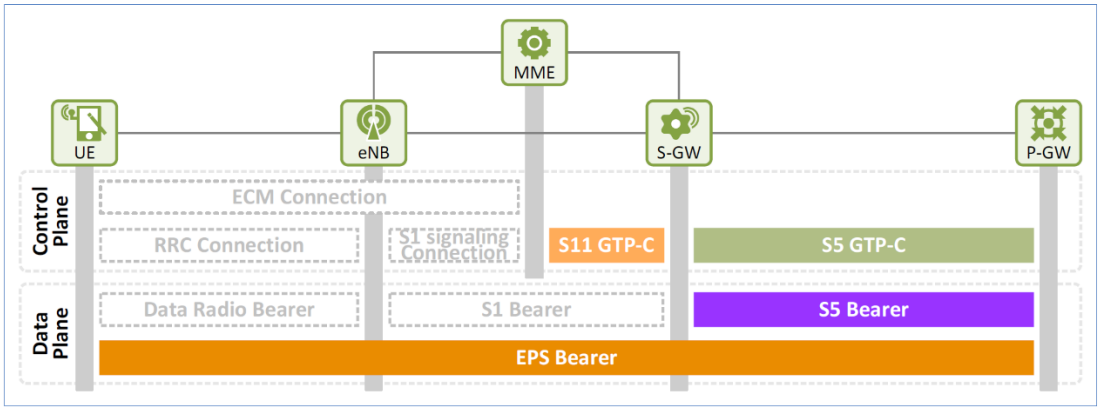
Quando l'utente è disconnesso dalla rete (stato A o B) oppure quando è connesso ma in stato Idle (stato D) la connessione ECM viene rilasciata.

Tabella 7 Informazioni sugli EPS bearer e la connesione di signaling NAS

Case	State	EPS Bearer			NAS Signaling Connection (= ECM Connection)		S11 Signaling Connection (MME – S-GW)	S5 Signaling Connection (S-GW – P-GW
		Radio Bearer (UE – eNB)	S1 Bearer (eNB – S-GW)	S5 Bearer (S-GW – P-GW)	RRC Conn. (UE – eNB)	S1 Conn. (eNB – MME)		
A	EMM-Deregistered + ECM-Idle + RRC-Idle	-	-	-	-	-	-	
B	EMM-Deregistered + ECM-Idle + RRC-Idle	-	-	-	-	-	-	
C	EMM-Registered + ECM-Connected + RRC-Connected	Established	Established	Established	Established	Established	Established	Established
D	EMM-Registered + ECM-Idle + RRC-Idle	-	-	Established	-	-	Established	Established



State C (EMM-Registered + ECM-Connected + RRC-Connected)



State D (EMM-Registered + ECM-Idle + RRC-Idle)

Figura 31 EPS Bearer e connessioni di signaling in stato EMM-Registered

2.1.4.3 Procedure di mobilità dell'UE eseguite nei vari stati EMM/ECM

La tabella 6 mostra le procedure di mobilità relativamente ai vari stati.

Di seguito viene precisato meglio il significato di alcuni termini, utili anche per la trattazione successiva.

Mobilità: Un UE in stato EMM-Registered (stato C o D), al di là del fatto che stia o meno utilizzando servizi, deve aggiornare la sua TA quando cambia. Se però si trova in stato ECM-Idle/RRC-Idle (stato D), l'UE deve aggiornare la sua TA periodicamente alla scadenza del TAU timer anche se la sua TA non è cambiata dall'ultimo aggiornamento. Il TA update è scatenato da un TAU Request message inviato dall'UE.

Mentre l'UE si trova in stato ECM-Idle/RRC-Idle (stato D), deve essere stabilita la connessione ECM/RRC e lo stato deve diventare ECM-Connected/RRC-Connected per poter far sì che l'UE aggiorni la sua TA.

Una volta che l'UE in stato C invia il suo TAU Request message e riceve il TAU Accept message dall'MME, la procedura di TAU è completata. Dopodiché la connessione ECM/RRC viene rilasciata e l'UE ritorna in stato ECM-Idle/RRC-Idle (stato D)

Paging: Quando un UE è connesso alla rete ma si trova in stato inattivo (stato D), se c'è traffico utente da consegnare, la rete avvia una procedura di Paging che porta l'UE a transitare in stato C. Il paging è effettuato sulla base delle informazioni Tracking Area Identifier (TAI) fornite dall'UE durante il suo ultimo TA Update.

Tabella 8 Procedure relative alla mobilità dell'utente

Case	State	Mobility	Tracking Area Update	Paging
A	EMM-Deregistered + ECM-Idle + RRC-Idle	PLMN/Cell Selection	-	-
B	EMM-Deregistered + ECM-Idle + RRC-Idle	PLMN/Cell Selection	-	-
C	EMM-Registered + ECM-Connected + RRC-Connected	Handover - Intra eNB Handover - X2 Handover - S1 Handover	TAU when TA change	-
D	EMM-Registered + ECM-Idle + RRC-Idle	Cell-Reselection	• TAU when TA change • Periodic TAU	Paging Control

2.1.4.4 ID dell'UE memorizzati nelle entità EPS nei vari stati EMM/ECM

La Tabella 9 contiene una lista di ID dell'UE che ogni entità EPS può avere in ognuno dei quattro stati. Un indirizzo IP viene assegnato dal PGW all'UE quando quest'ultimo si collega inizialmente alla rete, provocando la creazione di un default bearer ed è rilasciato quando il default bearer viene distrutto. Il GUTI è un ID temporaneo assegnato da un MME ad un UE qualora quest'ultimo completi con successo la procedura di Initial Attach ed è utilizzato in luogo dell'International Mobile Subscriber Identity (IMSI) che è un ID permanente e per questo meno sicuro per l'utilizzo lungo un collegamento radio. Se l'UE viene scollegato con successo dalla rete, l'UE e l'MME mantengono l'ultimo GUTI assegnato dall'UE e lo utilizzano come identificativo dell'UE per un successivo collegamento. Il C-RNTI è un ID che viene assegnato da un eNB per distinguere gli UE in una cella in stato RRC-Connected (stato C) ed è valido solo nella cella associata al C-RNTI assegnato.

eNB UE S1AP ID ed MME UE S1AP ID vengono utilizzati da un eNB e da un MME per distinguere gli UE lungo l'interfaccia S1-MME.

Old eNB UE X2APID e New eNB X2AP ID sono utilizzati da un serving eNB e da un target eNB per distinguere gli UE lungo l'interfaccia X2 quando un UE esegue un X2 handover da un source eNB ad un target eNB.

Tabella 9 ID dell'UE memorizzati in ogni entità EPS nei vari stati

Case	State	UE	eNB	S-GW	P-GW	MME	HSS	PCRF	SPR
A	EMM-Deregistered + ECM-Idle + RRC-Idle	IMSI	-	-	-	-	IMSI	-	IMSI
B	EMM-Deregistered + ECM-Idle + RRC-Idle	IMSI, GUTI	-	-	-	IMSI, GUTI	IMSI	-	IMSI
C	EMM-Registered + ECM-Connected + RRC-Connected	IMSI, GUTI, UE IP addr, C-RNTI	C-RNTI, eNB/MME UE S1AP ID, Old/New eNB UE X2AP ID	IMSI	IMSI, UE IP addr	IMSI, GUTI, UE IP addr, eNB/MME UE S1AP ID	IMSI	IMSI, UE IP addr	IMSI
D	EMM-Registered + ECM-Idle + RRC-Idle	IMSI, GUTI, UE IP addr	-	IMSI	IMSI, UE IP addr	IMSI, GUTI, UE IP addr	IMSI	IMSI, UE IP addr	IMSI

Capitolo III
Procedure di Mobilità nelle reti 4G LTE

3.1 Procedura di collegamento iniziale alla rete (Initial Attach Procedure)

3.1.1 Casi di Initial Attach

Quando un UE si collega ad una rete, un MME inizia una differente procedura di collegamento alla rete a seconda del tipo di richiesta ricevuta. La procedura inizia quando un utente invia un Attach Request ad un MME e termina quando l'MME ritorna un Attach Accept message all'UE. L'UE invia l'Attach Request message includendo il suo UE ID (IMSI o GUTI assegnato in precedenza prima della disconnessione dalla rete) per poter essere identificato. In risposta, l'MME nell'Attach Accept message, include il GUTI, che l'UE può utilizzare successivamente al posto dell'IMSI, e una TAI list che contiene le TA nelle quali l'UE può muoversi senza effettuare TA Updates.
Un MME può eseguire alcune o tutte le seguenti operazioni dopo aver ricevuto l'Attach Request prima di inviare l'Attach Accept message all'UE:

- **Acquisizione dell'ID dell'UE**
  La rete (MME) acquisisce un UE ID per l'identificazione e autenticazione dell'utente. Qui l'UE ID può essere un IMSI o il vecchio GUTI assegnato all'UE in precedenza prima della disconnessione. Un IMSI può essere acquisito per mezzo di messaggi di tipo Attach Request o Identity Response mentre un vecchio GUTI (Old GUTI) può essere ottenuto dall'UE attraverso un Attach Request message.
- **Autenticazione**
  Se la rete ha acquisito un IMSI o un vecchio GUTI come ID dell'UE attraverso un Attach Request Message ma il controllo di integrità sul messaggio fallisce, la rete controlla se l'utente ha il permesso di collegarsi alla rete eseguendo la procedura di autenticazione (EPS-AKA)
- **NAS Security Setup**
  Una volta che la procedura di autenticazione è stata completata, viene eseguita la procedura di NAS Security Setup per la derivazione delle chiavi atte alla crittazione e protezione di integrità dei messaggi NAS scambiati tra UE ed MME
- **Aggiornamento della posizione dell'UE (Location Update)**
  L'MME scarica le informazioni relative al profilo sottoscritto dall'utente dall'HSS e l'HSS

aggiorna le informazioni relative alla posizione dell'utente (in termini di MME al quale è agganciato).

- **Creazione della sessione EPS (EPS Session Establishment)**

  Una EPS Session ed un default EPS bearer vengono creati

Mentre le procedure di acquisizione dell'ID dell'UE e di EPS Session Establishment vengono eseguite in ogni caso, le restanti procedure (Autenticazione, NAS Security Setup e Location Update) vengono eseguite a seconda del tipo di Initial Attach.

In particolare, la scelta di effettuare o meno le procedure di Autenticazione, NAS Security Setup e Location Update dipende da alcuni interrogativi principali:

i) L'UE possiede ancora le informazioni[4,5] utilizzate per l'ultimo collegamento alla rete? (Last Attach Information: Old GUTI e NAS Security Context)

ii) A quale MME l'UE sta tentando di connettersi (quello al quale si era connesso precedentemente o uno a cui non si era mai collegato?)

iii) Esiste ancora un Last UE Context[6] valido all'interno della rete?

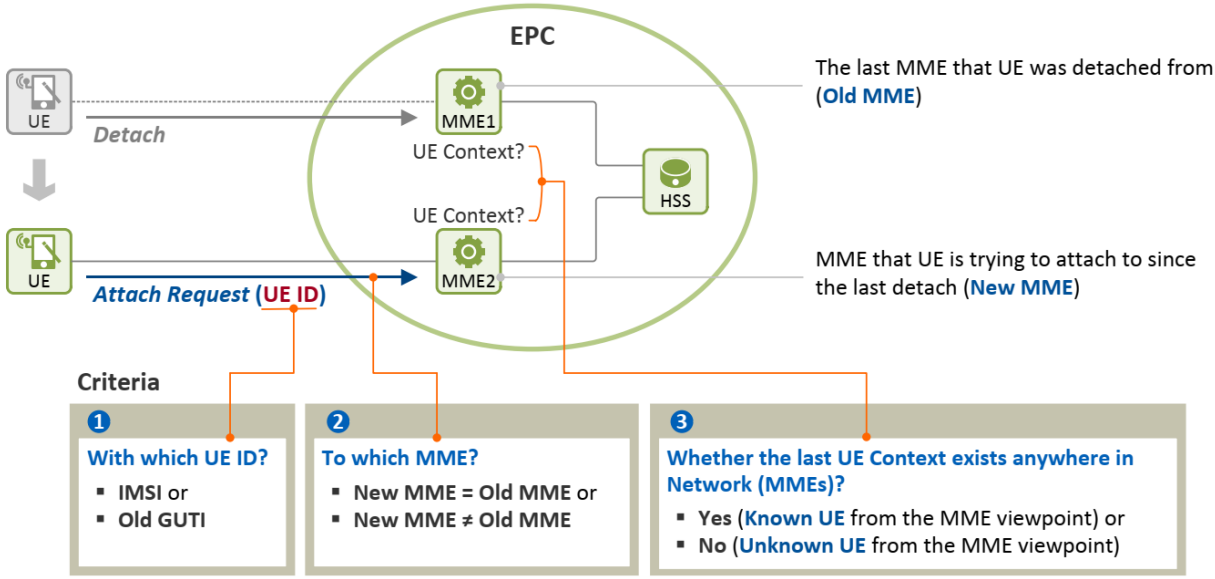


Figura 32 Criteri per la classsificazione dei tipi di Initial Attach

Di seguito verranno esaminati i vari casi possibili di Initial Attach suddividendoli per comodità, in due macro-raggrupamenti: il primo riguarda i casi in cui la rete (MME) non ha un Last UE Context

[4] Le informazioni di collegamento memorizzate da un UE (Last Attach Information) includono il vecchio GUTI dell'UE e il NAS Security Context

[5] Il termine Old GUTI (vecchio GUTI) si riferisce al GUTI assegnato all'UE prima che venisse disconnesso dalla rete. Se un UE viene disconnesso in maniera regolare dalla rete mantiene il suo GUTI e il suo NAS Security Context validi.

[6] Un Last UE Context memorizzato da un MME include l'ID dell'UE (IMSI e Old GUTI) e il MM Context (NAS Security Context e UE-AMBR)

valido per l'UE che richiede il collegamento alla rete ("UE sconosciuto"), il secondo quelli in cui da qualche parte nella rete esiste un Last UE Context valido ("UE noto"). Si noti che per i casi in cui come identificatore viene utilizzato un GUTI, il messaggio Attach Request si considera inviato integrity-protected.

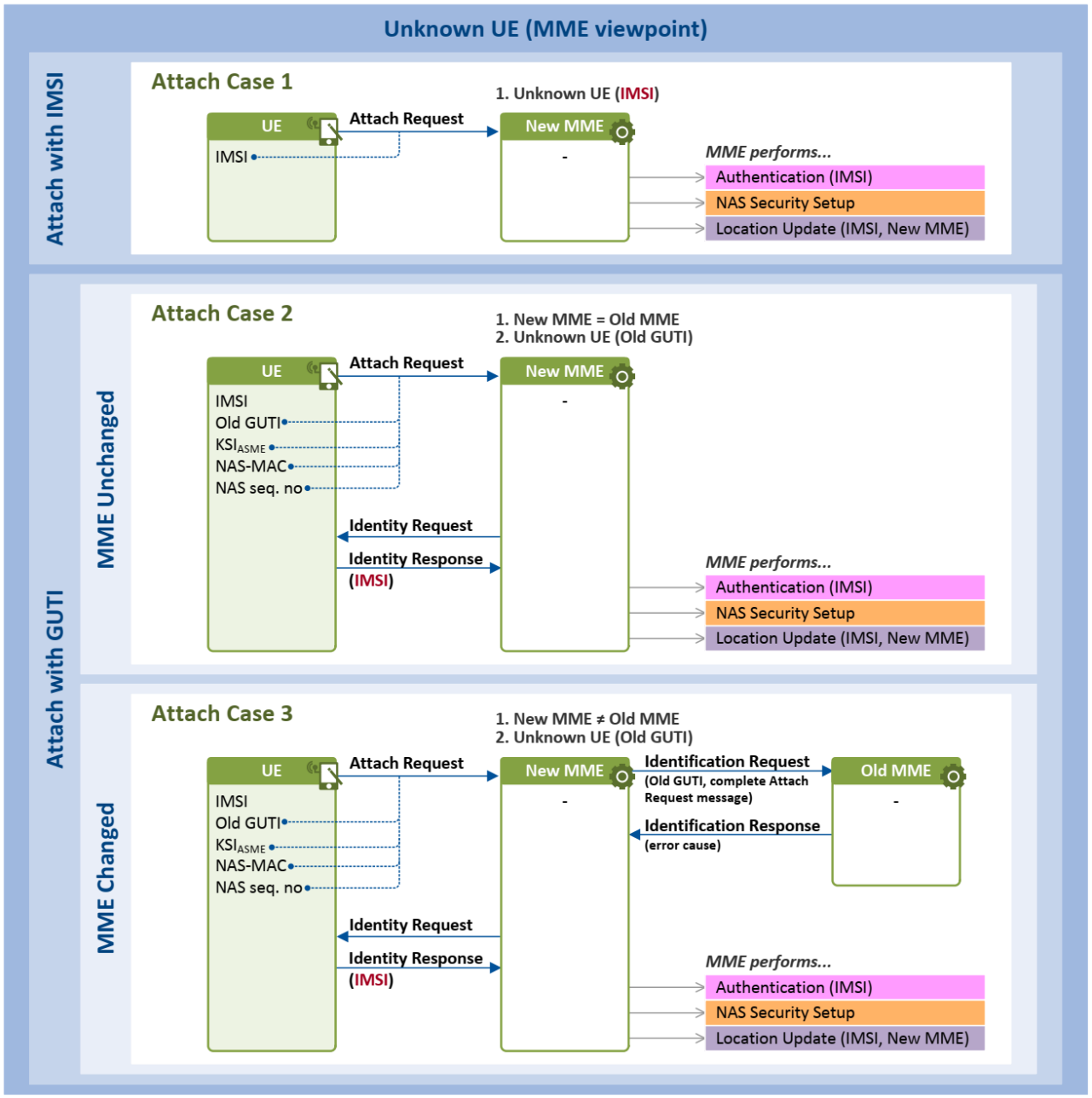


Figura 33 Casi di Initial Attach per "UE sconosciuto"

Caso 1: Un UE si connette utilizzando l'IMSI come ID

Questo caso si verifica quando né l'UE né la rete (MME) ha un Last UE Context. Lo scenario che si verifica in questo caso è il seguente:

1) Un UE invia ad un MME un Attach Request utilizzando il suo IMSI come ID. L'MME ottiene l'IMSI dal messaggio
2) L'MME, notando che l'UE ha richiesto il collegamento inviando l'IMSI, assume di non avere informazioni precedenti riguardanti quell'UE. Effettua quindi le procedure di autenticazione e NAS Security Setup
3) L'MME invia un Location Update message all'HSS, per informarlo che l'UE è registrato presso di lui e scarica le informazioni di sottoscrizione dell'utente dall'HSS

Caso 2: Un UE si collega all'MME al quale era già collegato in precedenza prima della disconnessione (New MME = Old MME), ma l'MME non ha un Last UE Context valido per l'UE

Questo caso si verifica quando un UE che ha mantenuto le Last Attach Information (Old GUTI e NAS Security Context) dopo la disconnessione dalla rete, si collega all'MME al quale era collegato in precedenza ma quest'ultimo non possiede un Last UE Context valido.

Uno scenario d'esempio che si può verificare in questo caso è il seguente:

1) Un UE invia al New MME un Attach Request message utilizzando il suo vecchio GUTI. L'Attach Request in questo caso viene inviata integrity-protected utilizzando la NAS integrity key (K_{NASint}) (i.e. includendo nel messaggio il NAS-MAC)
2) Poiché un GUTI include un GUMMEI che funge da MME ID, il nuovo MME riconosce che il vecchio GUTI era stato allocato da lui (Old MME = New MME). L'MME cerca di trovare l'UE Context relativo all'UE che si sta collegando ma non riesce a trovarlo (perché fallisce il controllo di integrità sul messaggio o il vecchio GUTI non è più presente nell'MME).
3) L'MME invia all'UE un Identity Request message, richiedendo l'IMSI come ID.
4) L'UE risponde con un Identity Response message che include il suo IMSI
5) L'MME esegue le procedure di autenticazione e NAS Security Setup dopodiché procede ad eseguire la richiesta di Location Update all'HSS

Caso 3: Un UE si sta collegando ad un nuovo MME al quale non si era mai collegato in precedenza (New MME ≠ Old MME), e l'MME non ha un Last UE Context valido per l'UE

Questo caso si verifica quando un UE, che mantiene ancora le Last Attach Information anche dopo la disconnessione, si collega ad un nuovo MME diverso dal precedente ma il vecchio MME non ha più l'UE Context relativo a quell'UE. Uno scenario d'esempio è il seguente:

1) Un UE invia al nuovo MME un Attach Request message (integrity-protected) utilizzando il suo Old GUTI come UE ID.
2) Quando il nuovo MME riceve il messaggio, riconosce che il vecchio GUTI non era stato allocato da lui in precedenza ma da un altro MME.
3) Il nuovo MME invia al vecchio MME un Identification Request (Old GUTI, Complete Attach Request message), inoltrandogli il vecchio GUTI e il messsaggio di Attach Request completo. In questo modo, il nuovo MME richiede al vecchio MME il Last UE Context relativo all'UE.
4) Quando riceve il messaggio, il vecchio MME cerca l'UE context relativo al GUTI inviatogli, ma senza successo.
5) Il vecchio MME invia al nuovo MME un messaggio Identification Response (error cause), informandolo che non è riuscito a trovare l'UE context richiestogli.
   A questo punto le cose procedono come nel Caso 2 agli step 3) ,4), 5) per cui il nuovo MME invia all'UE un messaggio Identity Request (IMSI), richiedendogli l'IMSI e l'UE gli risponde inviandogli l'IMSI attraverso un Identity Reponse message. Con l'IMSI ricevuto, l'MME può eseguire le procedure di Autenticazione, NAS Security Setup e Location Update.

I casi che seguono considerano invece che l'MME e l'UE abbiano entrambi un Last UE Context valido relativo all'UE. Di conseguenza si considera sempre che, come identificatore dell'UE, venga utilizzato un GUTI e che l'Attach request message sia inviato integrity-ptotected.

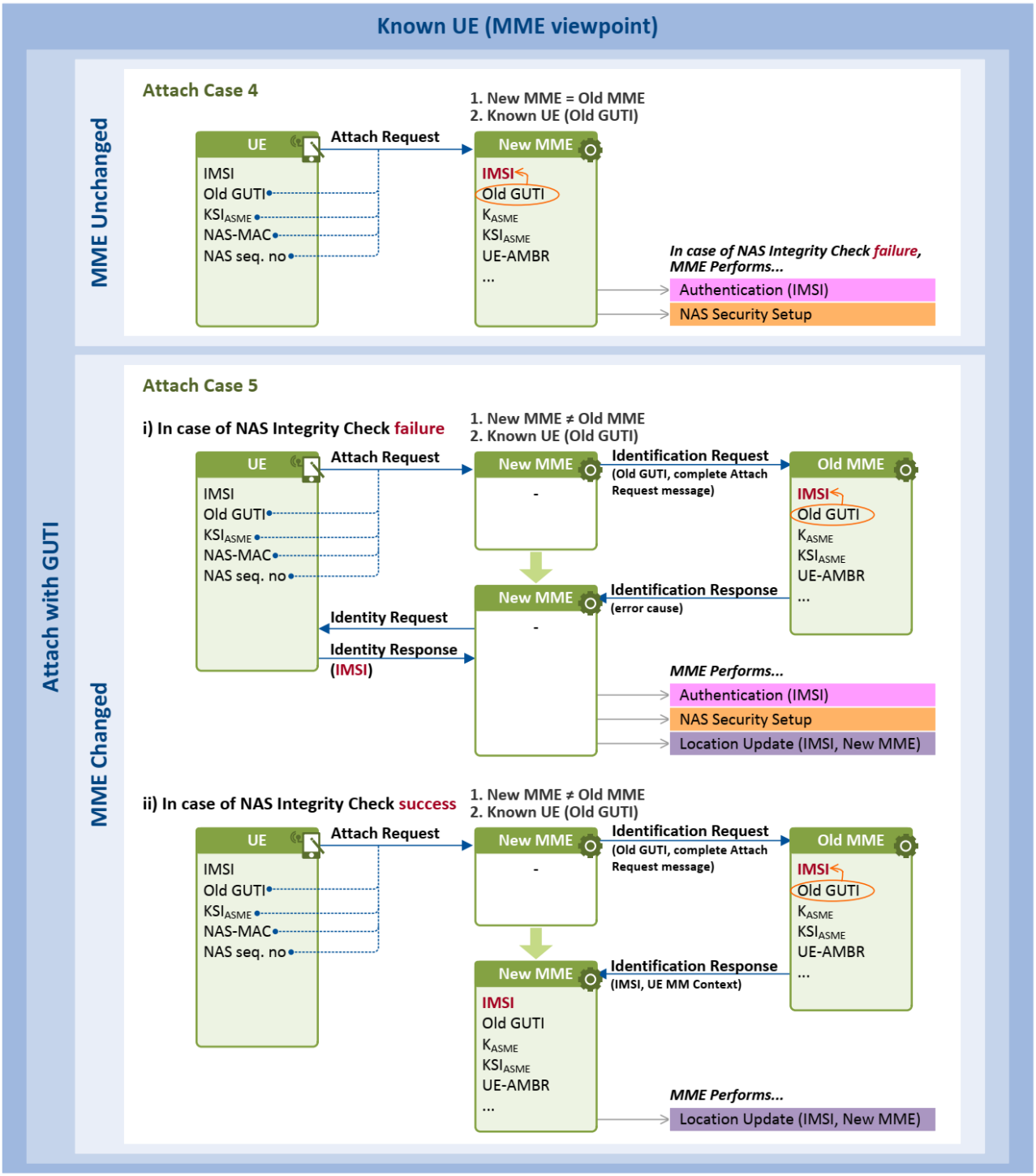


Figura 34 Casi di Initial Attach per "UE noto"

Caso 4: Un UE si sta collegando all'MME al quale era collegato anche prima della disconnessione (New MME = Old MME) e l'MME ha un valido Last UE Context per l'UE

In questo caso l'UE che possiede ancora le Last Attach Information (Old GUTI, NAS Security Context) si collega all'MME al quale era collegato anche prima della disconnessione e quest'ultimo possiede ancora un valido Last UE Context per l'UE. Uno scenario di esempio è il seguente:

1) Un UE invia al nuovo MME un Atach Request message (integrity-protected) utilizzando il suo Old GUTI come UE ID.
2) Il nuovo MME riconosce che il vecchio GUTI era stato allocato da sé stesso. Procede quindi cercando il vecchio GUTI in memoria e trova l'UE context (IMSI, MM Context (NAS Security Context, UE-AMBR)) valido relativo all'UE che si sta collegando.
3) L'MME effettua i controlli di integrità sul messaggio Attach Request ricevuto.
    i) Se il controllo di integrità sul NAS-MAC fallisce, l'MME deve autenticare l'utente usando l'IMSI ed eseguire le procedure di NAS Security Setup
    ii) Se il controllo di integrità dà esito positivo, l'MME può saltare le procedure di autenticazione e NAS Security Setup

Caso 5: Un UE si collega ad un nuovo MME al quale non si era mai collegato in precedenza (New MME ≠ Old MME) e il vecchio MME possiede il Last UE Context valido relativo all'UE

Questo caso si verifica quando un UE, possedendo ancora le Last Attach Information, si collega ad un nuovo MME (New MME) ed il vecchio MME ha ancora in memoria l'UE context valido relativo all'UE. Uno scenario d'esempio può essere il seguente:

1) Un UE invia al nuovo MME un Attach Request message (integrity-protected) utilizzando il suo Old GUTI come UE ID.
2) Il nuovo MME riconosce che il vecchio GUTI era stato assegnato da un altro MME (vecchio MME)
3) Il nuovo MME invia al vecchio MME un Identification Request (Old GUTI, complete Attach Request message), inoltrando il vecchio GUTI e l'Attach Request message ricevuto dall'UE. Così facendo, il nuovo MME richiede al vecchio il Last UE Context relativo all'UE
4) Quando riceve il messaggio, il vecchio MME cerca l'UE context e trova l'IMSI e il MM Context (NAS Security Context, UE-AMBR) relativi all'UE
5) Il vecchio MME effettua i controlli di integrità sull'Attach Request message
6) Poi trasmette i risultati del controllo al nuovo MME attraverso un Identification Response message
    i) Se il controllo di integrità fallisce, il vecchio MME invia al nuovo MME il messaggio indicando la causa dell'errore
    ii) Se il controllo termina con esito positivo, include nel messaggio l'UE context (IMSI, Old GUTI, MM Context) richiesto.

Nel caso in cui il controllo di integrità fallisca, le cose procedono come nel caso 3, per cui devono essere effettuate le procedure di acquisizione dell'IMSI autenticazione e NAS security Setup. Se il controllo termina con esito positivo, il nuovo MME riceve l'IMSI e il MM Context dal vecchio MME

e può saltare le procedure di autenticazione e NAS Security Setup come nel Caso 4. L'unica differenza rispetto al Caso 4 risiede nel fatto che l'UE si è collegato ad un nuovo MME differente dal vecchio per cui il nuovo MME dovrà aggiornare la posizione dell'UE nell'HSS. L'HSS provvederà poi a richiedere al vecchio MME la cancellazione dell'UE context relativo a quel determinato UE.

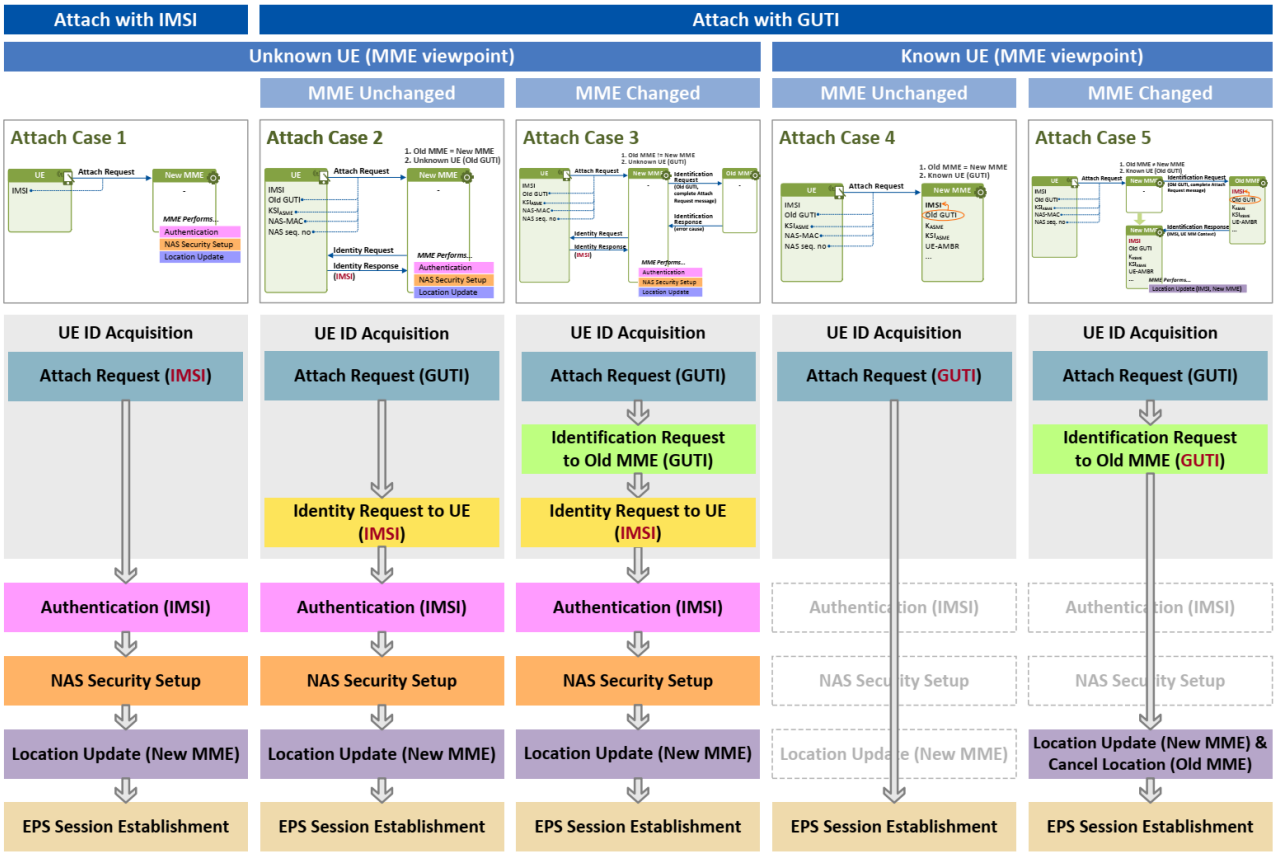


Figura 35 Call flow semplificato nei vari casi di Initial Attach

3.1.2 Dettaglio della procedura di Initial Attach

La Figura 36 illustra le procedure eseguite in fase di collegamento iniziale alla rete

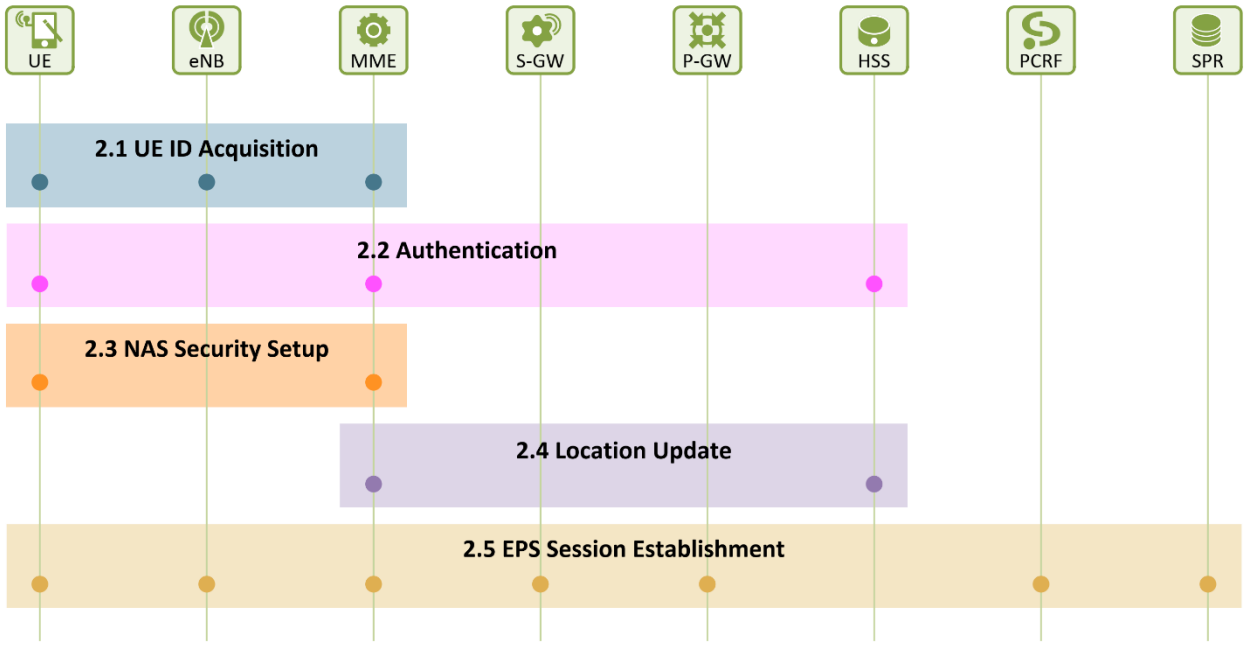


Figura 36 Procedure eseguite in fase di collegamento iniziale alla rete

▪Acquisizione dell'IMSI

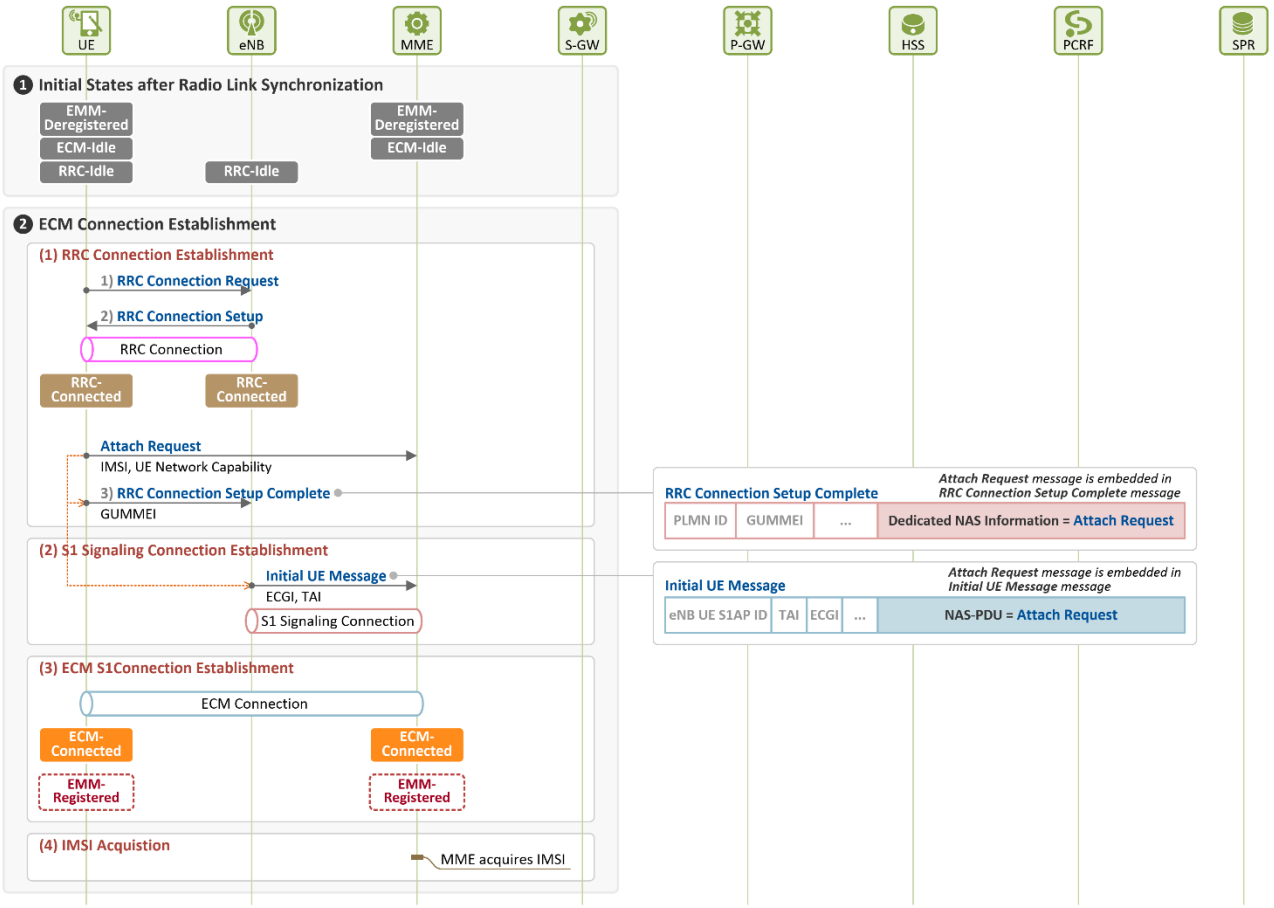


Figura 37 Procedura di acquisizione dell'IMSI

1 Initial State after Radio Link Synchronization

Affinché l'UE possa inviare la richiesta di collegamento iniziale alla rete deve prima connettersi all'eNB eseguendo le procedure di PLMN Selection e Cell Search per sincronizzare il collegamento radio, dopodiché può comunicare con l'eNB. In questo momento l'UE si trova in stato EMM-Deregistered, ECM/RRC-Idle.

2 ECM Connection Establishment

L'UE tenta il collegamento alla rete inviando un Attach Request message, includendo il suo IMSI. L'Attach Request (IMSI, UE Network Capability) message è un messaggio di livello NAS indirizzato dall'UE al NAS layer dell'MME. Per poter consegnare il messaggio è necessaria l'esistenza di una connessione di signalling ECM tra l'UE e l'MME, che comporta la creazione di una connessione di signalling RRC tra l'UE e l'eNB e la creazione di una S1 signalling connection tra l'eNB e l'MME. Infatti, i messaggi NAS sono trasportati come messaggi RRC (RRC Connection Setup Complete message) quando passano attraverso la connessione RRC e come messaggi S1AP (Initial UE Message) attraverso la connessione di signalling S1.

1) **Creazione della connessione RRC**

   1) **[UE→eNB] RRC Connection Request**

      Un UE richiede la creazione di una connessioen RRC inviando una RRC Connection Request(Establishment Cause =”Mobile Originating Signalling”). Questo valore di Establishment Cause viene utilizzato nel caso in cui un UE esegua una procedura di Attach, Detach o TAU). Il messaggio viene inviato dall’UE all’eNB usando il Signalling Radio Bearer 0, utilizzato da tutti gli UE agganciati ad una cella e il canale logico CCCH (Common Control Channel).

   2) **[UE ← eNB] RRC Connection Setup**

      All’atto della ricezione della richiesta l’eNB alloca un SRB (SRB1) dedicato all’UE inviandogli un RRC Connection Setup message attraverso SRB0 e CCH. Poiché l’utilizzo delle risorse in UL/DL da parte dell’UE è controllato dall’eNB, una volta che questo step è stato completato l’UE può utilizzare le risorse radio secondo la configurazione allocatagli con l’RRC Connection Setup message. Dopodiché transita in stato EMM Deregistered, ECM Idle ed RRC-Connected.

   3) **[UE → eNB] RRC Connection Setup Complete**

      L’UE notifica all’eNB che il setup della connessione RRC è stato completato inviandogli un RRC Connection Setup Complete attraverso SRB1 e DCCH (Dedicated Control Channel). Per una maggiore efficienza, l’Attach Request message destinato al NAS layer dell’MME viene inviato come payload del messaggio RRC RRC Connection Setup Complete, includendolo nel campo Dedicated NAS Information dell’RRC Connection Setup Complete.

2) **Creazione della connessione di signalling S1**

   Poiché i messaggi di controllo tra l’eNB e l’MME vengono inviati come messaggi S1AP lungo l’interfaccia S1.MME è necessario che venga stabilita una connessione S1 che è definita dalla coppia di ID (eNB UE S1AP ID, MME UE S1AP ID) allocati dall’eNB e dall’MME per identificare gli UE.

   L’Attach Request, essendo il primo messaggio NAS, giunge all’eNB prima che sia stabilita la connessione di signalling S1. L’eNB quindi alloca un eNB UE S1AP ID per la creazione della S1 signalling connection ed invia all’MME l’Attach Request message includendolo nel campo NAS-PDU dell’Initial UE Message. Un Initial UE Message contiene le seguenti informazioni:

Initial UE Message (eNB UE S1AP ID, NAS-PDU, TAI, ECGI, RRC Establishment Cause)

- **eNB UE S1AP ID**: ID che identifica l'UE dal punto di vista dell'eNB lungo l'interfaccia S1-MME
- **NAS-PDU**: un messaggio NAS (in questo caso Attach Request)
- **TAI**: indica la TA nella quale l'UE è collocato
- **ECGI**: indica la cella alla quale l'UE è agganciato
- **RRC Establishment Cause**: "mo-Signalling", indica che il signalling è stato generato dall'UE

Quando l'MME riceve l'Initial UE Message dall'eNB alloca un MME UE S1AP ID per identificare l'UE lungo l'interfaccia S1-MME

A questo punto la connessione ECM tra gli strati NAS di UE ed MME è stata stabilita. Di conseguenza, l'UE transita in stato EMM-Registered, ECM-Connected, RRC-Connected.

Il NAS layer dell'MME, a questo punto, ottiene dall'Attach Request message l'IMSI dell'UE e gli algoritmi di sicurezza (UE Security Capability) che l'UE supporta. Avendo queste informazioni può effettuare le procedure di autenticazione e NAS Security Setup per lo scambio in maniera sicura dei messaggi NAS.

