INDICE

Introduzione

Negli ultimi anni si è assistito ad uno sviluppo senza precedenti del settore delle telecomunicazioni. La maturazione raggiunta nel campo della tecnologia *wireless*, unita alla disponibilità di dispositivi portatili, sempre più potenti ed a basso costo, sta conducendo ad una "percezione" della rete Internet completamente differente da quella attuale:
le risorse disponibili nella "rete delle reti" saranno usufruibili ovunque, in qualsiasi momento, ma principalmente saranno disponibili a prescindere dalla stazionarietà o meno dell'utente.

Inizialmente considerato troppo avveniristico, a causa della mancanza di interesse commerciale e di infrastrutture di rete adeguate, il protocollo **Mobile IP** fornirà le fondamenta necessarie per la realizzazione degli obiettivi sopra delineati.
Sviluppato all'interno dell'Internet Engineering Task Force, Mobile IP permette di gestire la mobilità degli host a livello di rete e quindi in maniera indipendente dalle caratteristiche delle singole sotto-reti d'accesso.
Il principio di funzionamento del protocollo è semplice e deriva dall'esigenza di sopperire ai limiti imposti, dall'attuale pila protocollare TCP/IP, nei confronti della mobilità.
Il sistema di indirizzamento di Internet, sviluppato ed ottimizzato per un ambiente stazionario, prevede che ciascun host connesso alla rete sia identificabile mediante un indirizzo e che il routing dei pacchetti sia basato, principalmente, sul campo Destination Address dell'header IP.
Da tali caratteristiche deriva un ambiente non adeguato alla gestione della mobilità:

- un host mobile ha bisogno di un indirizzo stabile che gli consenta di essere raggiungibile da un qualsiasi altro utente della rete Internet;
- se l'indirizzo è stabile, lo è anche il routing dei pacchetti e quindi in caso di *roaming*, l'host non sarà più raggiungibile.

Mobile IP consente di risolvere tale incongruenza alla radice:
ad un terminale mobile, comunemente denominato *Mobile Node*, saranno associati due indirizzi. Il primo, *home address*, è permanente e sarà utilizzato dagli strati applicativi e dai protocolli di trasporto come un qualsiasi indirizzo IP. Il secondo, detto *care-of address*, è temporaneo e rispecchierà la posizione attuale dell'host.
Un Mobile Node otterrà un home address nella propria rete di appartenenza, *Home Network*, mentre il care-of address sarà acquisito nella rete "visitata", *Foreign Network*, mediante l'ausilio di un *Foreign Agent*.
Per consentire la raggiungibilità del terminale, l'indirizzo locale sarà comunicato ad un'entità presente nella Home Network denominata *Home Agent*. Compito dell'Home Agent sarà di intercettare i pacchetti destinati al Mobile Node ed inoltrarli al care-of-address.

Sviluppato come soluzione utile per reti locali, il protocollo Mobile IP, con l'introduzione del sistema GPRS e del futuro UMTS, sarà facilmente estendibile a soluzioni pubbliche.
Per consentirne una diffusione commerciale, gli Internet Service Provider dovranno arricchire le proprie infrastrutture delle funzionalità necessarie per supportare tale servizio.
In realtà dal punto di vista dei dispositivi di rete, il problema non è così imponente:
molti degli attuali router CISCO supportano il protocollo Mobile IP; in particolare, dalla Serie 2500, è possibile configurare le funzionalità dell'Home Agent e del Foreign Agent.

Di natura completamente differente è l'analisi dei problemi legati alle procedure di Autorizzazione Autenticazione ed Accounting.
Gli odierni operatori di telefonia cellulare ed Internet Service Provider autorizzano un utente ad usufruire delle proprie infrastrutture solamente dopo averlo autenticato; una volta verificatene le "credenziali", possono eseguire un monitoraggio dello sfruttamento delle risorse con lo scopo, ad esempio, di richiedere un eventuale pagamento del servizio offerto.
E' intuibile, quindi, la necessità di rendere il protocollo Mobile IP compatibile con il meccanismo sopra definito e generalmente denominato servizio di **Authentication, Authorization and Accounting (AAA)**.
E' innegabile, infatti, la grande importanza che rivestono tali procedure in caso di *roaming* di un'utente:

- forniscono ad un ISP un elevato grado di sicurezza sull'autenticità di un utente;
- permettono la realizzazione di un servizio. In altre parole un ISP sarà propenso ad accettare nuove tecnologie, quali ad esempio Mobile IP, solamente se può trarne dei benefici in termini monetari.