▪ **Autenticazione, NAS e AS Security Setup**

La procedura di autenticazione scelta per le reti LTE, detta EPS-AKA (Authentication and Key Agreement), è una procedura di mutua autenticazione in quanto la rete e l'UE si autenticano a vicenda. Dalla suddetta procedura viene derivata una top-level key (K_{ASME}) dalla quale vengono poi derivate le chiavi per la sicurezza di NAS e AS.

Lo scopo della sicurezza NAS è quello di consegnare in maniera sciura i messaggi di signalling NAS tra l'UE e l'MME lungo i canali radio attraverso i check di integrità (cioè verifica/protezione di integrità) e la cifratura dei messaggi eseguiti utilizzando le NAS Security Keys (rispettivamente K_{NASenc} per la crittazione/decrittazione dei messaggi e K_{NASint} per la protezione / verifica di integrità dei messaggi). Essendo queste chiavi derivate dalla top level key K_{ASME}, la procedura di NAS Security Setup dovrà essere ri-effettuata a fronte di ogni nuova autenticazione, poiché ad ogni nuova autenticazione la chiave K_{ASME} viene rigenerata.

Lo scopo della sicurezza dell'AS è di consegnare in maniera sicura i messaggi RRC tra un UE ed un eNB nel control plane e i pacchetti IP utente di user plane utilizzando le AS Security Keys.

Le AS Security Keys (K_{RRCint}, K_{RRCenc} e K_{UPenc}) vengono derivate dalla chiave K_{eNB} da un UE ed un eNB e vengono rigenerate ogni volta che un nuovo collegamento radio viene creato (cioè quando lo stato RRC passa da Idle a Connected). Le chiavi K_{RRCint} e K_{RRCenc} sono utilizzate per la crittazione e protezione di integrità dei messaggi RRC inviati attraverso un SRB (Signalling Radio Bearer) lungo il canale radio mentre la chiave K_{UPenc} è utilizzata per la consegna sicura dei pacchetti IP di user plane attraverso un DRB (Data Radio Bearer). La chiave K_{eNB} viene a sua volta generata da K_{ASME}. Poiché K_{ASME} non viene inviata all'eNB, l'MME deriva K_{eNB} e la inoltra all'eNB.

- **Location Update**

Una volta terminate le procedure di autenticazione e NAS Security Setup, l'MME deve registrare l'UE alla rete e scoprire quali servizi può utilizzare. Per fare ciò, l'MME notifica all'HSS che l'UE è collegato a quell'MME e procede a scaricare le informazioni realtive al profilo dell'utente dall'HSS. Questa procedura avviene utilizzando il protocollo Diameter lungo l'interfaccia S6a tra MME e HSS.

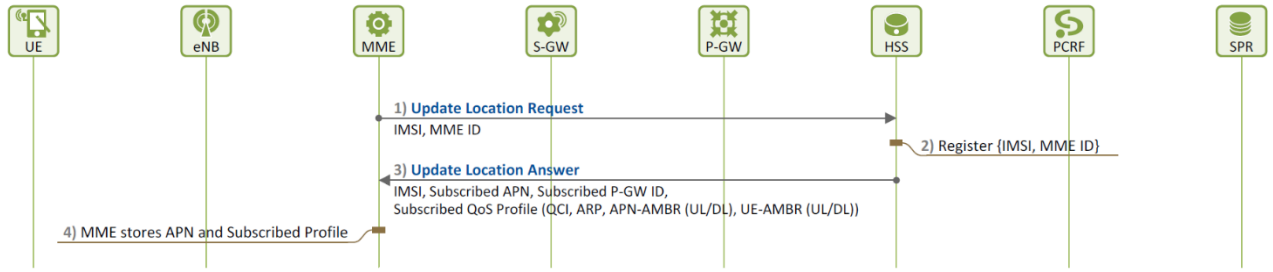


Figura 38 Procedura di Location Update

L'MME invia un Update Location Request (IMSI, MME ID) all'HSS per notificargli che l'UE è stato registrato ed ottenere le informazioni del profilo utente relative all'UE. L'HSS registra l'MME ID ad indicare in quale MME l'UE è registrato dopodiché risponde all'MME includendo le informazioni del profilo sottoscritto dall'utente in un Update Location Answer Message**,** cosicché questi possa creare la EPS session e il default EPS bearer. Le informazioni incluse

nel messaggio Update Location Answer sono le seguenti:

Update Location Answer (IMSI, Subscribed APN, Subscribed QoS profile)

- **Subscribed APN:** APN di default al quale un utente si collega (eg. Internet)
- **Subscribed PGW ID:** ID del PGW attraverso il quale accedere alla Subscribed APN
- **Subscribed QoS profile (UE-AMBR (UL/DL), QCI, ARP, APN-AMBR (UL/DL)**
  - **UE-AMBR (UL/DL):** Larghezza di banda aggregata di tutti i bearer non-GBR che un UE puo avere. Viene determinata dall'MME e controllata dall'eNB.
  - **QCI, ARP, APN-AMBR (UL/DL):** QoS applicato al Subscribed APN

Quando l'MME riceve l'Update Location Answer dall'HSS memorizza le informazioni di sottoscrizione contenute nel messaggio dalle quali può capire a quali servizi l'utente può accedere e con quale livello di QoS le risorse debbano essere allocate.

▪ **EPS Session Establishment**

L'MME, sulla base delle informazioni ottenute dall'HSS stabilisce una sessione EPS e un default EPS bearer per l'utente.

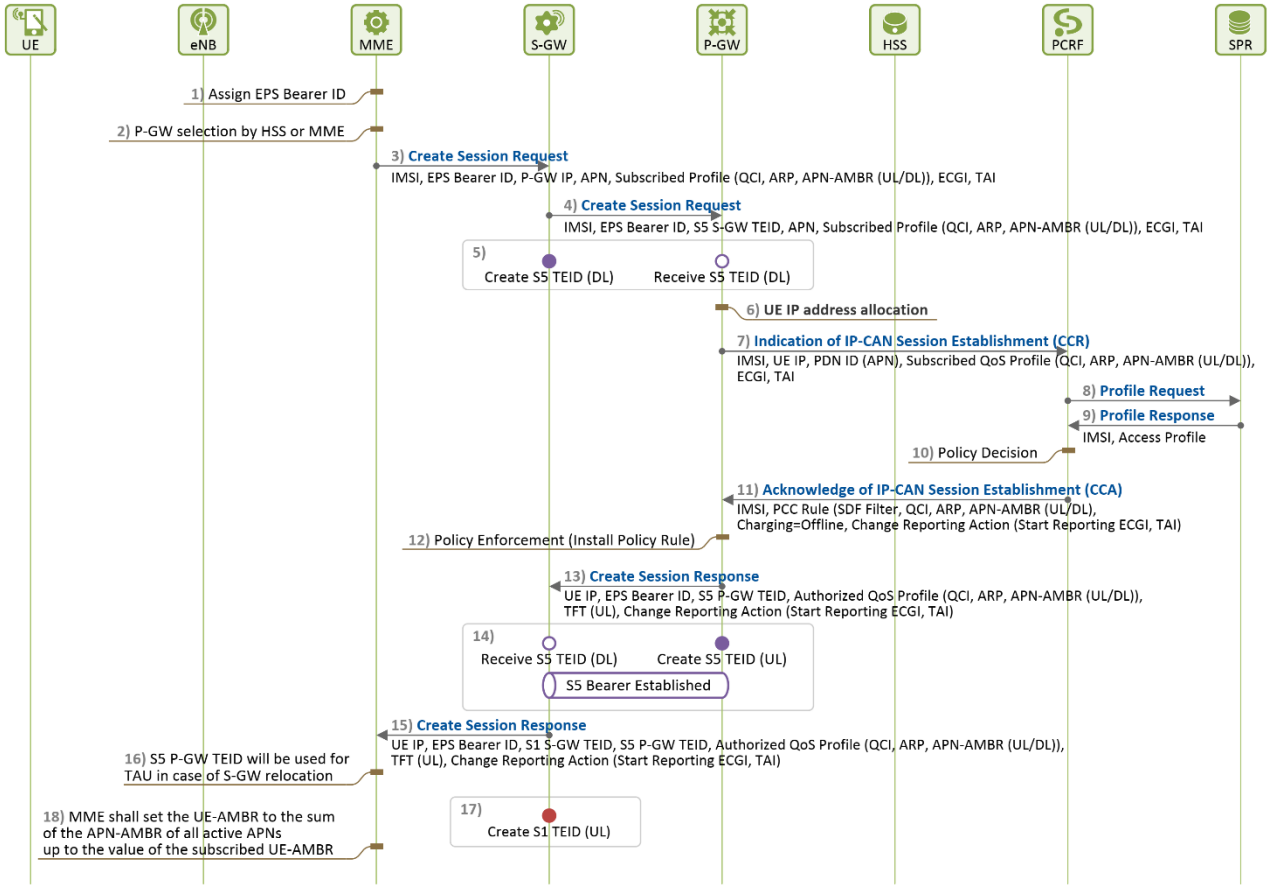


Figura 39 Procedura di EPS Sesison Estabilshment (1)

1) **[MME] Assegnazione dell'EPS Bearer ID (EBI)**

L'MME assegna un EPS Bearer ID per poter stabilire un default EPS bearer per il nuovo utente

2) **[MME] Selezione del PGW**

L'MME controlla l'APN ricevuto dall'HSS e decide a quale PGW collegarsi per accedere all'APN di default. Se l'allocazione del PGW ID è statica, l'MME utilizza il PGW ID presente all'interno delle informazioni ricevute dall'HSS, al contrario, se è dinamica esegue una query DNS utilizzando l'APN FQDN per ottenere una lista di indirizzi IP di PGW collegati alla PDN scelta, dal quale ne selezionerà uno sulla base delle policy definite dall'operatore. In questo momento, l'MME sceglie anche il SGW attraverso il quale far transitare i pacchetti da/per il PGW selezionato.

3)~5) [MME → SGW → PGW] Richiesta di creazione della EPS Session

L'MME richiede la creazione di una EPS Session e di un default EPS bearer inviando un Create Session Request message al PGW selezionato nello step precedente. L'MME include nel messaggio le informazioni di sottoscrizione ricevute dall'HSS cosicché il PGW (avente funzione di PCEF) possa utilizzarle quando deve notificare la creazione della EPS Session al PCRF, per ottenere le PCC Rules da applicare. L'MME invia quindi un messaggio Create Session Request al SGW selezionato allo step 2) attraverso il tunnel GTP-C[7] di control plane stabilito lungo l'interfaccia S11. Il messaggio contiene i seguenti parametri:

Create Session Request (IMSI, EPS Bearer ID, PGW IP, APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL), ECGI, TAI)

Successivamente, il SGW alloca un S5 TEID (S5 SGW TEID) per stabilire un tunnel GTP in DL tra sé stesso e il PGW ed include il TEID appena generato alla Create Session Request ricevuta dall'MME, inoltrando il tutto in un Create Session Request message indirizzato al PGW:

Create Session Request (IMSI, EPS Bearer ID, S5 SGW TEID, APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL), ECGI, TAI)

A questo punto il tunnel GTP-U S5 in DL tra SGW e PGW è stabilito e ciò consente al PGW di inviare il traffico in downlink al SGW.

6) **[PGW] Allocazione dell'IP dell'UE**

Il PGW, quando riceve la Create Session Request realizza che l'UE sta tentando di accedere

[7] Per brevità, quando vengono trattati i parametri relativi alla creazione di tunnel GTP sono menzionati solo i valori di user plane (GTP-U) tralasciando quelli di control plane (GTP-C)

alla rete nuovamente utilizzando l'IMSI, di conseguenza alloca un indirizzo IP all'UE che potrà utilizzarlo per la connessione alla PDN scelta

7) **~12) [PGW & PCRF] Notifica di creazione della EPS Session e determinazione delle PCC Rules**

Il PGW che agisce in funzione di PCEF inoltra le informazioni di sottoscrizione ricevute dal SGW al PCRF attraverso un messaggio CCR (CC-Request)**:**

CCR (IMSI, UE IP, PDN ID (APN, Subscribed Profile (QCI, ARP, APN-AMBR (UL/DL), ECGI, TAI)

Il PCRF determina le PCC policies da applicare alla EPS Session da creare e le invia al PGW, incluse in un CCA (CC-Answer) message:

CCA (IMSI, PCC Rule (SDF Filter, QCI, ARP, APN-AMBR (UL/DL), Charging = Offline, Change Reporting Action (Start Reporting ECGI, TAI))

Il PGW applica le PCC policies ricevute dal PCRF. Dato che le PCC policies sono applicate ad ogni SDF, il PGW crea il mapping tra le SDF e il Bearer EPS e prepara il profilo QoS da applicare al default EPS Bearer.

13) **~15) [MME ← SGW ← PGW] Risposta alla richiesta di creazione della EPS Session**

Il PGW deve informare l'MME circa le informazioni di QoS applicate alle sessioni EPS stabilite e al default bearer poiché i parametri stabiliti dal PCRF potrebbero essere differenti da quelli ottenuti dall'MME interrogando l'HSS.

Il PGW alloca un UL S5 TEID (PGW S5 TEID) per creare il tunnel GTP in UL con il SGW. Fatto questo, include il TEID creato e il profilo QoS da applicare al default bearer (S5 bearer) in un Create Session Response message che invia al SGW in risposta alla Create session Request ricevuta in precedenza.

Create Session Response (UE IP, EPS Bearer ID, S5 PGW TEID, Authorized QoS Profile (QCI, ARP, APN-AMBR (UL/DL)), TFT(UL), Change Reporting Action (Start Reporting ECGI, TAI))

A questo punto il tunnel S5 GTP-U in uplink è creato perciò il SGW e il PGW possono scambiarsi traffico in UL/DL tra loro. Di conseguenza, il PGW inizia ad inviare i pacchetti in DL al SGW che li manterrà in un buffer fin quando l'intero percorso in downlink non sarà attivo.

Quando riceve la Create Session Response dal PGW, il SGW memorizza l'UL S5 TEID (S5 PGW TEID) che deve essere utilizzato per inoltrare il traffico in UL ed alloca un UL S1 TEID

(S1 SGW TEID) per il tunnel GTP-U da utilizzare per creare il bearer S1. Dopodiché aggiunge l'S1 SGW TEID appena allocato al messaggio ricevuto dal PGW e lo inoltra all'MME in risposta alla Create Session Request ricevuta.

Il completamento di queste operazioni stabilisce il tunnel S1 GTP-U in UL ma, poiché l'eNB non ha ancora il S1 SGW TEID, non può, per il momento, inviare traffico in uplink al SGW. L'MME, inoltre, memorizza l'S5 PGW TEID cosicché, nel caso in cui l'UE esegua un TAU o un handover con cambio di SGW, possa inviarlo al nuovo SGW e quest'ultimo possa consegnare il traffico in UL al PGW.

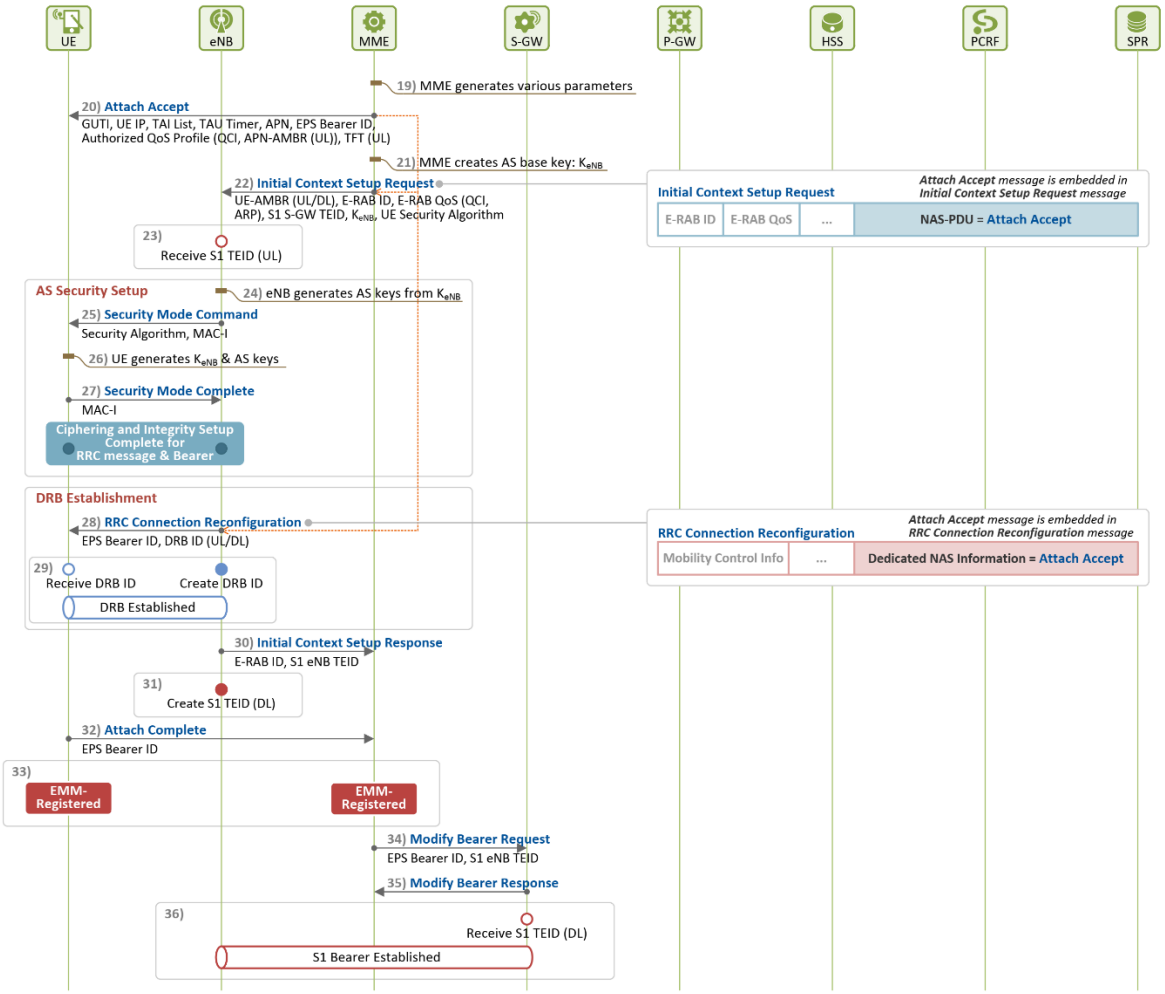


Figura 40 Procedura di EPS Session Establishment (2)

18) ~19) [MME] Generazione dei parametri richiesti per la creazione dell'E-RAB e il NAS Signaling

Quando riceve la Create Session Response dal PGW, l'MME viene a conoscenza che le risorse richieste sono state approvate ed allocate all'utente, perciò, procede col determinare vari parametri richiesti per il setup dell'E-RAB (DRB + S1 Bearer) e le informazioni necessarie per il NAS Signaling come segue:

- Alloca un GUTI che l'UE potrà utilizzare in futuro al posto dell'IMSI
- Determina i parametri richiesti per il controllo del TAU (TAI list, valore del TAU Timer)
- Calcola l'UE-AMBR per l'eNB, controllando che il valore ottenuto dall'HSS in precedenza non ecceda la somma degli APN-AMBR di ogni APN ed eventualmente utilizza questo valore al posto di quello presente nel profilo sottoscritto.
- Alloca un E-RAB ID

20) ~21) [UE ← MME] Attach Accept

L'MME include informazioni quali l'indirizzo IP dell'UE UE, il GUTI, i parametri di controllo del TAU (TAI list, TAU Timer), l'EPS Bearer ID, l'UE-AMBR e i parametri QoS ricevuti dal SGW in un messaggio Attach Accept[8] che invia come risposta all'Attach Request ricevuta dall'UE.

Il messaggio viaggia incapsulato in un Initial Context Setup Request (messaggio S1AP) attraverso la S1 signaling connection e successivamente in un RRC Reconfiguration Message attraverso la connessione RRC.

In questo momento l'MME crea KeNB, la AS Security base key, dalla top level key KASME per far sì che l'eNB possa a sua volta generare le AS security keys da utilizzare per la comunicazione sicura lungo il canale radio.

22) ~23) [eNB ← MME] Richiesta di setup dell'E-RAB

L'Initial Context Setup Request inviato dall'MME all'eNB trasporta le informazioni necessarie per la costruzione dell'S1 bearer con l'SGW e del DRB con l'UE. Le informazioni

[8] Il messaggio Attach Accept è un messaggio EMM che include il messaggio Activate Default EPS Bearer Context Request, un messaggio ESM quando viene inviato.

incluse nel messaggio sono le seguenti:

Initial Context Setup Request (UE-AMBR (UL/DL), E-RAB ID E-RAB QoS (QCI, ARP), S1 SGW TEID, KeNB, UE Security Algoritm, NAS-PDU)

- **UE-AMBR (UL/DL):** Parametro QoS controllato dall'eNB (poiché un UE utilizza sempre lo stesso eNB a prescindere da quale APN sta utilizzando)
- **E-RAB ID:** allocato dall'MME, viene utilizzato dall'eNB come EPS bearer ID
- **E-RAB QoS:** Determinato dall'MME sulla base dell'EPS bearer QoS ricevuto dal PGW
- **S1 SGW TEID:** UL S1 TEID ricevuto dal SGW
- **KeNB:** Generato dall'MME a partire da KASME e utilizzato dall'eNB per la derivazione delle AS security keys
- **UE Security Algorithm:** informazioni incluse nell'Attach Request ricevuta dall'UE. Indicano gli algoritmi per la criptazione e per la protezione di integrità dei dati lungo il collegamento radio e vengono utilizzate assieme a KeNB per il setup della sicurezza dell'Access Stratum
- **NAS-PDU:** Messaggio NAS trasportato come payload (**Attach Accept**)

Quando l'eNB analizza l'Initial Context Setup Request ricevuta ottiene l'S1 SGW TEID che può utilizzare per inoltrare il traffico in uplink al SGW. Per completare la costruzione del E-RAB, l'MME deve procedere a costruire il DRB con l'UE e ad inviare un DL S1 TEID all'MME cosicché questo possa poi inoltrarlo al SGW per completare la costruzione del DL S1 bearer.

24) ~27) AS Security Setup

Quando l'eNB riceve l'Initial Context Setup Request dall'MME tenta di comunicare con l'UE per il setup di un DRB. Per garantire la sicurezza dei messaggi scambiati lungo il canale radio, l'eNB esegue con l'UE la procedura per il setup della sicurezza dell'AS prima di inviare messaggi all'UE. A procedura completata, i messaggi RRC scambiati lungo il canale radio vengono inviati criptati e integrity-protected mentre il traffico dati utente viaggia criptato. A questo punto l'eNB inizia il setup del DRB.

28) ~29) Creazione del DRB

28) [UE ← eNB] Riconfigurazione della connessione RRC

L'eNB alloca gli UL/DL DRB ID e configura i parametri QoS del DRB a partire da quelli dell'E-RAB per poter costruire il DRB (un EPS bearer lungo il collegamento radio). Di conseguenza, invia un RRC Connection Reconfiguration message all'UE attraverso la

connessione RRC sicura. La connessione RRC era già stata stabilita all'inizio della procedura di Initial Attach ma deve essere riconfigurata poiché l'UE ora deve impostare alcuni parametri sulla base delle risorse allocate dalla rete. Il layer RRC procede quindi ad allocare risorse radio sulla base dei parametri di configurazione ottenuti dall'RRC Connection Reconfiguration message. Fatto ciò, estrare l'Attach Accept message, traportato come payload dell'RRC Connection Reconfiguration message e lo invia al NAS layer.

Quando il NAS layer dell'UE riceve il messaggio, ottiene l'IP dell'UE e il GUTI da utilizzare per le successive comunicazioni.

Il setup del DRB viene poi confermato dall'UE con un messaggio RRC Connection Reconfiguration Complete (non presente in Figura 40).

Una volta completato il setup del DRB l'UE inviare/ricevere traffico in UL/DL dall/all'eNB.

30) ~31) [eNB → SGW] Initial Context Setup Response

L'eNB alloca un DL S1 TEID (S1 eNB TEID) per il S1 bearer e lo include in un Initial Context Setup Reponse che invia all'MME in risposta all'Initial Context Setup Request message ricevuto in precedenza, affinché l'MME possa inoltrarlo al SGW. Finché il SGW non sarà a conoscenza dell'S1 eNB TEID allocato non potrà inviare traffico in DL all'eNB.

32) [UE → MME] Invio dell'Attach Complete message

L'UE invia un Attach Complete message all'MME in risposta all'Attach Accept message ricevuto in precedenza.

L'Attach Complete message viene trasportato attraverso un UL Information Transfer message lungo la connessione RRC e poi per mezzo di un Uplink NAS Transport lungo la S1 signaling connection.

33) [UE] [MME] Stato EMM

In questo momento l'UE e l'MME si trovano in stato EMM-Registered. Se al posto di un Attach Accept l'MME inviasse all'UE un Attach Reject message, l'UE dovrebbe rilasciare la connessione ECM/RRC e transitare in stato EMM-Deregistered.

34) [MME → SGW] Richiesta di modifica del Bearer S1

L'MME inoltra il DL S1 TEID (S! eNB TEID) ricevuto dall'eNB al SGW attraverso un Modify Bearer Request message.

35) [MME ← SGW] Risposta alla richiesta di modifica del bearer S1

Il SGW invia all'MME un Modify Bearer Response message in risposta al Modify Bearer Request message ricevuto. Ora, il SGW è pronto per inoltrare il traffico in DL lungo il bearer S1.

Ultimata la procedura di setup del bearer S1, l'eNB e il SGW possono scambiare traffico tra loro. Il default EPS bearer dall'UE al PGW è finalmente attivo e ciò consente la comunicazione in UL/DL tra l'UE e il PGW.

3.2. Procedura di disconnessione dalla rete (Detach Procedure)

Un utente di una rete LTE utilizza servizi dopo aver creato un EPS session e un default EPS bearer attraverso la procedura di Initial Attach.

In alcuni casi può essere l'UE stesso a disconnettersi dalla rete quando ha terminato l'utilizzo dei servizi, in altri può essere la rete stessa a disconnettere l'UE mentre sta ancora utilizzando servizi.

Quando l'utente viene disconnesso dalla rete, tutte le risorse di rete/radio allocate alla sessione EPS e ai bearer stabiliti per quell'utente vengono rilasciate. Il rilascio delle risorse provoca la cancellazione del Mobility Management Context (MM Context) e delle informazioni di sessione sugli EPS bearer che erano state impostate nelle entità EPS (UE e nodi della core network). A questo punto lo stato EMM di UE ed MME transita da Registered a Deregistered. Se l'utente viene disconnesso in maniera corretta dalla rete, il GUTI e il security context che ha utilizzato per accedere alla rete vengono mantenuti validi nell'UE e nell'MME, cosicché possano essere riutilizzati per un futuro nuovo collegamento.

La disconnessione (Detach) dalla rete può essere provocata dall'UE o dalla rete (MME o HSS). Quindi, la disconnessione può essere categorizzata in uno dei seguenti casi a seconda di quale sia l'entità che scatena la procedura:

1) **Disconnessione scatenata dall'UE**

   L'UE può iniziare la disconnessione:

   1) se viene spento

   2) se la carta SIM viene rimossa

   3) se tenta di utilizzare un servizio non EPS (e.g. Circuit Switching Fallback, SMS ecc.)

2) **Disconnessione scatenata dall'MME**

   La disconnessione scatenata dall'MME può essere divisa in due sotto-casi ulteriori: disconnessione esplicita (explicit detach) e disconnessione implicita (implicit detach). Nel caso di disconnessione esplicita, l'MME notifica all'UE il suo intento di disconnetterlo dalla rete inviandogli un Detach Request message e dicendogli se deve ricollegarsi o meno alla rete dopo la disconnessione. Nel caso di disconnessione esplicita, invece, l'MME inizia la procedura di disconnessione senza notificarlo all'UE (cioè senza inviargli un Detach Request

message) perché l'UE non è in grado di comunicare con la rete.

Quindi l'MME può scatenare:

1) Disconnessione esplicita (explicit detach)
    - Per esigenze di O&M (Operation & Maintenance) dell'operatore
    - Se la ri-autenticazione fallisce
    - Se non è in grado di fornire le risorse richieste all'utente
2) Disconnessione implicita (implicit detach)
    - Se non è in grado di comunicare con l'UE a causa di una bassa qualità del collegamento radio (radio link failure)

3) **Disconnessione scatenata dall'HSS**

    L'HSS può scatenare una disconnessione:

    1) se il profilo utente memorizzato nell'HSS è cambiato e quindi quello memorizzato nell'MME deve essere modificato di conseguenza
    2) Se un operatore vuole impedire l'accesso alla rete ad un UE "illegale" (e.g. un device rubato)

In tutti e tre i casi si assume che l'UE si trovi in stato EMM-Registered, ECM/RRC-Connected e che il servizio richiesto sia fornito solo tramite il default EPS bearer.

La Figura 41 mostra quali connessioni sono attive e in quale stato di control/user plane l'UE e l'MME si trovano prima di iniziare la procedura di detach e dopo averla terminata. Come si può notare, prima della disconnessione è attivo il default EPS bearer e tutte le connessioni di control plane ad esso relative e l'UE si trova in stato EMM-Registered, ECM/RRC-Connected. Dopo la disconnessione, il default EPS bearer e le connessioni di signaling non esistono più e l'UE si trova in stato EMM-Deregistered, ECM/RRC-Idle.

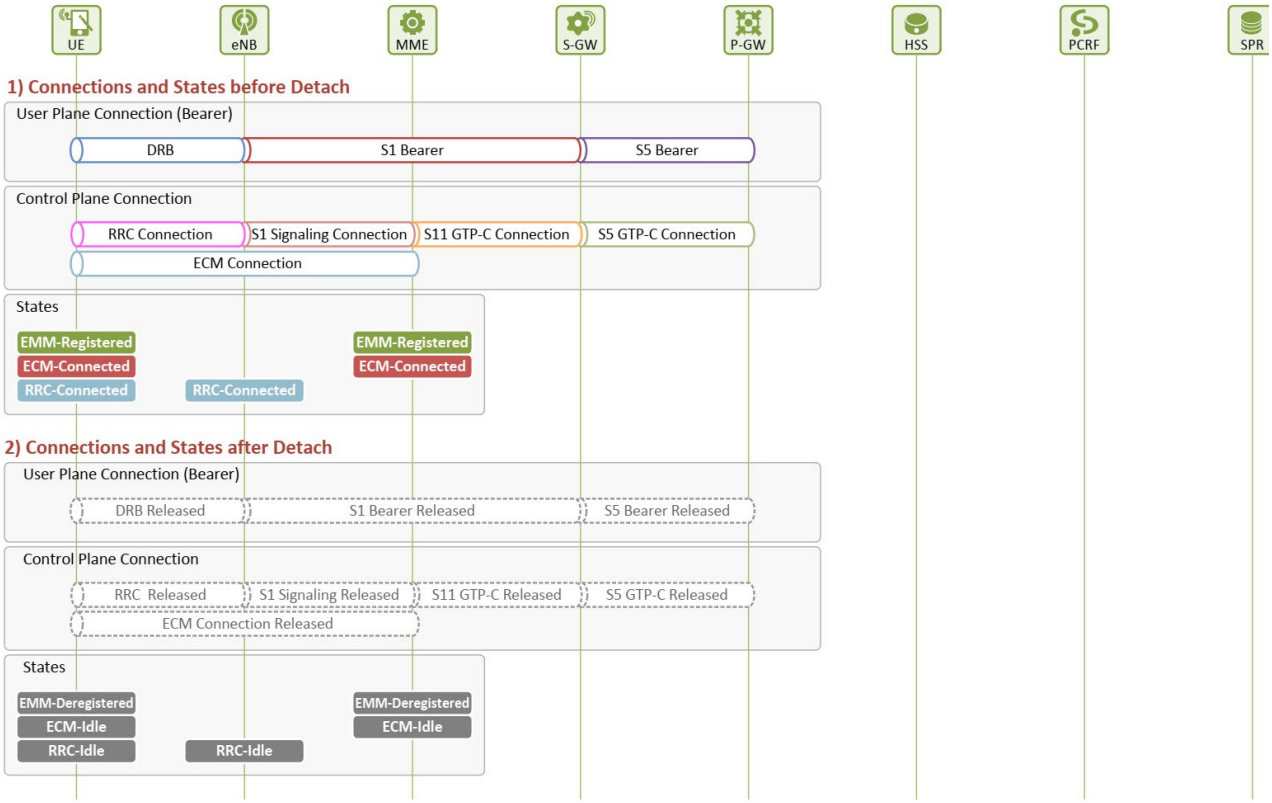


Figura 41 Connessioni e stati prima e dopo la disconnessione

3.2.1 Disconnessione scatenata dall'UE

La Figura 42 mostra come la disconnessione causata dall'UE avviene. La procedura inizia quando il triggering della disconnessione viene rilevato nell'UE provocando l'invio di un Detach Request message e termina quando l'UE riceve un Detach Accept message dall'MME, a meno che non sia stato spento dall'utente.

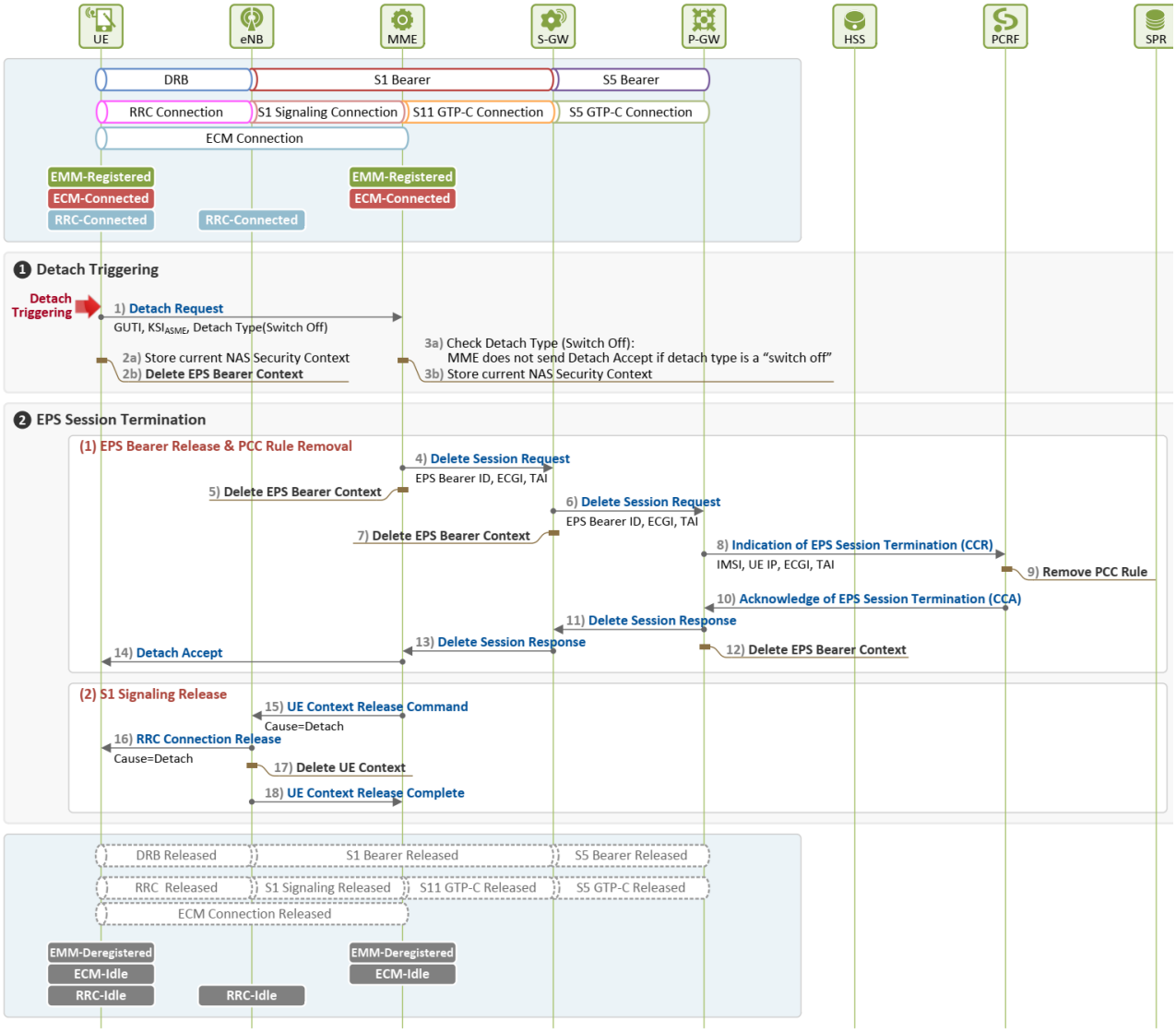


Figura 42 Procedura di Detach scatenata dall'UE

1 Detach Triggering nell'UE

Quando viene rilevato il triggering della disconnessione nell'UE, per cui l'UE e l'MME ne vengono a conoscenza, le due entità eseguono le seguenti procedure:

1) **[UE → MME] Detach Request**

   L' UE richiede all'MME di potersi disconnettere dalla rete inviandogli un Detach Request message. L'interpretazione del messaggio varia a seconda della direzione in cui viaggia. Nel caso in cui sia diretto dall'UE verso l'MME i parametri inclusi sono i

seguenti:

Detach Request (GUTI, KSI$_{ASME}$, Detach Type(Switch Off))

Il parametro Detach Type indica il tipo di detach:

- **Switch Off**: Indica se la disconnessione è dovuta ad uno spegnimento del dispositivo (1) o no (0)
- **Type of Detach**: indica se la disconnessiore irguarda i soli servizi EPS o anche quelli non-EPS

2) **[UE] Gestione dei Security e Bearer Contexts**

   Dopo aver inviato la Detach Request, l'UE memorizza il NAS Security Context corrente, il GUTI e le informazioni sulla TA dopodiché elimina l'EPS Bearer context.

3) **[MME] Ricezione della richiesta di disconnessione e Gestione del Security Context**

   Dopo aver ricevuto la Detach Request dall'UE, l'MME viene a conoscenza dell'intenzione dell'UE di disconnettersi dalla rete. Procede quindi col memorizzare il NAS Security context corrente dell'utente e controlla il tipo di detach, i.e. se è una normale disconnessione oppure se la disconnessione è dovuta ad uno spegnimento del dispositivo. Facendo ciò, l'MME sa se deve inviare o meno la Detach Accept all'UE

2 Terminazione della sessione EPS

Quando l'MME viene a conoscenza dell'intenzione dell'UE di disconnettersi dalla rete e che memorizza il NAS Security context corrente dell'utente e richiede la terminazione della sessione EPS attiva. La richiesta scatena la terminazione della sessione EPS da parte del PCEF (PGW) che provoca il rilascio di tutte le risorse di rete/radio allocate all'utente, come descritto di seguito

(1) Rilascio dell'EPS Bearer e rimozione delle PCC Rules impostate

4) **[MME → SGW] Richiesta di rilascio della sessione EPS**

   L'MME invia al SGW la richiesta di cancellazione della Eps Session e del default EPS bearer mediante un Delete Session Request message nel quale sono inclusi il default EPS bearer ID e le informazioni di posizione dell'UE (ECGI, TAI)

5) **[MME] Cancellazione dell'EPS Bearer Context**

   L'MME cancella l'EPS Bearer Context dopo aver inviato la Delete Session Request al SGW.

6) **[SGW → PGW] Richiesta di rilascio della sessione EPS**
   Il SGW inoltra al PGW la Delete Session Request ricevuta dall'MME
7) **[SGW] Cancellazione dell'EPS Bearer Context**
   Il SGW cancella l'EPS Bearer Context dopo aver inviato la Delete Session Request al PGW.
8) **[PGW → PCRF] Notifica di terminazione della sessione EPS**
   Il PGW notifica al PCRF per mezzo di un CCR (CC-Request) message che l'utente ha finito di utilizzare i servizi. In questo modo le procedure di terminazione della sessione EPS per mezzo del PCEF iniziano.
9) **[PCRF] Cancellazione delle PCC Rules**
   Il PCRF cancella la PCC rule relativa all'utente quando riceve il messaggio CCR dal PGW.
10) **[PGW ← PCRF] Notifica di terminazione della sessione EPS**
    Il PCRF notifica al PGW la cancellazione delle PCC Rules inviandogli un CCA (CC-Answer) message.
11) **[SGW ← PGW] Risposta alla richiesta di rilascio della sessione EPS**
    Quando il PCRF riceve il messaggio CCA dal PCRF invia al SGW una Delete Session Response in risposta alla richiesta inviatagli nello step 6)
12) **[PGW] Cancellazione dell'EPS Bearer Context**
    Il PGW cancella l'EPS Bearer Context relativo all'utente dopo aver inviato la Delete Session Response
13) **[MME ← SGW] Risposta alla richiesta di rilascio della sessione EPS**
    Quando il SGW riceve la Delete Session Response dal PGW, invia all'MME una Delete Session Response in risposta ala richiesta ricevuta nello step 4)
14) **[UE ← MME] Conferma di avvenuta disconnessione (Detach Accept)**
    Quando riceve la Delete Session Response, l'MME riconosce il fatto che il rilascio delle risorse allocate è stato approvato dal PCRF. Di conseguenza invia un Detach Accept message in risposta alla richiesta ricevuta nello step 1). Un Detach Accept message viene inviato solo se la Detach Request da parte dell'UE era dovuta a cause differenti dallo spegnimento del dispositivo (Switch Off = 0 in Detach Request).

(2) Rilascio della connessione di signalling S1

Dopo aver inviato la Detach Accept all'UE, l'MME e l'eNB rilasciano qualsiasi risorsa rimasta allocata per l'utente (S1 signaling connection, RRC connection, UE Context in eNB) poiché non servono più.

15) **[eNB ← MME] Richiesta di Rilascio della connessione di signaling S1**

L'MME invia all'eNB un UE Context Release Command per rilasciare la connessione di signaling S1.

16) **[UE ← eNB] Rilascio della connessione RRC**

L'eNB invia un RRC Connection Release message all'UE per rilasciare la connessione RRC rimasta ancora attiva.

17) **[eNB] Cancellazione dell'UE Context**

L'eNB cancella tutte le informazioni relative all'UE

18) **[eNB → MME] Notifica del completamento del rilascio della connessione di signaling RRC**

L'eNB invia all'MME un UE Context Release Complete message in risposta alla richiesta inviatagli nello step 15).

3.2.2 Disconnessione scatenata dall'MME

La figura 3 mostra come viene eseguita la procedura di explicit detach iniziata dall'MME. La procedura di detach per questo tipo di disconnessione inizia quando il triggering della disconnessione viene rilevato dall'MME, provocando l'invio di una Detach Request all'UE. La procedura termina col rilascio delle risorse allocate alla sessione EPS.

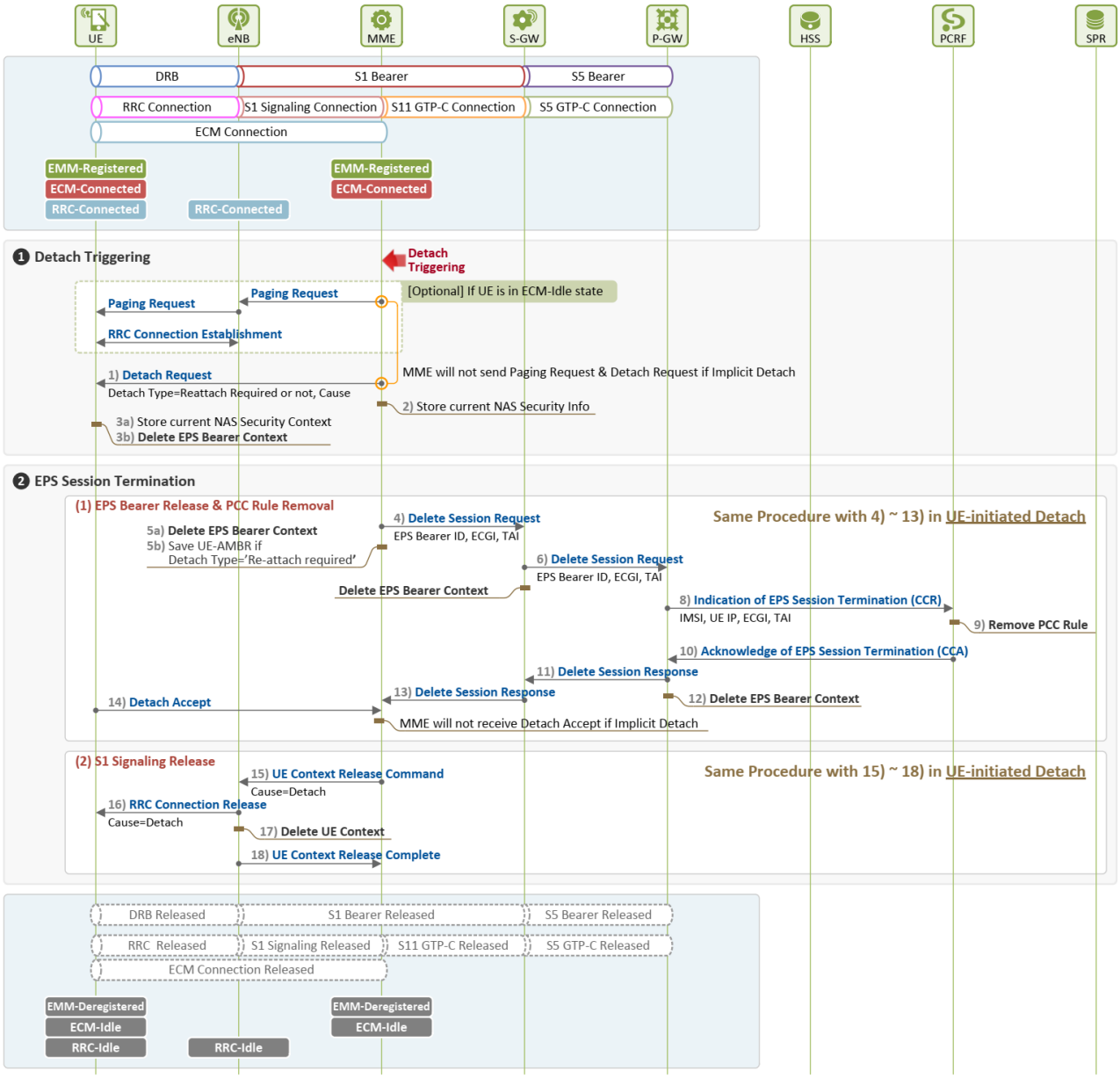


Figura 43 Procedura di Detach scatenata dall'MME

1 Detach Triggering nell'MME

Di seguito vengono descritte le procedure eseguite dopo che l'MME ha rilevato il triggering della disconnessione e prima che le procedure di terminazione della sessione EPS vengano eseguite. Se l'UE si trova in idle state in questo momento, l'MME deve effettuare le procedure di paging per risvegliarlo (come descritto meglio in seguito nella procedura di Network-triggered Service Request).

1) **[UE ← MME] Detach Request**

   Dato che la procedura in esame è di explicit detach, l'MME invia all'UE un Detach Request message per chiedergli di disconnettersi. I parametri inclusi nel messaggio, che

in questo caso è diretto dall'MME all'UE sono i seguenti:

Detach Request (Detach Type (Re-attach required or not), Cause)

- **Detach Type:** indica se è richiesto all'UE di riconnettersi o meno dopo la disconnessione
  - 001: Riconnessione richiesta
  - 010: Riconnessione non richiesta
- **Cause:** indica la causa della disconnessione

In caso di implicit detach invece, l'MME non invia un Detach Request message all'UE.

2) **[MME] Gestione del security context**

Dopo aver inviato la Detach Request all'UE, l'MME memorizza il NAS Security Context corrente prima di eliminare il context relativo alla sessione EPS. L'MME potrà, al prossimo collegamento dell'UE riutilizzare il NAS Security Context evitando così le procedure di autenticazione e NAS Security Setup

3) **[UE] Ricezione della richiesta di disconnessione e gestione dei Bearer e Security Context**

Dopo aver ricevuto la Detach Request dall'MME, l'UE viene a conoscenza del fatto che l'MME vuole disconnetterlo. Esamina quindi il valore del parametro Detach Type per stabilire se deve riconnettersi dopo la disconnessione. Dopodiché memorizza il NAS Security Context corrente ed elimina l'EPS bearer context.

❷ Terminazione della sessione EPS

Una volta che l'MME ha memorizzato il NAS Security Context richiede al PGW la terminazione della sessione EPS. Questa richiesta scatena le procedure di terminazione della sessione EPS da parte del PCEF (PGW)-initiated che rilasciano tutte le risorse di rete/radio allocate all'utente, come descritto di seguito

(1) Rilascio del Bearer EPS e rimozione delle PCC Rules

Mediante gli step 4) ~ 13), l'MME richiede la terminazione della EPS session, il PCRF cancella le PCC rules quando riceve la richiesta e il bearer S5 viene rilasciato, come accadeva anche per la procedura di detach UE-initiated. Nel caso in cui sia richiesta la riconnessione dopo la disconnessione (in base al valore del parametro Detach Type della Detach Request), l'MME può memorizzare il valore UE-AMBR corrente nello step 5) così da riutilizzarlo in seguito per costruire un EPS bearer più velocemente.

14) [UE → MME] Detach Accept

Dopo aver memorizzato il NAS Security Context e cancellato l'EPS Bearer context alla ricezione della Detach Request, l'UE invia un Detach Accept message in risposta all'Attach Request. In caso di implicit detach invece l'UE non invia un Detach Accept message.

(2) Rilascio della connessione di signaling S1

In questa fase, come già descritto in precedenza, l'MME rilascia tutte le risorse rimaste allocate (S1 signaling connection, RRC Connection e UE Context rimasto nell'eNB) dopo aver ricevuto il Detach Accept message dall'UE e il Delete Session Response message dal SGW. Gli step di questa fase sono identici a quelli intrapresi per la procedura di detach scatenata dall'UE tranne che per il fatto che se il parametro Detach Type indica che è richiesta la riconnessione, l'UE la effettua dopo la che connessione RRC è stata rilasciata.

3.2.3 Disconnessione scatenata dall'HSS

La Figura 44 illustra come l'HSS inizia la procedura di scollegamento dopo aver rilevato l'evento scatenante.

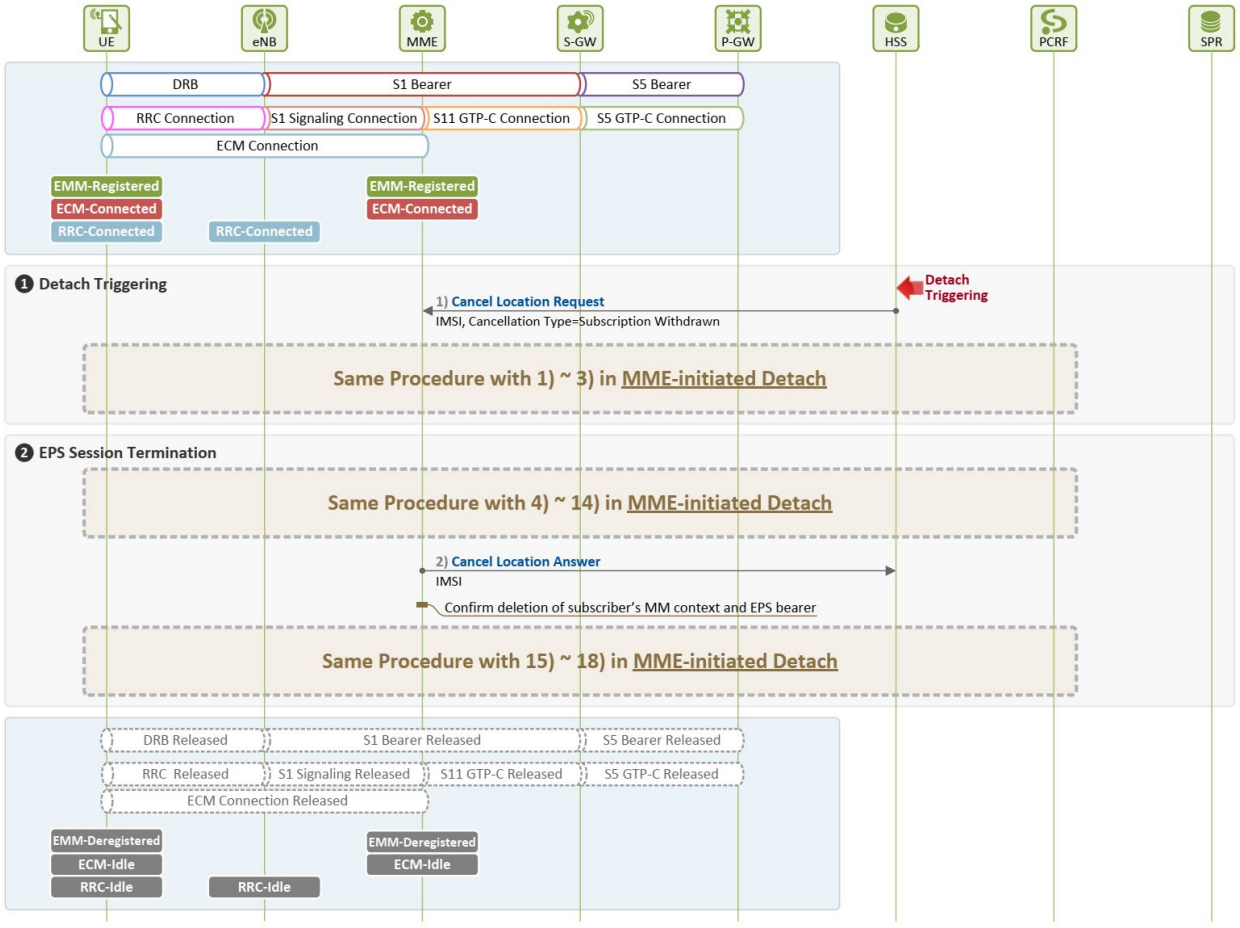


Figura 44 Procedura di Detach scatenata dall'HSS

1 Detach Triggering nell'HSS

Quando la disconnessione dalla rete viene scatenata dall'HSS per effetto del recesso, da parte dell'utente, dal contratto con l'operatore, l'HSS richiede immediatamente la rimozione del MM Context e dell'EPS bearer

1) **[MME ← HSS] Detach Request**

   L'HSS richiede all'MME (comunicando attraverso l'interfaccia S6a con protocollo Diameter) la disconnessione dell'utente inviando un Cancel Location Request (CLR) message contenente i seguenti parametri:

Cancel Location Request (IMSI, Cancellation Type)

- **IMSI:** IMSI dell'utente che deve essere disconnesso (cioè del quale devono essere eliminati MM Context ed EPS Bearer)
- **Cancellation Type = Subscription Withdrawn:** indica la ragione per la quale è richiesta la disconnessione. In questo caso per recesso dell'utente dal contratto

2 Terminazione della sessione EPS

Quando riceve la Cancel Location Request (CLR) dall'HSS, l'MME rilascia tutte le risorse allocate per l'utente così come avveniva per la procedura MME-initiated ma allo step 2), dopo aver ricevuto la Detach Accept dall'UE e la Delete Session Response dal SGW, deve aggiungere l'invio di un Cancel Location Answer message all'HSS per confermare l'avvenuta cancellazione del MM Context e dell'EPS Bearer allocato all'utente.

3.3 Rilascio del bearer S1 per inattività dell'UE

Quando un UE è inattivo (cioè è registrato alla rete ma non sta usando alcun servizio) non usa nessuna risorsa radio allocata dall'eNB. Quindi la rete, tra le varie risorse allocate per l'UE rilascia quelle relative all'accesso radio e cancella le informazioni ad esse associate (e.g. ID, parametri QoS ecc.)
Dalla prospettiva della rete rilasciare le connessioni S1 significa terminare la connessione di signaling S1 e la connessione RRC in control plane e il downlink S1 bearer e il DRB nello user plane associati con l'UE. Per un UE invece significa perdere la connessione RRC di control plane con l'eNB e il DRB di user plane. Una volta rilasciata la connessione S1, la connessione ECM tra UE ed MME non esiste più e tutti i context associati con l'UE presenti nell'eNB vengono eliminati Dopodiché l'UE transita da stato ECM-Connected a stato ECM-Idle, pur rimanendo sempre in stato EMM-Registered.
La procedura di S1 Release può essere scatenata sia dall'eNB che dall'MME. Il rilascio eNB-triggered può essere causato da:

- Inattività dell'utente
- Ripetuti fallimenti del controllo di integrità dei messaggi di signaling RRC
- Rilascio da parte dell'UE della connessione di signaling
- Errore non specificato
- Interventi di Operations & Maintenance

Il rilascio MME-triggered può avvenire a causa di:

- Errori di autenticazione
- Disconnessione dalla rete (Detach)

Inoltre, il rilascio delle connessioni S1 può essere dovuto anche ad altre ragioni quali control processing overload o mancanza di risorse disponibili per il processing del traffico user plane, ecc.

La Figura 45 mostra le connessioni stabilite in user e control plane e gli stati di UE ed MME prima e dopo la S1 release. Prima del rilascio, sono attivi un EPS bearer ed una connessione di signaling che consentono il trasporto del traffico tra l'utente e la rete (dall'UE al PGW). L'EPS bearer è composto da un DRB, un S1 bearer ed un S5 bearer mentre la connessione di signaling consiste di una connessione ECM (RRC ed S1 signaling connection) e di connessoni S11 ed S5. L' UE e l'MME si trovano in stato EMM-Registered/ECM-Connected mentre l'UE e l'eNB sono in stato RRC-Connected.

Mediante la procedura di S1 release però, il DRB e il downlink S1 bearer di user plane vengono eliminati e la connessione ECM di control plane viene persa, rilasciando le risorse E-UTRAN. Da notare è il fatto che vengono rilasciate esclusivamente le risorse per il DL S1 bearer mentre quelle per l'uplink vengono mantenute.

La procedura di S1 Release si differenzia da quella di Detach poiché, nel secondo caso, tutte le risorse allocate all'UE da parte della rete vengono rilasciate e l'UE transita in stato EMM-Deregistered mentre nel primo caso solo le risorse allocate dalla radio access network (E-UTRAN o eNB) vengono rilasciate mentre quelle allocate dalla core network vengono mantenute intatte. Di conseguenza nel caso di S1 Release, l'UE rimane in stato EMM-Registered ma transita in stato ECM-Idle. Dopodiché quando ci sarà nuovamente traffico in uplink/downlink la connessione ECM e i bearer DRB ed S1 verranno ristabiliti riportando l'UE in stato ECM-Connected e consentendo il transito del traffico.

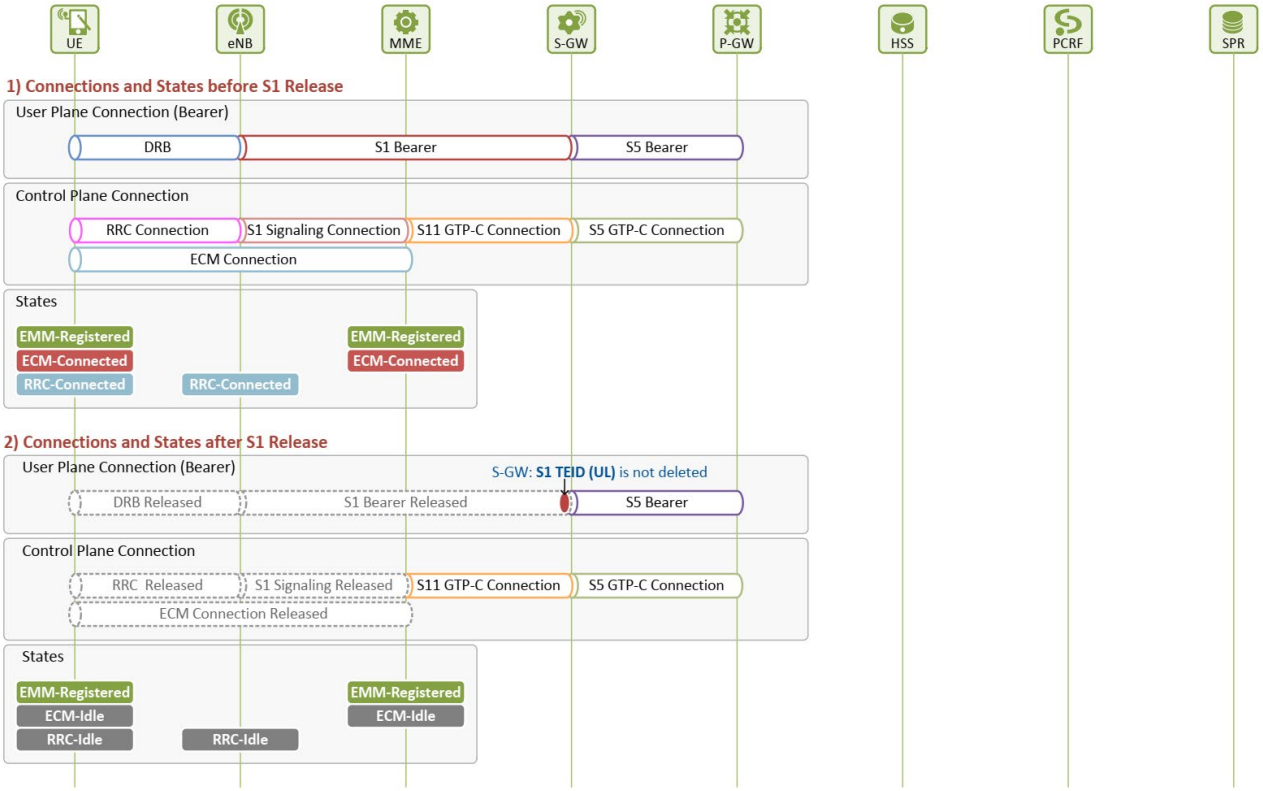


Figura 45 Connessioni e stati prima e dopo la S1 Release

La Figura 46 mostra le procedure per la S1 Release scatenate dall'eNB a seguito della rilevazione dell'inattività dell'utente (le stesse procedure si applicano anche per altre cause di S1 Release). In caso di S1 release scatenata dall'MME viene saltato lo Step 1) mostrato in Figura 46.

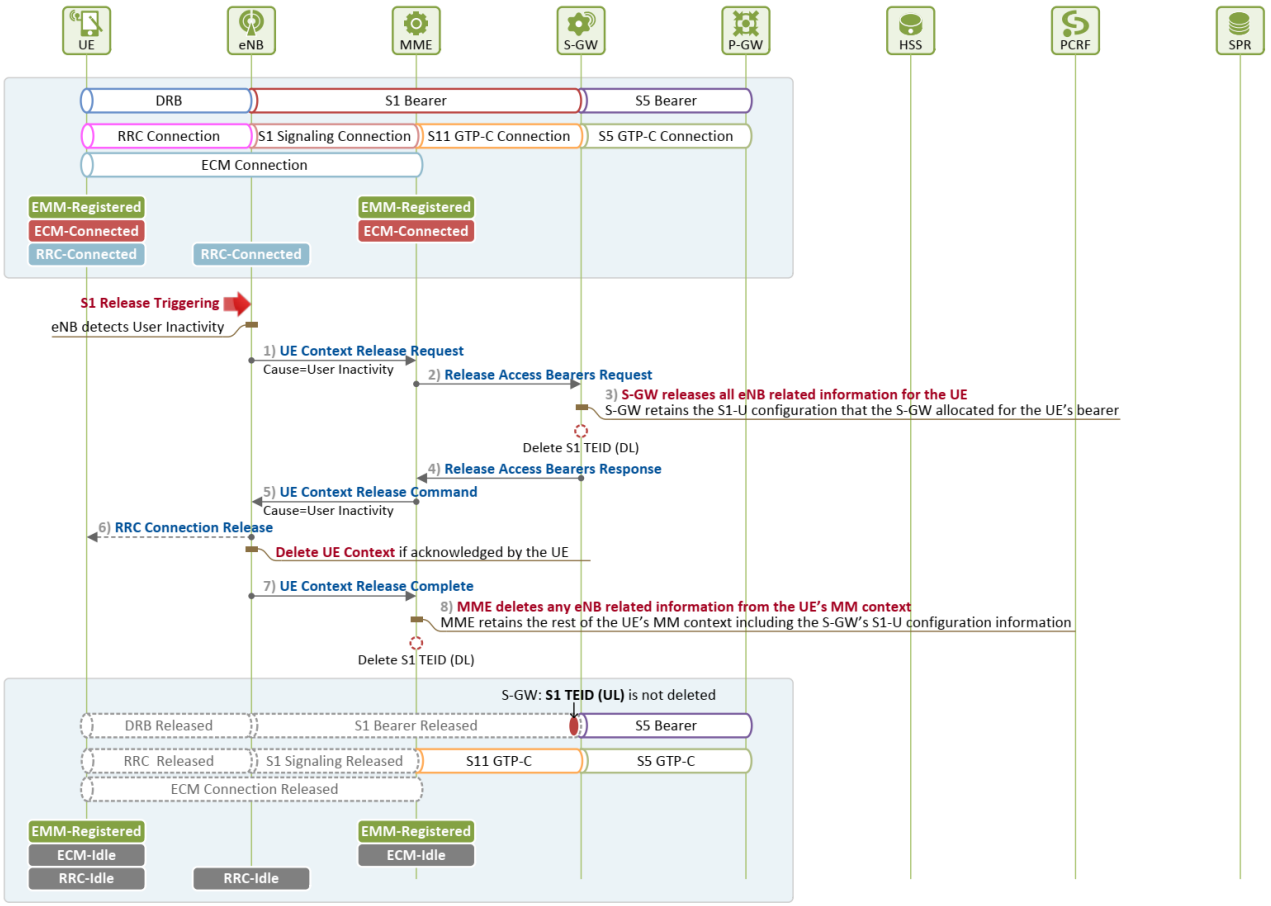


Figura 46 Procedure di S1 Release (eNB-initiated)

1) **[eNB → MME] Richiesta di rilascio dell'UE Context**

   L'eNB, dopo aver rilevato l'inattività dell'utente, invia all'MME un UE Context Release Request message indicando la causa del rilascio, per richiedere la cancellazione dell'UE context.

2) **[MME → SGW] Richiesta di rilascio dell'S1 Bearer**

   L'MME richiede al SGW il rilascio de risorse associate con l'eNB, che rappresenta l'endpoint in downlink del bearer S1, inviando al SGW un Release Access Bearers Request message. In questo modo, l'MME informa il SGW che non può più essere consegnato traffico in downlink all'UE.

3) **[SGW] Rilascio del Downlink S1 Bearer**

   Il SGW rilascia tutte le risorse del downlink S1 bearer associato con l'UE (relative all'eNB quali il DL S1 TEID allocato dall'eNB ecc.) ma mantiene le risorse dell'uplink S1 bearer (relative al SGW, quali l'UL S1 TEID allocato da sé stesso ecc.) intatte. Così facendo, quando i pacchetti in uplink arrivano, l'eNB può ottenere l'UL S1 TEID dall'MME e consegnare i pacchetti attraverso il bearer S1 senza ritardi.

4) **[MME ← SGW] Risposta alla richiesta di rilascio del DL S1 bearer**
   Il SGW conferma che le risorse relative al downlink S1 bearer sono state rilasciate inviando all'MME un Release Access Bearers Response message. A questo punto, se arrivano pacchetti in downlink destinati all'UE, il SGW li mantiene in un buffer e li consegnerà solo dopo che il bearer S1 sarà stato ristabilito mediante la procedura di Service Request.
5) **[eNB ← MME] UE Context Release Command**
   L'MME invia all'eNB un UE Context Release Command message per ordinare all'eNB di rilasciare l'UE context memorizzato.
6) **[UE ← eNB] Rilascio della connessione RRC**
   L'eNB, quando riceve il comando dall'MME, cancella tutti gli UE context (UE ID, informazioni sulla posizione dell'UE, AS Security Context, informazioni sul bearer EPS) che aveva memorizzato. Se la connessione RRC non è ancora stata rilasciata, l'eNB invia all'UE un RRC Connection Release message per rilasciarla. Così facendo, l'eNB rilascia tutte le risorse radio e i bearer allocati all'UE e cancella gli UE context.
7) **[eNB → MME] UE Context Release Complete**
   L'eNB invia all'MME un UE Context Release Complete message in risposta alla richiesta inviatagli allo step 5). L'MME poi conferma che tutti gli UE context sono stati rilasciati
8) **[MME] S1 Release**
   L'MME cancella tutte le informazioni riguardanti l'UE relative all'eNB, ad eccezione delle informazioni sull'uplink S1 bearer, in tutti gli UE contexts mantenendo però le informazioni non collegate all'eNB.

3.4 Service Request

La procedura di Service Request viene eseguita quando un UE inattivo vuole ritornare ad utilizzare i servizi della rete LTE perché c'è nuovo traffico (in UL o DL). Trovandosi in Idle state le risorse E-UTRAN (allocate dall'eNB) sono state rilasciate e l'UE si trova in stato ECM/RRC-Idle. Di conseguenza, affinché l'UE possa inviare o ricevere traffico utente in DL o UL, ha bisogno di transitare in stato ECM/RRC-Connected attraverso la procedura di Service Request, cosicché le risorse E-UTRAN possano essere allocate nuovamente.

3.4.1 Casi di Service Request

Quando un UE è ancora registrato alla rete ma la sua connessione S1di signalling e il DL S1 Bearer sono rilasciati per inattività, non ha risorse radio disponibili, perciò si trova in stato EMM-Registered ma ECM-Idle. Se, in questo stato, viene generato nuovo traffico dall'UE o dalla rete all'UE, l'UE richiede alla rete di poter utilizzare i servizi, transitando in stato ECM-Connected**.** Vengono quindi attivati una connessione ECM (RRC + S1 signaling connection) ed un E-RAB (DRB+ S1 bearer) rispettivamente nel control e user plane, permettendo all'UE di inviare o ricevere traffico. Nel caso la rete debba inviare traffico all'UE, dapprima informa l'UE cosicché quest'ultimo possa effettuare una Service Request

Quando l'UE ha nuovo traffico da inviare o viene a conoscenza che c'è traffico in entrata dalla rete, invia all'MME un messaggio di Service Request**,** transitando in stato ECM/RRC-Connected**.** Dopodiché l'UE, utilizzando le risorse radio e di rete allocate, può inviare o ricevere traffico. La procedura di Service Request può essere avviata da un UE o dalla rete e può essere categorizzata nei seguenti due casi:

1) **Nuovo traffico generato dall'UE (UE-triggered Service Request)**
   Quando ci sono dati in uplink da inviare dall'UE alla rete
2) **Nuovo traffico generato dalla rete (Network-triggered Service Request)**
   Quando ci sono dati in downlink da inviare dalla rete all'UE

La Figura 47 mostra le connessioni stabilite nel control e user plane e gli stati di UE ed MME prima e dopo la Service Request. Prima della service request, l'UE si trova in stato EMM-Registered ed ECM/RRC-Idle**.** Le sole risorse allocate sono quelle della EPC mentre quelle allocate dalla E-UTRAN sono già rilasciate. Nel control plane, i tunnel S5 GTP-C ed S11 GTP-C rimangono attivi mentre la connessione ECM viene rilasciata. Nello user plane, il bearer S5 e l'uplink S1 bearer vengono mantenuti attivi mentre il downlink S1 bearer e il DRB vengono rilasciati.

Dopo la service request, l'UE, ora che ha le risorse E-UTRAN allocate, si trova in stato EMM-Registered ed ECM/RRC-Connected. Tutti i bearer e le connessioni di signaling vengono ristabilite così da poter far fluire il traffico tra l'UE e la rete.

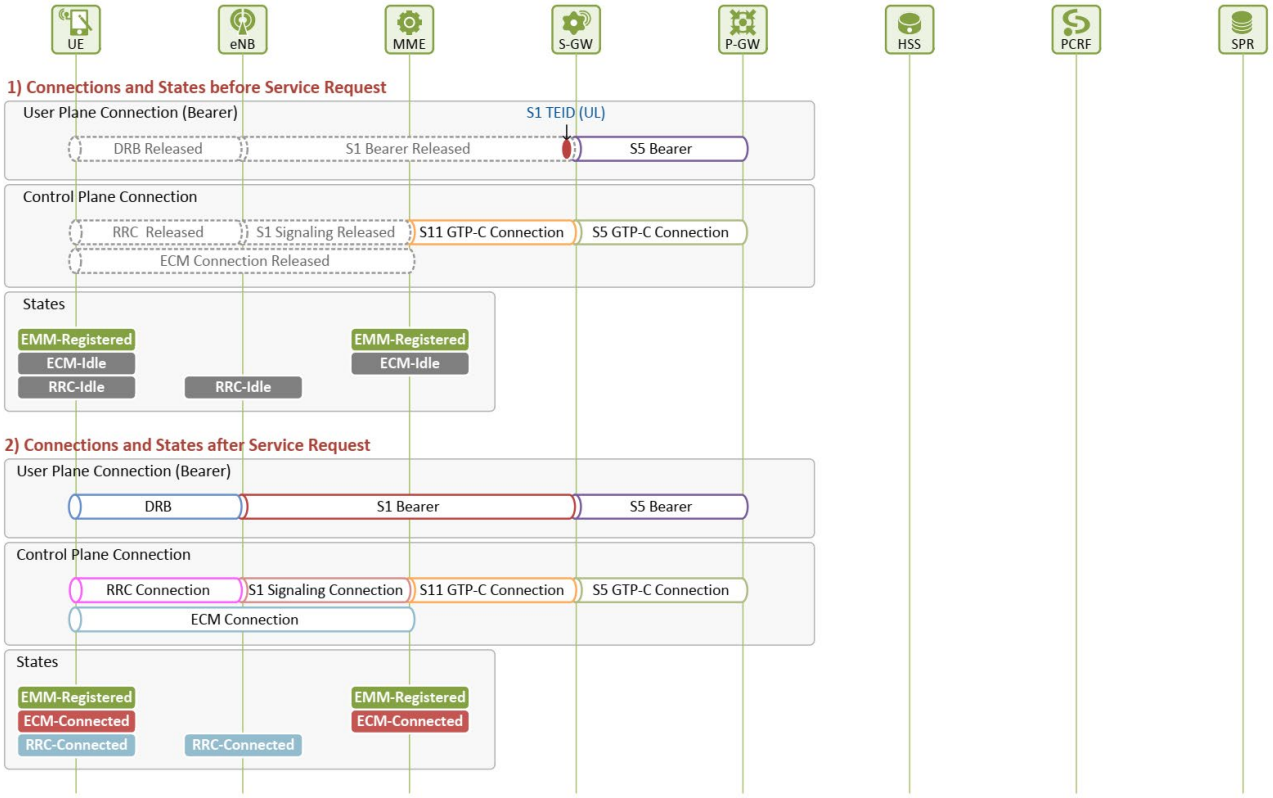


Figura 47 Connessioni e Stati EMM/ECM/RRC prima e dopo la Service Request

3.4.1.1 UE-triggered Service Request

Le figure 2 e 3 illustrano le procedure per una UE-triggered service request causata da traffico in uplink dall'UE. Il NAS layer dell'UE indica all'MME che l'UE ha dati da trasmettere, inviando un Service Request message. Come risultato, le risorse richieste per la trasmissione dati vengono allocate dalla rete. Dato che l'UE è rimasto registrato alla rete, il suo NAS security context (K_{NASenc}, K_{NASint}, ecc.) è ancora valido nell'UE e nell'MME.

Utilizzando il security context, l'UE può inviare una Service Request criptata con l'encryption-key (K_{NASenc}) ed integrity-protected con la integrity key (K_{NASint}). Quando l'MME riceve il messaggio, determina se eseguire o meno le procedure di autenticazione dell'utente attraverso il controllo di integrità e la decrittazione del messaggio, dopodiché l'eNB procede con la creazione di un E-RAB.

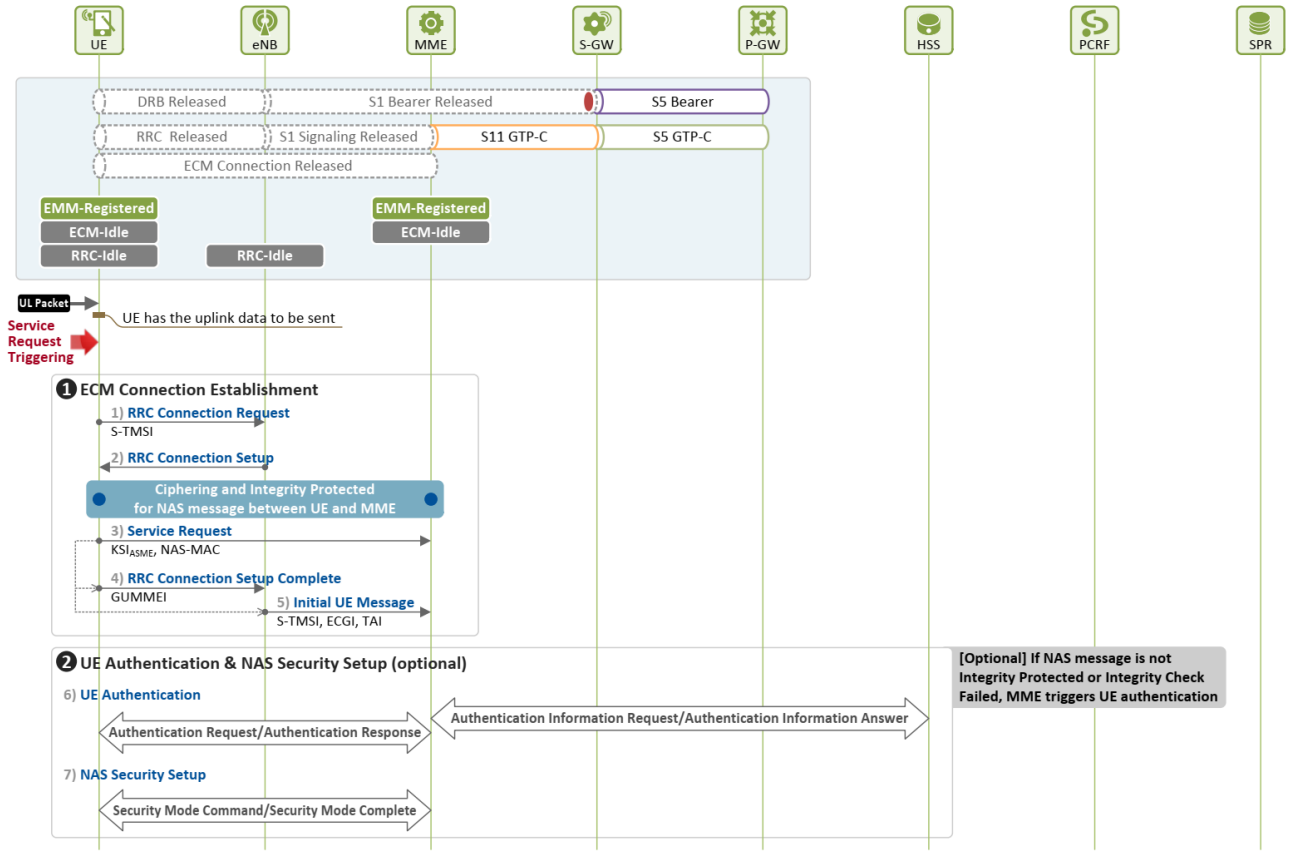


Figura 48 Procedure per la UE-triggered Service Request (1)

1 ECM Connection Establishment

Quando c'è nuovo traffico da inviare, l'UE invia all'MME una Service Request per stabilire una connessione ECM. Il Service Request message viene consegnato all'MME attraverso la connessione RRC stabilita lungo il collegamento radio, e poi attraverso la S1 signaling connection stabilita tra l'eNB e l'MME. In questo caso, assumiamo che il GUTI e il NAS security context sono mantenuti validi sia nell'UE che nell'MME.

1), 2) [UE-eNB] Setup della connessione RRC

Il NAS layer all'UE fornisce all'RRC layer il S-TMSI[9]. Il layer RRC, utilizzando il S-TMSI come UE ID, invia un **RRC Connection Request** message all'eNB per poter stabilire una connessione RRC. L'eNB risponde con un **RRC Connection Setup** message all'UE.

3), 4), 5) [UE → MME] Richiesta di creazione della connessione ECM

Il NAS layer dell'UE invia un Service Request message all'MME per creare una connessione ECM. Esistendo una connessione in precedenza prima di transitare in idle state, il NAS Security Context è stato memorizzato dall'UE e dall'MME. Quindi il messaggio include il

[9] Un S-TMSI è un identificativo utilizzato per identificare univocamente un UE all'interno di un gruppo di MME. Viene utilizzato qualora la rete di un operatore non abbia più di un gruppo di MME poiché è più corto del GUTI consentendo di avere una maggiore efficienza di trasmissione radio.

NAS base key identifier (KSI_{ASME}) ed è inviato crittografato con la chiave K_{NASenc} e integrity-protected con la chiave NAS_{int}. Il Service Request message viene inviato all'eNB incluso in un RRC Connection Setup Complete message lungo il collegamento radio tra UE ed eNB. Poi, viene incapsulato in un messaggio S1AP, Initial UE Message nel tragitto tra l'eNB e l'MME. L'eNB, in questo momento alloca l'eNB UE S1AP ID e lo include nell'Initial UE Message inviato all'MME. Quando l'MME riceve l'Initial UE Message, l'MME alloca l'MME S1AP UE ID per completare la creazione della connessione di signaling S1 tra l'eNB e sé stesso.

2 Autenticazione dell'UE e NAS Security Setup (Opzionale)

6) [UE – MME -HSS] Autenticazione dell'UE

Dopo aver ricevuto il Service Request message dall'UE, l'MME esegue il controllo di integrità sul NAS-MAC. Se il controllo termina con esito positivo, l'MME può utilizzare il NAS Security Context corrente per la trasmissione dei messaggi NAS. In caso contrario, dovrà ri-eseguire le procedure di autenticazione dell'UE.

7) [UE – MME] NAS Security Setup

Terminata la procedura di autenticazione, l'UE e l'MME, attraverso la procedura di NAS Security Setup, generano le NAS security keys (K_{NASenc}, K_{NASint}) da utilizzare per lo scambio dei messaggi NAS in sicurezza.

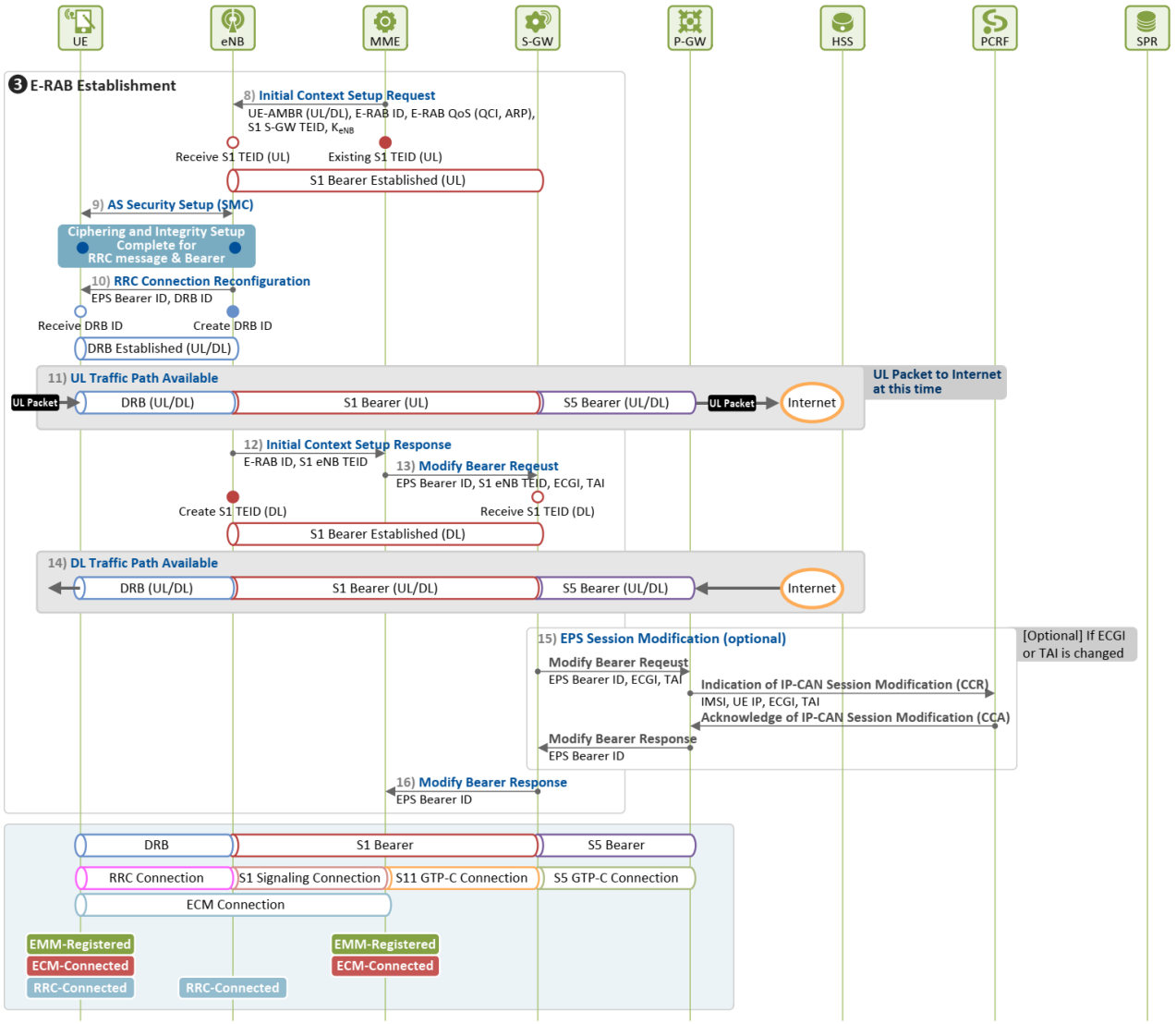


Figura 49 Procedure per la UE-triggered Service Request (2)

3 Creazione dell'E-RAB

Dopo aver ricevuto la Service Request dall'UE, l'MME chiede all'eNB di creare un DRB e un DL S1 bearer attraverso le procedure di creazione dell'E-RAB.

8) [eNB ← MME] Richiesta di creazione dell'E-RAB

Quando l'MME riceve la Service Request dall'UE realizza che deve essere creato un E-RAB. Quindi, invia un eNB Initial Context Setup Request message all'eNB per far sì che questo crei un DRB con l'UE ed un bearer S1 con il SGW. Il messaggio contiene le seguenti informazioni:

Initial Context Setup Request (E-RAB ID, K_{eNB}, S1 SGW TEID, MME UE S1AP ID)

- **E-RAB ID**
- **K_{eNB}:** AS Security base key necessaria per il setup della sicurezza dell'AS con l'UE
- **S1-SGW TEID:** identifica l'UL S1 bearer connesso al SGW per l'eNB
- **MME UE S1AP ID:** identifica la connessione di signalling S1 con l'MME per l'eNB

9) [UE – eNB] AS Security Setup

Quando riceve l'Initial Context Setup Request dall'MME, l'eNB realizza che deve costruire un DRB ed un S1 bearer per far sì che il traffico possa viaggiare tra la rete e l'UE. Prima di creare un DRB però, l'eNB esegue le procedure di setup della sicurezza dell'AS per garantire una comunicazione sicura lungo il DRB e il SRB con l'UE. Quindi attraverso le procedure di AS Security Setup l'UE e l'eNB derivano le chiavi K_{RRCint} e K_{RRCenc} da utilizzare per la criptazione e l'integrity-ptotection dei messaggi RRC e la chiave K_{UPenc} per la criptazione del traffico dati utente.