Nel contesto sopra delineato deve essere inserito il lavoro compiuto nel corso di questa tesi e sviluppato nell'ambito delle attività di ricerca svolte allo IASI-CNR (Istituto per l'Analisi dei Sistemi Informatici del Consiglio Nazionale delle Ricerche) ed in particolare nell'ambito del progetto NetLab (Network Laboratory).
L'obiettivo della tesi è di progettare e realizzare un'architettura che consenta di far interagire il protocollo Mobile IP con le procedure AAA.
Un'attenta ricerca di mercato ha permesso di costatare che il protocollo AAA attualmente più diffuso tra gli Internet Service Provider è **RADIUS**. Si può così delineare maggiormente l'obiettivo da raggiungere:

sviluppare un sistema nel quale le procedure di Autenticazione, Autorizzazione ed Accounting siano basate sul protocollo RADIUS.
Le attività svolte a tale scopo sono state molteplici:

- *scelta delle implementazioni del protocollo Mobile IP e Radius*;
- *individuazione delle specifiche di sistema*;
- *progettazione di una* ***Radius Mobility Interface (RMI)***, attraverso la quale rendere possibile il colloquio tra Mobile IP e Radius.
  Le difficoltà incontrate in questa fase non sono state poche in quanto si è dovuto sviluppare un vero e proprio protocollo e quindi prendere in considerazioni tutte le problematiche dovute sia al rispetto delle caratteristiche di Mobile IP e Radius, che alla corretta temporizzazione dei messaggi;
- *realizzazione della Radius Mobility Interface*, che ha comportato un'attenta analisi del codice sorgente del software Mobile IP prescelto. Infatti, da quanto è stato detto, l'interfaccia necessita di interagire non solo con Radius, ma anche con il protocollo Mobile IP. Dal lato Radius si è riusciti ad ottenere una completa indipendenza dalla particolare implementazione del protocollo, mentre, nei confronti di Mobile IP, si sono dovute apportare delle modifiche al software scelto. E' importante rilevare che le soluzioni adottate, per consentire lo scambio d'informazioni tra la RMI ed il software Mobile IP, si basano su caratteristiche che derivano dalle specifiche dello standard e che quindi devono essere soddisfatte da tutte le diverse implementazioni. In tal senso, anche dal lato Mobile IP, si è riusciti ad ottenere un alto livello d'indipendenza;
- *configurazione del laboratorio* e quindi istallazione dell'architettura AAA per Mobile IP;

- *verifica delle presentazioni dell'architettura* attraverso l'utilizzo di un set di test mirati all'analisi del rispetto delle specifiche progettuali.

Per fornire una visione più ampia dell'intero processo di Accounting, è stato proposto un modello che preveda l'iterazione, dell'architettura sviluppata, con dei *Billing Server*.
L'obiettivo è di rimarcare l'importanza che l'*Accounting Management* riveste in un *Busyness System*. Si è già detto che lo scopo finale della procedura di Accountig, per finalità di *billing*, consiste nel disporre delle informazioni necessarie per richiedere il pagamento di un servizio offerto.
Attraverso i protocolli AAA è possibile ricavare parametri di Accounting inerenti l'utilizzo fisico delle risorse: byte inviati, byte ricevuti, paccheti inviati, pacchetti ricevuti.
Non è da escludere, inoltre, che l'utente desideri usufruire di servizi di valore aggiunto come l'invio e la ricezione di e-mail, la consultazione di pagine web a pagamento, etc.
Da tali considerazioni deriva che le "sorgenti" su cui basare l'accounting sono molteplici, o viceversa, le informazioni necessarie ad un Billing Server per redigere numericamente il resoconto delle attività dell'utente derivano da molti parametri.

Struttura della tesi

PARTE PRIMA: Stato dell'arte del protocollo Mobile IP

Costituita dai primi tre capitoli della tesi si pone come obiettivo l'analisi dettagliata delle caratteristiche del protocollo Mobile IP.

Nel primo capitolo è fornita una descrizione completa dello standard Mobile IP specificato nell'ultima versione della Request for Comments numero 2002.

Concettualmente Mobile IP può essere considerato come l'unione di tre procedure distinte:

- *Agent Discovery*

  Attraverso la procedura di Agent Discovery, il Mobile Node è in grado di determinare se è connesso con la propria Home Network o con una Foreign Network, di determinare il care-of address ed infine di gestire l'eventuale spostamento tra reti differenti.

- *Registration*

  La procedura di Registrazione è un meccanismo flessibile che permette al Mobile Node di comunicare informazioni di raggiungibilità al proprio Home Agent. In particolare attraverso tale meccanismo il Mobile Node può richiedere un servizio di re-instradamento, quando si trova in una Foreign Network; può comunicare il care-of address; può rinnovare una registrazione ed infine può de-registrarsi quando torna nella home nework.

- *Tunneling*

  A seguito della registrazione di un Mobile Node, l'Home Agent deve intercettare i datagrammi destinati al Mobile Node (avranno il campo Destination Address coincidente con l'home address), effettuare una opportuna procedura di incapsulamento ed inviarli verso il care-of address. Il percorso seguito da un datagramma incapsulato è detto tunnel.

Nel secondo capitolo si presentano le tecniche di ottimizzazione del protocollo. In particolare sono esposte delle procedure che consentono di introdurre delle soluzioni per i seguenti problemi:

- *Gestione non efficiente del routing*

  I datagrammi inviati al Mobile Node da un Correspondent Node (cioè da un qualsiasi dispositivo in comunicazione con il Mobile Node) devono transitare preliminarmente per l'Home Network.