Una volta completate con successo le procedure di AS Security Setup, i messaggi RRC vengono scambiati lungo il canale radio criptati e integrity-protected e il traffico dati utente viene inviato criptato. Successivamente, l'eNB inizia la creazione del DRB

10), 11) [UE ← eNB] Creazione del DRB

L'eNB alloca un DRB ID per creare un DRB (cioè un EPS bearer lungo il collegamento radio) ed invia un RRC Connection Reconfiguration message all'UE dopo aver configurato i parametri QoS del DRB a partire da quelli dell'E-RAB ottenuti dall'MME. L'UE, quando riceve il messaggio, genera il DRB e il SRB2.

Una volta che il DRB è stato creato risulta attivo un uplink EPS bearer lungo tutto il percorso dall'UE al PGW che consente al flusso dati in uplink generato dall'UE di viaggiare.

12), 13), 14) & 16) [eNB → SGW] Creazione del Downlink S1 Bearer

Nello step 12), l'eNB alloca un downlink S1 TEID (S1 eNB TEID) per il bearer S1 e lo inoltra all'MME includendolo in un Initial Context Setup Response message da inviare in risposta all'Initial Context Setup Request ricevuta nello step 8). Poi nello Step 13) l'MME consegna l'S1 eNB TEID al SGW includendolo in un Modify Bearer Request message che invia al SGW. Con queste informazioni, il SGW crea un downlink S1 bearer e ne dà notizia all'MME inviando ad esso un Modify Bearer Response message nello Step 16).

La creazione del tunnel S1 GTP-U in downlink dal SGW all'eNB completa il setup del downlink EPS bearer dal PGW all'UE consentendo la consegna del traffico in downlink all'UE.

15) EPS Session Modification (UE Location Registration) (Opzionale)

Nel caso in cui la cella a cui è attualmente agganciato l'UE (ECGI) o la TA in cui si trova siano cambiate al momento in cui viene effettuata la Service Request, il SGW riporta l'evento al PGW, il quale a sua volta lo riferisce al PCRF attraverso le procedure di EPS Session Modification[10].

3.4.1.2 Network-triggered Service Request

Le figure 4 e 5 mostrano le procedure effettuare per una Service Request Network-triggered. Questa richiesta viene effettuata quando la rete ha traffico in downlink da consegnare ad un UE in Idle state- L'MME non conosce la posizione di un UE in Idle state a livello di cella, quindi deve informare l'UE che ha traffico da inviargli mediante le procedure di paging per poter poi ristabilire le risorse allocate all'E-RAB che erano state rilasciate.

[10] Durante la fase di collegamento iniziale alla rete (Initial Attach) il PCRF può fornire a MME, SGW e PGW delle "reporting policies" circa lo spostamento dell'UE mediante i parametri Change Reporting Action inclusi in un messaggio CCA

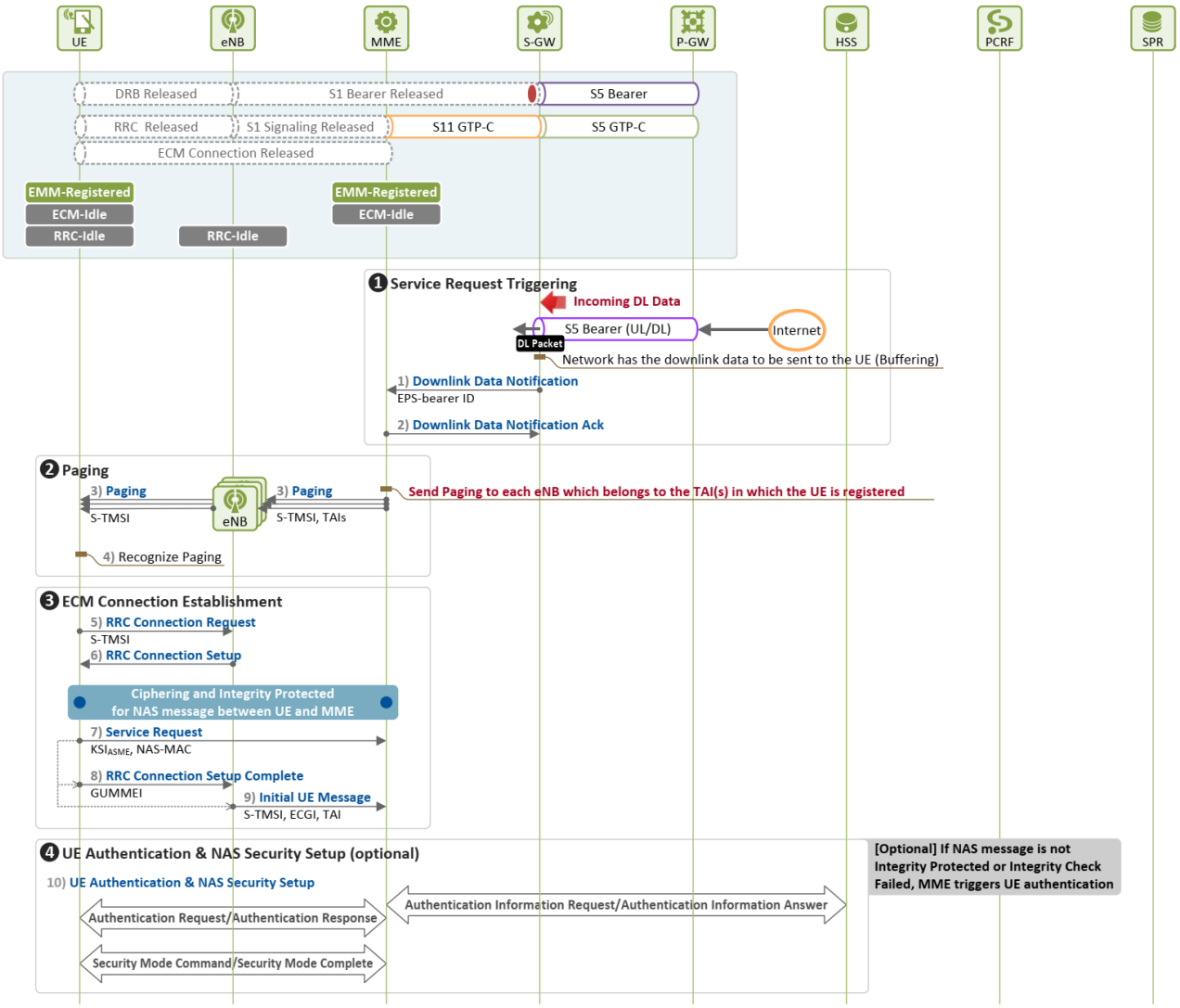


Figura 50 Procedure per la Network-triggered Service Request (1)

1 Triggering della Service Request

Il SGW riceve pacchetti dati in downlink dal PGW attraverso il bearer S5 ma non può inviarli all'eNB perché il downlink S1 bearer non è attivo (i.e. il SGW non ha un S1 eNB TEID) perciò mantiene i pacchetti in un buffer e individua l'MME a cui l'UE è registrato.

Successivamente, il SGW invia un Downlink Data Notification Message all'MME per informarlo che devono essere stabiliti la connessione di signaling e i bearer per l'UE.

2 Paging

L'MME sa che l'UE si trova in una delle sue TA ma non conosce precisamente a quale cella sia agganciato. Allora invia un messaggio di Paging a tutti gli eNB nella TA in cui l'UE è registrato. Gli eNB diffondono in broadcast il messaggio di Paging attraverso il PCH (Paging Channel) cosicché l'UE possa riceverlo durante il suo monitoraggio regolare del PCH.

❸ Creazione della connessione ECM

Quando l'UE viene a conoscenza che c'è traffico in arrivo destinato ad esso invia un Service Request message per stabilire una connessione ECM. La procedura di setup della connessione ECM inizia come sempre con un RRC Connection Request message che l'UE invia all'eNB per creare una connessione RRC (si veda il dettaglio dei messaggi illustrato in Figura 50).

❹ Autenticazione dell'UE e NAS Security Setup (Opzionale)

L'MME, quando riceve la Service Request dall'UE svolge le procedure di autenticazione e genera le NAS Security Keys (K_{NASenc}, K_{NASint}) attraverso le procedure di setup della NAS Security se il controllo di integrità sul messaggio fallisce.

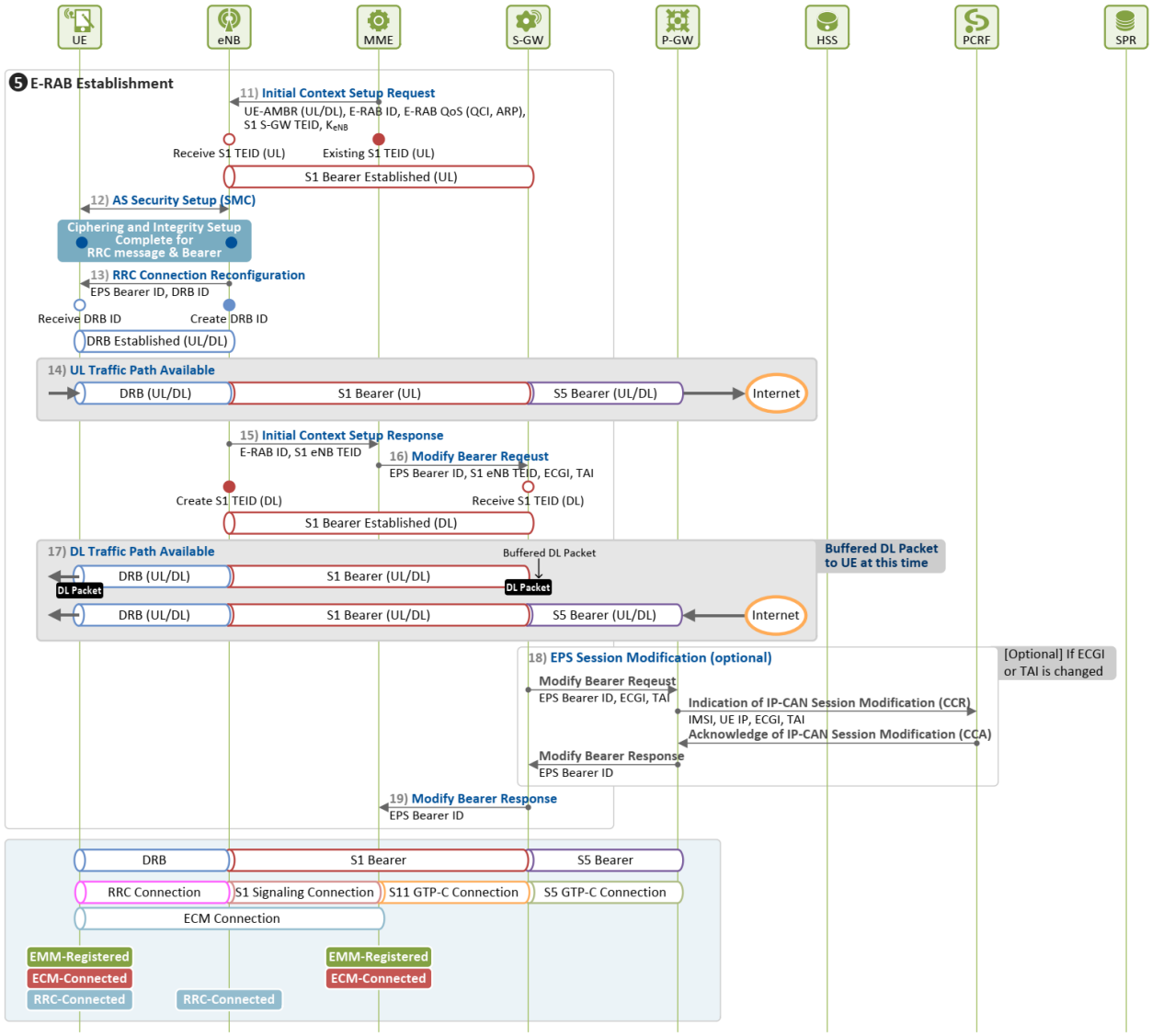


Figura 51 Procedure per la Network-triggered Service Request (2)

5 **Creazione dell'E-RAB**

Dopo aver ricevuto la Service Request dall'UE, l'MME crea un DRB e un downlink S1 bearer mediante le procedure di E-RAB Establishment già illustrate in precedenza.

3.5 TAU Periodico

3.5 Tracking Area Update Periodico

Una procedura di Tracking Area Update (TAU) viene intrapresa quando l'UE entra in una TA che non è presente nella lista di TAI allocatagli dall'MME in fase di Initial Attach o quando il TAU timer scade.

Un UE in Idle state notifica la sua posizione corrente all'MME inviando un TAU Request message quando il TAU timer scade, transitando in stato Connected per poi ritornare successivamente in stato Idle dopo aver eseguito la procedura.

3.5.1 Concetto di TAU Periodico

Un UE, mentre si trova in stato Connected ha un bearer EPS end-to-end che lo collega alla rete (PGW). L'MME tiene traccia della cella nella quale si trova l'UE, cosicché quando arriva traffico a lui destinato può inoltrarglielo immediatamente.

Quando invece un UE entra in stato Idle la connessione di signaling e i bearer (E-RAB bearer) tra l'UE e la rete (MME) vengono rilasciati. Di conseguenza, la rete perde la conoscenza della posizione dell'UE. La rete però deve sempre essere a conoscenza della posizione corrente degli UE, in qualunque stato essi si trovino (Idle o Connected) per poter inviare traffico anche a quelli che si trovano in stato Idle.

È necessario quindi, che gli UE in Idle state notifichino periodicamente alla rete (all'MME) la loro posizione (i.e. in quale Tracking Area si trovano) anche quando non hanno dati da inviare. Una TA è un gruppo di celle gestite da un MME. La posizione di un UE in Idle state è nota a livello di TA.

A tal fine, l'MME fornisce all'UE una TAI list ed un TAU timer (T3412) includendolo un un Attach Accept message, quando l'UE si collega inizialmente alla rete. Utilizzando queste informazioni, l'UE esegue un TAU quando il TAU timer scade.

Quando un MME riceve le informazioni circa la TA da un UE, aggiorna le informazioni memorizzate riguardanti l'UE (TA, cella). Nel caso in cui ci sia traffico destinato all'UE mentre quest'ultimo si trova in Idle state, l'MME informa l'UE che è presente nuovo traffico per esso inviando un Paging Message alle celle appartenenti alla TA che è stata indicata dall'UE come sua posizione corrente.

La Figura 52 mostra un esempio di procedura TAU eseguita da un UE in Idle state. L'UE (UE1) si è collegato alla Cella 2 dell'eNB 1 all'atto del suo collegamento iniziale e gli è stata assegnata una TAI list (e.g. TAI={TAI1, TAI2}) e il TAU timer (e.g. T3412 = 60 min.) attraverso il messaggio di Attach Accept inviatogli dall'MME. Successivamente, dopo essere transitato in Idle state, si sposta attraverso ❶ → ❷ → ❸ → ❹.

Ai fini di questo esempio si considera che, i) l'UE viaggi solo attraverso le TA che sono nella TAI list inizialmente allocatagli attraverso la Attach Accept message, ii) l'MME a cui l'UE riporta la sua TA è quello che mantiene l'UE context ad esso relativo e iii) sia l'UE che l'MME hanno mantenuto il NAS Security Context (K_{NASint}, K_{NASenc}, etc.) valido.

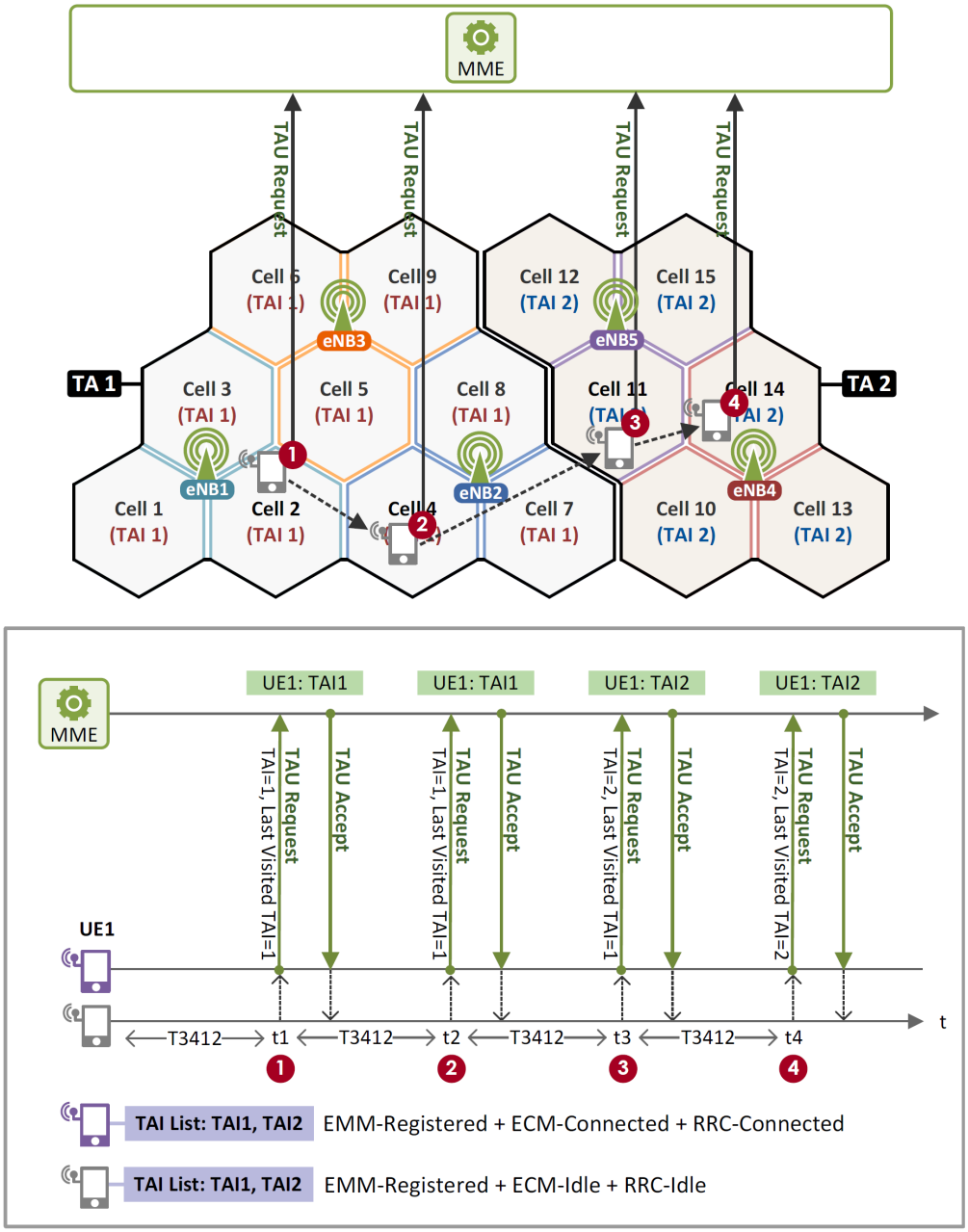


Figura 52 Concetto di TAU Periodico

Dopo essersi connesso ed essere transitato in Idle state nella Cella 2, l'UE1 si risveglia stabilendo una connessione ECM di signaling con l'MME quando il TAU timer scade al tempo t1. Dopodiché, invia all'MME un TAU Request (TAI=TAI1, Last Visited TAI=TAI1) message che include il TAI della sua cella corrente e l'ultimo TAI visitato (quello riportato attraverso l'ultima TAU request) (1). Poil'UE1 ritorna in stato Idle dopo aver ricevuto il TAU Accept message. Dopo aver ricevuto il TAU Request message dall'UE, l'MME controlla se l'ultimo TAI dell'UE (TAI dell'ultimo TAU) è cambiato oppure no ed effettua l'aggiornamento delle informazioni memorizzate, se necessario.

Se c'è traffico diretto all'UE1, e quindi il SGW notifica all'MME la presenza di traffico in DL, l'MME guarda in quale TA si trovava l'UE l'ultima volta che ha effettuato l'aggiornamento ed invia in Paging Message alle celle appartenenti a quella TA. Dopodiché se l'UE1 si sposta alla Cella 4 e il TAU timer scade, l'UE1 invia all'MME un TAU Request (TAI=TAI1, Last Visited TAI=TAI1) message con ancora TAI=TAI1 perché si trova ancora in TA1.

Se poi l'UE1 si sposta alla Cella 11 e il timer scade, invia all'MME il TAU Request (TAI=TAI2, Last Visited TAI=TAI1) message, includendo TAI2 al posto di TAI1 poiché adesso si trova nella TA2. A questo punto l'MME aggiorna di conseguenza il TAI of Last TAU dell'UE1 con TAI2.

La Figura 53 mostra le connessioni stabilite, nonché gli stati di UE ed MME nello user e nel control plane prima e dopo la procedura di TAU periodico.

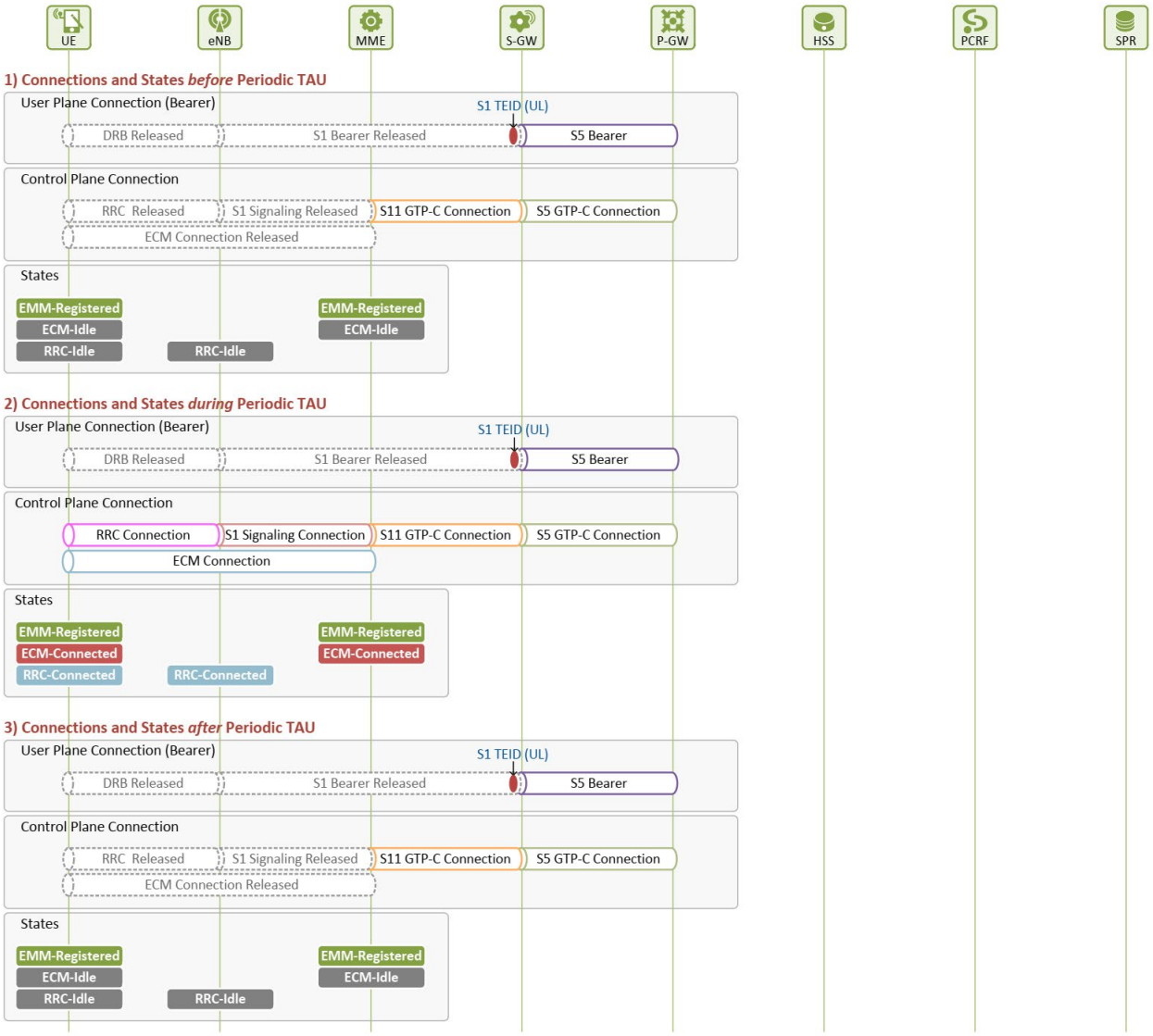


Figura 53 Connessioni e Stati prima/dopo il TAU

Gli stati di un UE prima e dopo un TAU periodico sono i seguenti:

(i) Prima della procedura, l'UE si trova in stato EMM-Registered, ECM-Idle ed RRC-Idle e le risorse allocate dalla E-UTRAN, vale a dire l'E-RAB (ad eccezione dell'UL S1 bearer) e la connessione ECM di signaling tra l'UE e l'MME, non sono presenti

(ii) Durante la procedura, l'UE si trova in stato EMM-Registered, ECM-Connected ed RRC-Connected. La procedura di TAU periodico però è differente dalla procedura di Initial Attach o Service Request poiché non viene creato l'E-RAB ma solo la connessione di signaling ECM per la consegna di messaggi NAS relativi al TAU periodico.

(iii) Dopo la procedura, la connessione di signaling ECM creata tra le due entità viene rilasciata, e l'UE ritorna in stato EMM-Registered, ECM-Idle/RRC-Idle.

La Figura 54 mostra le transizioni di stato di un UE che effettua una procedura di TAU periodico.

Alla scadenza del timer T3412, l'UE che è stato in Idle state invia all'MME una TAU Request riportando la sua TA corrente e quella precedente (e poi transita in stato Connected). Poi l'MME ritorna un TAU Accept message all'UE dopo aver aggiornato le informazioni memorizzate. Al termine dell'operazione, la connessione di signaling tra le due entità viene rilasciata e l'UE ritorna in Idle state.

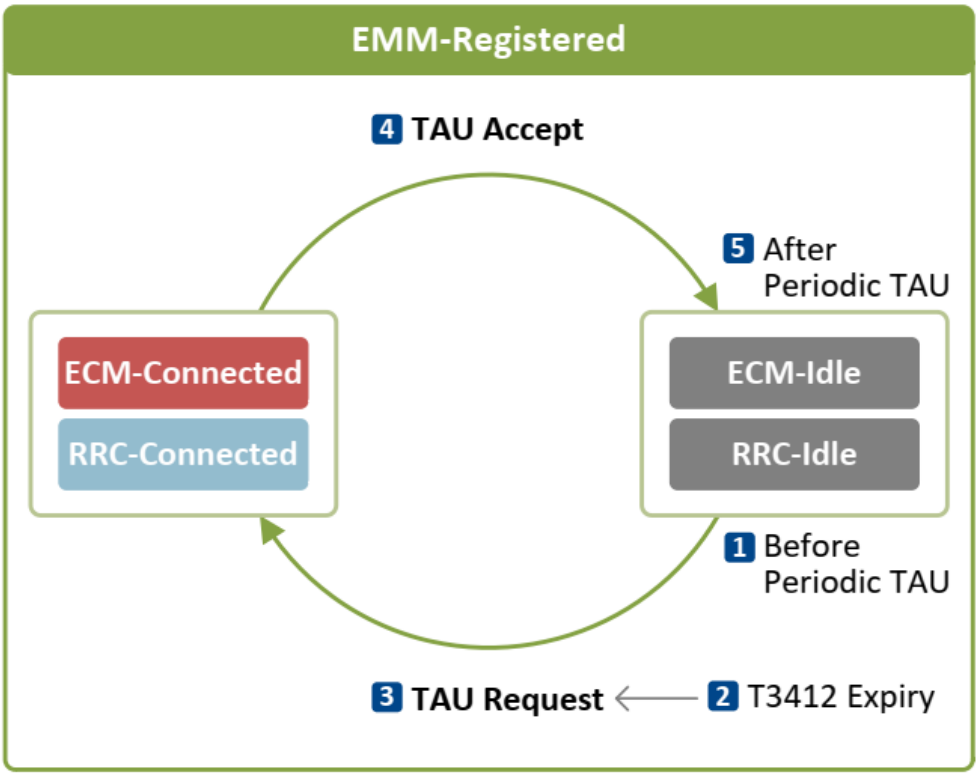


Figura 54 Transizioni di stato di un UE che effettua un TAU periodico

3.5.2 Dettaglio della procedura di TAU periodico

Le figure 4 e 5 illustrano le procedure di TAU periodico eseguite da un UE in Idle state. In Figura 55, il NAS layer dell'UE riporta la nuova TA in cui si trova l'UE all'MME inviando ad esso un TAU Request message con tipo di update indicato come "Periodic Updating"[11]. Poiché un "Periodic Updating" TAU non richiede la creazione di un EPS bearer, l'UE invia il TAU Request message dopo aver stabilito solo la connessione ECM senza eseguire le procedure di EPS Session Establishment. Quando l'UE riceve il TAU Accept message dall'MME, rilascia la ECM signaling connection. Il TAU Request message viene inviato integrity-ptotected per cui spetta all'MME decidere se eseguire

[11] Se un UE, in stato ECM/RRC-Connected si sposta agganciandosi in una cella che non si trova nella TAI list, invia un TAU Request message con update type "TA Updating"

o meno le procedure di autenticazione dell'UE e NAS Security Setup in base all'esito dei controlli di integrità sul messaggio.

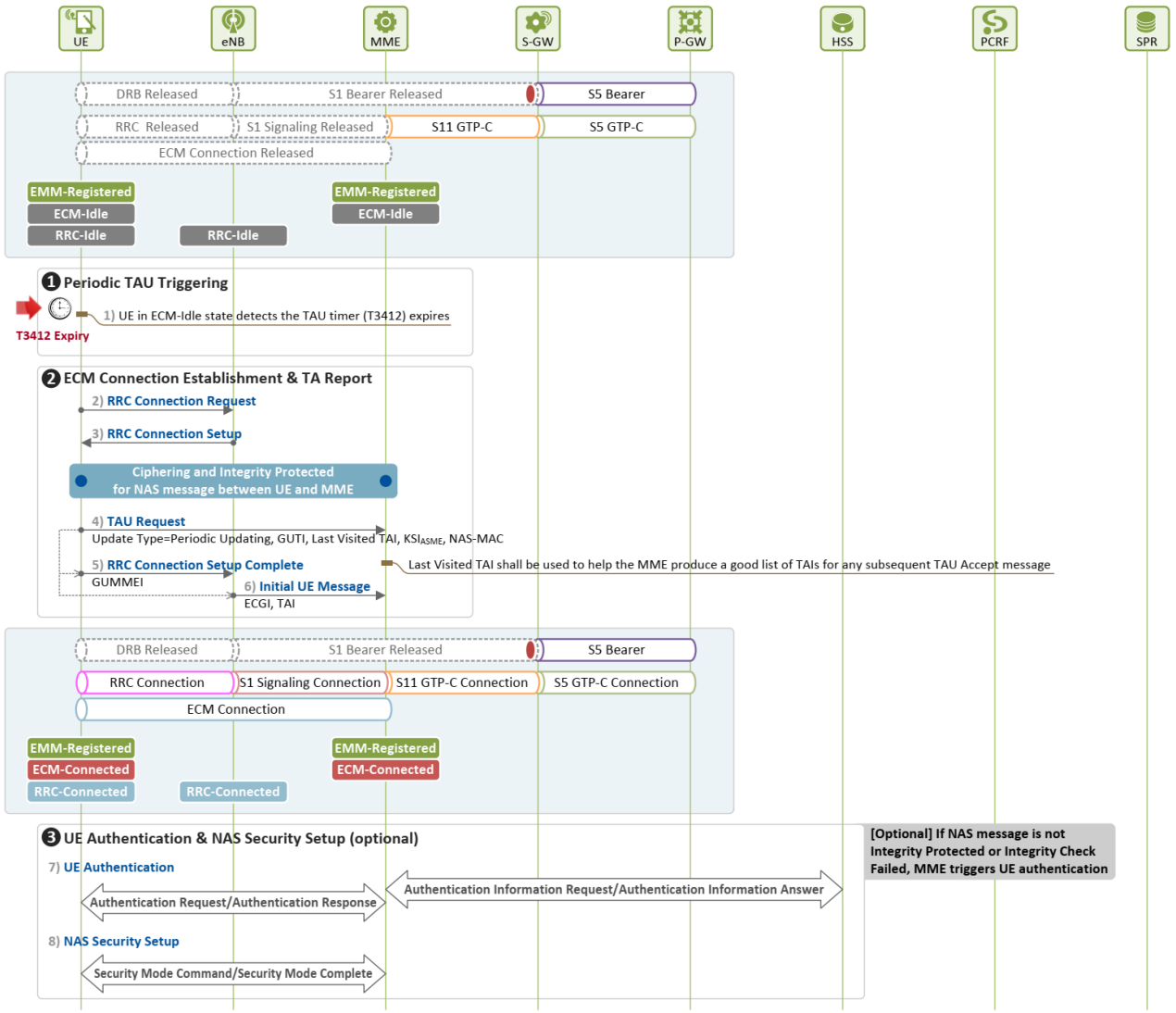


Figura 55 Procedure per il TAU Periodico (1)

1 Triggering del TAU Periodico

1) [UE] Scadenza del TAU Timer

L'UE in Idle state scatena la procedura di TAU periodico per riportare la sua posizione corrente all'MME quando il TAU Timer (T3412) scade.

2 Creazione della connessione ECM e TA Report

Il NAS layer dell'UE configura un TAU Request message e lo invia con i parametri RRC (ad es. GUMMEI) giù al layer RRC dell'UE

2), 3) [UE – eNB] Creazione della connessione RRC

Quando riceve il TAU Request message, il layer RRC dell'UE invia all'eNB un RRC Connection Request message chiedendogli di riservare risorse di signaling. L'eNB crea la

connessione RRC allocando un canale SRB ed inviando all'UE un RRC Connection Setup message

4), 5), 6) [UE → MME] Richiesta di creazione della connessione ECM e TA Report

Il TAU Request message viene inviato incluso in un RRC Connection Setup Complete message, un messaggio RRC, dall'UE all'eNB e poi incapsulato in un Initial UE Message, un messaggio S1AP, dall'eNB all'MME. Dato che il NAS Security Context è stato mantenuto valido sia nell'UE che nell'MME, il TAU Request message viene inviato integrity-protected con la NAS integrity key e criptato con la encryption key. Il messaggio di TAU Request per la procedura di TAU periodico include le seguenti informazioni:

TAU Request (Update Type = Periodic Updating, Active Flag = 0, GUTI, Last Visited TAI, KSI_{ASME}, NAS-MAC)

- **Update Type:** indica il tipo di TAU. Valorizzato a "Periodic Updating" quando la TAU Request avviene perché è scaduto il TAU Timer.
- **Active Flag:** indica quando c'è traffico dati utente in uplink o signaling da inviare. Se ce n'è, questo parametro viene impostato ad 1, causando la creazione di un EPS bearer e il mantenimento della connessione ECM anche al termine del TAU.
- **GUTI**
- **Last Visited TAI:** TAI riportato l'ultima volta in cui è stata effettuata una TAU Request (TAI in cui l'UE è stato registrato per l'ultima volta)
- **KSI_{ASME}:** indice per K_{ASME}, la NAS security base key
- **NAS-MAC:** MAC utilizzato quando il TAU Request message è integrity-protected utilizzando la NAS integrity key.

Per una consegna più rapida del TAU Request message ricevuto dal NAS layer, il layer RRC dell'UE invia all'eNB il messaggio piggybacked in un RRC Connection Setup Complete message, l'ultimo step delle procedure di setup della connessione RRC. L'RRC Connection Setup Complete message include un GUMMEI, derivato dal GUTI ricevuto dal livello NAS, che indica l'MME a cui l'UE è registrato. Poiché in generale, un eNB può essere connesso con più di una rete di un operatore e più MME, l'eNB, quando riceve l'RRC Connection Setup Complete message, controlla se l'MME indicato è connesso con esso oppure no. Nel caso in cui non lo sia si ha una variazione alla procedura che non verrà discussa.

Proseguendo, l'eNB invia il TAU Request message, includendolo in un Initial UE Message, all'MME ed alloca anche un eNB S1AP UE ID che inserisce nel messaggio. L'MME quando riceve l'Initial UE Message, alloca un MME S1AP ID, creando una connessione S1 di

signaling tra le due entità. Questa operazione conclude la creazione della ECM signaling connection tra UE ed MME e consente all'UE di transitare in stato Connected.

❸ Autenticazione dell'UE e NAS Security Setup

7) [UE – MME HSS] Autenticazione dell'UE

L'MME, quando riceve il TAU Request message dall'UE, effettua un controllo di integrità sul messaggio. Se il controllo passa, l'MME può saltare le procedure di autenticazione dell'UE e NAS Security Setup continuando ad utilizzare il NAS Security Context memorizzato per l'invio di messaggi NAS. Se invece termina con esito negativo, deve eseguire l'autenticazione dell'UE.

8) [UE – MME] NAS Security Setup

Completata la procedura di autenticazione l'UE e l'MME eseguono la procedura di NAS Security Setup per derivare, sulla base di una nuova K_{ASME}, le NAS security keys (K_{NASint}, K_{NASenc}) da utilizzare nello scambio di messaggi NAS.

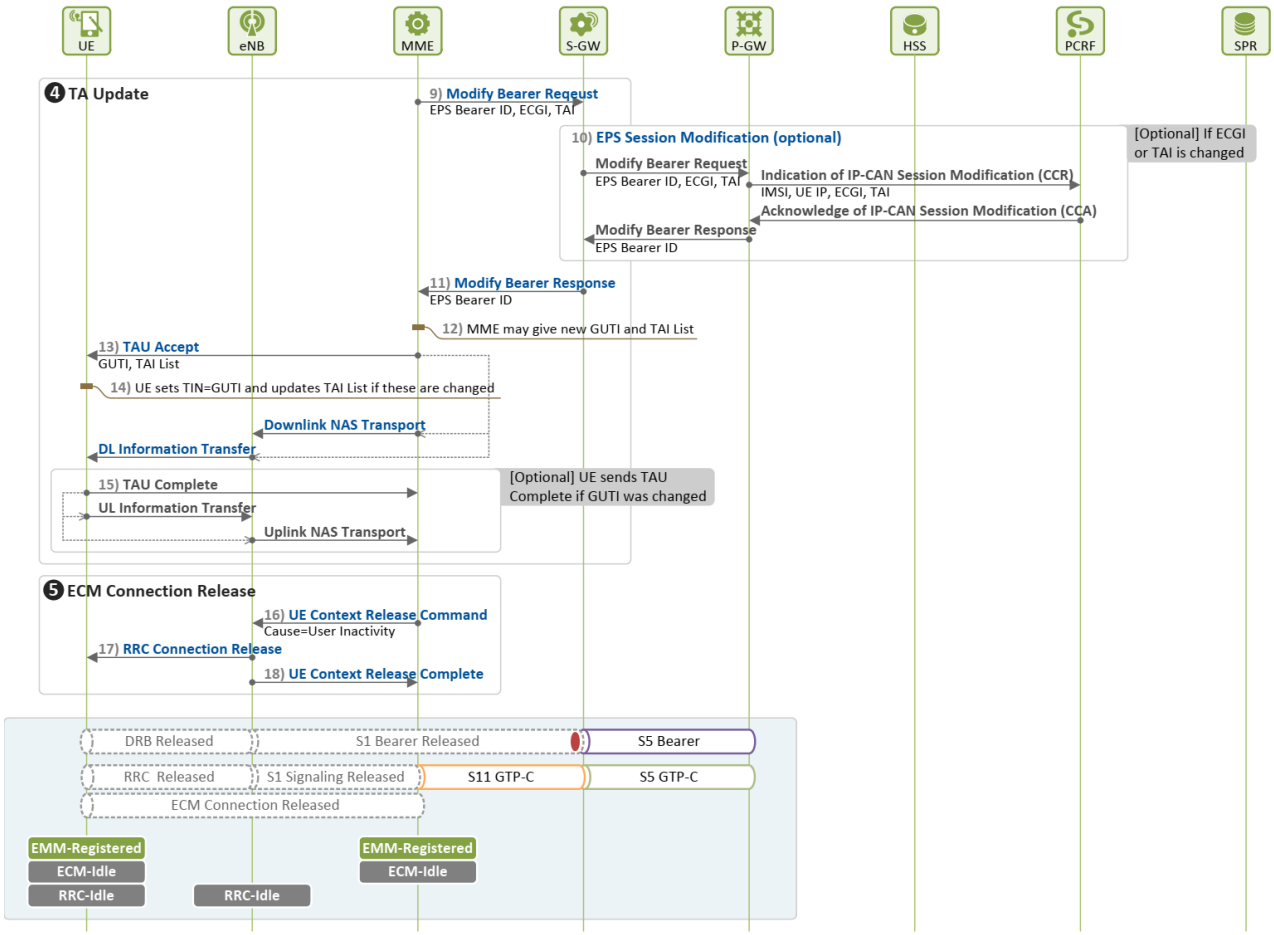


Figura 56 Procedure per il TAU Periodico (2)

4 TA Update

9) [MME → SGW] TA Update

Quando l'MME riceve la TAU Request dall'UE, resetta il TAU Timer ed invia al SGW una Modify Bearer Request inoltrandogli le informazioni sulla posizione dell'UE (ECGI, TAI).

10) EPS Session Modification (Opzionale)

Il SGW che riceve le informazioni sulla posizione dell'UE controlla se la cella (ECGI) o la TA (TAI) dell'UE sono cambiati. Se lo sono, invia una Modify Bearer Request al PGW per informarlo del cambiamento. Il PGW provvederà a riportare le stesse informazioni al PCRF mediante le procedure di EPS Session Modification

11) [MME ← SGW] Risposta alla TA Update Request

Il SGW invia all'MME una Modify Bearer Response in risposta alla Modify Bearer Request ricevuta allo Step 9)

12) [MME] Preparazione del messaggio TAU Accept

L'MME può configurare una nuova TAI list che rifletta meglio la posizione corrente dell'UE o allocare un nuovo GUTI, in base all'implementazione.

13) [UE ← MME] Invio del TAU Accept Message

L'MME invia all'UE un TAU Accept Message, integrity-protected e criptato. Questo messaggio viene inviato incapsulato in un Downlink NAS Transport message, un messaggio S1AP, dall'eNB all'MME e poi attraverso un DL Information Transfer message, un messaggio RRC, dall'UE all'eNB.

14) [UE] Aggiornamento di TIN e TAI list

Quando l'UE riceve la TAU Accept dall'MME, controlla i valori di GUTI e TAI list. Se questi sono cambiati, aggiorna il TIN (Temporary Identifier used in Next update) e la TAI list con questi nuovi valori. In questo caso per TIN si intende uno user ID che dovrà essere utilizzato la prossima volta in cui l'UE invierà un TAU Request message, e viene aggiornato col valore del GUTI incluso in un TAU Accept message ogni volta che viene ricevuto il messaggio.

15) [UE] Conferma della ricezione del nuovo GUTI

Se viene allocato un nuovo GUTI dall'MME, l'UE invia un TAU Complete message all'MME per confermare l'avvenuta ricezione del nuovo GUTI.

5 Rilascio della connessione ECM

16) [eNB ← MME] Richiesta all'E-UTRAN di cancellazione dell'UE Context

Dopo aver aggiornato le informazioni sulla posizione dell'UE, l'MME invia un UE Context

Release Command message all'eNB per far sì che questo rilasci la connessione ECM utilizzata per il TAU periodico e cancelli l'UE context memorizzato.

17) [UE ← eNB] Rilascio della connessione RRC

Quando riceve l'UE Context Release Command message dall'MME, l'eNB cancella l'UE context e rilascia tutte le risorse E-UTRAN che erano state allocate all'UE. Poi invia all'UE un RRC Connection Release message per rilasciare la connessione RRC, rilasciando quindi anche il SRB Signaling Radio Bearer) allocato all'UE.

18)[eNB → MME] Notifica della cancellazione dell'UE Context dalla E-UTRAN

L'eNB, invia un UE Context Release Complete message all'MME, segnalando che la S1 signaling connection è stata rilasciata.

Ora la connessione ECM stabilita per la consegna della TAU Request non esiste più quindi l'UE transita di nuovo in stato Idle (ECM/RRC-Idle).

3.6 Handover

3.6.1 Panoramica dell'handover LTE

Il vantaggio più grande di un device mobile rispetto ad uno fisso è che un utente può spostarsi continuando ad utilizzare i servizi. Questa mobilità ha consentito agli utenti di utilizzare i servizi che desiderano in qualunque posto essi si trovino in ogni momento in cui lo desiderano.

A causa di questo beneficio gli utenti di telefonia mobile hanno già da tempo soppiantato il numero di quelli di telefonia fissa.

Gli utenti di telefonia mobile possono usare servizi mentre si spostano grazie al fatto che le reti mobili supportano gli handover. Uno User Equipment (UE) può spostarsi da una base station/cell ad un'altra senza perdere dati in ingresso o in uscita e comunicare con la rete senza interruzioni durante questo spostamento (i.e. eseguendo un handover). Questo assicura che l'utente sia servito senza soluzione di continuità a prescindere dalla cella alla quale è connesso.

Tabella 10 Procedure eseguite durante la fase di Handover

Procedura	Direzione o Entità coinvolte	Descrizione
Measurement Configuration	eNB → UE	Specifica le misurazioni che devono essere eseguite dall'UE
Measurement Report	UE → eNB	Indica i risultati delle misurazioni eseguite

Handover Decision	eNB sorgente	Prende decisioni circa le celle target e il tipo di handover che verrà eseguito (X2-based o S1-based)
Handover Preparation	Varia a seconda del tipo di handover effettuato	Prepara il percorso di inoltro dei dati
Handover Execution		Inoltra i dati
Handover Completion		Cambia i percorsi dei dati

Un UE ha un'antenna che può cercare più canali in più bande di frequenza. Quindi dopo aver effettuato le misurazioni su più celle vicine, generalmente si collega a quella la cui potenza di segnale ricevuta è maggiore (a meno che non ci siano restrizioni dovute a politiche dell'operatore o a motivi di controllo della congestione). Dopodiché, quando il segnale ricevuto dalla cella a cui l'UE è attualmente agganciato diventa debole a causa dello spostamento dell'utente o per la presenza di oggetti che schermano la ricezione ecc., e il segnale da una cella vicina diventa sempre più potente viene iniziato un handover. Questo consente all'UE di accedere alle celle vicine e stabilire una nuova connessione con esse.

Quando un UE stabilisce una connessione RRC con un eNB, quest'ultimo lo informa in occasione di quali eventi debba essere riportata la potenza del segnale ricevuto, inviando un messaggio di configurazione (RRC Connection Reconfiguration Message). L'UE tiene traccia della potenza del segnale ricevuto sia della serving cell attuale che delle celle vicine. Quando si verifica uno degli eventi specificati, riporta la potenza di segnale ricevuta all'eNB attraverso un messaggio detto Measurement Report. L'eNB all'atto della ricezione del messaggio decide se iniziare un handover, tenendo in conto sia la potenza del segnale riportata dall'UE che il carico già presente sulle celle vicine. Giunto ad una decisione, esegue un handover alla target cell selezionata.

3.6.1.1 Misurazione del segnale

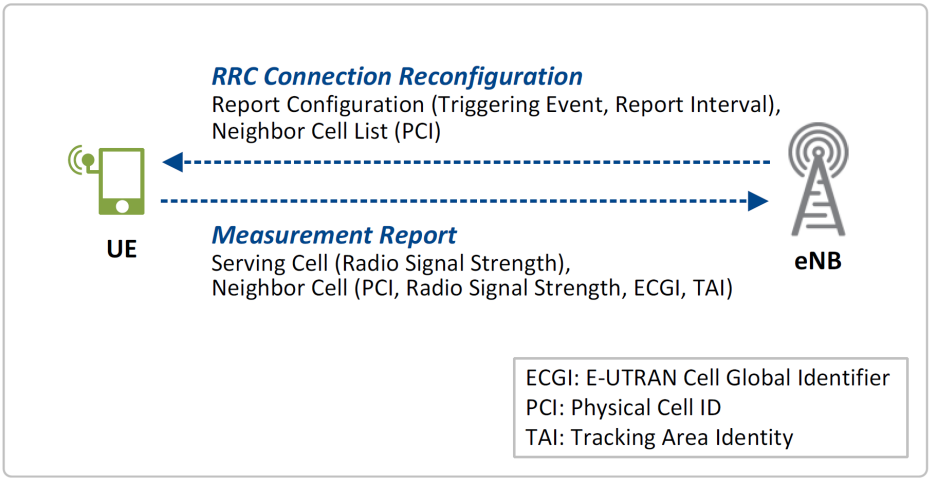


Figura 57 Visione semplificata dei messaggi di Measurement Configuration e Measurement Report

In figura è mostrata un'illustrazione semplificata dei messaggi di Measurement Configuration e Measurement Report usato dall'UE.

1) **Measurement Configuration**

   La measurement configuration è fornita dall'eNB all'UE ed indica quali informazioni devono essere riportate. L'eNB fornisce la measurement configuration all'UE per mezzo di un RRC Configuration Message quando stabilisce una connessione RRC con l'UE. Nel messaggio sono incluse le seguenti informazioni:

   - **Measurement Object**: fornisce informazioni circa le celle da misurare all'UE includendo il numero di canale, il Physical Cell ID (PCI) delle celle da misurare, il cell ID delle celle in blacklist, i valori di offset per ogni cella ecc.
   - **Reporting configuration**: specifica gli eventi scatenanti che richiedono all'UE di inviare un Measurement Report alla rete (Triggering event)
   - **Measurement ID**: ID che identifica i measurement objects
   - **Quantity configuration**: indica i valori che devono essere misurato dall'UE. Questi valori generalmente sono il Reference Signal Received Power (RSSI) ed il Received Signaling Strength Indicator (RSSI).
   - **Measurement Gap**: indica a quale intervallo le celle vicine devono essere misurate dall'UE.

Comunque sia, in caso di misurazione delle celle vicine intra-frequenza (i.e. se la cella vicina non usa la stessa frequenza della serving cell), l'UE dovrebbe dapprima sincronizzarsi sulla frequenza della cella vicina e poi misurare la potenza del segnale ricevuto usando i measurement gaps durante il periodo di inattività in DL/UL.

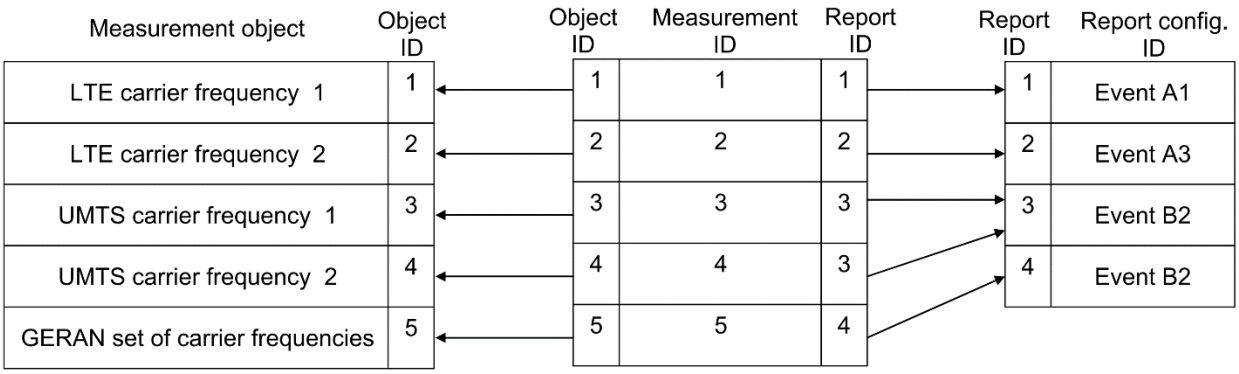


Figura 58 Esempio di measurement configuration

2) Measurement Report Triggering

L'UE misura la potenza del segnale della serving cell e delle neigbor cells. Successivamente, riporta i risultati ottenuti all'eNB periodicamente o quando un measurment event è scatenato dal soddisfacimento di uno dei reporting criteria configurato in fase di Measurement Configuration.

Event Type	Description
Event A1	Serving becomes better than threshold
Event A2	Serving becomes worse than threshold
Event A3	Neighbour becomes offset better than serving
Event A4	Neighbour becomes better than threshold
Event A5	Serving becomes worse than threshold1 and neighbour becomes better than threshold2
Event A6	Neighbour become offset better than S Cell (This event is introduced in Release 10 for CA)

Tabella 11 Tipi di eventi che possono scatenare un Measurement Report

Un Measurement Report è scatenato quando il valore misurato oltrepassa (diventa maggiore o minore) di un certo valore target. Il valore target può essere inteso come una soglia che è una sorta di valore assoluto oppure come offset che è un valore relativo in riferimento ad un altro, ad esempio il valore della serving cell.

Nella realtà però il valore misurato può fluttuare abbastanza frequentemente a causa di un errore di misurazione da parte del modem dell'UE oppure a volte a causa di fluttuazioni del canale radio stesso. Nella maggior parte dai casi, la rete non è interessata a fluttuazioni così piccole e non vuole ricevere troppi measurement reports. Al fine di prevenire questo genere di measurement report troppo frequenti causati da un piccolo range di variazioni è stato introdotto il parametro di "Isteresi".

Caso 1: Isteresi = 0

Il valore misurato fluttua attorno al valore target causando molti measurement report non necessari

Caso 2: Isteresi != 0

Sebbene il valore misurato fluttui attorno al target non scatena un measurement report a meno che non fluttui più ampiamente dell'isteresi (in rosa)

Evento A3

L'evento A3 è un evento che comunemente provoca un handover.

Quando la potenza del segnale di una cella vicina (M_{Nbr}) diventa maggiore di quella della serving cell attuale (M_{Ser}), tenendo conto dell'isteresi, e la differenza è più grande del valore di un offset stabilito (Off) l'evento A3 viene scatenato e l'UE riporta i risultati della misurazione all'eNB. L'isteresi (Hys) come detto in precedenza indica un certo valore di margine tra la serving cell e la target cell. L'eNB decide di eseguire l'handover se l'evento A3 è stato scatenato e le condizioni scatenanti durano per un tempo superiore al periodo di Time To Trigger specificato.

- **Event A3 Entering Condition:** $M_{Nbr} - Hys > M_{Ser} + Off$
- **Event A3 Leaving Condition:** $M_{Nbr} + Hys < M_{Ser} + Off$

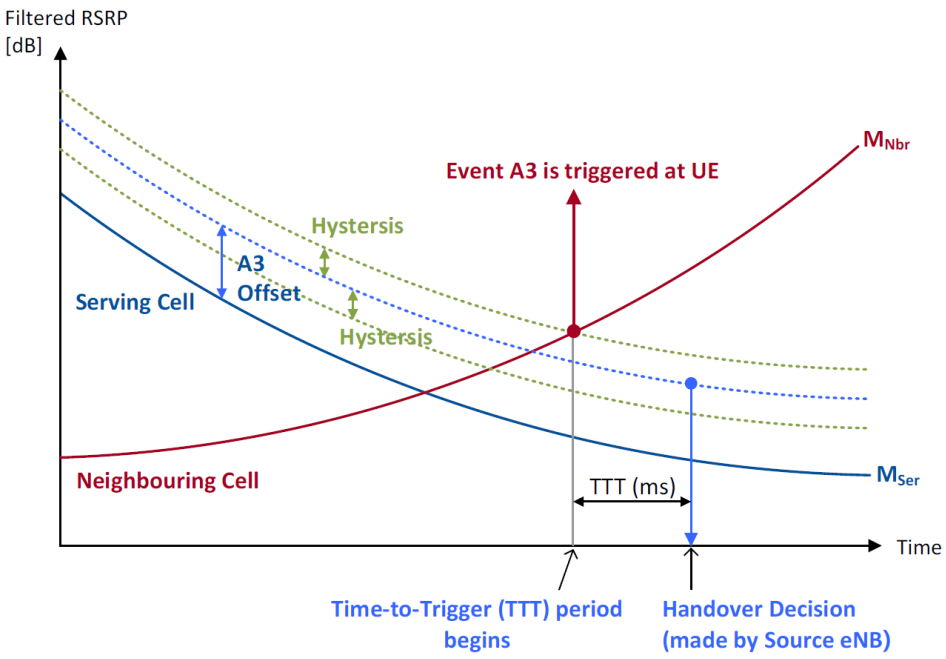


Figura 59 Measurement event A3

3.6.1.2 Decisione di effettuare l'handover

Quando l'evento A3 viene riportato, l'eNB decide quale tipo di handover eseguire e verso quale cella target eseguirlo dopodiché inizia la procedura. Gli handover possono essere categorizzati in più tipologie differenti, ma in generale vengono suddivisi secondo due categorizzazioni principali:

(1) <u>Prima categorizzazione:</u> a seconda che le entità della EPC siano cambiate o meno dopo l'handover

Un handover può essere categorizzato in una delle tre tipologie – intra-LTE, inter-LTE e inter-RAT handovers – a seconda del fatto che le entità della EPC alle quali l'UE è connessa siano cambiate dopo l'handover o meno.

- **Intra-LTE handover**
  - **Intra-MME/SGW handover**: Né il serving MME né il SGW vengono cambiati dopo l'handover
- **Inter-LTE handover**: Il serving MME e/o il SGW vengono cambiati dopo l'handover
  - **Inter-MME handover**: il serving MME viene cambiato ma il SGW rimane lo stesso dopo l'handover
  - **Inter-SGW handover**: Il SGW dell'UE viene cambiato ma l'MME rimane lo stesso dopo l'handover
  - **Inter-MME/SGW handover**: sia il serving MME che il SGW sono cambiati dopo l'handover
- **Inter-RAT handover**: Handover tra reti che usano tecnologie di accesso radio differenti
  - **UTRAN ad E-UTRAN**
  - **E-UTRAN ad UTRAN, ecc.**

(2) <u>Seconda categorizzazione:</u> A seconda che le entità dell'EPC siano coinvolte o meno nell'handover

A seconda che le entità della EPC siano coinvolte o meno nella preparazione ed esecuzione dell'handover tra un source eNB e un target eNB, un handover LTE può essere un handover X2-based se eseguito utilizzando l'interfaccia X2 che interconnette direttamente gli eNB tra loro oppure eseguendo l'handover S1 based su interfaccia S1 (che coinvolge la EPC).

La Figura 60 illustra un esempio dei due tipi di handover eseguiti mentre l'UE si sposta.

La Figura 61 mostra invece come un source eNB sceglie quale tipo di handover effettuare, X2 o S1, quando un handover viene scatenato.

X2 Handover

L'interfaccia X2 connette due eNB tra loro. Se c'è una connessione X2 tra l'eNB sorgente e l'eNB target e tale connessione è disponibile per l'handover, l'handover X2 viene iniziato e l'intera gestione dello stesso avviene senza l'intervento della EPC (MME)

S1 Handover

L'interfaccia S1 connette E-UTRAN (eNB) ed EPC (i.e. MME per messaggi del control plane o SGW per i pacchetti utente).

Se non c'è connettività X2 tra un source eNB ed un target eNB, oppure c'è connettività X2 tra l'eNB sorgente e l'eNB target ma l'handover X2 non è permesso, oppure ancora La preparazione dell'handover tra una serving cell e una target cell fallisce, allora viene tentato un handover S1.

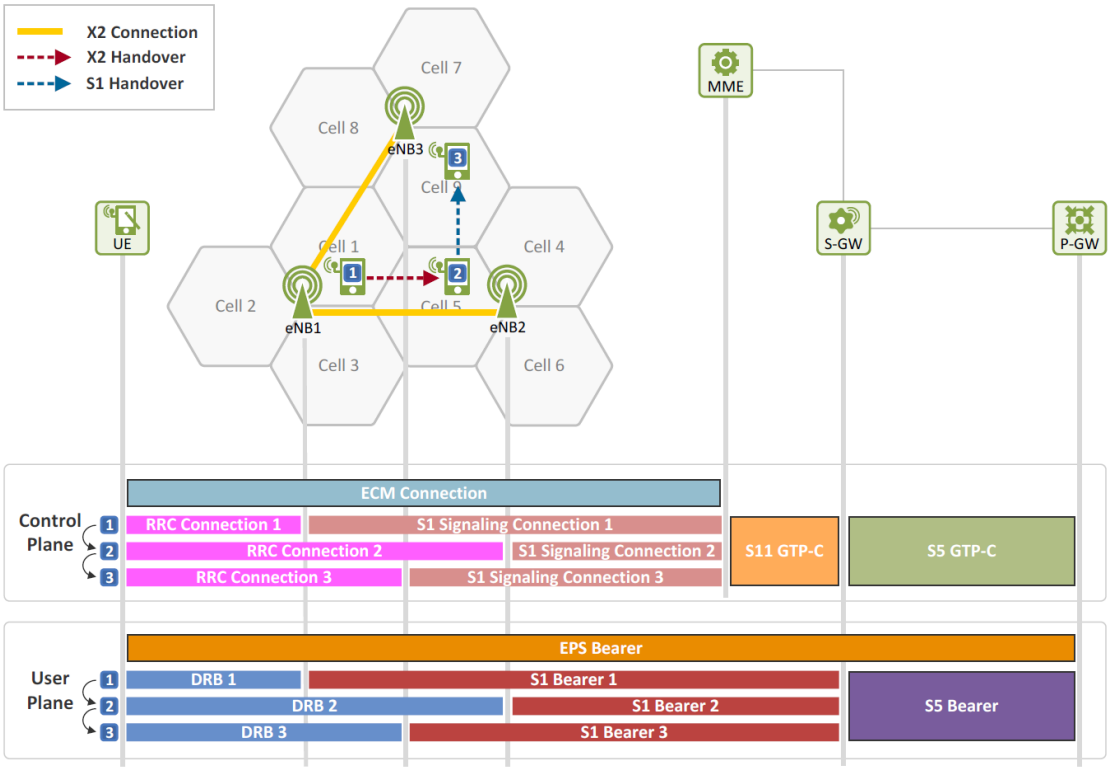


Figura 60 Esempi di Handover su interfacce X2 ed S1

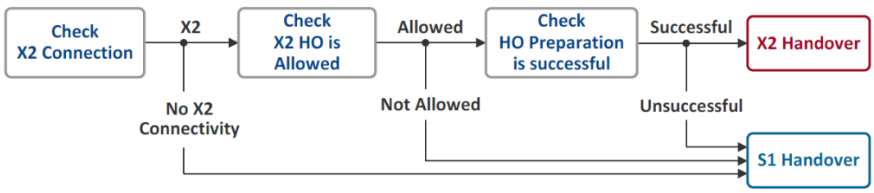


Figura 61 Decisione sul tipo di Handover da eseguire

3.6.1.3 Fasi di una procedura di Handover

Sulla base della measurement configuration ricevuta, l'UE riporta i risultati ottenuti all'eNB che sulla base di essi decide se iniziare l'handover. La procedura di handover consta di tre fasi.

1) **Preparazione dell'handover**

   Durante questa fase, un source eNB ed un target eNB si preparano per l'handover. In caso di handover X2-based, i due eNB comunicano direttamente tra loro attraverso signaling sull'interfaccia X2 e portano a termine l'handover senza l'intervento dell'MME. Al contrario se si tratta di S1 handover, l'MME viene coinvolto attraverso signaling sull'interfaccia S1 per la gestione dell'handover.

   Il source eNB invia l'UE context dell'utente (i.e. security context, QoS context ecc.) al target eNB per controllare se quest'ultimo è in grado di soddisfare i requisiti in termini di qualità di servizio richiesta. Se così è, il target eNB costruisce un bearer in downlink (DL packet forwarding bearer) per l'inoltro dei pacchetti. Dopodiché alloca il C-RNTI che l'UE deve utilizzare quando accede al target eNB e lo inoltra al source eNB.

   Questo completa la fase di preparazione dell'handover. A questo punto il DL packet forwarding bearer è un tunnel diretto che connette i due eNB tra loro nel caso di X2 handover oppure un tunnel indiretto che connette tutte e tre le entità coinvolte, cioè il source eNB, il SGW e il target eNB, in caso di S1 handover.

   La Figura 62 mostra i percorsi di inoltro dei pacchetti durante questa fase:

   - bearer UL/DL di trasporto del traffico (linea continua a doppio senso),
   - percorso di trasporto dei messaggi di controllo (linea tratteggiata)
   - percorso di DL packet forwarding (linea continua a senso unico).

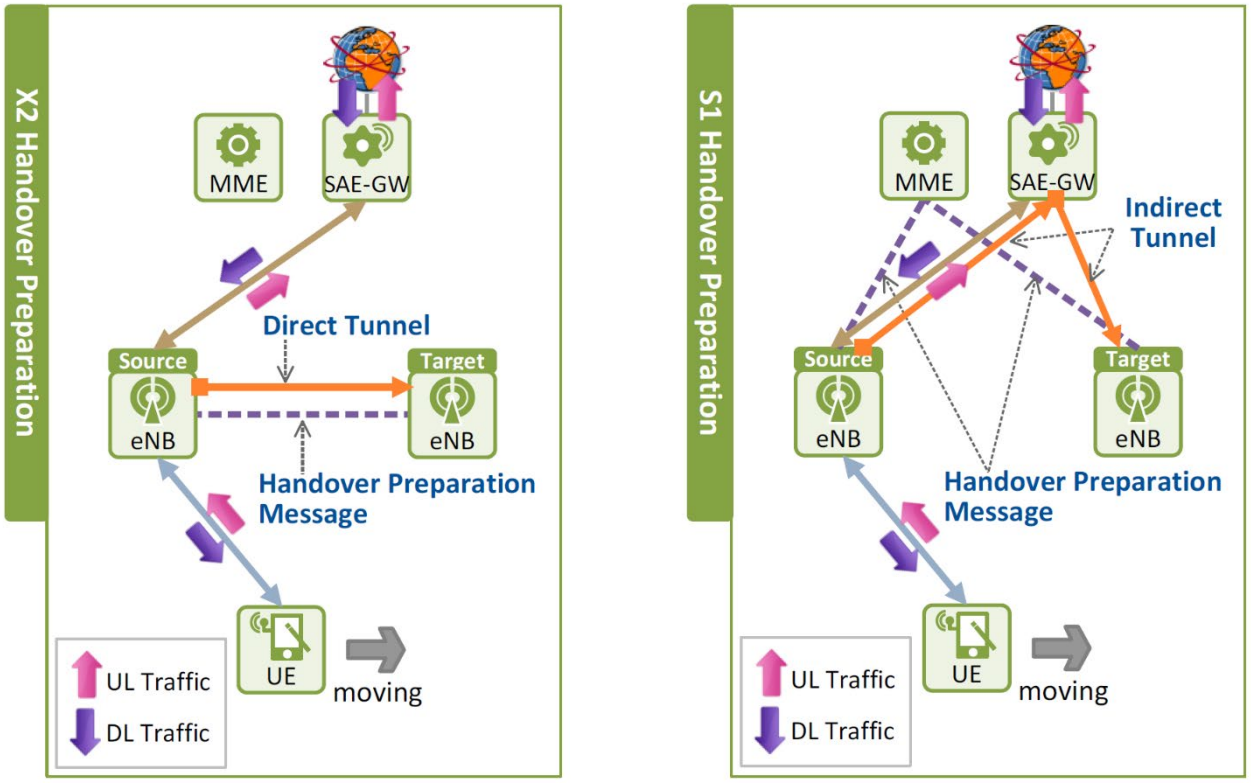


Figura 62 Fase di preparazione dell'handover

2) Esecuzione dell'handover

Durante questa fase viene portato a termine l'handover. L'UE si disconnette dall'eNB sorgente, e si connette al target eNB, accedendo ad una nuova cella. Una volta che le risorse necessarie per l'inoltro sono state allocate tra i due eNB (i.e. un DL packet forwarding bearer) e le nuove risorse per l'UE sono state allocate nel target eNB (i.e. un DRB, DL S1 bearer, C-RNTI ecc.) durante la fase di preparazione, i due eNB sono pronti per l'handover.

Il source eNB ordina quindi all'UE di effettuare un handover inviandogli un Handover Command message.

Durante la fase di esecuzione dell'handover, l'UE usa il C-RNTI che era stato allocato dal target eNB nella fase di preparazione. Questo gli consente di accedere al target eNB più velocemente. Quando i pacchetti in DL arrivano al source eNB vengono inoltrati al target eNB attraverso il DL forwarding bearer e bufferizzati li finché l'UE non ha completato l'accesso al target eNB. Questo meccanismo assicura che nessun pacchetto vada perso lungo il tragitto. I pacchetti in UL in arrivo dall'UE, invece, non vengono inoltrati finché l'UE non ha acceduto al target eNB con successo.

Quando l'UE avrà completato l'accesso radio al target eNB, i pacchetti in UL potranno essere immediatamente inoltrati al SGW tramite il target eNB.

La Figura 63 mostra il percorso di consegna dei pacchetti in DL durante la fase di esecuzione dell'handover e il percorso di consegna dei pacchetti in UL attraverso il target eNB dopo la fase di esecuzione dell'handover.

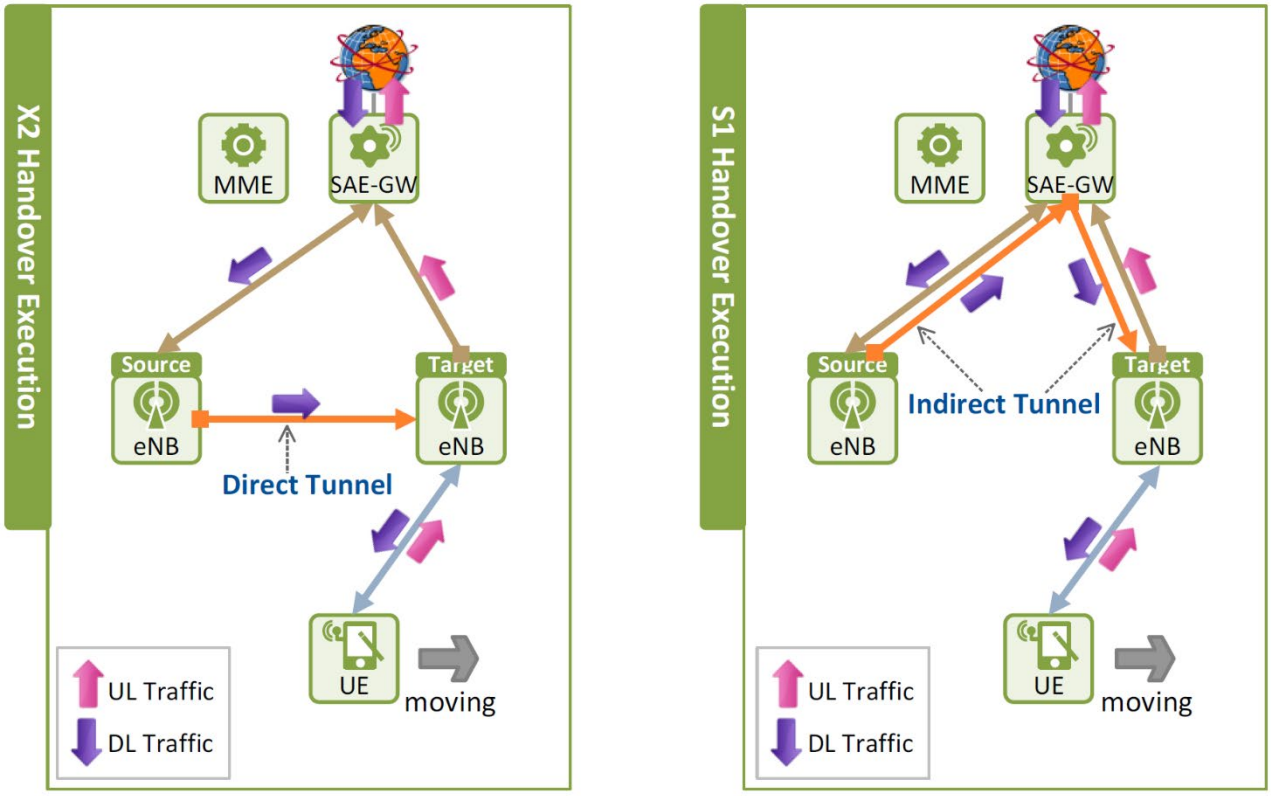


Figura 63 Fase di esecuzione dell'handover

3) Completamento dell'handover

Una volta che l'UE ha completato con successo l'accesso al target eNB, il DL S1 bearer è connesso al target eNB invece che al source eNB. Una volta che il percorso è stato cambiato, il forwarding bearer utilizzato per inoltrare i pacchetti in DL durante la fase di esecuzione dell'handover è rilasciato.

La Figura 64 mostra come il traffico (sia in DL che in UL) viene instradato lungo il nuovo percorso dei bearer dopo la fine della fase di completamento dell'handover

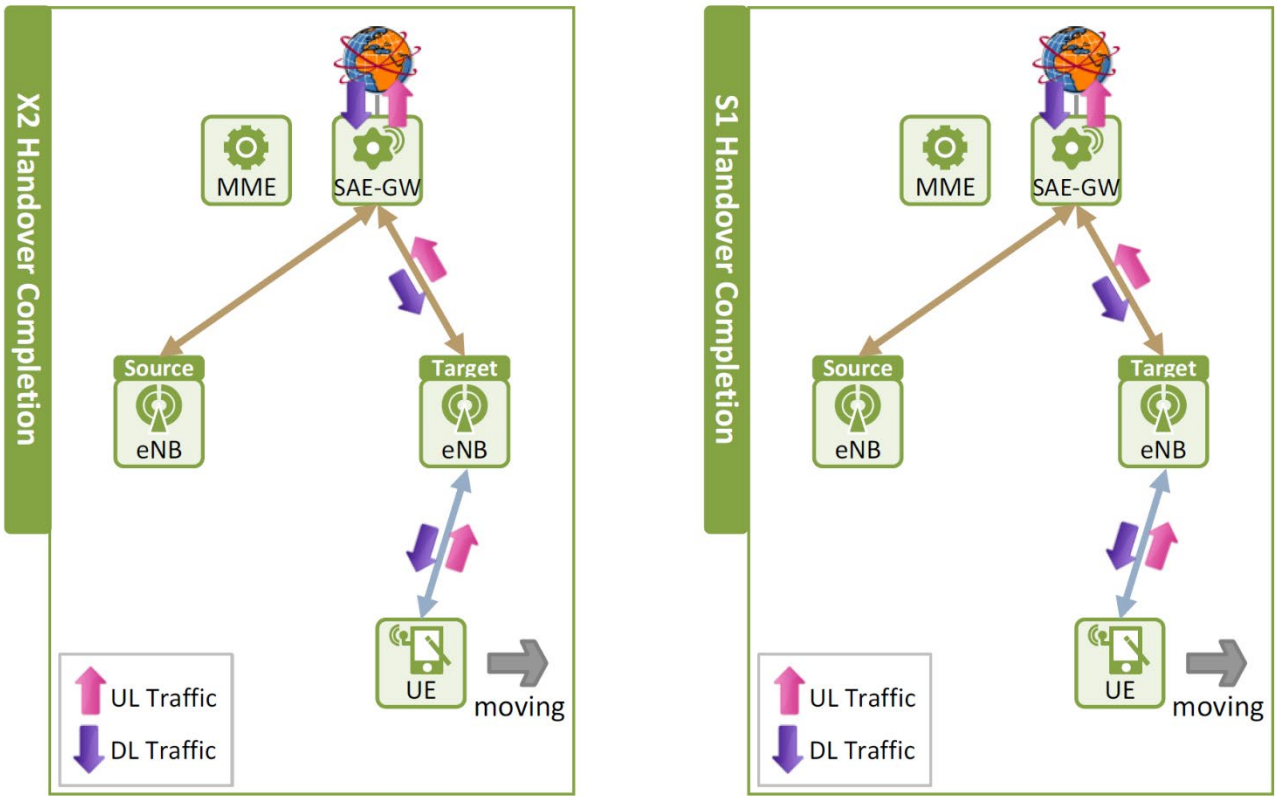


Figura 64 Fase di completamento dell'handover

3.6.1.4 Handover Interruption Time

Durante la fase di preparazione dell'handover, le entità della rete allocano risorse in anticipo per assicurare che nessun pacchetto in DL sia perso mentre l'handover viene eseguito. Comunque sia, in handover reali, un periodo di interruzione è inevitabile. Durante questo periodo, cioè tra il tempo in cui l'UE si disconnette dal source eNB e prima che si riconnetta completamente al target eNB, i pacchetti non possono essere consegnati tra l'UE e le celle. Se questa interruzione dura troppo a lungo, la continuità di servizio non può più essere garantita e gli utenti potrebbero riscontrare una bassa qualità di servizio.

1. time required for DL synchronization to the target eNB
2. RACH waiting time
3. time required for sending dedicated RACH preamble to request UL resources
4. time required for detecting preamble from the target eNB and processing the same
5. time required for preparing a RACH Response message
6. time required for decoding the RACH Response message
7. time required for informing the UE has completed a handover to the target eNB
8. time required for obtaining the target eNB's confirmation on the completed handover

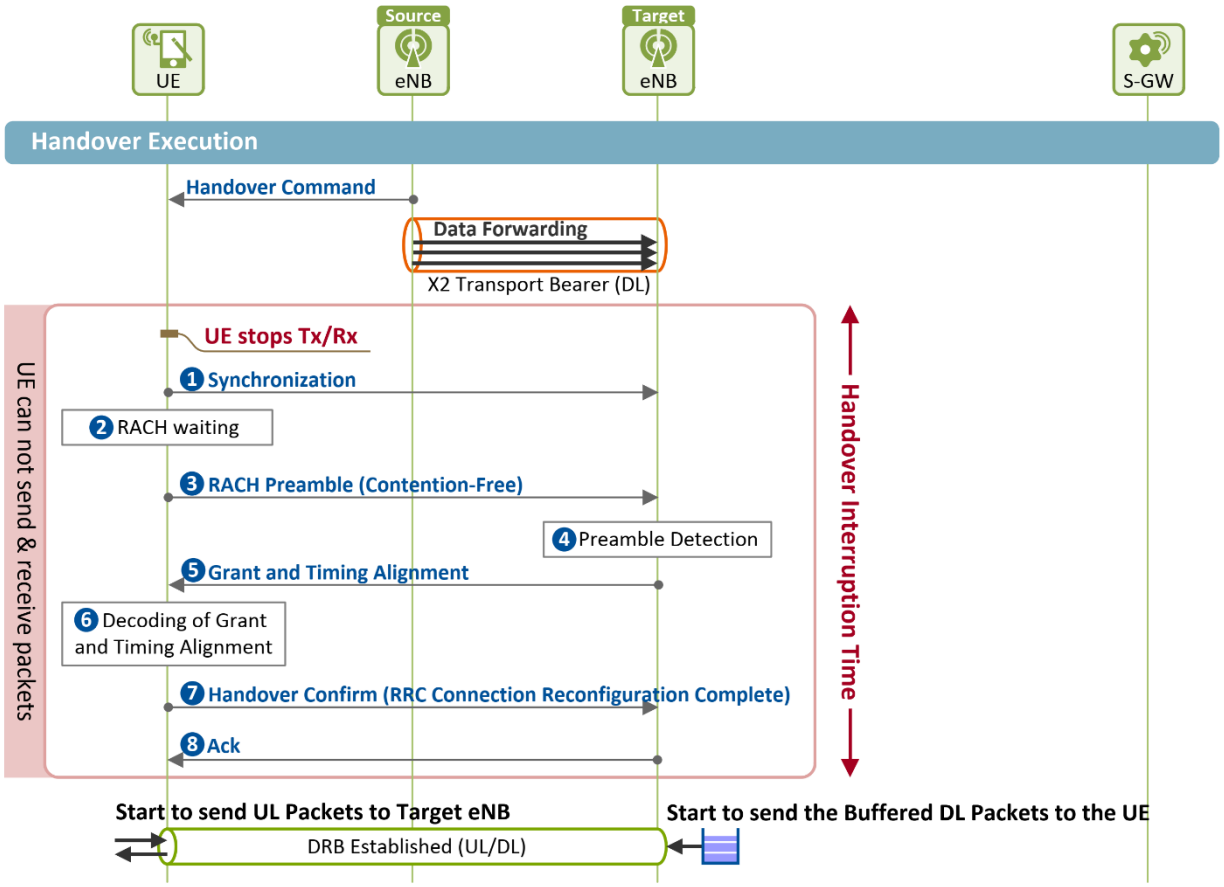


Figura 65 Handover Interruption Time

3.6.2 Handover X2 senza TAU

3.6.2.1 X2 Protocol Stacks

L'X2 handover è eseguito tra un source eNB ed un target eNB attraverso l'interfaccia X2. Nelle reti LTE i due eNB possono comunicare tra loro attraverso l'interfaccia X2, il che differenzia questa rete dalle generazioni precedenti (2G e 3G) in cui l'unico modo che un eNB aveva per conoscere lo stato

degli eNB vicini era interpellando la core network. Comunque sia, oggi le reti LTE permettono agli eNB di scambiare direttamente informazioni di stato tra loro attraverso l'interfaccia X2 e di eseguire in maniera indipendente l'handover senza l'intervento di nodi della EPC.

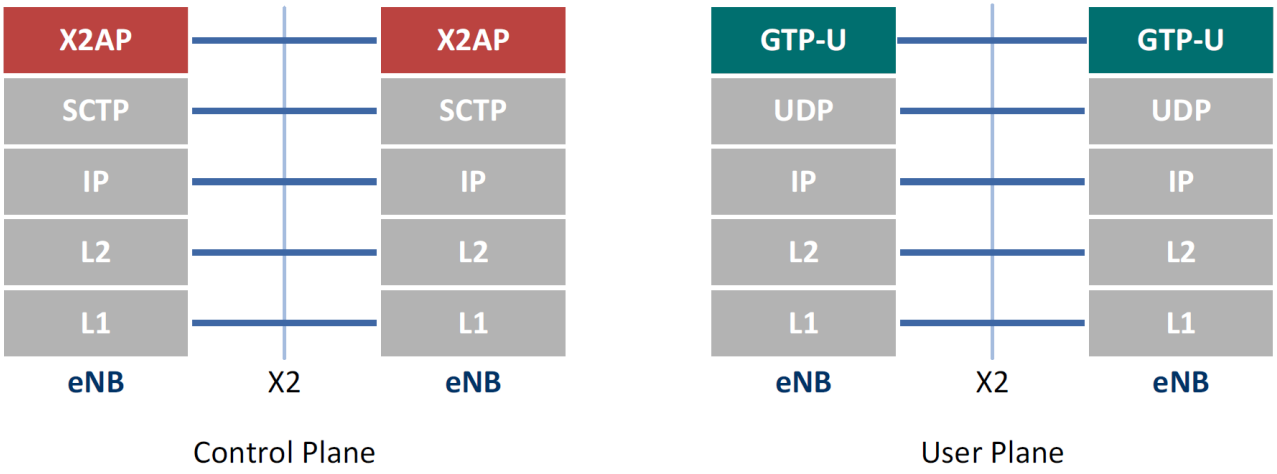


Figura 66 Protocol stacks su interfaccia X2

Nel control plane, due eNB servono più utenti attraverso il signaling con protocollo X2AP che avviene lungo una singola connessione Stream Control Transmission Protocol (SCTP). Nel layer X2AP, gli utenti sono identificati per mezzo di una coppia di eNB UE X2AP ID (Old eNB UE X2AP ID, New eNB UE X2AP ID)[12]. Nel data plane i due eNB sono connessi da un tunnel GTP, come nel bearer S1/S5. Viene generato un tunnel GTP per ogni utente, ed ogni utente è identificato dai Tunnel Endpoint Identifiers (TEID) allocati. Nel caso in cui un UE abbia più bearer attivi viene generato un tunnel GTP per ogni bearer, ma questo caso non verrà trattato nel prosieguo.

3.6.2.2 Messaggi X2AP relativi alla funzione di Mobility Management

La Tabella 12 mostra i messaggi X2AP utilizzati durante l'X2 handover:

- **Handover Request** message: Questo messaggio è usato in fase di preparazione dell'handover: viene inviato da un source eNB ad un target eNB ed include l'UE context di un utente
- **Handover Request Acknowledge** message: Questo messaggio è utilizzato durante la fase di preparazione dell'handover. Viene inviato dal target eNB al source eNB se l'allocazione di risorse è stata completata correttamente nel target eNB.

[12] Old eNB UE X2AP ID viene allocato da un source eNB mentre New eNB X2AP ID viene allocato da un target eNB

- **Handover Preparation Failure** message: Questo messaggio è utilizzato durante la fase di preparazione dell'handover. Viene inviato dal target eNB al source eNB se l'allocazione delle risorse nel target eNB fallisce.
- **SN Status Transfer** message: Questo messaggio viene utilizzato durante la fase di esecuzione dell'handover. Il source eNB lo invia al target eNB per indicargli da quale pacchetto dovrebbe iniziare ad inviare o ricevere
- **UE Context Release** message: Questo messaggio viene utilizzato durante la fase di completamento dell'handover. Il target eNB lo invia al source eNB per informarlo che può eliminare l'UE context memorizzato.
- **Handover Cancel** message: Questo messaggio viene utilizzato durante la fase di preparazione dell'handover dal target eNB al source eNB quando per qualche motivo, deve richiedere l'interruzione della procedura di handover in corso.

Procedura	**Messaggio iniziale**	**Messaggio di risposta**	
		Successo	**Insuccesso**
Handover Preparation	**Handover Request**	**Handover Request Acknowledge**	**Handover Preparation Failure**
SN Status Transfer	**SN Status Transfer**	**-**	**-**
UE Context Release	**UE Context Release**	**-**	**-**
Handover Cancel	**Handover Cancel**	**-**	**-**

Tabella 12 Messaggi X2AP per la funzione di Mobility Management

3.6.2.3 Panoramica della procedura di X2 Handover

La Figura 67, illustra in maniera semplificata ciò che avviene prima, durante (le fasi di preparazione, esecuzione e completamento) e dopo l'X2 handover.