- *Gestione non efficiente degli handoff*

  I datagrammi inviati ad un Mobile Node impegnato in un handoff (cioè in un cambio del punto di accesso ad Internet) sono persi con una probabilità molto elevata.

- *Gestione non efficiente della procedura di registrazione*

  Ogni qual volta il Mobile Node acquisisce un nuovo care-of address, o necessita di rinnovare il lifetime della registrazione, deve comunicare con il proprio Home Agent.

Infine nel terzo capitolo si caratterizza l'applicabilità di Mobile IP in previsione di ciò che costituirà l'ossatura della futura rete Internet, cioè di IPv6.
Mobile IP potrà essere considerato, in un certo senso, come parte integrante di IPv6 in quanto interagirà con esso per sfruttarne le potenzialità e migliorare così le proprie funzionalità.
Alla base di Mobile IPv6 vi sono gli stessi concetti che hanno condotto allo sviluppo di MIPv4: viene mantenuta l'idea di una Home Network, di un Home Agent e dell'uso di un tunnel per consegnare i datagrammi dalla Home Network alla posizione corrente del Mobile Node.
Non è più necessaria la presenza del Foreign Agent e quindi il Mobile Node dovrà acquisire autonomamente il care-of address (ad esempio, attraverso la procedura denominata Neighbor Discovery).
La caratteristica principale di MIPv6 consiste nell'integrazione delle procedure d'ottimizzazione del routing con le caratteristiche funzionali dello stesso protocollo; in altre parole mentre una migliore efficienza di MIPv4 può essere

ottenuta modificando opportunamente il protocollo, in MIPv6 l'applicabilità delle tecniche d'ottimizzazione è un requisito obbligatorio.

PARTE SECONDA: Esempi di applicabilità del protocollo Mobile IP

Completata la descrizione delle caratteristiche del protocollo Mobile IP, ho ritenuto importante fornire una visione dei possibili scenari applicativi.

Nel quarto capitolo è presentato un protocollo per la gestione della mobilità degli host all'interno di reti d'accesso di tipo *wireless*.
Lo standard Mobile IP è stato sviluppato con l'obiettivo di risolvere problemi legati alla "macro" mobilità (o mobilità globale) degli host, non è quindi ottimizzato per gestire la mobilità all'interno delle singole sotto-reti che forniscono l'accesso ad Internet (denominata "micro" mobilità o mobilità locale).
La struttura di rete mobile che si prenderà in considerazione prevede che all'interno di ciascuna *wireless access network* la micro mobilità degli host sia gestita tramite il protocollo Cellular IP il quale dovrà anche cooperare con Mobile IP per consentire al Mobile Node di muoversi tra le diverse reti d'accesso. Il vantaggio di aver separato la gestione della mobilità locale da quella globale, risiede nel fatto che non sarà necessario informare l'Home Agent degli spostamenti compiuti dall'host all'interno di una rete d'accesso ma solamente di quelli compiuti per muoversi da una rete all'altra.
Cellular IP sfrutta alcuni principi dei sistemi cellulari, ma a differenza di questi possiede una serie di vantaggi, tra i quali:

- completa compatibilità con il protocollo IP;
- facilità con cui controlla gli handoff degli host;
- possibilità di poter implementare il protocollo sia su piccole LAN che su reti con vasta area di copertura, cioè su ambienti architetturali molto differenti tra loro;

- assenza di dispositivi centralizzati che memorizzano la posizione attuale del Mobile Node all'interno della *wireless access network*, in tal senso Cellular IP può essere considerato un protocollo distribuito;

Data la grande importanza dei sistemi GPRS/UMTS, nel quinto capitolo è fornita una descrizione delle caratteristiche che consentiranno di "affiancare" le funzionalità proprie del protocollo Mobile IP con quelle del sistema GPRS (ed il futuro UMTS).
L'introduzione del protocollo Mobile IP dovrà avvenire in maniera graduale, in particolare si prevede un'evoluzione basata su tre fasi successive:

- **Fase 1**

  Rappresenta la minima configurazione necessaria per consentire ad un operatore di rete di usufruire delle caratteristiche del protocollo Mobile IP.

- **Fase 2**

  Saranno introdotte delle soluzioni per consentire una migliore gestione del routing dei pacchetti.

- **Fase 3**

  L'architettura di rete sarà modificata in maniera tale da consentire una completa applicabilità del protocollo Mobile IP.

PARTE TERZA: Visione generale delle problematiche di Authentication, Authorization and Accounting

Costituita dal sesto e settimo capitolo, in tale sezione sono esaminate tutte le problematiche legate alle procedure di Authentication, Authorization and Accounting.

A causa del grande sviluppo della rete Internet e delle molteplici applicazioni usufruibili dall'utente (*video on demand, video conferecing, Internet radio, IP telephony, electronics commerce,* etc.), ha assunto un ruolo molto importante lo studio dell'*Accounting Management*. A dimostrazione del grande interesse nei confronti di tale settore, è menzionabile il fatto che, all'interno dell'Internet Engineering Task Force, sia stato creato uno specifico Working Group denominato "Authentication, Authorization and Accounting working group".