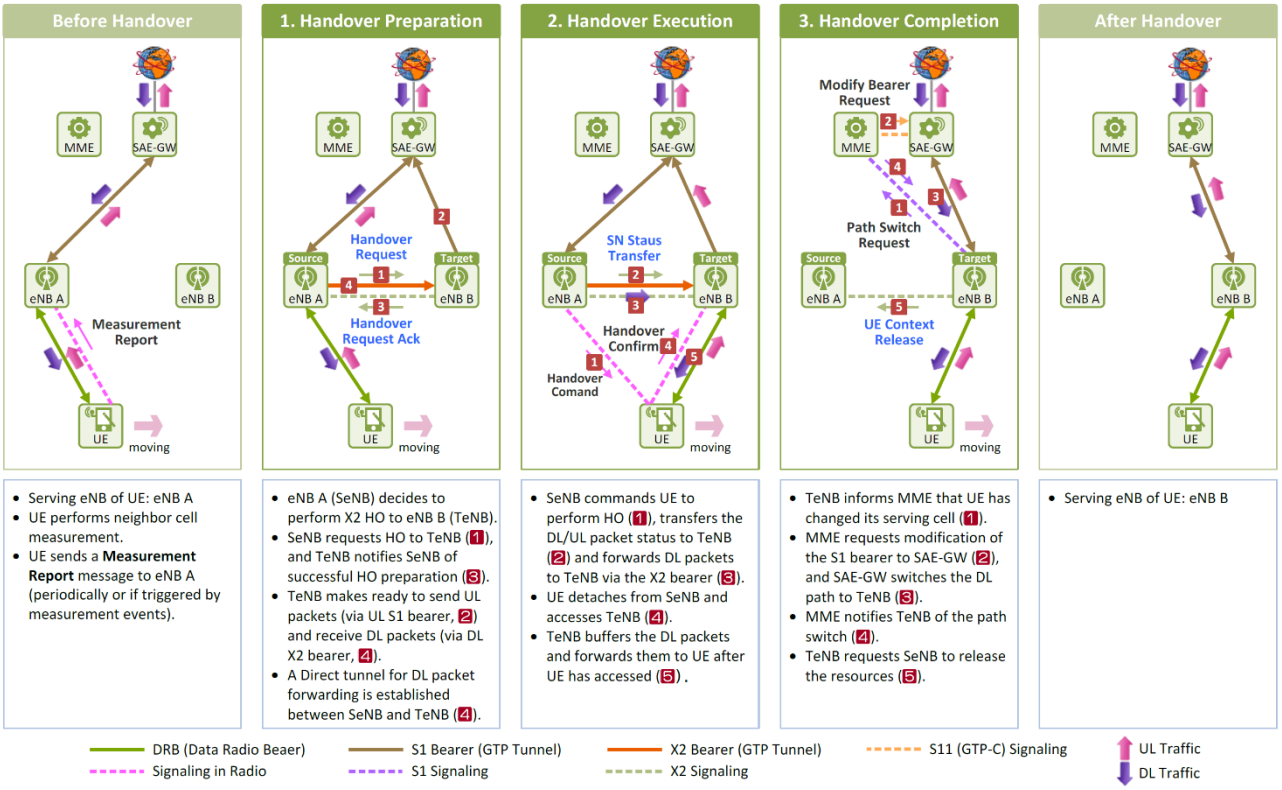


Figura 67 Procedura semplificata di X2 Handover

▪ **Prima dell'Handover X2**

Nella Figura 67, prima dell'handover l'UE è servito dall'eNB A (o per meglio dire da una serving cell appartenente all'eNB A) al quale è connesso. Quando l'UE rileva un measurement event, invia un Measurement Report message all'eNB A.

▪ **Preparazione dell'handover X2**

Il source eNB (eNB A nella Figura 67) sceglie un target eNB (eNB B nella Figura 67) verso il quale effettuare l'handover, sulla base delle informazioni delle celle vicine di cui è a conoscenza e delle informazioni sulla potenza del segnale delle stesse incluse nel Measurement Report. Dopodiché, prepara un X2 handover col target eNB attraverso il signaling X2. Nel frattempo, il target eNB alloca in anticipo risorse cosicché i servizi attualmente disponibili all'utente al source eNB possano esserlo anche all'atto del collegamento al target eNB.

Inoltre, al fine di assicurare un handover veloce, il target eNB invia tutte le informazioni necessarie all'utente per connettersi alla cella target (e.g. C-RNTI) al source eNB che a sua volta le inoltra all'UE dando inizio alla fase di esecuzione. Il target eNB alloca le risorse necessarie come segue:

- Quando il source eNB invia al target eNB un Handover Request message che include l'UE context dell'utente **(1),**
- Il target eNB:
    - Ottiene le informazioni necessarie (S1-SGW TEID) per poter creare un UL S1 bearer attraverso il quale trasportare i pacchetti in UL **(2).**
    - Alloca il TEID per il bearer X2 (tunnel GTP-U) attraverso il quale ricevere i pacchetti in DL mentre l'UE tenta di collegarsi al target eNB (cioè si trova nel periodo di Handover Interruption Time).
    - Alloca le risorse per il Data Radio Bearer (DRB) e il C-RNTI che l'UE deve usare nel collegamento alla cella target
    - Invia un Handover Request Ack message al source eNB **(3)**.
- Una volta ricevuto il messaggio, il source eNB instaura un bearer X2 attraverso il quale inviare i pacchetti in DL al target eNB.

▪ **Esecuzione dell'handover X2**

Quando i due eNB coinvolti hanno completato la preparazione dell'handover, viene dato l'ordine all'UE di eseguirlo:

- Il source eNB:
    - Ordina all'UE di effettuare un handover verso la target cell inviandogli un Handover Command message che include tutte le informazioni necessarie per poter accedere alla target cell **(1)**
    - Informa il target eNB circa il numero di pacchetto in UL/DL dal quale dovrebbe iniziare a ricevere o ad inviare quando inizia a comunicare con l'UE, inviandogli un SN Status Transfer message **(2)**
    - Inoltra i pacchetti in DL ricevuti dal SGW al target eNB attraverso il bearer X2 stabilito tra sé stesso e il target eNB **(3)**
- L'UE si disconnette dal source eNB ed accede al target eNB **(4)**
- Il target eNB può iniziare ad inviare e ricevere pacchetti una volta che l'UE si è connesso con successo ad esso **(5).**

▪ **Completamento dell'handover X2**

Come visto sinora, tutte le procedure eseguite durante la fase di esecuzione dell'handover (cioè da quando il source eNB decide di eseguire l'handover, finché l'UE non risulta connesso al target eNB)

avvenivano solo tra i due eNB e nessuna informazione circa l'handover veniva riportata all'EPC (MME). Una volta che l'handover è stato completato il target eNB informa la EPC come segue:

- Quando l'UE ha completato l'accesso al target eNB quest'ultimo invia un Path Switch Request message all'MME per richiedere che i percorsi dei bearer EPS vengano aggiornati **(1)**
- Quando riceve il messaggio, l'MME viene a conoscenza della nuova serving cell dell'UE, e richiede al SGW di modificare il percorso del bearer S1.
- All'atto della ricezione della richiesta, il SGW stabilisce un DL S1 bearer (S1 Target eNB TEID) connesso al target eNB. Dopodiché smette di inviare i pacchetti in DL al source eNB ed inizia ad inviarli al target eNB attraverso il nuovo DL bearer appena creato. **(2)**
- L'MME informa il target eNB che il percorso del DL S1 bearer è stato modificato. **(3)**
- Il target eNB invia al source eNB un UE Context Release message, ordinando a quest'ultimo di eliminare l'UE context. **(4)**

▪ **Dopo l'handover X2**

L'UE è servito dall' eNB B (per la precisione da una serving cell appartenente all'eNB) al quale si è agganciato.

3.6.2.4 Informazioni sullo stato dell'UE e delle connessioni attive prima e dopo l'handover X2

1) **Prima dell' Handover X2**

   L'UE si trova in stato EMM-Registered ed ECM/RRC-Connected e mantiene tutte le risorse allocate dall'E-UTRAN e dalla EPC

2) **Durante l'Handover X2**

   Anche durante la fase di handover, lo stato dell'UE a livello NAS rimane uguale ed un X2 bearer e una X2 signaling connection sono attive lungo l'interfaccia X2 tra source e target eNB. In Figura 68, lo Step 2) mostra le connessioni e gli stati durante il periodo di Handover Interruption Time. Durante questo periodo non è attivo il collegamento radio ma l'UE rimane comunque in stato Connected.

3) **Dopo l'Handover X2**

   L'UE rimane in stato EMM-Registered ed ECM/RRC-Connected. È stato stabilito un nuovo E-RAB (DRB + S1 bearer) col target eNB e sono state create una nuova connessione RRC e una nuova S1 signaling connection (eNB(B) S1AP UE ID) nel control plane

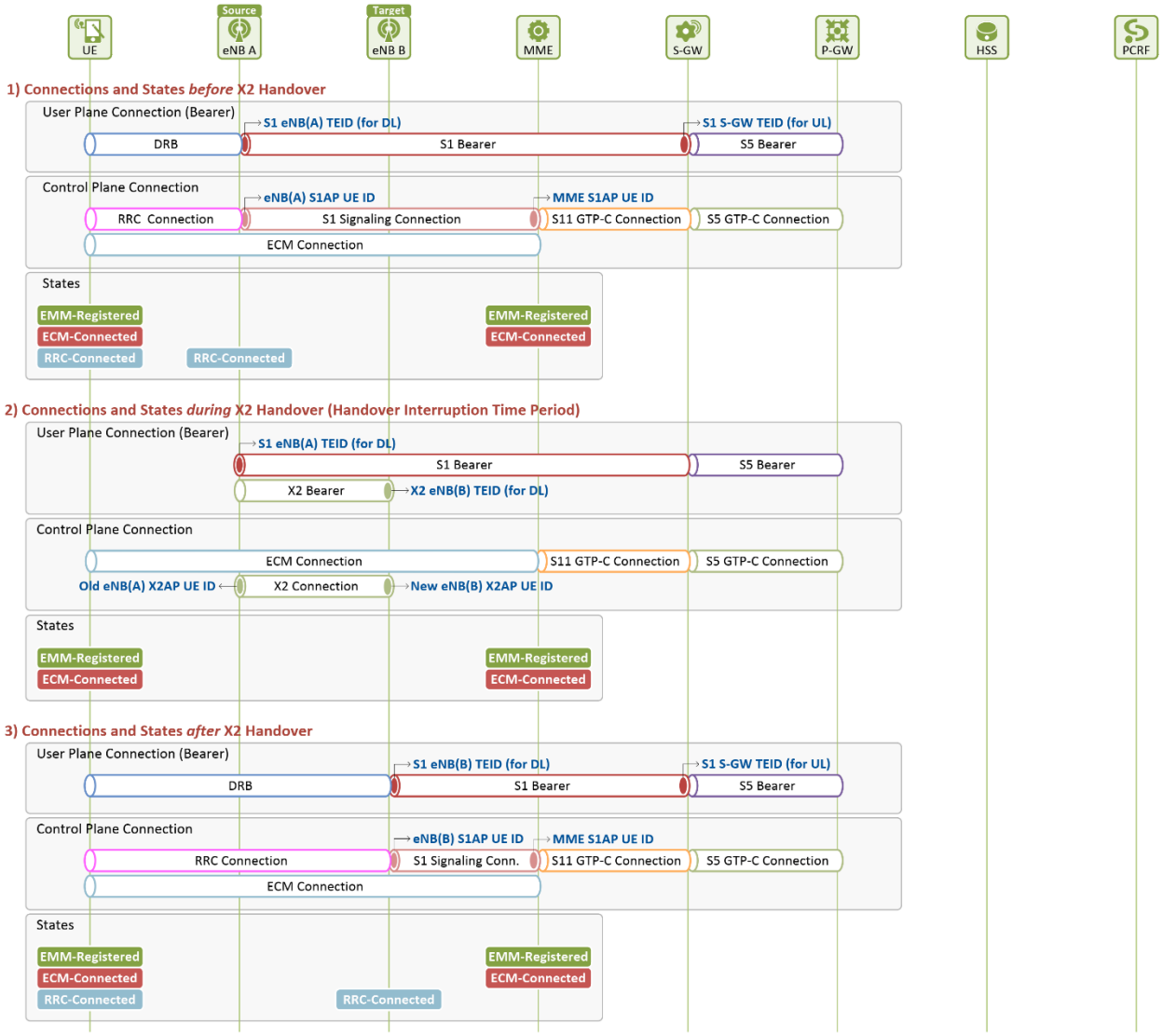


Figura 68 Connessioni e stati prima e dopo l'X2 handover

3.6.2.5 Dettaglio della procedura di X2 Handover

La Figura 69 mostra l'EPS bearer e le connessioni di signaling prima dell'handover X2 ed anche le procedure dettagliate della fase di preparazione dello stesso.

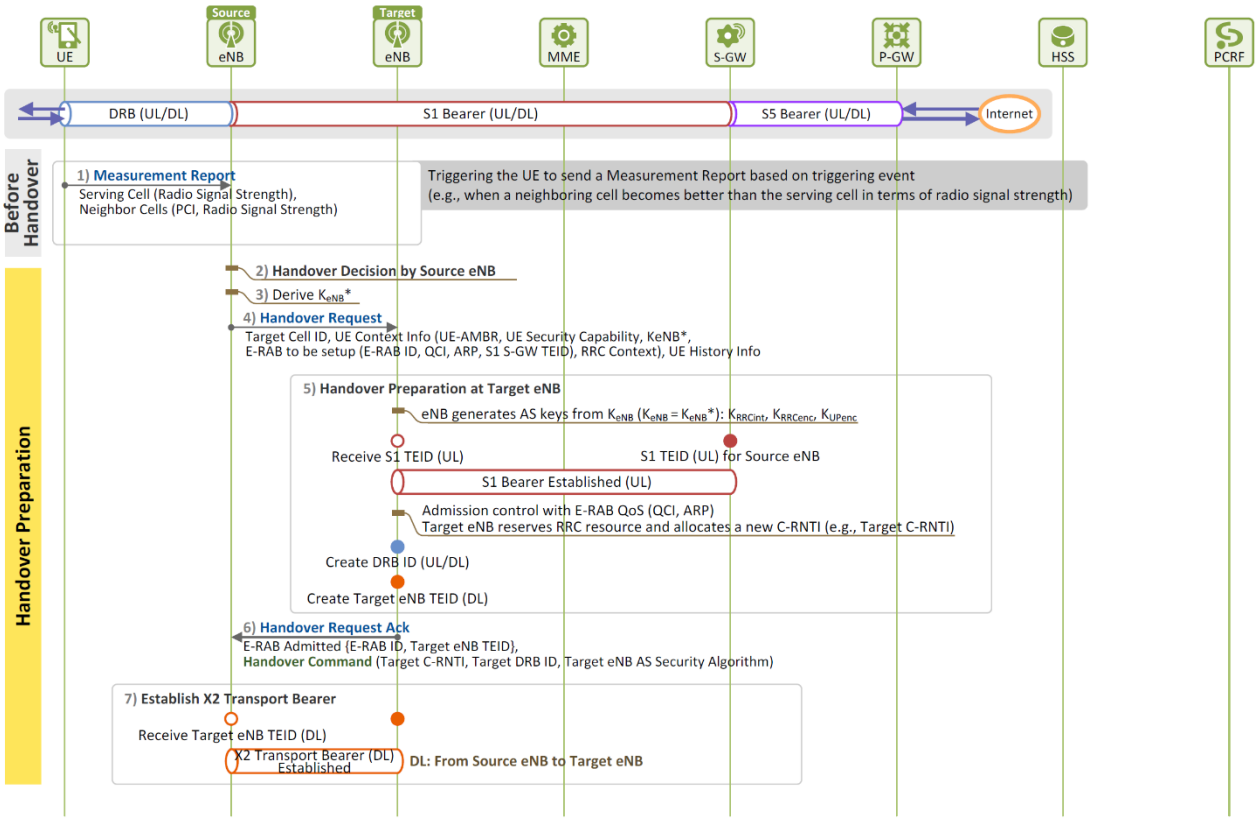


Figura 69 X2 Handover - Fase di preparazione dell'handover

- **Prima dell'handover**

1) **[UE → eNB] Measurement Report**

   Quando un measurement event viene scatenato, l'UE misura la potenza del segnale delle celle vicine

- **Preparazione dell'handover**

2) **[Source eNB] Decisione di effettuare l'handover**

   Il source eNB seleziona un target eNB sulla base delle informazioni incluse nel Measurement Report message inviato dall'UE, e della neighbor cell list che mantiene.

3) **[Source eNB] Derivazione dell'AS Security Base Key (KeNB*) che il Target eNB dovrà usare per la derivazione delle AS Security Keys**

   Quando si effettua un handover, il serving eNB di un UE viene cambiato. Durante questo cambiamento, i messaggi (di signalling e i pacchetti dati utente) scambiati lungo il canale radio devono comunque essere consegnati senza interruzioni e in maniera sicura. La consegna in maniera sicura lungo il canale radio è data dall'utilizzo delle chiavi di sicurezza dell'Access

Stratum (AS). In una procedura di AS Security Setup con coinvolgimento dell'MME , l'MME avrebbe derivato la AS Security base key K_{eNB} dalla top level key K_{ASME} per poi inviarla all'eNB. L'eNB, utilizzando K_{eNB}, avrebbe a sua volta derivato le AS security keys (K_{RRCint}, K_{RRCenc}, K_{UPenc}). Nel caso di X2 handover, poiché esso è eseguito tra due eNB senza intervento dell'EPC (MME) il target eNB non può ottenere KeNB* (cioè la KeNB che deve essere utilizzata dal target eNB) dall'MME. Per questo motivo, una volta deciso di effettuare l'handover, il source eNB deriva la AS security base key che dovrà utilizzare il target eNB e gliela invia.

4) **[Source eNB → Target eNB] Richiesta dell'handover X2**

Il source eNB richiede un handover al target eNB inviandogli un Handover Request message. Per mezzo di questo messaggio, consegna al target eNB le informazioni dell'UE context che ha memorizzato e l'UE history che mostra a quali celle l'UE si è connesso prima dell'ultimo handover alla target cell. Le informazioni incluse nel messaggio sono le seguenti:

Handover Request(Target Cell ID, UE Context Info(UE-AMBR, UE Security Capability, K_{eNB}*, E-RAB to be setup (E-RAB ID, QCI, ARP, S1 SGW TEID), RRC Context, UE History Info))

- **Target Cell ID:** E-UTRAN Global Cell Identifier (ECGI) della target cell
- **UE Context Info:** UE context memorizzato nel source eNB
  - **UE-AMBR:** valore fornito dall'HSS ma può essere modificato dall'MME. Questo valore può essere impostato per l'eNB ed utilizzato per controllare il valore dell'MBR aggregato per i bearers non-GBR.
  - **UE Security Capability:** algoritmi di sicurezza supportati dall'UE (sia di cifratura che integrità).
  - **K_{eNB}*:** AS security base key generata dal source eNB per il target eNB (i.e. **K_{eNB}** che il target eNB dovrà utilizzare).
  - **E-RAB to be setup:** informazioni sull'E-RAB (anche in termini di QoS) mantenute nel source eNB
- **UE History Info:** informazioni circa le celle alle quali l'UE ha acceduto durante lo stato attivo, includendo l'ECGI di ogni cella, tipo e durata di permanenza dell'UE all'interno della stessa.

5) **[Target eNB] Preparazione dell'handover X2**

All'atto della ricezione dell'Handover Request message, il target eNB inizia la preparazione dell'handover per assicurare una fornitura di servizio senza interruzioni all'UE.

i) Prima di tutto deriva le AS security keys per la cifratura e controllo di integrità dei messaggi scambiati lungo il canale radio utilizzando la K_{eNB}* ricevuta dal source eNB. Usando queste chiavi il target eNB può comunicare in sicurezza con l'UE lungo il canale radio una volta che avrà acceduto al target eNB.

ii) Successivamente, il target eNB, sulla base delle informazioni ricevute circa l'E-RAB da costruire, controlla se lo stesso livello di QoS fornito dal source eNB è disponibile anche presso il target eNB. Se lo è, stabilisce un UL S1 bearer connesso al SGW utilizzando le informazioni relative all'UL S1 bearer (S1 SGW TEID) memorizzate nel source eNB.

iii) Poi, sulla base delle informazioni di QoS dell'E-RAB, il target eNB riserva le risorse RRC da utilizzare lungo il canale radio (ad es. effettua l'allocazione del DRB ID ecc.) ed alloca il C-RNTI

iv) Mentre l'UE sta eseguendo l'handover (cioè dopo che si è disconnesso dal source eNB finché non si connette al target eNB) i pacchetti in DL in arrivo al source eNB devono essere inoltrati al target eNB. Per fare ciò, il target eNB alloca l'X2 Target eNB TEID (DL TEID del tunnel GTP X2) affinché il source eNB possa creare un bearer di trasporto X2 (tunnel GTP).

6) **[Source eNB ← Target eNB] Notifica al source eNB del completamento della fase di preparazione**

Il target eNB invia al source eNB tutte le informazioni circa le risorse preparate nello step 5) includendole in un Handover Request Ack message. Le informazioni incluse sono le seguenti:

Handover Request Ack(E-RAB Admitted (E-RAB ID, Target eNB TEID), Handover Command (Target C-RNTI, Target DRB ID, AS Security Algorithm of Target eNB))

- **E-RAB Admitted:** include l' E-RAB ID allocato dal target eNB e il TEID del bearer X2 attraverso il quale i pacchetti vengono inoltrati al target eNB
- **Handover Command:** Transparent Container trasmesso dal target eNB al source eNB, che contiene informazioni delle quali l'UE necessita per poter accedere al target eNB
  - **Target C-RNTI:** C-RNTI allocato dalla target cell per identificare l'UE ad essa collegato
  - **Target DRB ID:** ID del DRB che il target eNB ha creato per la trasmissione dei pacchetti dati utente lungo il canale radio
  - **AS Security Algorithm of Target eNB:** Algoritmi di sicurezza dell'AS supportati dal target eNB

7) **[Source eNB] Creazione del Bearer X2 per l'inoltro dei pacchetti in DL**

Al momento della ricezione dell'Handover Request Ack, il source eNB sa che il target eNB può servire l'UE. Allora, utilizzando l'X2 Target eNB TEID, costruisce un X2 bearer affinché i pacchetti in DL possano essere inoltrati al target eNB durante la fase di esecuzione dell'handover.

▪ **Esecuzione dell'handover**

La Figura 70 mostra la procedura per la fase di esecuzione delll'X2 handover.

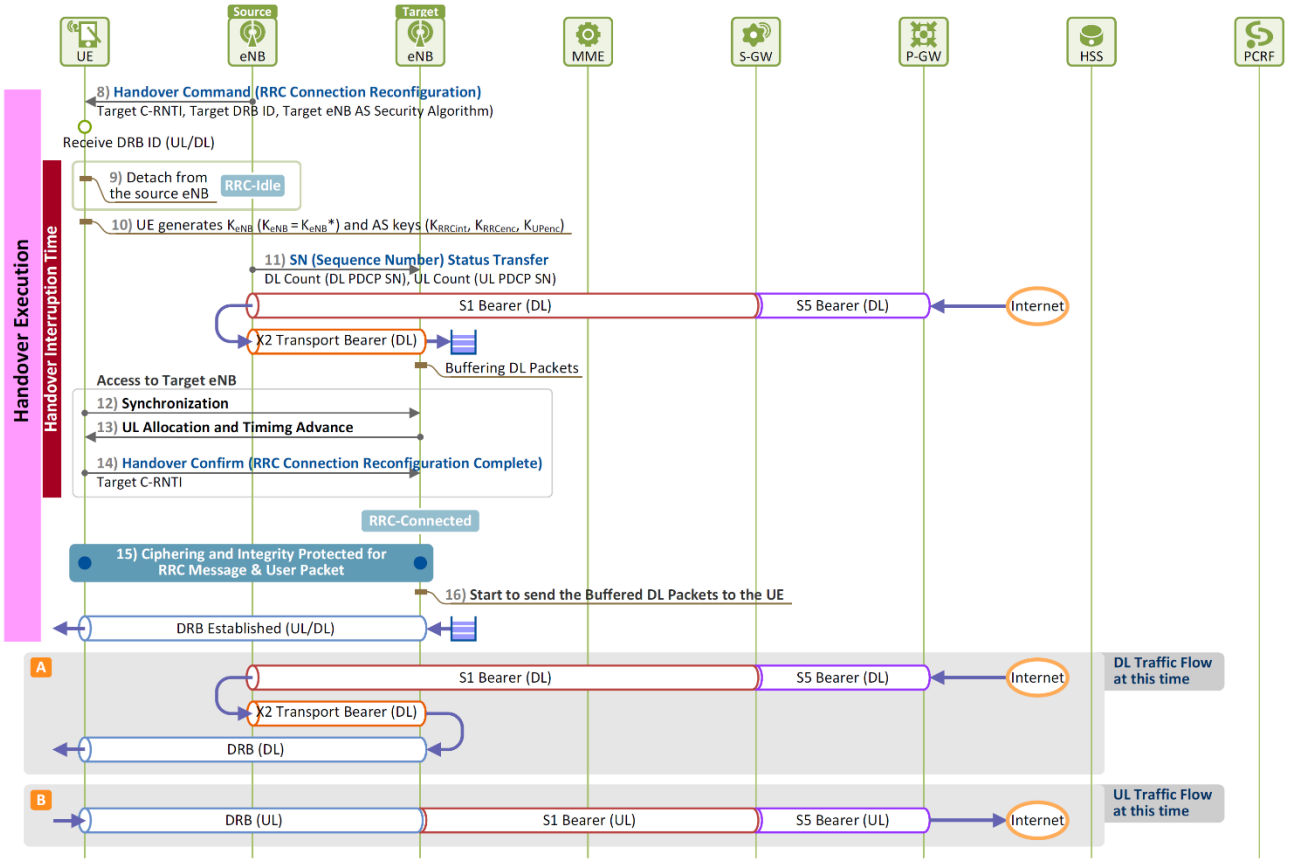


Figura 70 X2 Handover - Fase di esecuzione

8) **[UE ← Source eNB] Ordine di eseguire l'handover**

Una volta che il source eNB ha completato la preparazione dell'handover col target eNB, ordina all'UE di eseguire un handover inviandogli un Handover Command message.

9) **[UE] Esecuzione dell'handover**

L'UE, dall'Handover Command message ricevuto, ottiene il C-RNTI e il DRB ID da utilizzare nel collegamento alla target cell e si disconnette dal source eNB. Da questo momento tutto il traffico di pacchetti tra l'UE e il source eNB si ferma ed inizia il periodo di Handover Interruption Time.

10) [UE] AS Security Setup

L'UE deriva le AS security keys da utilizzare nel collegamento radio col target eNB.

11) [Source eNB → Target eNB] Notifica del Sequence Number del pacchetto dal quale iniziare ad inviare/ricevere

Il source eNB informa il target eNB circa il numero di pacchetto dal quale dovrebbe iniziare ad inviare (o a ricevere) inviandogli un SN Status Transfer message che include DL Count ed UL Count. Le informazioni incluse nel messaggio sono le seguenti:

SN Status Transfer (DL Count, UL Count)

- **DL Count:** Numero del primo pacchetto da inviare all'UE
- **UL Count:** Numero del primo pacchetto da ricevere dall'UE

Dopo aver inviato l'SN Status Transfer message al target eNB, il source eNB inizia ad inoltrare i pacchetti in DL in arrivo dal SGW al target eNB attraverso l'X2 bearer costruito sull'interfaccia X2. Il target eNB bufferizza i pacchetti e attende che l'UE abbia completato l'accesso alla target cell.

12) ~ 14) [UE, Target eNB] L'UE accede al Target eNB

12) 13) L'UE effettua le necessarie procedure di sincronizzazione col target eNB.

14) L'UE invia al target eNB un Handover Confirm message includendolo in un RRC Connection Reconfiguration Complete message. Ora, l'UE può inviare/ricevere pacchetti a/dal target eNB, e il periodo di handover interruption time termina.

15) [UE – Target eNB] Comunicazione sicura lungo il collegamento radio

Tutti i messaggi di signalling RRC e i pacchetti utente inviati lungo il collegamento radio tra l'UE e il target eNB sono ora consegnati in sicurezza usando le chiavi di sicurezza dell'AS. I messaggi di signalling sono protetti per quel che concerne l'integrità e criptati mentre i pacchetti utente vengono criptati prima di essere inviati.

16) [Target eNB] Ripresa della consegna dei pacchetti in DL all'UE

Poiché ora l'UE è connesso con successo al target eNB, quest'ultimo inizia ad inviare i pacchetti in DL precedentemente bufferizzati attraverso il seguente percorso: (rif. [A] nella Figura 70):

S5 Bearer → S1 Bearer (@source eNB) → X2 Bearer → DRB (@target eNB)

Nel caso di pacchetti inviati dall'UE, il target eNB controlla se i pacchetti in UL sono ricevuti in

ordine e poi li inoltra al SGW attraverso il seguente percorso (rif. [B] nella Figura 70):

DRB (@target eNB) → S1 bearer (@target eNB) → S5 bearer

- **Completamento dell'handover**

La Figura 71 illustra la fase di completamento dell'handover

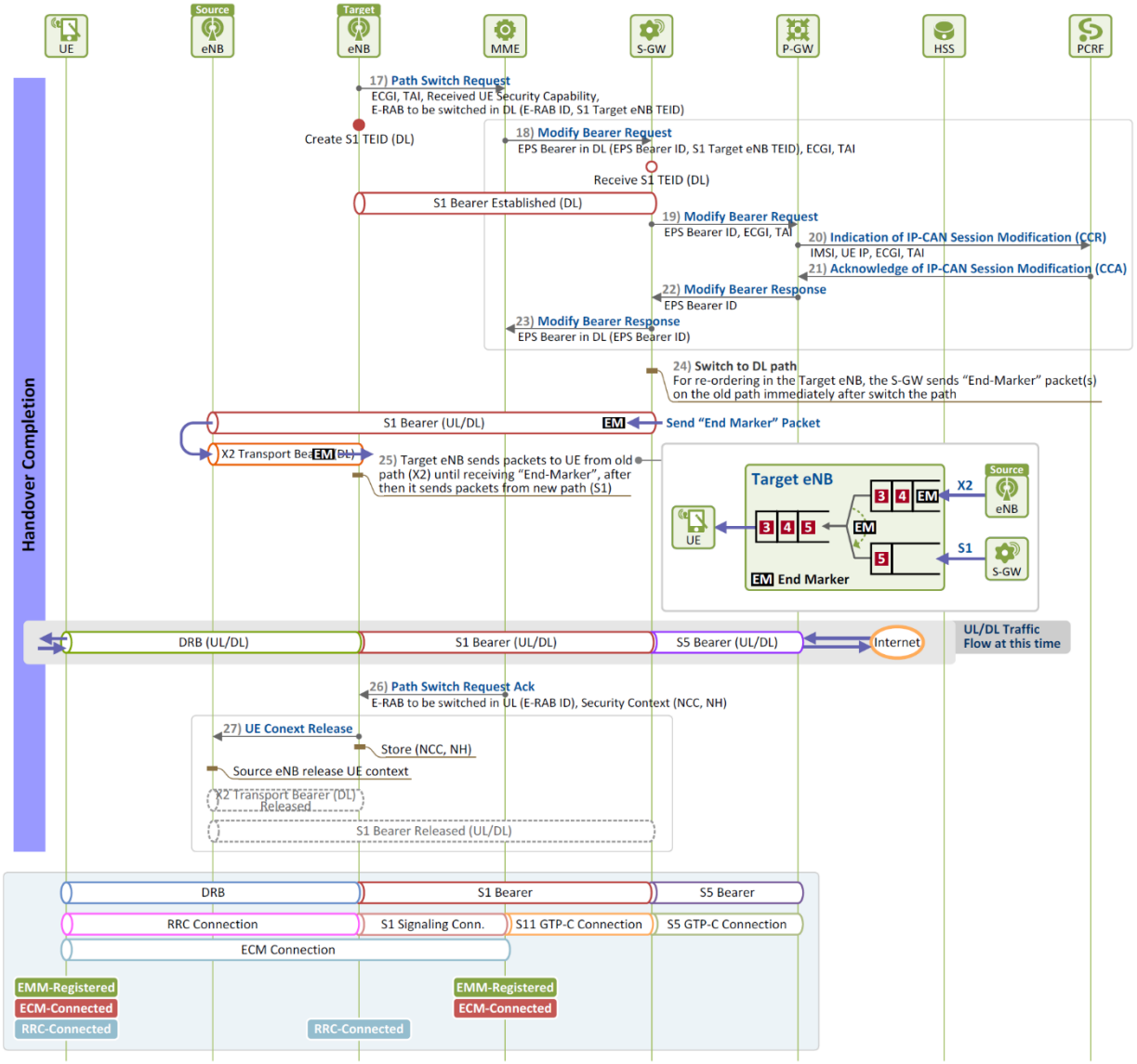


Figura 71 X2 Handover- Fase di completamento

17) [Target eNB → MME] Richiesta di Path Switch dell'EPS Bearer (S1 Bearer)

Il target eNB notifica all'EPC (MME) che la serving cell dell'UE è cambiata inviando un Path Switch Request message col quale richiede che il percorso dell'EPS bearer venga modificato.

18) ~ 23) Modifica del bearer EPS

L'MME inoltra l'S1 Target eNB TEID che è stato allocato dal target eNB al SGW inviandogli un Modify Bearer Request message col quale gli richiede di cambiare il percorso del DL S1 bearer.

Il SGW crea quindi il DL S1 bearer connesso al target eNB, come richiesto. Alcuni SGW, in base alle opzioni impostate durante la fase di Initial Attach, devono riferire al PCRF se la serving cell dell'UE è cambiata nel momento in cui una nuova EPS session viene instaurata. In questo caso, il SGW invia un Modify Bearer Request message al PGW e il PGW riporta tale avvenimento al PCRF in base alle procedure di modifica dell'EPS session.

24) [SGW] Modifica del percorso dell'EPS Bearer ed invio dei pacchetti EM

Ora che il percorso del DL S1 bearer è stato modificato, il SGW cambia il percorso di consegna dei pacchetti in DL facendoli transitare lungo il DL S1 bearer connesso al target eNB. Per fare ciò, per prima cosa invia un End Marker (EM) per indicare l'ultimo pacchetto che viene fatto transitare lungo il DL S1 bearer connesso al source eNB.

Dopodiché vengono inviati i pacchetti in DL al target eNB attraverso il DL S1 bearer modificato.

25) [Target eNB] Riordino dei pacchetti

Ora il target eNB riceve i pacchetti in DL inoltrati dal source eNB attraverso l'X2 transport bearer e quelli inviati dal SGW attraverso il DL S1 bearer modificato. Di conseguenza dovrebbe essere in grado di consegnare i pacchetti all'UE nell'ordine corretto. Innanzitutto, il target eNB inoltra i pacchetti in DL ricevuti dall'X2 transport bearer all'UE. Successivamente, quando l'EM arriva, sa che questo pacchetto è l'ultimo in arrivo dall'X2 transport bearer, per cui inizia ad inviare i pacchetti in DL ricevuti dall'S1 bearer all'UE.

26) [Target eNB ← MME] Notifica della modifica del percorso dei bearer

L'MME notifica al target eNB che il SGW ha cambiato il percorso dell'EPS bearer (S1 bearer) inviando un Path Switch Request Ack message. Poi, inoltra il security context richiesto per l'handover affinché il target eNB possa utilizzarlo nel caso in cui l'UE effettui un altro handover ad un'altra cella.

27) [Source eNB ← Target eNB] Richiesta di rilasciare l'UE context

Il target eNB memorizza il security context e poi invia al source eNB un UE Context Release message, informandolo che può eliminare l'UE context poiché il percorso dei bearer in UL/DL è stato modificato.

3.6.3 Handover S1 senza TAU

3.6.3.1 S1 Protocol Stacks

Gli handover S1 sono eseguiti tra un source eNB ed un target eNB attraverso l'interfaccia S1 che connette eNB ed EPC. Gli eNB comunicano con l'MME attraverso signaling S1AP nel control plane, e con il SGW attraverso il tunnel GTP nello user plane. La Figura 72 mostra i protocol stack sull'interfaccia S1 nei control e user planes.

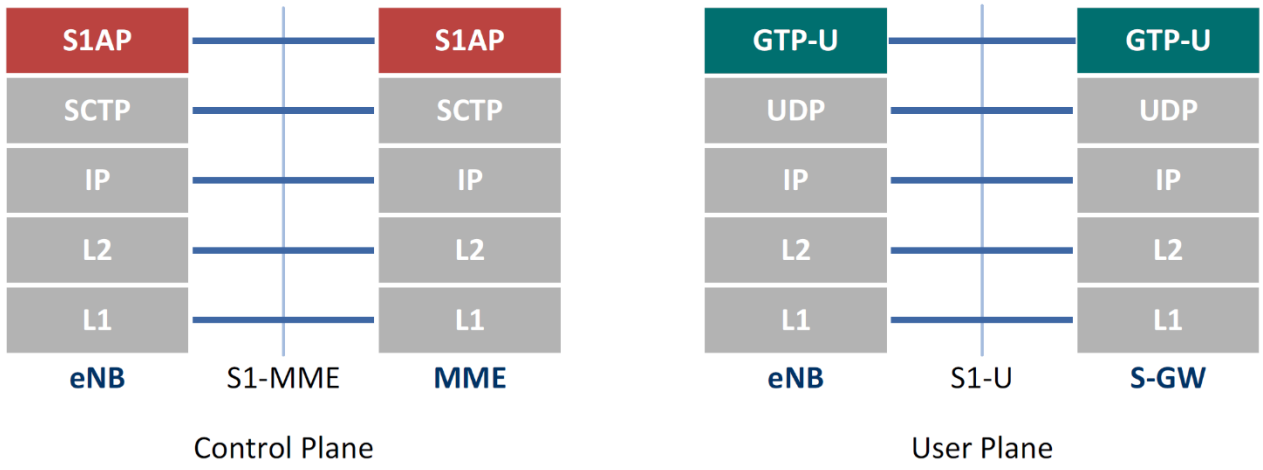


Figura 72 Protocol stack su interfaccia S1

Quando un nuovo eNB viene installato, viene eseguita una procedura di "S1 Setup" tra l'eNB e il/gli MME. L'eNB fornisce all'MME le sue informazioni di configurazione inviando un S1 Setup Request (eNB ID, eNB Name, TAC) message. Poi, ogni MME ritorna un S1 Setup Response (GUMMEI, MME Name, Relative MME Capacity) message all'eNB cosicché quest'ultimo possa aggiornare le sue informazioni di configurazione. Il parametro "Relative MME Capacity" è utilizzato per effettuare il load balancing tra gli MME in un MME pool area. Il suo valore mostra la capacità relativa di ogni MME di gestire connessioni da parte degli UE. Gli eNB connessi a più di un MME usano questo valore al momento di stabilire una nuova connessone con un UE.

Le connessioni relative ad un determinato UE tra un eNB e la EPC sono le seguenti: nel control plane ogni connessione di signaling tra un eNB ed un MME relativa ad un determinato utente è fornita attraverso l'S1 Application Protocol (S1AP) signaling connection ed identificata dalla coppia {eNB UE S1AP ID, MME UE S1AP ID}. Nello user plane, ogni S1 bearer relativo ad un utente tra l'eNB e il SGW è implementato attraverso tunnel GTP ed identificato da {DL S1 TEID (S1 eNB TEID), UL S1 TEID (S1 SGW TEID)}.

3.6.3.2 Messaggi e procedure S1AP relative all'handover S1

Tabella 13 Procedure e Messaggi del protocollo S1AP relative all'Handover S1

Elementary Procedure	**Messaggio iniziale**	**Messaggio di risposta**	
		Successo	**Insuccesso**
Handover Preparation	**Handover Required**	**Handover Command**	**Handover Preparation Failure**
Handover Resource Allocation	**Handover Request**	**Handover Request Acknowledge**	**Handover Failure**
Handover Cancellation	**Handover Cancel**	**Handover Cancel Acknowledge**	**-**
UE Context Release	**UE Context Release Command**	**UE Context Release Complete**	**-**
SN Status Transfer	**eNB Status Transfer MME Status Transfer**	**-**	**-**
Handover Notification	**Handover Notify**	**-**	**-**

Di seguito viene presentata una breve spiegazione per ognuno dei messaggi elencati sopra:

- **Handover Required** message: Questo messaggio è usato durante la fase di preparazione dell'handover. Viene inviato dal source eNB all'MME ed include informazioni circa il target eNB e le risorse radio della source cell.
- **Handover Request** message: Questo messaggio è usato durante la fase di preparazione dell'handover. Viene inviato dall'MME ad un target eNB ed include l'UE context dell'utente.
- **Handover Request Acknowledge** message: Questo messaggio è usato durante la fase di preparazione dell'handover. Viene inviato dal target eNB all'MME quando l'allocazione delle risorse per l'UE è stata completata con successo nel target eNB. Il target eNB alloca il DL S1 TEID per l'S1 bearer da utilizzare dopo l'handover e il DL S1 TEID per il bearer S1 (tunnel indiretto) da utilizzare per la consegna dei pacchetti in DL durante l'handover, e poi li inoltra includendoli nel messaggio.
- **Handover Command** message: Questo messaggio è utilizzato durante la fase di preparazione dell'handover ed è inviato dall'MME al source eNB. Include le informazioni richieste quando l'UE accede al target eNB (e.g. Target C-RNTI, Target eNB AS Security Algorithm, DRB

ID, etc.) e l'UL S1 TEID per il bearer S1 (tunnel indiretto) che dovrà essere usato dal SGW per la consegna dei pacchetti in DL durante l'handover.

- **eNB Status Transfer** message: Questo messaggio è utilizzato durante la fase di esecuzione dell'handover e viene inviato dal source eNB all'MME per indicare il numero di pacchetto dal quale il target eNB dovrebbe iniziare a ricevere od inviare.
- **MME Status Transfer** message: Questo messaggio è utilizzato durante la fase di esecuzione dell'handover, ed è inviato dall'MME al target eNB. Indica da quale pacchetto il target eNB dovrebbe iniziare a ricevere o inviare.
- **Handover Notify** message: Questo messaggio è utilizzato durante la fase di completamento dell'handover e viene inviato dal target eNB all'MME per indicare che l'UE ha completato l'handover al target eNB
- **UE Context Release Command** message: Questo messaggio è utilizzato durante la fase di completamento dell'handover ed è inviato dall'MME al source eNB per informarlo che può eliminare l'UE context.
- **UE Context Release Complete** message: Questo messaggio è utilizzato durante la fase di completamento dell'handover, ed è inviato dal source eNB all'MME per informarlo che l'UE context è stato eliminato.

3.6.3.3 Panoramica della procedura di Handover S1

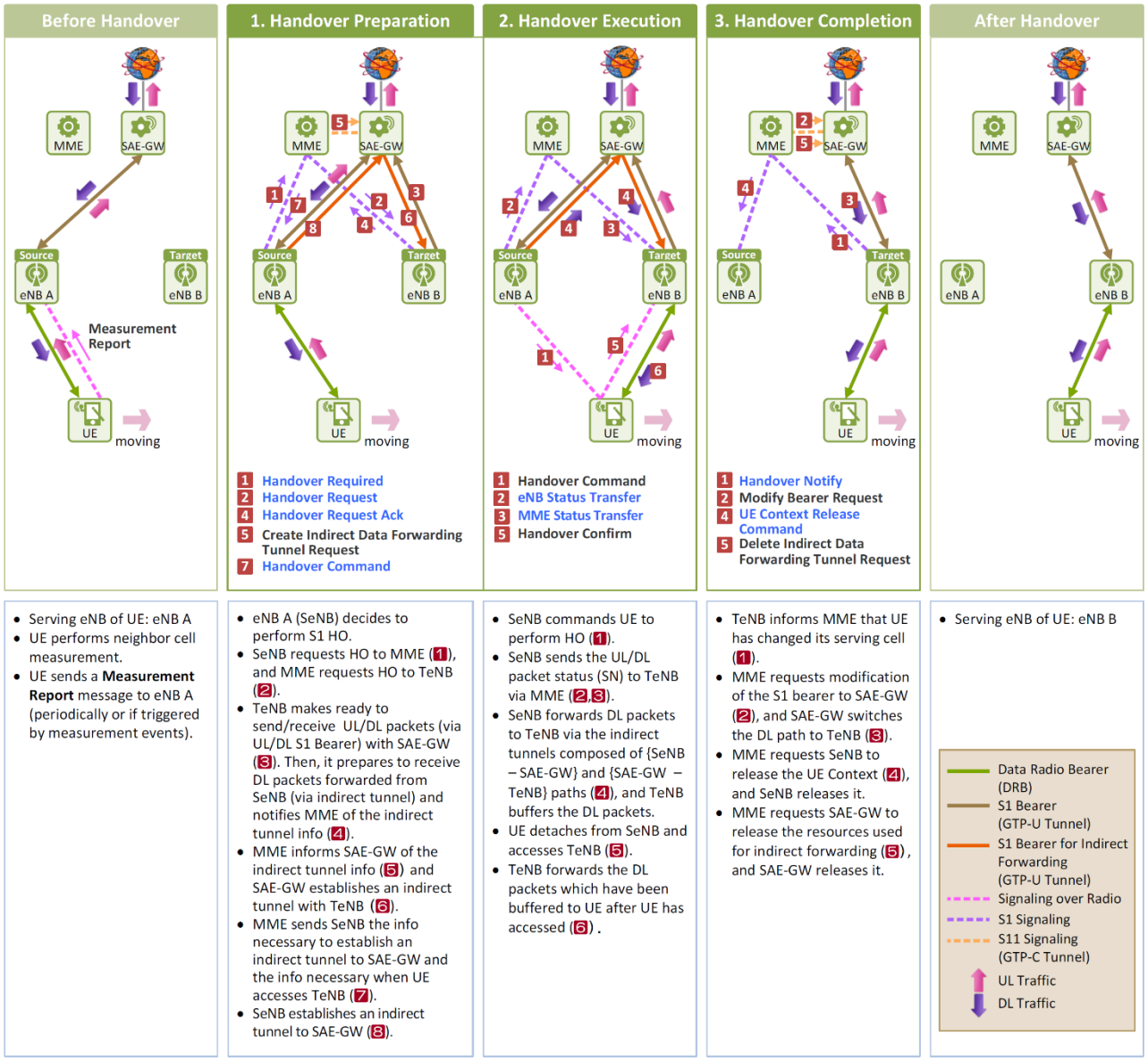


Figura 73 Procedura semplificata di Handover S1

La Figura 73 mostra a grandi linee le procedure richieste prima, durante (fase di preparazione, esecuzione e completamento) e dopo l'handover S1. Per convenienza le entità SGW e PGW sono raggruppate insieme sotto il nome di SAE-GW mentre il source e il target eNB sono denominati rispettivamente SeNB e TeNB.