Intitolato Internet Accounting, il sesto capitolo fornisce una descrizione esauriente di tutti gli aspetti legati a tale settore, con particolare attenzione allo studio dell'Accounting Management per finalità di billing.

In termini molto generali un'architettura di Accounting Management richiede l'iterazione tra dispositivi di rete, Accounting Server e Billing Server.

Scopo dei dispositivi di rete è di "raccogliere" informazioni sul consumo delle risorse e di aggregarle secondo opportune regole. Tali informazioni dovranno poi essere elaborate da un Accounting server il cui obiettivo sarà quello di eliminare eventuali dati non necessari e generare dei *Session Record,* vale a dire effettuare un'ulteriore compattazione e suddivisione dei dati (ad esempio potrebbero essere creati dei Session Record che consentano di distinguere un traffico locale da quello che coinvolge domini differenti). Il ciclo si conclude con la "manipolazione", da parte di un Billing Server, dei Session Record.

Nel capitolo è fornita una classificazione attraverso la quale è possibile individuare sia i parametri su cui basare il processo di Accounting, sia delle architetture di rete che consentano di gestire lo stesso processo. Tale classificazione si base sul tipo di servizio che deve essere addebitato all'utente:

- *Content/Service Accounting*

  L'utente deve pagare il servizio da lui richiesto. Questo significa che i parametri che devono essere considerati, sono quelli legati al "tipo" di richiesta effettuata dall'utente. Esempi possono essere video clips, contenuti di pagine web, servizi di e-mail, etc.

- *Trasport Accounting*

  L'utente deve sostenere le spese legate alla consegna del servizio richiesto. E' quindi necessario verificare l'utilizzo delle risorse di rete. Inoltre, in previsione della possibilità di consentire ad un utente di scegliere la qualità con cui ottenere il servizio, sarà essenziale monetizzare in maniera differente tale qualità.

Nella parte conclusiva del capitolo sono presentate le modalità attraverso le quali inserire il protocollo Mobile IP nel contesto dell'Accounting Management, in particolare sono presentate delle soluzioni per il Content/Service Accounting.
E' intuibile la necessità di coinvolgere, nelle procedure di accounting, non solo l'ISP con il quale il Mobile Node ha stipulato una forma di contratto (*Home ISP*), ma anche il fornitore di servizio che mette a disposizione le proprie risorse in caso di *roaming* del Mobile Node (*Foreign ISP*).

Il settimo capitolo è concettualmente suddivisibile in due parti distinte.
Inizialmente sono presentati i protocolli AAA, con particolare attenzione al protocollo RADIUS.
Radius è l'acronimo di Remote Authentication Dial In User Service e rappresenta il protocollo attualmente più diffuso tra gli Internet Service Provider.
Consente di autenticare le credenziali di un utente, autorizzare l'utente ad instaurare una connessione ed eventualmente procedere all'accounting dello stesso.
Il protocollo si basa sul paradigma client/server:

- un Network Access Server (NAS) opera come un client di Radius: riceve le richieste di connessione da parte dell'utente e fornisce al Radius Server le informazioni per l'autenticazione dello stesso;

- un Radius Server, attraverso la consultazione di un database, verificherà le credenziali dell'utente e fornirà al NAS le informazioni necessarie per soddisfare o meno la richiesta di connessione. Inoltre il Radius server può agire come un proxy client verso altri Radius server o altri tipi di server di autenticazione.

Nella seconda parte del capitolo sono introdotte delle architetture nelle quali si affianca il protocollo Mobile IP con le procedure AAA. Sono evidenziate le entità archiretturali che dovranno essere inserite in tali sistemi e le iterazioni tra le stesse.
Un host mobile (*client*), autenticabile all'interno del proprio dominio d'appartenenza (*home domain*), può avere l'esigenza di usufruire delle risorse di un dominio (*foreign domain*) diverso dal proprio. All'interno del foreign domain, descrivibile anche come un *local domain* dato che rispecchia l'attuale posizione dell'host, vi può essere un dispositivo, denominato *attendant*, il cui scopo è quello di verificare le credenziale dell'host prima di fornirgli l'acceso alle infrastrutture del sistema. Molto probabilmente l'attendant non sarà in grado di autenticare l'utente e quindi dovrà consultare un AAA server, appartenete al suo stesso dominio (*AAA Local Authority*), il quale, a sua volta, chiederà conferma delle credenziali dell'host all'AAA server che gestisce l'home domain (*AAA Home Authority*).
Le soluzioni proposte non sono concorde con le specifiche del protocollo Radius, da ciò deriva che, nello sviluppo della Radius Mobility Interface, si potrà usufruire solamente dei principi che sono alla base delle architetture presentate nel capitolo.

PARTE QUARTA: Sviluppo della Radius Mobility Interface

La tesi si conclude con lo sviluppo dell'architettura AAA, basata sul protocollo Radius.

In fase di progettazione di un sistema, un requisito fondamentale è quello di delineare il problema da risolvere. In altre parole, volendo sviluppare un sistema AAA per Mobile IP, di quali mezzi si può disporre?
Per rispondere a tale domanda, si è resa necessaria una ricerca di mercato in grado di fornire riscontri circa l'attuale stato dell'arte delle tecnologie richieste. Dalla ricerca svolta è emerso che il protocollo AAA attualmente più diffuso risulta Radius.
Da ciò deriva che, nella prima parte dell'ottavo capitolo, si è cercato di circoscrivere il problema attraverso l'individuazione precisa delle specifiche di progetto. Per raggiungere tale obiettivo ho ritenuto importante classificare i requisiti in tre gruppi distinti:

- **Software**

  La fase di progettazione del sistema dovrà porre le basi per l'effettiva implementazione dello stesso, da ciò deriva la necessità di individuare un'implementazione del protocollo Mobile IP e del protocollo RADIUS. La scelta è ricaduta sui software Dynamic-Hut Mobile IP e Merit Radius Server sviluppati, rispettivamente, presso l'Università di Helsinki e l'Università del Michigan.

- **Authentication and Authorization**

  Un Internet Service Provider consentirà ad un Mobile Node di usufruire delle proprie risorse solamente dopo averne verificato le "credenziali". E' importante, quindi, delineare con precisione le azioni da svolgere per il corretto conseguimento di tale obiettivo.

- **Accounting**

  Dal punto di vista dell'ISP, le procedure di accounting sono il mezzo per ricevere il pagamento per il servizio offerto. Si dovranno cosi individuare i parametri più significativi per ciò che concerne l'utilizzo delle risorse da parte del Mobile Node.

Successivamente si è passati alla progettazione vera e propria del sistema che ha consentito di caratterizzare la Radius Mobility Interface e quindi di individuare le funzionalità che dovrà possedere sia nei confronti del protocollo Mobile IP che nei confronti del protocollo Radius.
Per delinearne maggiormente le funzionalità, sono state analizzate separatamente le procedure di Autenticazione e quelle di Accounting ed inoltre si è fatto uso di diagrammi temporali attraverso i quali è possibile individuare sia il flusso dei messaggi scambiati tra le diverse entità che la corretta sequenza temporale con cui devono essere trasmessi.

Nel nono capitolo sono illustrate le soluzioni adottate per l'effettiva implementazione dell'architettura AAA, per Mobile IP, basata sul protocollo Radius.
In primo luogo è stato necessario effettuare uno studio delle risorse disponibili, all'interno del laboratorio NetLab, che ha permesso di individuare la dislocazione delle diverse entità architetturali coinvolte:
Radius Server, Foreign Agent, Home Agent e Mobile Node.
Si è poi passati alla fase d'istallazione dei software Dynamic-Hut Mobile IP e Merit Radius ed alla loro corretta configurazione.
Infine si sono individuate le metodologie per l'effettiva implementazione della Radius Mobility Interface.
Personalmente ho ritenuto opportuno sviluppare la RMI attraverso due approcci differenti tra loro:

- la parte relativa alle procedure di autenticazione ed autorizzazione è stata implementata utilizzando il linguaggio C (lo stesso del software Dynamic-Hut Mobile IP) e quindi creando delle funzioni specifiche;
- la parte relativa alle procedure di accounting è stata sviluppata attraverso uno Script Shell e quindi sfruttando le potenzialità messe a disposizione dalla Shell Bash del sistema operativo Linux.

E' importante rilevare che il principio seguito in fase di realizzazione del sistema è stato di non apportare nessun tipo di modifica al software Merit Radius e di interagire con l'implementazione di Mobile IP attraverso caratteristiche derivanti dalle specifiche dello stesso protocollo.
In tal modo la Radius Mobility Interface potrà "colloquiare" facilmente con software Mobile IP differenti da quello preso in considerazione.
Per implementare le procedure di Accounting si è dovuto risolvere un ulteriore problema:
scopo finale delle procedure di Accounting è quello di ottenere un "resoconto" delle attività del Mobile Node.
E' stato necessario, quindi, stabilire le modalità attraverso le quali monitorare i parametri di Accounting: pacchetti inviati, pacchetti ricevuti, byte inviati, byte ricevuti.
Si è così deciso di adottare *tcpdump*, uno sniffer di rete disponibile nella maggior parte delle versioni del sistema operativo Linux ed altamente configurabile.

La tesi si conclude con il decimo capitolo nel quale si sono verificate le prestazioni del sistema proposto attraverso l'utilizzo di test.
I risultati dei test sono stati presentati in forma tabellare e le notazioni utilizzate sono state:

- **Nome test**: identifica univocamente ciascun test.
- **Ambiente di test**: è fornita una schematizzazione delle risorse utilizzate per effettuare il particolare test.
- **Obiettivo**: rappresenta lo scopo del test.
- **Azioni**: elenco delle azioni svolte per eseguire i test.
- **Risultato**: esito del test e breve descrizione.