- **Prima dell'handover S1**

Nella Figura 73, l'UE viene servito dall'eNB A al quale è connesso. Quando l'UE rileva un measurement event, invia un Measurement Report all'eNB A.

▪ **Preparazione dell'Handover S1**

Il source eNB (eNB A in Figura 73) sceglie un target eNB (eNB B in Figura 73) verso il quale effettuare l'handover, sulla base delle informazioni sulle celle vicine di cui è a conoscenza e delle informazioni sulla potenza del loro segnale incluse nel Measurement Report message. Dopodiché, quando realizza che un handover verso il target eNB attraverso la connessione X2 non è possibile, decide di eseguire un handover S1 e si prepara ad eseguirlo attraverso l'MME. Entrambi gli eNB comunicano con l'MME attraverso S1AP signaling. A questo punto, il target eNB alloca risorse radio in anticipo per assicurarsi che gli stessi servizi attualmente forniti dal source eNB siano disponibili anche al target eNB. L'MME fornisce poi al source eNB le informazioni richieste dall'UE per poter accedere alla target cell.

Nel frattempo, il target eNB e il SGW allocano le risorse richieste per creare un tunnel indiretto attraverso il quale i pacchetti in DL in arrivo al source eNB possono essere inoltrati al SGW e poi al target eNB mentre l'handover viene eseguito. Ciò avviene nel seguente modo:

- Il source eNB invia le informazioni circa il target eNB, includendole in un Handover Required message, all'MME **(1)**
- L'MME invia poi al target eNB un Handover Request message che include l'UE context e le informazioni di sicurezza dell'AS richieste dal target eNB per derivare le AS security keys **(2)**
- **Target eNB**
    - Crea un UL S1 bearer attraverso il quale inoltrare i pacchetti in UL dopo l'handover utilizzando il S1 SGW TEID ottenuto dall'MME ed alloca il S1 target eNB TEID per un DL S1 bearer da utilizzare ad handover terminato **(3)**
    - Alloca il S1 target eNB TEID per il tunnel che connette il SGW e il target eNB (questo tunnel è parte di un tunnel indiretto che connette tutto il percorso tra il source eNB, il SGW e il target eNB) da utilizzare per inoltrare i pacchetti in DL mentre l'UE tenta di accedere (cioè effettua l'handover) al target eNB.
    - Configura un Handover Command message che include le informazioni richieste dall'UE per accedere alla target cell (e.g. Target C-RNTI, Target DRB ID ecc.)
    - Invia le informazioni ricavate all'MME includendole in un Handover Request Ack message. **(4)**.
- L'MME, all'atto della ricezione del messaggio, include il S1 Target eNB TEID che il Target eNB ha allocato per il tunnel indiretto in un Create Indirect Data Forwarding Tunnel Request message che invia al SGW. **(5)**

- **S-GW**
    - Crea un tunnel indiretto connesso al target eNB **(6)**
    - Alloca l'S1 SGW TEID per il tunnel che connette il source eNB e il SGW (questo tunnel è una parte del tunnel indiretto che collega tutto il percorso tra il source eNB, il SGW e il target eNB), e lo invia all'MME attraverso un Create Indirect Data Forwarding Tunnel message.
- L'MME include l'S1 SGW TEID che il SGW ha allocato per il tunnel indiretto e le informazioni richieste dall'UE per accedere alla target cell, in un Handover Command message, che invia al source eNB **(7)**.
- Poi, il source eNB crea un tunnel indiretto connesso al SGW. **(8)**.

Alla fine di tutti questi step, l'intero tunnel che connette tutte le tre entità, il source eNB, il SGW e il target eNB è stabilito.

▪ **Esecuzione dell'Handover S1**

Ora, i due eNB sono pronti per eseguire un handover, per cui l'UE può eseguirlo.

- **Source eNB**
    - Ordina all'UE di eseguire un handover alla target cell inviandogli un Handover Command message che include tutte le informazioni richieste dall'UE per accedere alla target cell **(1)**
    - Informa l'MME circa il numero di pacchetto in UL/DL dal quale dovrebbe iniziare a ricevere/inviare da/a l'UE inviandogli un eNB Status Transfer message **(2)**
    - Invia i pacchetti in DL ricevuti dal SGW al target eNB attraverso il tunnel indiretto connesso al target eNB passando per il SGW **(4)**
- L'MME informa il target eNB circa il numero di pacchetto in UL/DL dal quale dovrebbe iniziare ad inviare/ricevere a/da l'UE inviando un MME Status Transfer message **(3)**.
- L'UE si disconnette dal source eNB, e si connette dal target eNB **(5)**.
- Una volta che l'UE ha acceduto con successo al target eNB, può iniziare immediatamente ad inviare o ricevere pacchetti **(6)**.

▪ **Completamento dell'Handover S1**

Siccome l'MME già sapeva che l'UE stava per eseguire l'handover, il target eNB, a differenza dell'handover X2, non richiede all'MME di eseguire la modifica dei percorsi dei bearer. Invece, una volta che l'UE si è connesso al target eNB, quest'ultimo invia all'MME un Handover Notify message per indicare che l'UE ha completato l'handover.

- Non appena l'UE si è connesso, il target eNB invia all'MME un Handover Notify message per informarlo sul completamento dell'handover **(1)**
- Poi, l'MME richiede al SGW la modifica del bearer S1 **(2)**. Il SGW modifica il percorso del DL S1 bearer per connetterlo al target eNB, come richiesto **(3).**
- Il SGW cambia il percorso del bearer come segue:
    - Dapprima termina la consegna dei pacchetti in DL inviando un End Marker (EM) packet attraverso il bearer connesso al source eNB.
    - Poi crea il DL S1 bearer che è connesso al target eNB e riprende la consegna dei pacchetti in DL attraverso il target eNB.
- Il target eNB invia i pacchetti in DL all'UE come segue:
    - Invia i pacchetti in DL in arrivo attraverso il tunnel indiretto all'UE finché non giunge il pacchetto EM.
    - Una volta che il pacchetto EM è arrivato, invia all'UE i pacchetti in arrivo attraverso il nuovo percorso
- L'MME:
    - Richiede al source eNB di rilasciare le risorse S1 relative al source eNB e l'UE Context che ha mantenuto inviandogli un UE Context Release Command message. **(4)**
    - Richiede al SGW di rilasciare le risorse associate al tunnel indiretto inviando un Delete Indirect Data Forwarding Tunnel Request message **(5)**

▪ **Al termine dell'handover S1**

L'UE è servito dall'eNB B (da una serving cell nell'eNB B) al quale si è connesso.

3.6.3.4 Informazioni sullo Stati dell'UE e delle connessioni attive prima e dopo l'Handover S1

La Figura 74 illustra le connessioni stabilite in user e control plane e gli stati di UE ed MME prima, durante e dopo l'S1 handover.

▪ **Prima dell'handover S1**

L'UE si trova in stato EMM-Registered ed ECM/RRC-Connected ed utilizza tutte le risorse allocate da E-UTRAN ed EPC.

▪ **Durante l'handover S1**

Anche durante la fase di handover lo stato dell'UE a livello NAS non cambia. Sia il source che il target eNB sono connessi allo stesso MME attraverso la S1 signaling connection stabilita lungo l'interfaccia S1-MME. Entrambi sono anche connessi al SGW per mezzo del tunnel indiretto creato lungo l'interfaccia S1-U per il forwarding dei pacchetti in downlink. In Figura 74 lo step 2) mostra le connessioni e gli stati durante il periodo di handover interruption time. Durante questo periodo non è attivo alcun collegamento radio ma l'UE rimane in stato Connected.

▪ **Dopo l'handover S1**

L'UE si trova in stato EMM-Registered ed ECM/RRC-Connected. È stato creato un nuovo E-RAB connesso col nuovo eNB in user plane mentre una nuova connessione RRC è statat creata nel control plane

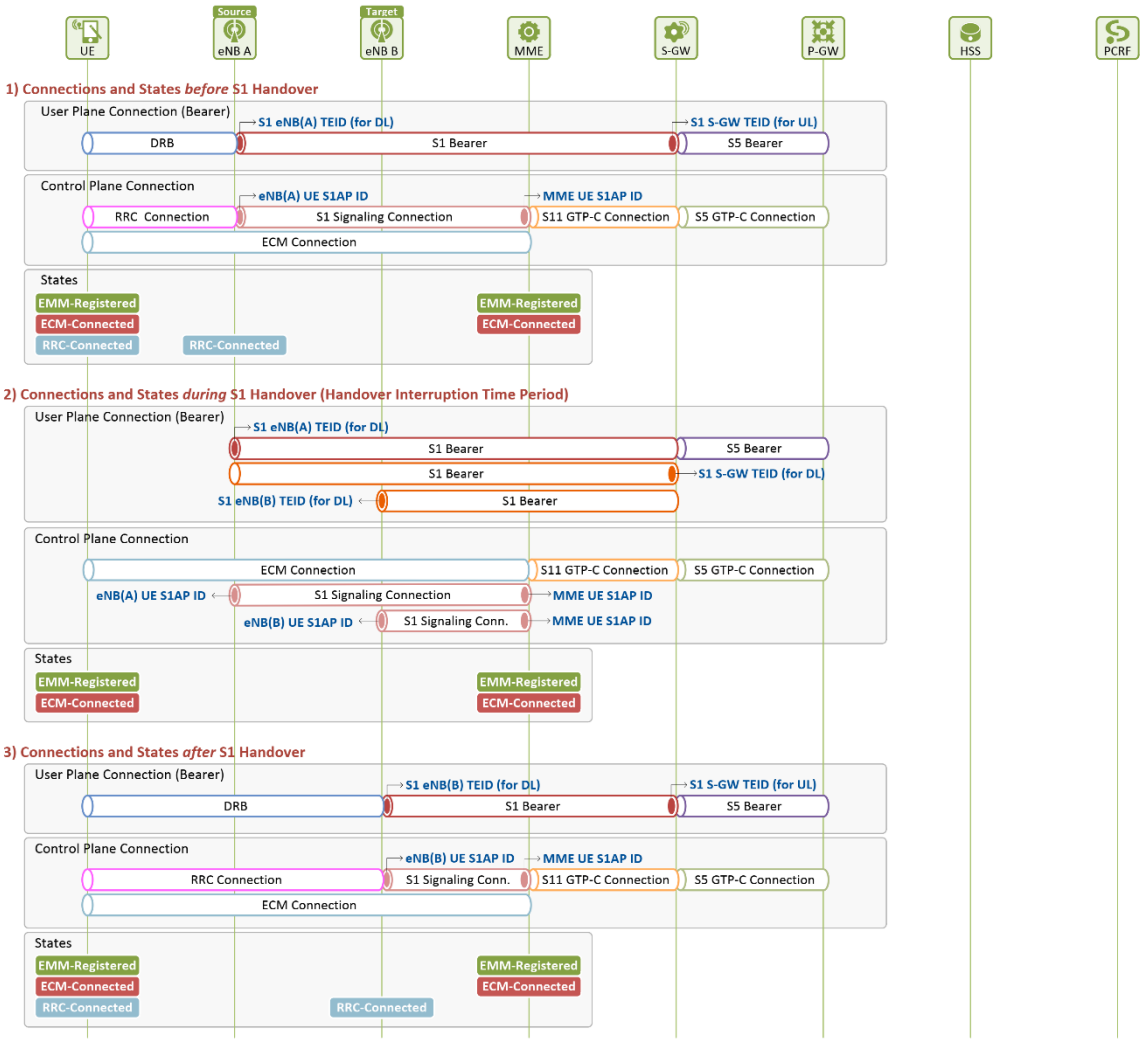


Figura 74 Stati e connessioni prima e dopo l'S1 handover

3.6.3.5 Dettaglio della procedura di Handover S1

La Figura 75 mostra l'EPS bearer e le connessioni di signaling prima dell'handover S1 e le procedure dettagliate della fase di preparazione.

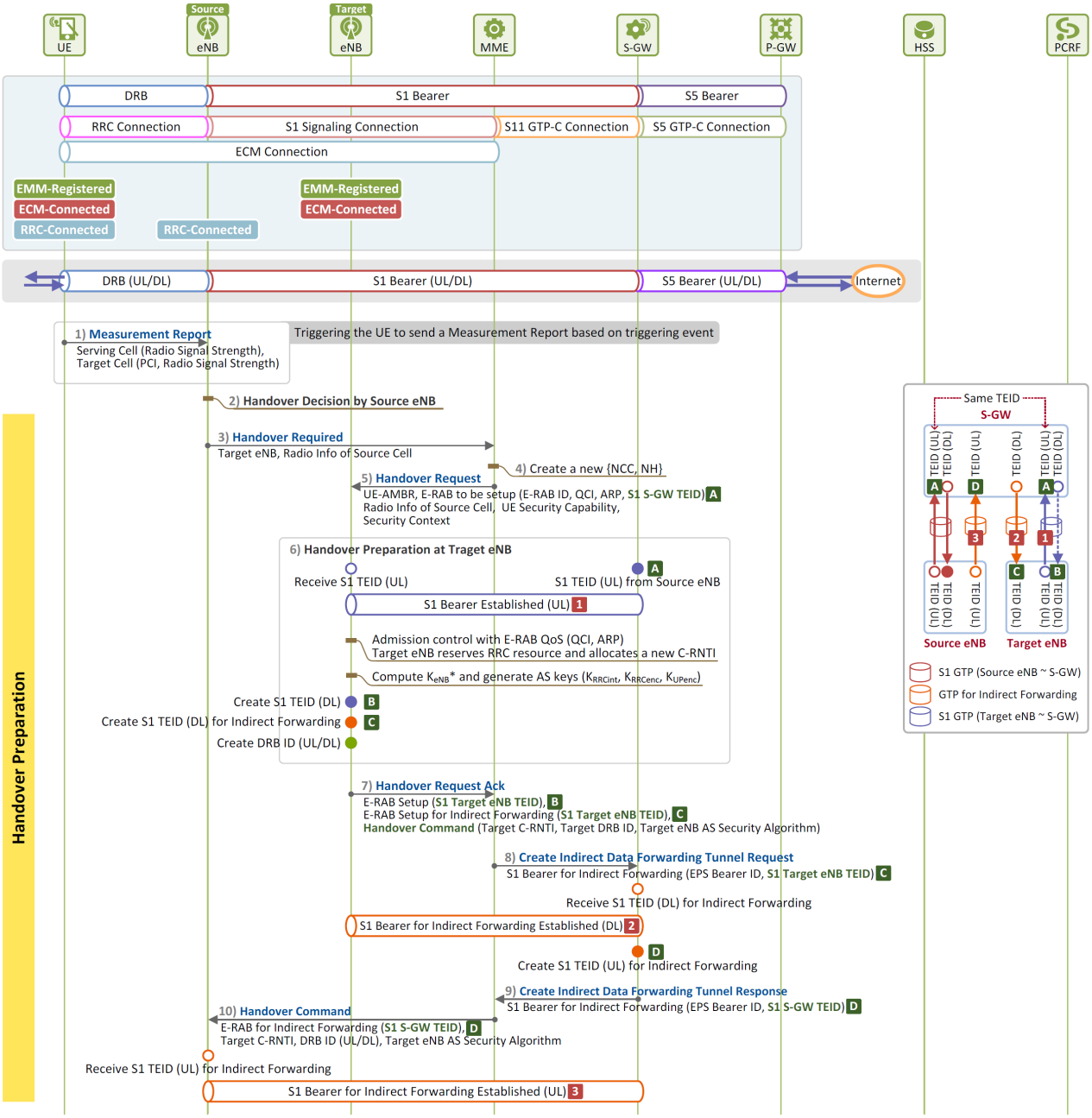


Figura 75 S1 Handover – Fase di preparazione

- **Prima dell'Handover**

1) **[UE → eNB] Measurement Report**

   Quando un measurement event viene scatenato, l'UE misura la potenza del segnale delle celle vicine ed invia un Measurement Report message all'eNB associato (serving cell).

- **Preparazione dell'handover**

2) **[Source eNB] Decisione di effettuare l'handover**

Il source eNB seleziona un target eNB sulla base delle informazioni incluse nel Measurement Report message inviato dall'UE e delle informazioni contenute nella neighbor cell list che ha memorizzato. Una volta che ha constatato la mancanza di una connessione X2 diretta tra i due eNB (source e target), il source eNB decide di effettuare un S1 handover.

3) **[Source eNB → MME] Richiesta di Handover**

Il source eNB invia un Handover Required message all'MME richiedendo un handover al target eNB. Le informazioni incluse nel messaggio sono le seguenti:

Handover Required (Handover Type, Target eNB ID, Source to Target Transparent Container):

- **Handover Type:** Indica il tipo di handover iniziato. In questo caso poiché da una rete LTE rimaniamo sempre all'interno della stessa sarà di tipo "IntraLTE"
- **Target eNB ID:** include il Target Global eNB ID e la Selected TAI
- **Source to Target Transparent Container:** è utilizzato per l'inoltro di informazioni relative al collegamento radio in maniera trasparente dalla source cell alla target cell attraverso l'EPC (MME).

4) **[MME] Derivazione del Security Context da inoltrare al target eNB**

L'MME deriva il Security Context richiesto dal target eNB per poter derivare a sua volta la AS security base key.

5) **[Target eNB ← MME] Richiesta al target eNB di effettuare l'Handover**

L'MME invia un Handover Request message al target eNB, richiedendo un handover per

conto del source eNB. Le informazioni incluse nel messaggio sono le seguenti:

Handover Request (UE-AMBR, E-RAB to be setup (E-RAB ID, QCI, ARP, S1 SGW TEID), Source to Target Transparent Container, UE Security Capability, Security Context)

- **UE-AMBR:** fornito dall'HSS, ma opzionalmente modificabile dall'MME. Questo valore può essere impostato per eNB ed è utilizzato per controllare il Maximum Bit Rate aggregato per tutti i bearer non-GBR.
- **E-RAB to be setup:** informazioni sull'E-RAB dell'UE memorizzate nel Source eNB. Include l'E-RAB ID, parametri QoS, informazioni sull'UL S1 bearer (S1 SGW TEID) **[A]**
- **Source to Target Transparent Container:** è utilizzato per l'inoltro delle informazioni radio-related della source cell (e.g. tecnologie di accesso radio disponibili nell'UE, informazioni di configurazione della connesione RRC, ecc.) alla target cell trasparentemente attraverso la EPC (MME).
- **UE Security Capability:** algoritmi di sicurezza supportati dall'UE (sia di integrità che di cifratura)
- **Security Context:** include le informazioni richieste dal target eNB per poter derivare la AS security base key K_{eNB}^{*}.

6) [Target eNB] Preparazione dell'handover S1

All'atto della ricezione dell'Handover Request message, il target eNB inizia la preparazione dell'handover per assicurare una fornitura di servizio ininterrotta all'UE.

(i) Allocazione delle risorse per il nuovo bearer S1: Il target eNB, sulla base delle informazioni circa l'E-RAB da costruire ("E-RAB to be setup") controlla se lo stesso QoS fornito dal source eNB è disponibile anche nel target eNB. Se lo è, costruisce un UL S1 bearer connesso al SGW, utilizzando le informazioni sull'UL S1 bearer (S1 SGW TEID**[A]**) memorizzate nel source eNB. Dopodiché alloca l'S1 Target eNB TEID**[B]** per preparare il DL S1 bearer da utilizzare quando l'handover sarà terminato.

(ii) Allocazione delle risorse relative al tunnel indiretto: Mentre l'UE sta eseguendo l'handover (i.e. dopo che si è disconnesso dal source eNB, finché non si connette al target eNB), dovrebbe esistere un tunnel indiretto per il reindirizzamento dei pacchetti che arrivano al source eNB verso il target eNB passando per il SGW. Per fare ciò, il target eNB alloca l'S1 Target eNB TEID**[C]** affinché il SGW possa stabilire un tunnel indiretto connesso al target eNB.

(iii) Allocazione delle risorse riservate all'UE per il collegamento radio: Sulla base delle informazioni di QoS dell'E-RAB il target eNB riserva risorse RRC che devono essere utilizzate dall'UE nel collegamento radio (e.g. allocazione del DRB ID, ecc.) ed alloca il C-RNTI.

(iv) Derivazione della chiave K_{eNB}^*: Il target eNB deriva K_{eNB}^* utilizzando le informazioni del security context che ha ricevuto dall'MME per l'handover e poi ottiene le AS security keys (K_{RRCint}, K_{RRCenc}, K_{UPenc}). Quando l'UE, poco dopo, si connette al target eNB i due possono comunicare tra loro in sicurezza lungo il collegamento radio utilizzando le chiavi appena derivate.

7) **[Target eNB → MME] Notifica all'MME del completamento della fase di preparazione**
Il target eNB invia all'MME tutte le informazioni circa le risorse preparate nello step 6), includendole in un Handover Request Ack message. Le informazioni incluse nel messaggio sono le seguenti:

Handover Request Ack (E-RAB Admitted (E-RAB ID, S1 Target eNB TEID, DL S1 Target eNB TEID), Handover Command (Target C-RNTI, Target DRB ID, AS Security Algorithm of Target eNB))

- **E-RAB Admitted:**
  - **E-RAB ID:** E-RAB ID allocato dal target eNB
  - **S1 Target eNB TEID:** DL S1 TEID[B] che il target eNB ha allocato al SGW per la creazione dell'S1 bearer connesso a se stesso da utilizzare dopo l'handover.
  - **DL S1 Target eNB TEID:** DL S1 TEID[C] che il target eNB ha allocato per la creazione di un tunnel indiretto attraverso il quale consegnare pacchetti in DL.
- **Handover Command:** Transparent Container, consegnato dal target eNB al source eNB, che contiene le informazioni radio della target cell di cui l'UE ha bisogno per poter accedere al target eNB.
  - **Target C-RNTI:** C-RNTI allocato dalla target cell per identificare l'UE.
  - **Target DRB ID:** ID del DRB che il target eNB ha riservato per poter inviare i pacchetti utente lungo il collegamento radio.
  - **AS Security Algorithm of Target eNB:** Algoritmi di sicurezza dell'AS supportati dal target eNB.

8) **[MME → SGW] Richiesta di creazione di un S1 bearer per la consegna dei pacchetti in DL**

   L'MME invia al SGW un Create Indirect Data Forwarding Tunnel Request message, richiedendo la creazione di un tunnel indiretto per consegnare i pacchetti in DL mentre l'UE sta eseguendo l'handover. Il messaggio include il GTP TEID (S1 Target eNB TEID[C]) che il target eNB ha allocato per il tunnel

9) **[MME ← SGW] Notifica che il bearer S1 per la consegna dei pacchetti in DL è stato creato**

   Il SGW, quando riceve il Create Indirect Data Forwarding Tunnel Request message, crea un tunnel indiretto in DL connesso al target eNB. Dopodiché alloca l'S1 SGW TEID[D] e lo inoltra per mezzo di un Create Indirect Data Forwarding Tunnel Response message all'MME cosicché il source eNB può creare un tunnel indiretto connesso al SGW.

10) **[Source eNB ← MME] Notifica del completamento dell'Handover**

    L'MME invia al source eNB un Handover Command message che include il S1 SGW TEID[D] ricevuto dal SGW nello step 9), e le informazioni contenute nell'Handover Command ricevuto dal target eNB nello Step 7).

    Il source eNB viene a conoscena dall'Handover Command message che il target eNB e la EPC sono pronte per l'handover dell'UE.

▪ **Esecuzione dell'Handover**

La Figura 76 mostra le procedure per la fase di esecuzione dell'handover S1.

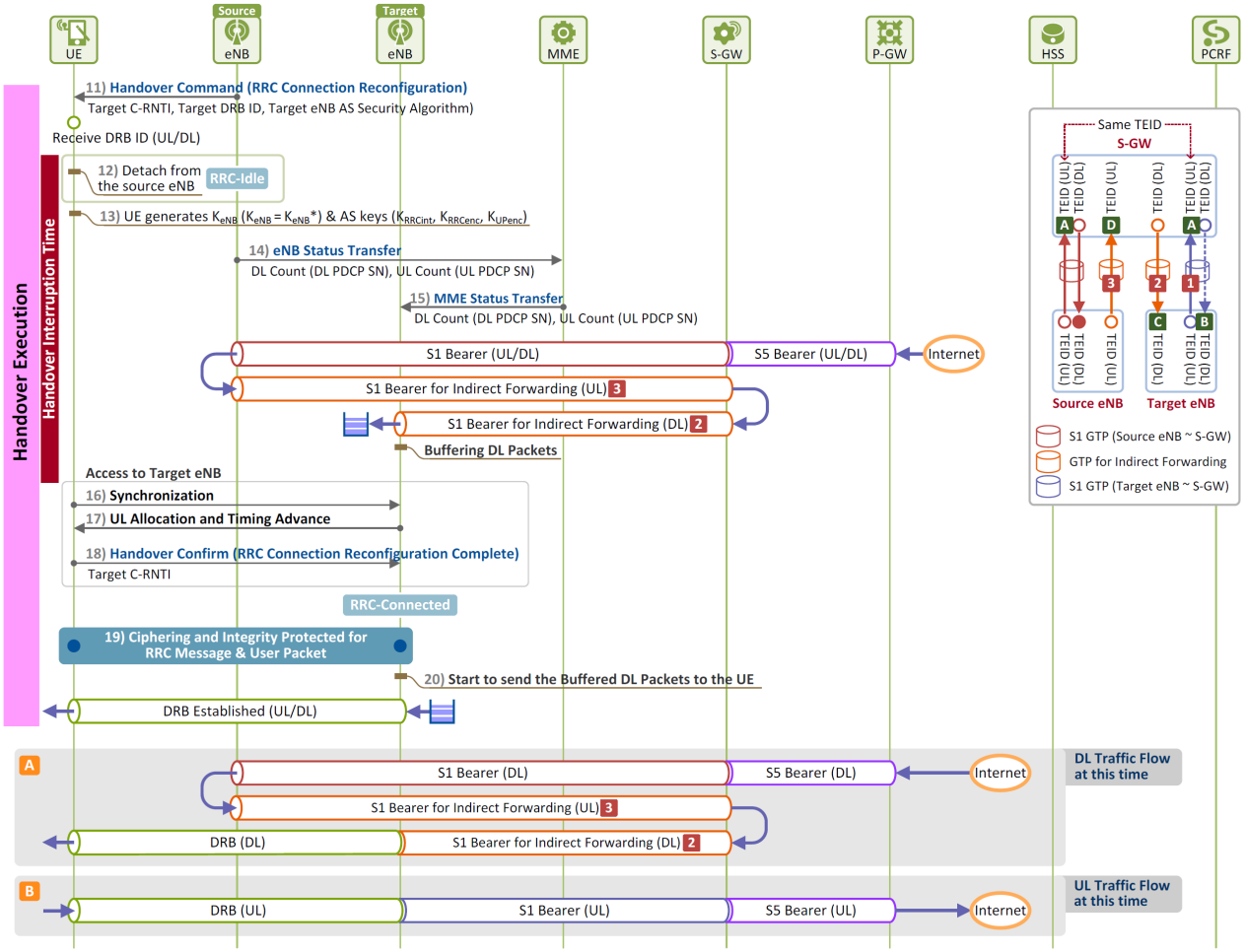


Figura 76 S1 Handover – Fase di esecuzione

11) [UE ← Source eNB] Ordine all'UE di effettuare un handover

Una volta che il source eNB è pronto per l'handover, ordina all'UE di effettuare l'handover inviando un Handover Command message. L'Handover Command message viene consegnato all'UE, includendolo in un RRC Connection Reconfiguration message.

12) [UE] Esecuzione dell'handover

Una volta che l'UE ottiene, dall'Handover Command message ricevuto, il C-RNTI e il DRB ID da utilizzare nella target cell, si disconnette dal source eNB. Ora, tutti gli scambi di pacchetti tra l'UE e il source eNB vengono fermati ed incomincia l'handover interruption time.

13) [UE] AS Security Setup

L'UE deriva le AS security keys da utilizzare per la comunicazione radio col target eNB. Dapprima deriva K_{eNB}^*, la AS base key, dopodiché utilizzando la chiave appena ricavata e gli

algoritmi di sicurezza dell'AS selezionati dal target eNB deriva le AS security keys (K_{RRCint}, K_{RRCenc}, K_{UPenc}).

14) **~15) [Source eNB → MME, MME → Target eNB] Notifica del numero di pacchetto dal quale iniziare a ricevere/inviare**

Il source eNB invia un eNB Status Transfer mssage che include DL Count e UL Count all'MME il quale a sua volta inoltra queste informazioni per mezzo di un MME Status Transfer message al target eNB. Da queste informazioni il target eNB viene a conoscenza del numero di pacchetto dal quale deve iniziare ad inviare/ricevere al/dall'UE. Le informazioni incluse nel messaggio sono le seguenti:

eNB Status Transfer (DL Count, UL Count):

- **DL Count:** Contatore del primo pacchetto da inviare all'UE
- **UL Count:** Contatore del primo pacchetto da ricevere dall'UE

Dopo aver inviato l'eNB Status Transfer message, il source eNB inizia ad inoltrare i pacchetti in DL in arrivo dal SGW al target eNB attraverso il tunnel indiretto stabilito lungo l'interfaccia S1. Il target eNB bufferizza i pacchetti ed attende che l'UE abbia completato l'accesso.

16) **~18) [UE, Target eNB] Accesso dell'UE al target eNB**

L'UE avverte il segnale di sincronizzazione dal target eNB per eseguire la sincronizzazione. Una volta completate le procedure di sincronizzazione invia al target eNB un Handover Confirm message includendolo in un RRC Connection Reconfiguration message. Ora, l'UE può inviare/ricevere pacchetti da/al target eNB per cui l'handover interruption time termina.

19) **[UE ~ Target eNB] Comunicazione sicura lungo il collegamento radio**

Tutti i messaggi di signaling RRC e i pacchetti dati utente che vengono inviati lungo il canale radio tra l'UE ed il target eNB sono ora consegnati in sicurezza utilizzando le chiavi di sicurezza dell'AS. In particolare i messaggi di signaling RRC vengono protetti per l'integrità e criptati mentre i pacchetti dati utente sono criptati prima di essere inviati.

20) **[Target eNB] Ripresa della consegna dei pacchetti in DL all'UE**

Quando l'UE risulta connesso con successo al target eNB, quest'ultimo riprende ad inviare i pacchetti bufferizzati lungo il seguente percorso (rif. **[A]** nella Figura 76).

S5 bearer (PGW a SGW) → S1 bearer **(**SGW a source eNB) → S1 bearer (source eNB a SGW) → S1 bearer (SGW a target eNB) → DRB **(**target eNB ad UE)

Nel caso in cui i pacchetti siano inviati dall'UE, il target eNB controlla se i pacchetti in UL sono ricevuti in ordine corretto, dopodiché provvede ad inoltrarli al SGW lungo il seguente percorso (rif. **[B]** nella Figura 76):

DRB (UE a target eNB) → S1 bearer (target eNB a SGW) → S5 bearer (SGW a PGW).

- **Completamento dell'Handover**

La Figura 77 mostra le procedure per la fase di completamento dell'handover S1.

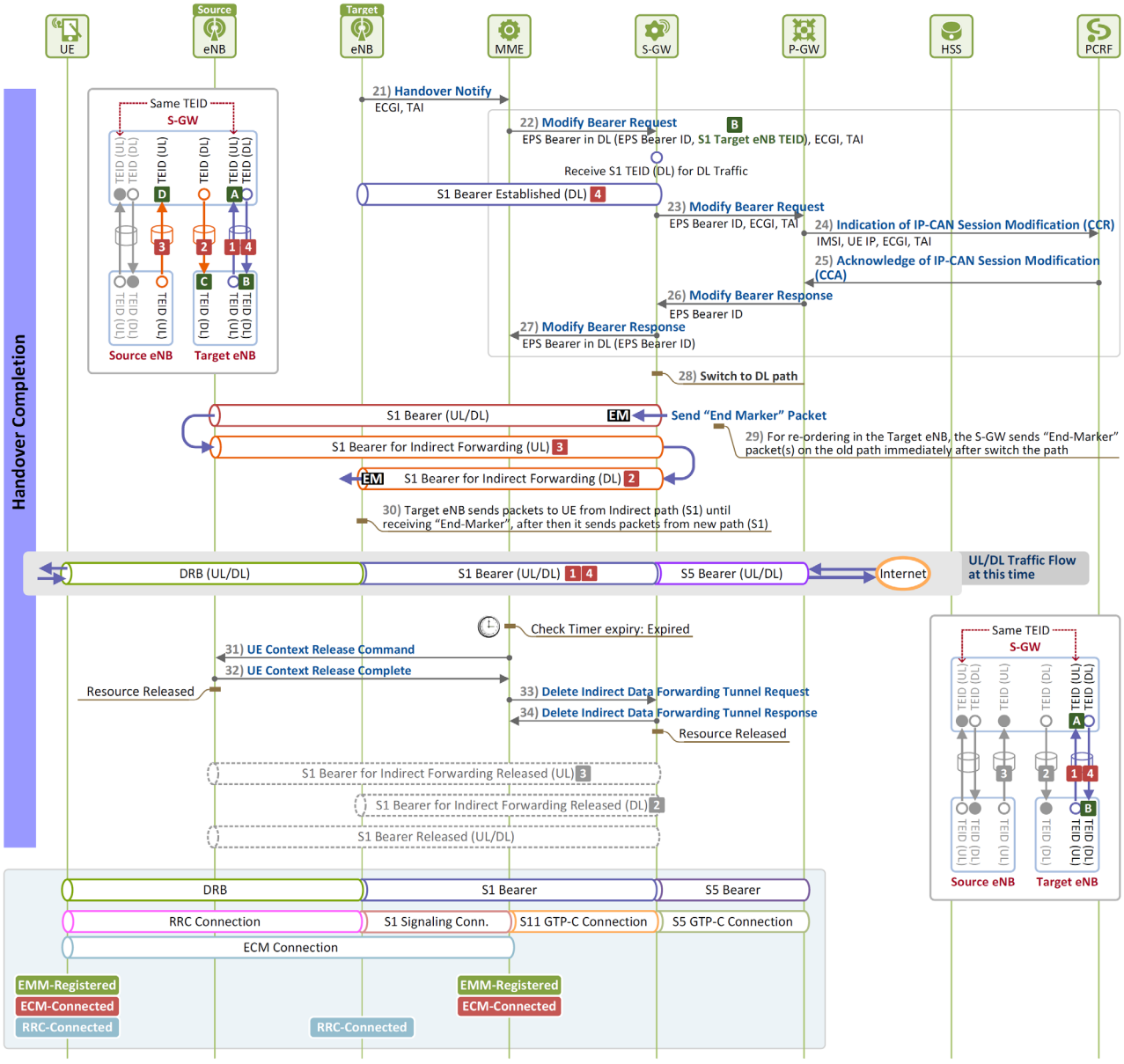


Figura 77 S1 Handover - Fase di completamento

21) [UE ← Source eNB] Richiesta di Path Switch dell'EPS bearer (S1 bearer)

Una volta che l'UE ha acceduto correttamente al target eNB, quest'ultimo notifica alla EPC (MME) che l'UE ha completato con successo l'handover S1 inviando un Handover Notify message che include il suo ECGI e il TAI.

22) ~27) Modifica del Bearer EPS

L'MME inoltra il S1 Target eNB TEID [A] che è stato allocato dal target eNB al SGW inviando un Modify Bearer Request message. In questo modo richiede al SGW di modificare il percorso del bearer. Dopodiché il SGW crea un DL S1 bearer connesso al target eNB, come richiesto. In alcuni casi, sulla base delle opzioni impostate durante la fase di Initial Attach dell'UE, è richiesto al SGW da parte della rete di riportare se la serving cell dell'UE è cambiata. In questo caso, il SGW invia un Modify Bearer Request message al PGW il quale a sua volta notifica al PCRF, sulla base delle procedure di modifica della EPS session, che la serving cell dell'UE è cambiata.

28) ~29) [SGW] Modifica del percorso dell'EPS Bearer (S1 bearer)

Il SGW cambia il percorso dei pacchetti in DL utilizzando il DL S1 bearer connesso al target eNB. Per fare ciò, dapprima invia un End Marker (EM) ad indicare l'ultimo pacchetto in transito lungo il DL S1 bearer connesso al source eNB. Dopodiché, invia i pacchetti in DL al target eNB attraverso il DL S1 bearer modificato.

30) [Target eNB] Riordino dei pacchetti

Ora il target eNB riceve i pacchetti in DL inoltrati dal source eNB attraverso il tunnel indiretto e quelli inviati dal SGW attraverso il nuovo percorso. In questo modo, dovrebbe essere in grado di consegnarli all'UE nell'ordine corretto. Prima di tutto, inoltra i pacchetti in DL ricevuti attraverso il tunnel indiretto all'UE. Poi quando l'EM arriva, riconosce che quello appena inoltrato era l'ultimo di quel percorso, di conseguenza, da lì in avanti inoltra all'UE i pacchetti ricevuti dal nuovo percorso.

31) ~32) [Source eNB ←→ MME] Rilascio dell'UE Context e delle risorse S1 appartenenti al source eNB

L'MME informa il source eNB che può rilasciare l'UE context e le risorse (S1 bearer e tunnel indiretto) che ha riservato lungo l'interfaccia S1 e inviando un UE Context Release Command message. Il source eNB allora rilascia l'UE context e le risorse S1 ed informa l'MME di tale azione, inviandogli un UE Context Release Complete message.

33) ~34) [MME ←→ SGW] Rilascio del tunnel indiretto

L'MME invia al SGW un Delete Indirect Data Forwarding Tunnel Request message, richiedendo il rilascio del tunnel indiretto.

All'atto della ricezione della richiesta, il SGW rilascia il tunnel indiretto, ed informa l'MME di ciò inviandogli un Delete Indirect Data Forwarding Tunnel Response Message.

3.6.4 Handover con TAU

La Figura 78 mostra una procedura di handover eseguita quando l'UE in stato Connected si sposta in una TA nella quale non è registrato. Quando l'UE ha effettuato il collegamento iniziale alla rete, l'MME ha selezionato TA1 e TA2 come TA per l'UE e gli ha inviato la TAI list = {TAI = 1, TAI = 2}, includendolo nel messaggio Attach Accept. Inizialmente l'UE era agganciato all'eNB 2 (Cella 5) nella TA1. Ora si sta muovendo verso l'eNB 5 (Cella 13) nella TA3 che non è presente nella sua TAI list. In questo caso consideriamo solo handover intra-LTE per cui assumiamo che entrambi gli eNB, eNB2 ed eNB 5 siano connessi allo stesso MME ed allo stesso SGW.

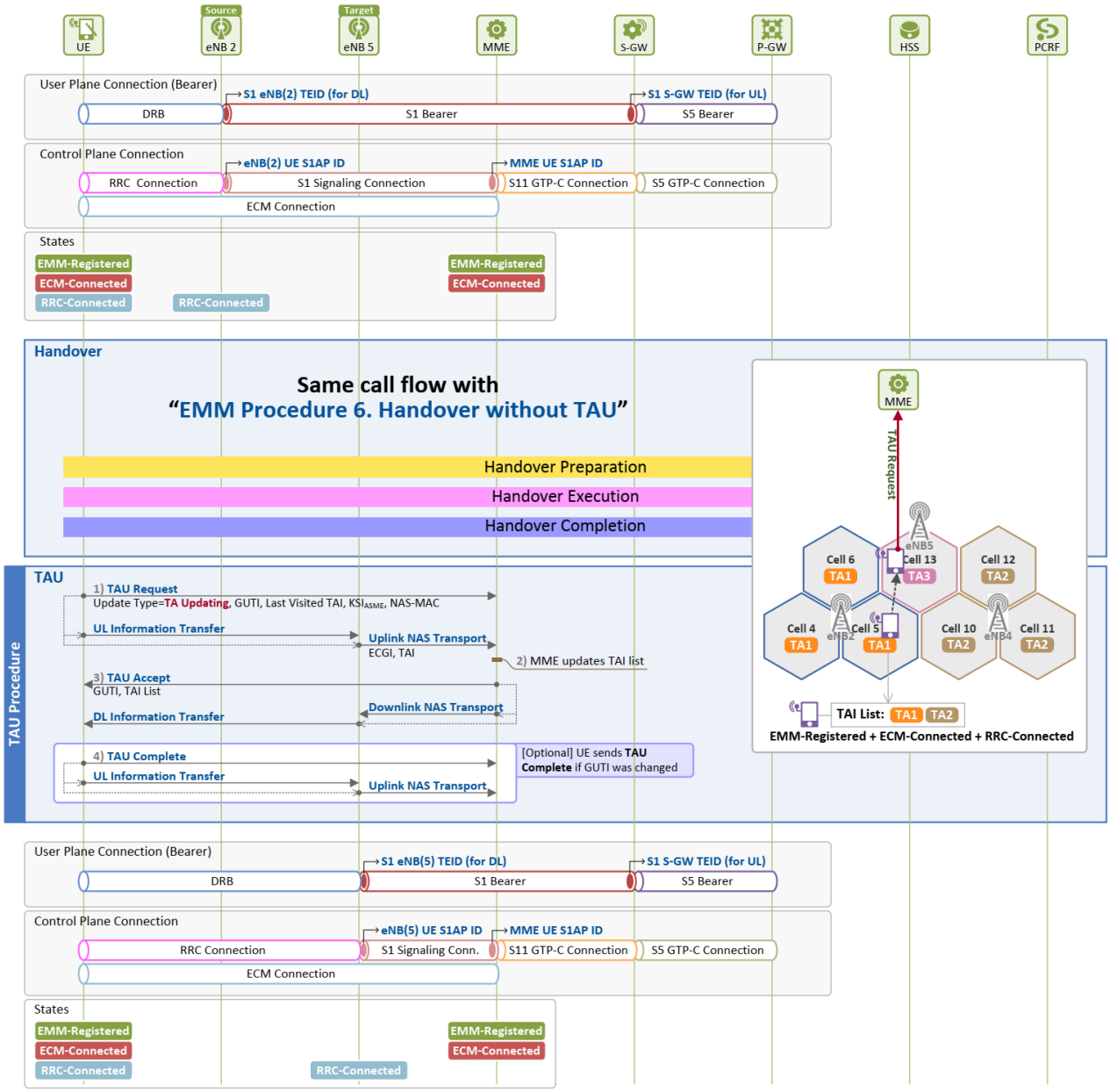


Figura 78 Handover (ad una TA non registrata)

▪ **Handover**

Nella Figura 78, mentre l'UE si dirige verso l'eNB 5 viene scatenato un handover event. L'UE misura la potenza del segnale della serving cell e delle celle vicine e invia i risultati all'eNB 2, includendoli nel Measurement Report message. Per prima cosa, il source eNB (e.g. eNB 2 in Figura 78) sceglie il tipo di handover da effettuare, X2 o S1 (in un handover X2 è il source eNB che seleziona il target eNB (e.g. eNB 5 in Figura 78), mentre nell'handover S1 è l'MME a sceglierlo) dopodiché viene eseguito l'handover.