1 Caratteristiche e specifiche funzionali del protocollo Mobile IP

La grande diffusione di dispositivi portatili, quali ad esempio laptop computers, PDA (*Personal Digital Assistant*) e telefoni cellulari ha favorito la domanda di accesso ad Internet indipendentemente dalla tecnologia e dal punto di accesso stesso.
Purtroppo il sistema di indirizzamento di Internet, sviluppato ed ottimizzato per un ambiente stazionario, non è in grado di gestire adeguatamente la mobilità degli host.
In particolare dato che:

- ogni indirizzo IP generalmente identifica un host;
- il routing è basato sul sistema d'indirizzamento e questo è gestito in modo gerarchico (tramite subnet-mask) per agevolare l'instradamento;

l'eventuale spostamento di un host richiede l'attuazione di una delle due seguenti procedure:

- modifica dell'indirizzo IP dell'host;
- modifica delle tabelle di routing della rete in accordo alla nuova posizione.

Entrambe le alternative possiedono dei limiti: la prima non consente il mantenimento delle connessioni relative al livello di trasporto; la seconda ha

evidenti problemi di scalabilità poiché richiede una disponibilità di spazio, per le tabelle di routing, proporzionale al numero di host mobili.
Per sopperire ai problemi sopra esposti l'IETF (Internet Engineering Task Force) ha proposto il ***Mobile IP Support***, uno standard a livello di rete che, influenzando l'instradamento dei pacchetti, riesce a gestire adeguatamente la mobilità in Internet.

Scopo del seguente capitolo è quello di fornire una descrizione basilare dello standard Mobile IP proposto in [1].

1.1 Obiettivi

Il protocollo Mobile IP permette di gestire la mobilità degli host in maniera tale da conseguire i seguenti obiettivi [2]:

- ***Trasparenza***

  La mobilità è trasparente alle applicazioni ed ai protocolli di livello di trasporto, ad esempio le connessioni TCP non terminano in seguito ad una variazione del punto d'accesso ad Internet da parte degli host.

- ***Compatibilità con Ipv4***

  Un host può interagire con uno fisso anche se quest'ultimo non implementa lo standard Mobile IP.

- ***Scalabilità***

  Mobile IP supporta la mobilità sull'intera rete Internet indipendentemente dalle caratteristiche delle singole sotto-reti e permette la gestione di milioni di host mobili.

- ***Sicurezza***

  Mobile IP fornisce meccanismi per garantire l'autenticità dei messaggi scambiati.

Tali obiettivi devono essere raggiunti, senza modificare gli attuali protocolli di routing, senza modificare il sistema d'indirizzamento e richiedendo all'host mobile di non cambiare punto d'accesso ad Internet con una frequenza maggiore di una volta per secondo.

1.2 Entità architetturali

Come indicato in figura 1 la gestione della mobilità ha richiesto l'introduzione di nuove entità architetturali:

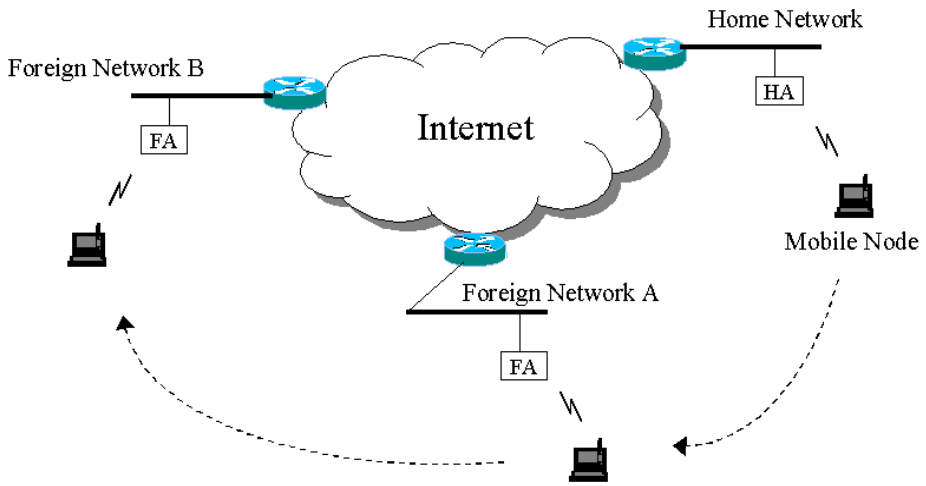


Figura 1: Entità Architetturali

- ***Mobile Node (MN)***

  Un dispositivo che usufruisce di prestazioni di mobilità. Un Mobile Node è in grado di comunicare con un qualsiasi host (fisso o mobile) mantenendo la propria identità ed avendo un suo indirizzo IP stabile, indipendentemente dal proprio *point of attachment* ad Internet.

- ***Home Agent (HA)***

  Un'entità logica residente in un router della rete d'appartenenza del Mobile Node (*Home Network*). La sua funzione è di mantenere delle informazioni circa la posizione attuale del Mobile Node; in particolare

quando il Mobile Node non è connesso alla Home Network, compito dell'Home Agent è quello di intercettare i datagrammi destinati al Mobile Node e di inoltrarli allo stesso.