▪ **Tracking Area Update (TAU)**

1) **[UE → MME] TAU Request**

Quando si aggancia al target eNB (eNB 5), l'UE riconosce che l'eNB 5 non appartiene alle TA ad esso assegnate. Di conseguenze, non appena l'handover è stato completato invia una TAU Request (Update Type = TA Updating, GUTI, Last Visited TAI, KSI_{ASME}, NAS-MAC) all'MME per richiedere il TA Update. Il messaggio include le seguenti informazioni:

TAU Request (Update Type = TA Updating, GUTI, Last Visted TAI, KSI_{ASME}, NAS-MAC)

- **Update Type:** Indica il tipo di TAU. Impostato a TA Updating a meno che l'UE non si sposti in una TA registrata
- **GUTI**
- **Last Visited TAI:** TAI riportato nell'ultima TAU Request effettuata
- **KSI_{ASME}:** message authentication code utilizzato per la protezione di integrità del messaggio con la NAS integrity key.

Il TAU Request message viene inviato mediante un messaggio UL Information Transfer (messaggio RRC), dall'UE all'eNB e poi attraverso un messaggio S1AP, Uplink NAS Transport (NAS-PDU (TAU Request), ECGI, TAI) dall'eNB all'MME. Il messaggio Uplink NAS Transport, che include la TAU Request e l'ECGI e TAI della cella corrente viene inoltrato all'MME.

Dato che un NAS Security Context è già stato creato tra l'UE e l'MME, il TAU Request message inviato dall'UE è integrity-protected con la NAS integrity key (K_{NASint}). Se i controlli effettuati sull'intergrità del messaggio ricevuto dall'MME falliscono, l'MME esegue le procedure di autenticazione e NAS Security Setup. In questa trattazione viene considerato il solo caso in cui il controllo di integrità sul messaggio termina con esito positivo

2) **[MME] TA Update: Allocazione delle nuove TA**

   Siccome l'UE si è spostato in una TA non registrata, l'MME seleziona un insieme di TA da allocare e configura una nuova TAI list per l'UE. In questo momento può venire allocato anche un nuovo GUTI, in base alla specifica implementazione delle procedure da parte degli operatori.

3) **[UE ← MME] TAU Accept**

   L'MME invia la nuova TAI list allocata all'UE (ed eventualmente un nuovo GUTI) includendola in un TAU Accept (GUTI, TAI list) message criptato ed integrity-protected che viene inviato attraverso un Downlink NAS Transport Message dall'MME all'eNB (come messaggio S1AP) e poi attraverso un DL Information Transfer message (come messaggio RRC) dall'eNB all'UE.

4) **[UE → MME] TAU Complete**

   Se è stato allocato un nuovo GUTI, l'UE invia all'MME un TAU Complete message per confermare l'avvenuta ricezione del nuovo GUTI.

A questo punto, la procedura di Tracking Area Update è completata e l'UE con la su nuova TAI list (ed eventualmente un nuovo GUTI) può essere servito dal nuovo eNB (eNB 5).

3.7 Cell Reselection

Mentre l'handover controlla la mobilità dell'UE in stato Connected (**EMM-Registered, ECM-Connected, RRC-Connected),** la procedura di Cell Reselection esegue lo stesso compito quando l'UE si trova in Idle mode (**EMM-Registered, ECM-Idle, RRC-Idle).**

Durante un handover è la rete (MME o source eNB) che decide verso quale cella effettuare l'handover. Durante la cell reselection, invece, è l'UE che determina a quale cella agganciarsi.

Una Cell Reselection procedure può essere di due tipi come mostrato in Figura 79 sotto. In Figura 79, l'UE è agganciato alla Cella 5 che appartiene alla TA list {TA1, TA2} assegnata in precedenza dall'MME al tempo del collegamento iniziale e si trova attualmente in Idle state.

I due tipi di Cell Reselection possono essere:

- **Cell Reselection senza TAU** (7️⃣): l'UE si sposta in una TA che è registrata all'MME (cioè che appartiene alla TAI list assegnata all'UE), come ad es. la TA2 in Figura 79. La procedura di Cell Reselection viene eseguita ma non è richiesto un Tracking Area Update (TAU).
- **Cell Reselection con TAU (**9️⃣**)**: l'UE si sposta in una TA che NON E' registrata presso l'MME (cioè che NON E' presente nella TAI list assegnata all'UE), come ad es. la TA3 in

Figura 79. Dopo la cell reselection viene eseguito un TAU.

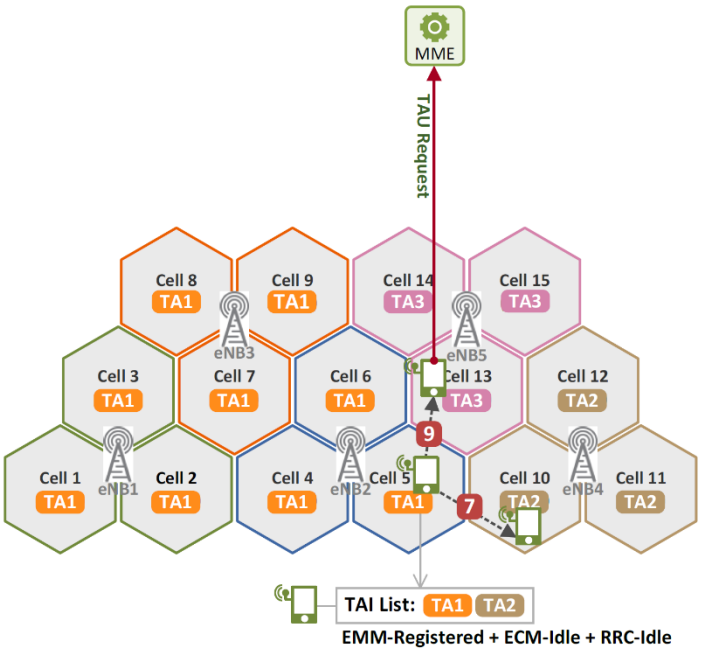


Figura 79 I due tipi di Cell Reselection

3.7.1 Panoramica della procedura di Cell Reselection

Come già detto in precedenza, è l'UE a controllare la procedura di cell reselection. L'UE ottiene le informazioni necessarie per la cell reselection (ad es. i valori di soglia utilizzati per decidere se misurare o meno la potenza del segnale delle celle vicine etc.) dalle system information diffuse in broadcast dall'eNB.

L'UE in Idle state, si risveglia al termine di ogni ciclo DRX per misurare il segnale della sua serving cell ($Q_{rxlevmeas}$) e calcoalre il livello di segnale ricevuto (Srxlev) della serving cell per decidere se deve rimanere o spostarsi su un'altra cella.

Se il livello di segnale ricevuto dalla serving cell (**Srxlev**) è maggiore del valore di soglia impostato (s-IntraSearch), l'UE rimane agganciato alla serving cell attuale. In caso contrario, scatena una procedura di Cell Reselection.

L'UE classifica quindi ogni cella (R_s, R_n) sulla base della potenza del segnale misurato della serving cell ($Q_{meas,s}$) e delle neighbour cells ($Q_{meas,n}$). I parametri richiesti sono diffusi in broadcast dalle System Information. La serving cell è valutata considerando un valore di isteresi (q-Hyst) che viene aggiunto al valore effettivamente misurato, mentre le neigbour cells sono valutate sottraendo al valore misurato un offset (q-OffsetCell). Se ci sono celle che soddisfano il criterio ($R_n > R_s$), l'UE si aggancia alla cella migliore. La cell reselection viene eseguita solo se il criterio di riselezione rimane soddisfatto per un certo periodo di tempo (t-ReselectionEUTRA). Inoltre, per prevenire cell

reselection troppo frequenti gli operatori possono applicare anche degli scaling factors ai parametri q-Hyst e t-ReselectionEUTRA in considerazione della velocità di movimento dell'UE.

3.7.2 System Information

Col termine System Information si intendono le informazioni diffuse in broadcast dall'eNB e consistono di MIB (Master Information Block) e SIB (System Information Blocks, SIBs 1~16). MIB, SIB1 e SIB 2 sono obbligatorie mentre le altre sono facoltative. Tutte le SI sono consegnate all'UE per mezzo di messaggi RRC, MIB, SIB1 o SI. Un SI message consiste di un gruppo di SIB (SIBs 2~16), escludendo MIB e SIB1.

L'UE effettua la cell reselection procedure sulla base delle SI diffuse in broadcast da un eNB. MIB, SIB1 e SIB2 sono applicati a tutti gli UE, sia che si trovino in stato Connected che Idle. Al contrario le SIB 3~8 sono usati solo per la cell reselection in Idle state.

Tabella 14 System Information relative alla Cell Reselection

Type		Description	Parameters
Mandatory	MIB	• Mandatory for UE to access a cell	DL bandwidth, SFN, HARQ channel (PHICH) info
	SIB 1	• Provides-information relating to granting/restricting cell access • Defines scheduling of other SIBs	Access restriction info, Cell selection info, Scheduling info for other SIBs
	SIB 2	• radio resource configuration information common for all UEs	Common and shared channel info (RACH, BCCH, PCCH, PRACH, PDSCH, PUSCH, PUCCH, Sounding RS, UL Power Control), Sub-frame for MBSFN
Cell reselection-related SIBs	SIB 3	• Information commonly used in all types of cell reselection (intra-frequency, inter-frequency and/or inter-RAT) • Intra-frequency cell reselection information other than neighbor cell related	q-Hyst, s-NonIntraSearch, threshServingLow, cellReselectionPriority q-RxLevMin, p-Max, s-IntraSearch, t-ReselectionEUTRA, q-QualMin
	SIB 4	• Information on neighbor cells related only to intra-frequency cell reselection	intraFreqNeighCellList (*physCellId, q-OffsetCell*), intraFreqBlackCellList (*physCellId Range*), CSG-PCI Range
	SIB 5	• Information on other E-UTRA frequencies and neighbor cells related only to inter-frequency cell reselection	Supported E-UTRA frequency list (E-UTRA frequency, Neighbor cell list, Black cell list, Reselection threshold)
	SIB 6	• Information for Inter-RAT (UTRA) cell reselection	UTRA frequency
	SIB 7	• Information for Inter-RAT (GERAN) cell reselection	GERAN frequency
	SIB 8	• Information for Inter-RAT (CDMA2000) cell reselection	CDMA 2000 frequency

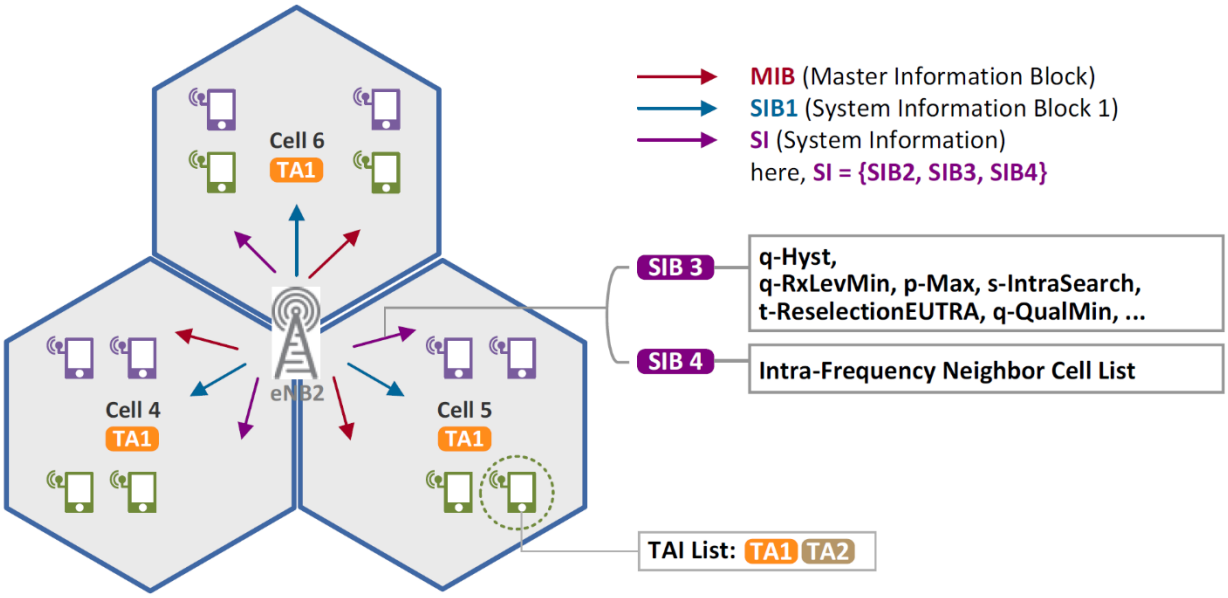


Figura 80 SIB relativi alla Cell Reselection diffuse dall'eNB2

	Parameters	Description
SIB 3	cellReselectionInfoCommon	Cell reselection information common for all cells
	q-Hyst	· hysteresis value for ranking criteria
	speedStateReselectionPars	· Reselection parameters depending on UE's speed
	mobilityStateParameters	· Parameters to determine the mobility state of UE
	q-hystSF	· Scaling factor for Q_{hyst} that varies depending on UE's speed · If medium or high mobility state is detected, sf-Medium or sf-High value is added to Q_{hyst} value
	Sf-Medium	
	Sf-High	
	intraFreqCellReselectionInfo	Cell reselection information to be sued for intra-frequency cells
	q-RxLevMin	· Minimum Rx level required for UE to continue to camp on the cell [dBm]
	p-Max	· Maximum TX power level allowed for UE [dBm] · Used to limit the Tx power of UE, and used in computing $P_{Compenation}$ (see Section 2.3)
	s-IntraSearch	· Srxlev threshold value that triggers intra-frequency measurement [dB] · If Srxlev is lower than *s-IntraSearch*, UE begins to measure neighbor cells within the same frequency.
	allowedMeasBandwidth	· DL Bandwidth to be measured by UE
	presenceAntennaPort1	· Indicates whether neighbor cells use Antenna Port 1 or not
	neighCellConfig	· Information relating to MBSFN of neighbor cells
	t-ReselectionEUTRA	· Cell reselection timer value. A cell reselection criterion has to be satisfied for longer than this value in order for reselection to be performed.
	t-ReselectionEUTRA-SF	· Scaling factor for t-ReselectionEUTRA that varies depending on UE's speed.
	lateNonCriticalExtension	Intra-frequency cell reselection information added in Release 9
	s-IntraSearchP	· Srxlev threshold value that triggers intra-frequency measurement [dB]
	s-IntraSearchQ	· Squal threshold value that triggers intra-frequency measurement [dB]
	q-QualMin	· Minimum quality level required for UE to continue to camp on the cell [dB]
SIB 4	intraFreqNeighCellList[7]	List of intra-frequency neighbor cells that have cell specific q-Offset values
	physCellId	· PCI of a neighbor cell
	q-OffsetCell	· Offset between the current cell on which the UE is camping and neighbor cell
	intraFreqBlackCellList	List of neighbor cells that are not subject to reselection
	physCellId Range	· PCI range

Figura 81 Parametri per la Cell Reselection (SIB 3 e 4)

3.7.3 Dettaglio della procedura di cell reselection senza TAU

In Figura 82, l'UE ha selezionato la Cella 5 e gli era stata allocata una TA list di {TA1, TA2} dall'MME al termine della procedura di initial attach. Successivamente l'UE è transitato in Idle state, rimanendo connesso alla Cella 5.

La Figura 82 mostra l'UE agganciato alla Cella 5 mentre esegue una procedura di cell reselection intra-frequency andandosi ad agganciare alla Cella 10 dell'eNB 4. In questo caso, il mobility state dell'UE è "Normal" per cui non vengono considerati scaling factors.

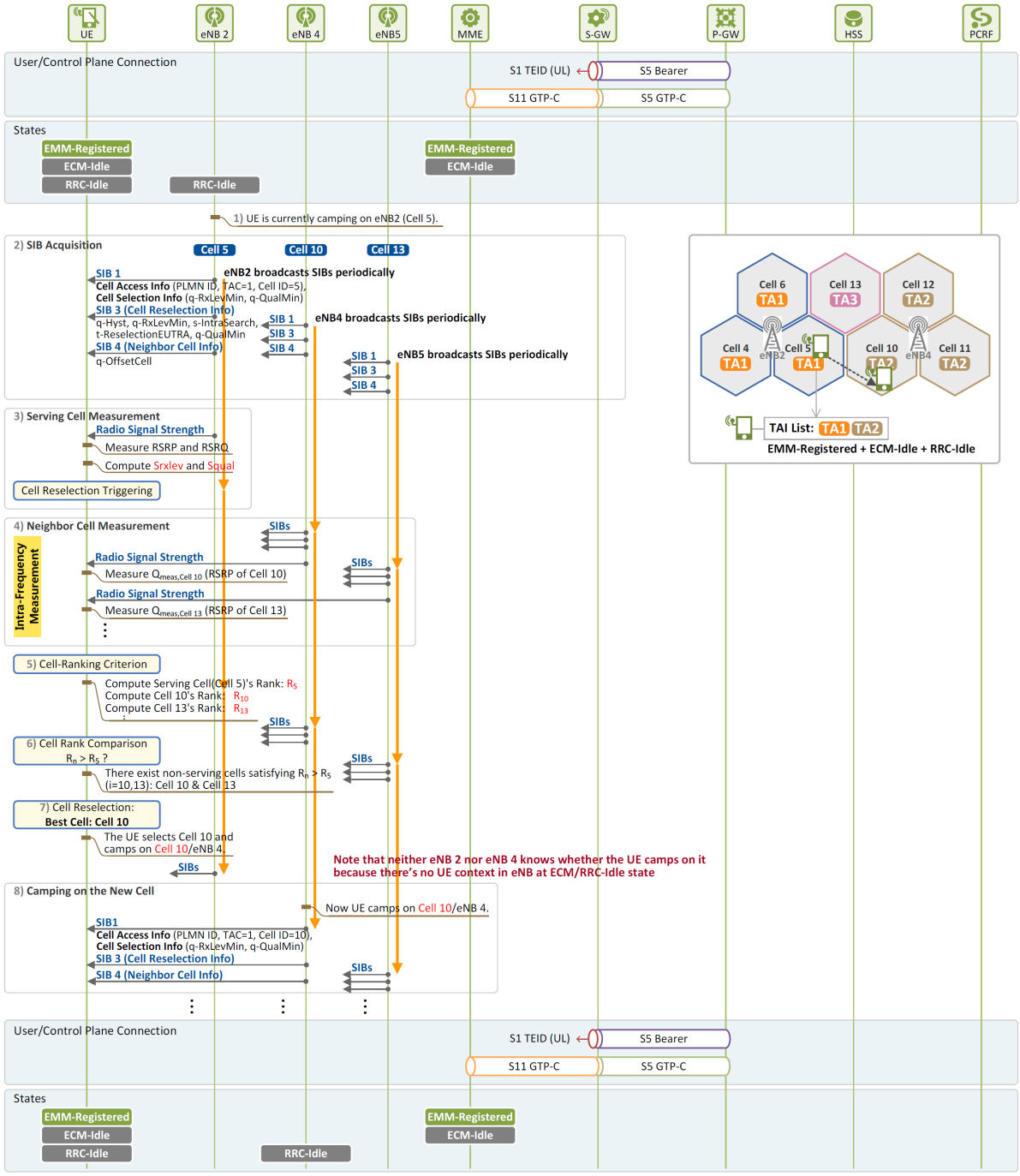


Figura 82 Procedura Intra-frequency Cell Reselection (UE si sposta in una TA registrata)

1) **[UE] L'UE è agganciato alla Serving Cell**

   L'UE è agganciato alla sua serving cell (i.e. Cella 5 in eNB2) e si trova in Idle mode

2) **[UE] L'UE ottiene le SI dalla Serving Cell**

   L'UE ottiene le SI richieste per la cell reselection dalla serving cell. Se ogni neigbor cell ha valori di offset differenti, la serving cell fornisce all'UE la lista delle neigbor cells attraverso la SIB 4. Dopodiché l'UE acquisisce i parametri richiesti per il triggering della cell reselection ed il ranking della serving cell e delle neighbour cells attraverso i SIBs 3 e 4.

3) **[UE] Misurazione della potenza del segnale della Serving Cell**

   Al termine di ogni ciclo DRX (Discontinuous Reception), l'UE si risveglia e misura il segnale della serving cell (RSRP ed RSRQ) per ottenere $Q_{rxlevmeas}$ e $Q_{qualmeas}$.

   Sulla base dei valori ottenuti, calcola il cell reselection received level (Srxlev) e il cell reselection quality level (Squal). L'UE sulla base poi dei valori di soglia ricevuti attraverso i SIB (s-IntraSearchP ed s-IntraSearchQ) determina se è necessario selezionare una nuova cella alla quale agganciarsi. Se i criteri sono soddisfatti allora esegue la cell reselection (che inizia dallo step 4)

4) **[UE] Misurazione del segnale delle celle vicine**

   L'UE misura la potenza del segnale (RSRP) delle celle vicine che sono nella stessa frequenza della serving cell ($Q_{meas,n}$, n=4, 6, 10, 13)

5) **[UE] Ranking delle celle in base ai valori ottenuti**

   Una volta che l'RSRP delle celle è stato misurato, l'UE calcola il ranking della serving cell (Cella 5) e delle celle vicine (Celle 4, 6, 10, 13).

6) **[UE] Comparazione dei risultati di ranking ottenuti**

   Ora, l'UE compara il Rank R_5 e il Rank R_n (n = 4,6, 10, 13) e controlla se esiste una neigbour cell per la quale risulta Rn > Rs. Se questo non avviene continua a rimanere agganciato alla serving cell attuale.

7) **[UE] Selezione di una nuova cella**

   L'UE compara le due celle che soddisfano il criterio, R_{10} ed R_{13}, e seleziona R_{10}, la cella con ranking migliore come sua nuova serving cell.

8) **[UE] Collegamento alla nuova cella**

   L'UE si aggancia quindi alla nuova cella. Dopo aver ricevuto il SIB 1 diffuso in broadcast dalla Cella 1, viene a conoscenza del fatto che la Cella 10 si trova in una TA presente nella TAI list allocatagli, per cui non deve effettuare un TAU.

   Da qui in avanti, l'UE si risveglia alla fine di ogni ciclo DRX per monitorare le system e paging information della Cella 10 e misurare il segnale ricevuto (in termini di potenza e qualità).

3.7.4 Cell reselection con TAU

La Figura 83 illustra la procedura di cell reselection richiesta quando un UE in Idle state si sposta in una TA nella quale non è registrato. In Figura 83, l'UE agganciato alla Cella 5 dell'eNB 2 si sposta verso la Cella 13 dell'eNB 5.

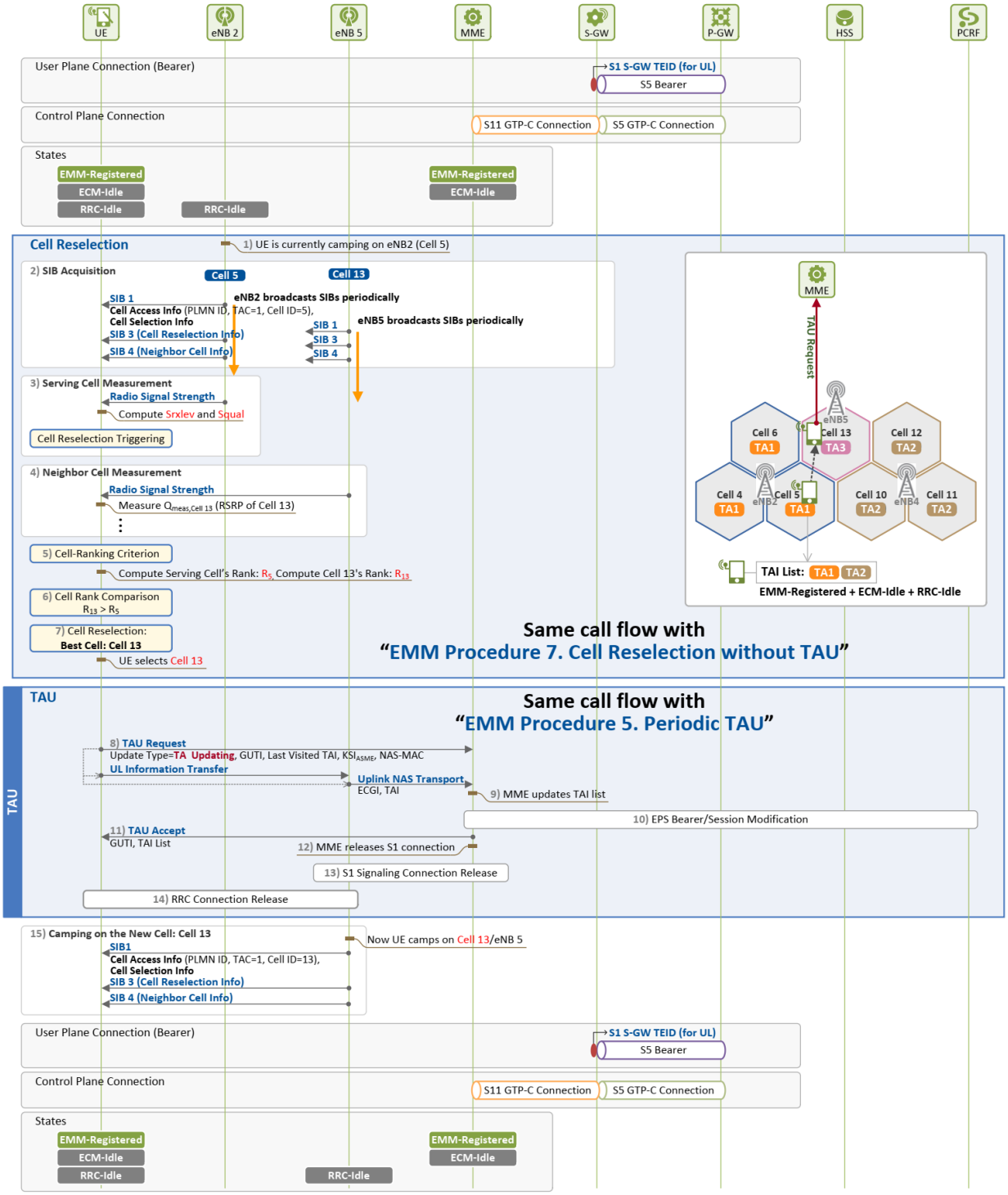


Figura 83 Intra-frequency cell reselection (quando l'UE si sposta in una TA non registrata)

▪**Cell Reselection**

1)~7) [UE] Cell Reselection

L'UE si sposta verso l'eNB5, scatenando una cell reselection. Misura quindi la potenza del segnale delle celle vicine, le classifica e poi seleziona la Cella 13 (all'eNB 5) come la migliore cella che soddisfa i criteri per la cell reselection. La procedura utilizzata per la cell reselection è la stessa già indicata in precedenza per il caso di Cell Reselction senza TAU.

▪ **Tracking Area Update**

Quando seleziona la Cella 13 (all'eNB 5) durante la procedura di Cell Reselection, l'UE sa che la cella non appartiene ad una delle TA assegnategli in precedenza. Quindi, esegue un TAU non appena la procedura di Cell Reselection termina. La procedura di TAU è la stessa che viene effettuata per il TAU periodico e l'unica differenza risiede nell'evento che scatena la procedura di TAU. Nel caso di TAU periodico, l'UE esegue un TAU per riferire la sua posizione corrente alla rete in seguito alla scadenza del TAU timer mentre nel caso di TAU eseguito dopo una cell reselection, l'UE lo effettua perché si è spostato in una TA non registrata. Quindi nel caso di TAU in seguito a cell reselection il parametro "Update Type" nella TAU Request viene valorizzato a "TA Updating" mentre nel caso di TAU periodico viene impostato a "Periodic Updating".

8) [UE → MME] TAU Request

L'UE richiede il TA Update inviando una TAU Request (Update Type = TA Updating, GUTI, Last Visited TAI, KSI_{ASME}, NAS – MAC) all'MME. Il messaggio viene inviato integrity-protected con la NAS integrity key. L'UE stabilisce una connessione RRC con l'eNB ed invia il messaggio transitando quindi dallo stato Idle (EMM-Registered, ECM/RRC-Idle) allo stato Connected (EMM-Registerd, ECM/RRC-Connected).

9) [MME] TA Update: Allocazione di una nuova TA

Quando l'MME riceve la TAU Request inoltratagli attraverso un Uplink NAS Transport message, l'MME identifica la TA nella quale l'UE si trova attualmente (ad es. TA3 in Figura 83) dal TAI incluso nell'Uplink Nas Transport message ed anche l'ultima TA riportata (TA1 nel caso in Figura 83) dal parametro Last Visited TAI incluso nella TAU Request.

Siccome la TA in cui l'UE si trova attualmente non appartiene alla TAI list allocatagli in precedenza, l'MME in base al valore del parametro "Last Visited TAI" alloca un nuovo set di TA che rifletta al meglio la posizione corrente dell'UE e la sua velocità di movimento. Perciò, ad un UE che si muove velocemente può essere assegnato un range più ampio di TA così da ridurre il traffico di signaling causato dal TAU. In tal caso però, il carico di signaling causato

dal paging può aumentare e la risposta ad un messaggio di paging può impiegare più tempo ad arrivare quando una chiamata o un pacchetto è in attivo per un UE in Idle state. Nell'allocazione delle TAI list viene quindi considerato il trade-off che si ha tra il carico di signaling per TAU e le performance di paging.

L'MME, inoltre, aggiorna il valore "Last Visited TAI" incluso nell'UE context con il valore corrente del TAI dell'UE.

10) [MME, SGW, PGW, PCRF] EPS Bearer/Session Modification

Dato che la posizione dell'UE è cambiata, l'MME informa il SGW di questo cambiamento inviando un Modify Bearer Request message. Se all'MME è richiesto di riportare il cambiamento di TA al PCRF, in base ai parametri "Change Report Action" ricevuti dal PCRF quando è stata creata la EPS Session in fase di initial attach, viene eseguita una procedura di EPS Session Modification per riportare il cambiamento di TA al PCRF.

11) [UE ← MME] TAU Accept

L'MME invia all'UE una nuova TAI list (ed eventualmente un nuovo GUTI) attraverso un TAU Accept (GUTI, TAI list) message. Le informazioni incluse nel messaggio sono quelle già riportate per il caso di Handover con TAU ed il mesaggio viene inviato criptato ed integrity-protected.

12)~15) [UE, eNB, MME] Transizione in Idle state

Dopo aver concluso la procedura di TAU, l'MME rilascia la connessione di signaling S1 (tra sé e l'eNB 5) dopodiché l'eNB 5 rilascia la connessione RRC stabilita con l'UE. Fatto questo, la connessione ECM tra UE ed MME non esiste più quindi l'UE transita di nuovo in Idle state. Una volta in Idle state, l'UE è agganciato alla cella 13. Si risveglierà poi al termine di ogni ciclo DRX per misurare il segnale della cella 13 in termini di potenza e qualità (RSRP ed RSRQ).

Conclusioni

In questo lavoro è stata illustrata l'architettura di una rete mobile (con particolare riferimento alle reti mobili 4G) nonché il funzionamento in dettaglio delle procedure di mobilità che garantiscono all'utente la possibilità di usufruire dei servizi offerti da varie reti esterne (ad es. Internet, IP Multimedia Subsystem ecc.) in qualunque posto egli si trovi.

Le reti 4G però presentano ancora latenze troppo elevate in relazione alle esigenze di real-time processing dei dati. Ad oggi sempre più dati non risiedono all'interno di data center centralizzati ma vengono prodotti in tempo reale da sensori connessi in rete sparsi nel territorio e devono essere elaborati il più possibile vicino al sito di produzione al fine di non incorrere in latenze maggiori previste dall'utilizzo di infrastrutture cloud pubbliche (c.d. *edge computing*).

Risulta quindi evidente che un'architettura come quella delineata nel Capitolo 1 non sia la scelta ottimale per gestire queste nuove richieste in quanto non è facilmente scalabile dato che non vi è una netta separazione tra Control Plane e User Plane.

In realtà la EPC, rispetto alle generazioni precedenti è stata progettata avendo già in mente una certa separazione delle funzioni di control plane da quelle di user plane ponendo però maggior attenzione sulla separazione delle funzioni di mobility management che riguardano puramente il control plane da quelle di session management che riguardano anche lo user plane. Nell'architettura presentata però il SGW ed il PGW combinano insieme funzioni di control plane e user plane relative alla gestione delle sessioni e di conseguenza non è possibile scalare le parti di control e user plane in maniera indipendente.

Come detto in precedenza la necessità di separare control plane e user plane è diventata sempre più evidente con la crescita del numero di device IoT connessi in rete mediante accesso LTE nonché di piattaforme per il video streaming, content sharing e social media. Queste varie tipologie di servizi disponibili hanno requisiti differenti in termini di scalabilità e deployment dei vari nodi tali da non richiedere uno scaling in maniera identica di parti di user plane e control plane. Alcuni di questi scenari, ad esempio, possono richiedere di avere componenti di user plane processing più vicini a dove l'utente si connette.

Nella 3GPP Release 14 è stato introdotto il concetto di Control and User Plane Separation (CUPS) che riguarda tra le altre cose proprio la separazione delle funzionalità di control plane e user plane di SGW e PGW andando ad avere quindi 4 entità separate SGW-CP, PGW-CP, SGW-UP e PGW-UP.

La separazione tra Control Plane e User Plane introdotta con la Release 14 è poi tra gli elementi fondanti dell'architettura di rete 5G dove è presente sin dal design iniziale.

Inoltre, tra le reti 4G e 5G si evidenzia un cambiamento in termini di concezione dell'architettura per quel che concerne la parte della rete che ha funzionalità di signaling che passa da "nodi" o "elementi

di rete" interconnessi da interfacce punto a punto a funzioni di rete (Network Functions (NF)) che espongono e rendono disponibili servizi alle altre funzioni di rete.

Ogni Network Function offre quindi uno o più servizi alle altre Network Functions della rete esponendoli mediante delle Network Function interfaces connesse alla Service Based Architecture comune. Ciò significa quindi che i servizi offerti da una specifica Network Function sono resi disponibili mediante un API. La scelta effettuata per la definizione delle API è ricaduta sull'utilizzo di interfacce basate su HTTP REST in considerazione anche del fatto che le applicazioni software che implementano le Network Functions si presume che vengano eseguite in un ambiente "IT-like" o in un ambiente distribuito, tipicamente un cloud data center dove l'utilizzo del paradigma REST è giù ampiamente consolidato.

In definitiva, le reti 4G nell'architettura illustrata non sono in grado di soddisfare al meglio i differenti requisiti che emergono dai seguenti tre casi d'uso:

- Enhanced Mobile Broadband (eMBB): applicazioni estremamente "video-centriche" che consumano una grande quantità di banda e generano la maggior parte del traffico sulla rete.
- Massive Machine-Type Communications (mMTC): più comunemente conosciute come, Internet of Things ma in scala molto maggiore con miliardi di dispositivi connessi in rete che generano singolarmente minor traffico ma nel complesso originano un'enorme quantità di dati da elaborare (più o meno in tempi brevi)
- Ultra Reliable Low Latency Communications (URLLC): applicazioni safety-critical come il "remote surgery" o comunicazioni "Vehicle to X" che richiedono la maggior parte delle funzioni di rete allocate ai margini della rete ai fini di ridurre al massimo la latenza (inferiore al millisecondo) ed un'elevata affidabilità

Per adattarsi al meglio alle esigenze di ognuno dei casi d'uso sopra esplicitati, nelle reti 5G è stato introdotto il concetto di *network slicing* che prevede la definizione di vere e proprie reti logiche separate, ognuna delle quali configurata opportunamente per soddisfare i vari requisiti e create sulla base di un'infrastruttura comune

Lista degli acronimi

AKA	Authentication and Key Agreement
AMBR	Aggregated Maximum Bit Rate
APN	Access Point Name
ARP	Allocation and Retention Priority
AS	Access Stratum
ASME	Access Security Management Entity
C-RNTI	Cell Radio Network Temporary Identifier
CS	Circuit-Switched
CSG	Closed Subscriber Group
DL	Downlink
DNS	Domain Name Server
DRB	Data Radio Bearer
DRX	Discontinuous Reception
ECGI	E-UTRAN Cell Global Identifier
ECI	E-UTRAN Cell Identifier
ECM	EPS Connection Management
EMM	EPS Mobility Management
eNB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
EPS-AKA	Evolved Packet System – Authentication and Key Agreement
E-RAB	E-UTRAN Radio Access Bearer
ESM	EPS Session Management
E-UTRA	Evolved Universal Terrestrial Radio Access
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FQDN	Fully Qualified Domain Name
GBR	Guaranteed Bit Rate
GTP	GPRS Tunneling Protocol
GTP-C	GTP Control
GTP-U	GTP User
GUMMEI	Globally Unique MME Identifier

GUTI	Globally Unique Temporary Identifier
HSS	Home Subscriber Server
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LBI	Linked EPS Bearer Identity
LTE	Long Term Evolution
MAC	Medium Access Control
MBR	Maximum Bit Rate
MCC	Mobile Country Code
MM	Mobility Management
MME	Mobility Management Entity
MMEC	MME Code
MMEGI	MME Group Identifier
MNC	Mobile Network Code
MNO	Mobile Network Operator
MSIN	Mobile Subscriber Identification Number
M-TMSI	MME Temporary Mobile Subscriber Identity
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code per NAS per Integrity Protection
NCC	Next hop Chaining Counter
NH	Next Hop
NE	Network Equipment
OCS	Online Charging System
OFCS	Offline Charging System
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCI	Physical Cell ID
PCRF	Policy and Charging Rules Function
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PGW	Packet Data Network Gateway
PLMN	Public Land Mobile Network

QCI	QoS Class Identifier
QoS	Quality of Service
RAT	Radio Access Technology
RLC	Radio Link Control
RLF	Radio Link Failure
RRC	Radio Resource Control
RRM	Radio Resource Management
RSRP	Reference Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indicator
S1-AP	S1 Application Protocol
SCTP	Stream Control Transmission Protocol
SDF	Service Data Flow
SGW	Serving Gateway
SI	System Information
SIB	System Information Block
SMS	Short Message Service
SN	Sequence Number
SPR	Subscriber Profile Repository
SRB	Signaling Radio Bearer
S-TMSI	SAE Temporary Mobile Subscriber Identity
TA	Tracking Area
TAC	Type Allocation Code
TAC	Tracking Area Code
TAI	Tracking Area Identity
TAU	Tracking Area Update
TEID	Tunnel Endpoint Identifier
TFT	Traffic Flow Template
TIN	Temporary Identifier used in Next update
TMSI	Temporary Mobile Subscriber Identity
UE	User Equipment
UDP	User Datagram Protocol
UL	Uplink
UMTS	Universal Mobile Telecommunication System

USIM	UMTS Subscriber Identity Module
UTRA	Universal Terrestrial Radio Access
VPLMN	Visited Public Land Mobile Network
X2AP	X2 Application Protocol

Indice delle figure

Indice delle tabelle

Bibliografia e Sitografia

1) Grasselli C., 2019, “Multi-domain orchestration of virtualized mobile core networks”
2) Di Santi S., 2019, “5G Network Architecture”
3) https://www.netmanias.com/en/?m=view&id=techdocs&no=5904
4) https://www.netmanias.com/en/?m=view&id=techdocs&no=5905
5) https://www.netmanias.com/en/?m=view&id=techdocs&no=5906
6) https://www.netmanias.com/en/?m=view&id=techdocs&no=5907
7) https://www.netmanias.com/en/?m=view&id=techdocs&no=5908
8) https://www.netmanias.com/en/?m=view&id=techdocs&no=5909
9) https://www.netmanias.com/en/?m=view&id=techdocs&no=6098
10) https://www.netmanias.com/en/?m=view&id=techdocs&no=6102
11) https://www.netmanias.com/en/?m=view&id=techdocs&no=6108
12) https://www.netmanias.com/en/?m=view&id=techdocs&no=6110
13) https://www.netmanias.com/en/?m=view&id=techdocs&no=6134
14) https://www.netmanias.com/en/?m=view&id=techdocs&no=6193
15) https://www.netmanias.com/en/?m=view&id=techdocs&no=6224
16) https://www.netmanias.com/en/?m=view&id=techdocs&no=6257
17) https://www.netmanias.com/en/?m=view&id=techdocs&no=6286
18) https://www.netmanias.com/en/?m=view&id=techdocs&no=6322
19) https://www.netmanias.com/en/?m=view&id=techdocs&no=6324
20) https://www.netmanias.com/en/post/blog/5930/lte-tau/lte-tracking-area-ta-and-tracking-area-update-tau
21) https://www.netmanias.com/en/post/blog/5927/lte/lte-gtp-tunnel-1-today-we-will-talk-about-gtp-tunnels-used-in-the-lte-network
22) https://www.netmanias.com/en/post/blog/5928/lte/lte-gtp-tunnel-2-today-we-will-find-more-about-lte-gtp-tunnels-that-we-have-discussed-previously
23) https://www.netmanias.com/en/post/blog/5929/lte/lte-user-identifiers-imsi-and-guti
24) https://www.avnet.com/wps/portal/abacus/resources/article/the-evolution-of-cellular-networks/
25) https://www.brainbridge.be/en/blog/1g-5g-brief-history-evolution-mobile-standards
26) https://www.carritech.com/news/evolution-mobile-communication-1g-5g/
27) https://www.blueplanet.com/resources/what-is-network-slicing.html

28) https://www.sicomtesting.com/blog/dal-1g-al-5g-il-passato-e-il-futuro-degli-standard-gsm-umts-hspa-ed-lte/

29) https://www.fastweb.it/internet/storia-rete-cellulare/

30) https://www.3gpp.org/technologies/keywords-acronyms/96-nas

31) https://www.sharetechnote.com/html/Handbook_LTE_MultiCell_Measurement_LTE.html

32) Olsson M, Sultana S., Rommer S., Frid L., Mulligan C., 2012, "EPC and 4G Packet Networks: Driving the Mobile Broadband Revolution – Second Edition" Ed. Academic Press

33) Sesia S., Toufik I. Baker M., 2011, "LTE- The UMTS Long Term Evolution. From Theory to Practice – Second Edition" Ed. John Wiley & Sons Ltd.

34) Rommer S., Hedman P. Olsson M., Frid L., Sultana S., Mulligan C, "5G Core Networks. Powering digitalization", 2020, Ed. Academic Press – Elsevier

Ringraziamenti

Ringrazio il prof. Franco Callegati per il supporto offertomi durante la stesura di questo elaborato.
Ringrazio inoltre i miei familiari, in particolare mia mamma Serena, mio babbo Ettore e mio fratello Raffaele per avermi supportato e sopportato durante tutti questi anni (in special modo mio fratello per avermi aiutato durante la redazione del presente elaborato).