- ***Foreign Agent (FA)***

  Un'entità logica residente in un router della rete "visitata" dal Mobile Node (*Foreign Network*). Coopera con l'Home Agent per completare la consegna dei datagrammi IP destinati al Mobile Node: riceve i pacchetti inviati dall'Home Agent e li consegna al Mobile Node.

Ogni Mobile Node è caratterizzato attraverso due indirizzi IP: il primo, detto ***home address***, è permanente e viene assegnato dall'amministratore della Home Network. Non ci sono differenze tra un indirizzo assegnato ad un host fisso ed un home address assegnato ad un Mobile Node (ad esempio le connessioni TCP sono identificate da questo indirizzo). In altre parole ad eccezione di alcuni messaggi di controllo, il Mobile Node utilizzerà l'home address come source address di tutti i datagrammi da lui inviati. Il secondo, detto ***care-of address***, è temporaneo e rispecchia la posizione corrente del Mobile Node. Sostanzialmente il care-of address viene fornito al Mobile Node quando accede ad Internet attraverso una Foreign Network.
In figura sono rappresentati i concetti sopra esposti:

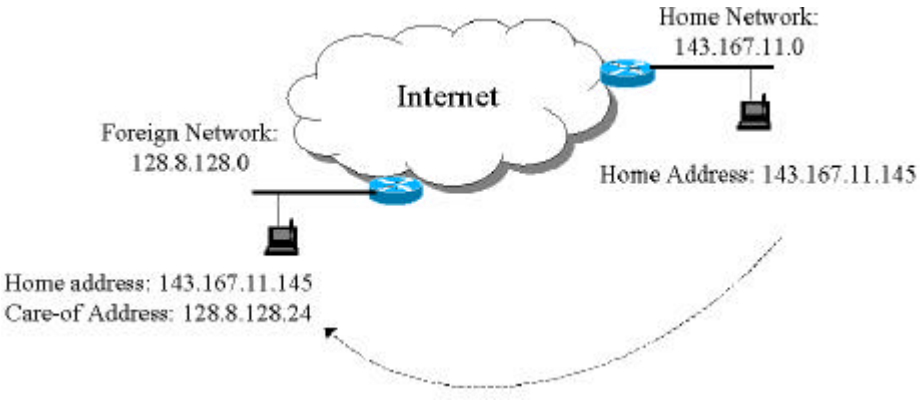


Figura 2: Home Address e Care-of Address

Quando il Mobile Node risiede nella propria Home Network sarà caratterizzato unicamente attraverso l'indirizzo IP 143.167.11.145; in seguito ad uno spostamento, il Mobile Node, oltre a mantenere il precedente indirizzo, acquisirà anche un indirizzo locale, 128.8.128.24.

Mobile IP fornisce due modalità alternative per consentire ad un Mobile Node di acquisire il care-of address:

- un ***co-located care-of address*** è un care-of address acquisito dal Mobile Node come un indirizzo IP locale ed associato con una delle sue interfacce di rete. Tale indirizzo può essere ottenuto attraverso protocolli quali il DHCP (Dinamic Host Configuration Protocol) o il PPP (Point to Point Protocol). In entrambi i casi si vedrà che è lo stesso Mobile Node a ricevere i datagrammi inviati dall'Home Agent senza che sia necessario che questi passino preliminarmente per un Foreign Agent. L'utilizzo di un co-located care-of address fornisce il vantaggio di non aver bisogno del Foreign Agent, ma richiede la disponibilità di un elevato numero d'indirizzi IP.

- un ***Foreign Agent care-of address*** è un care-of address acquisito attraverso un Foreign Agent, in altre parole il Foreign Agent "caratterizzerà" il Mobile Node con uno dei propri indirizzi IP. Da ciò deriva che sarà il Foreign Agent a ricevere i datagrammi inviati dall'Home Agent per poi consegnarli al Mobile Node. L'utilizzo di un Foreign Agent care-of address permette a più Mobile Node di condividere lo stesso care-of address, però richiede la presenza di un Foreign Agent nella Foreign Network.

1.3 Tipi di Home Network

Esistono tre configurazioni base per la Home Network [3]. La prima rappresenta una rete "standard" con un router d' accesso ed un nodo Home Agent distinto dal router (figura 3a). Nel caso della figura 3b il router d'accesso

svolge anche la funzione di Home Agent. Completamente differenti dai precedenti è il caso della figura 3c: si tratta di una rete "virtuale" senza alcuna realizzazione fisica, l'Home Agent viene visto dal resto della rete come un router di accesso ad una rete (la Home Network) che non esiste fisicamente.

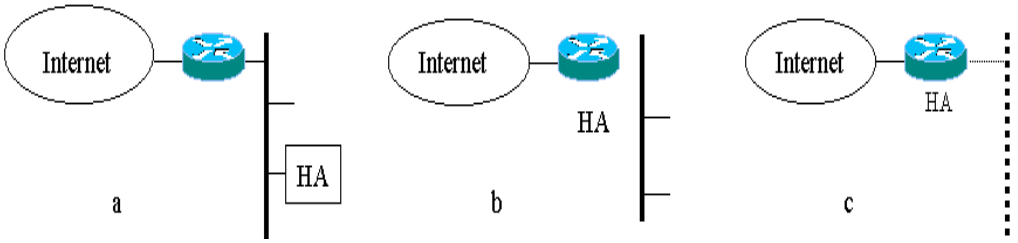


Figura 3: Tipi di Home Network

1.4 Descrizione del protocollo

Prima di definire la procedura attraverso la quale è gestita la mobilità, occorre precisare quali sono le principali funzioni supportate dallo standard. Tali funzioni saranno ampliamente descritte in seguito, per il momento è sufficiente fornirne una spiegazione sommaria.

Agent Advertisement

Attraverso messaggi denominati Agent Advertisement, i mobility agent (Home Agent e Foreign Agent) rendono nota la propria disponibilità a fornire un servizio. A sua volta un Mobile Node può sollecitare lo svolgimento di un servizio attraverso messaggi di Agent Solicitation.

Registration

Permette ad un Mobile Node di registrare il care-of address, ottenuto in una visited network, con il proprio Home Agent.

Tunneling

A seguito della registrazione di un Mobile Node, l'Home Agent deve intercettare i datagrammi destinati al Mobile Node (avranno il campo destination address coincidente con l'home address), effettuare un'opportuna procedura d'incapsulamento ed inviarli verso il care-of address. Il percorso seguito da un datagramma incapsulato è detto tunnel.

Il protocollo Mobile IP può essere schematizzato attraverso la seguente procedura che fa uso delle funzioni sopra esposte:

- Foreign Agent e Home Agent pubblicizzano la loro presenza attraverso opportuni messaggi di Agent Advertisement; un Mobile Node può facoltativamente sollecitare l'emissione di tali messaggi attraverso messaggi di Agent Solicitation;
- attraverso la ricezione di un Agent Advertisement un Mobile Node è in grado di determinare se la sua attuale collocazione è nella Home Network o in una Foreign Network;
- se il Mobile Node si trova nella propria Home Network opera senza alcun supporto di Mobile IP; se è di ritorno nell'Home Network si de-registra dall'Home Agent;
- se il Mobile Node arriva in una Foreign Network, si procura un care-of address; questo può essere ottenuto attraverso il Foreign Agent o tramite altri meccanismi (ad esempio attraverso il protocollo DHCP);
- se il Mobile Node è fuori dalla propria Home Network, registra il care-of address attraverso messaggi di *Registration Request* e *Registration Reply* scambiati direttamente con l'Home Agent (se il Mobile Node ha acquisito un co-located care-of address) oppure tramite il Foreign Agent (se il Mobile Node ha acquisito un Foreign

Agent care-of address). In figura è mostrato questo secondo caso: il Mobile Node, in seguito alla ricezione di un Agent Advertisement, invierà un Registration Request Message al Foreign Agent; quest'ultimo, dopo opportuni controlli sul contenuto del messaggio, lo rilancerà all'Home Agent il quale, attraverso un Registration Reply Message, comunicherà l'esito della richiesta di registrazione al Foreign Agent. La procedura di registrazione si conclude con l'ulteriore scambio del Registration Reply Message tra il Foreign Agent ed il Mobile Node:

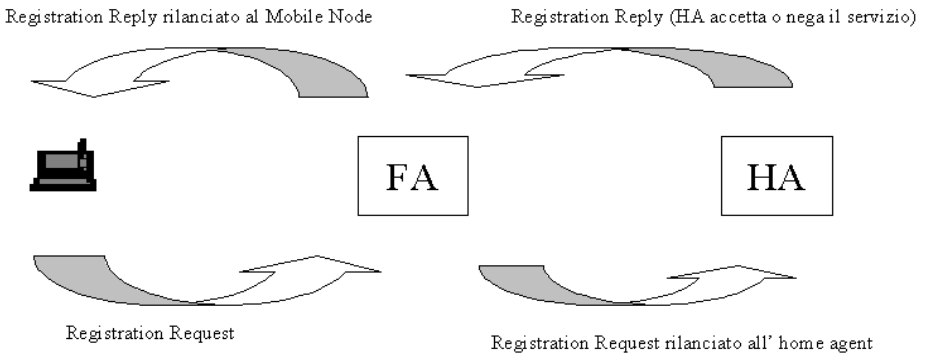


Figura 4: Procedura di registrazione

- quando il Mobile Node si trova in una Foreign Network, i datagrammi a lui inviati (attraverso il relativo home address) da un qualsiasi altro dispositivo della rete Internet, sono intercettati dall'Home Agent, inoltrati (tunneling) verso il care-of address e ricevuti al punto di uscita del tunnel (che può essere il Mobile Node stesso o il Foreign Agent). Nel caso in cui sia il Foreign Agent a ricevere i datagrammi destinati al Mobile Node, li estrae dal tunnel e li consegna al Mobile Node. In figura è schematizzato l'incapsulamento del datagramma intercettato dall'Home Agent ed inviato al Foreign Agent:

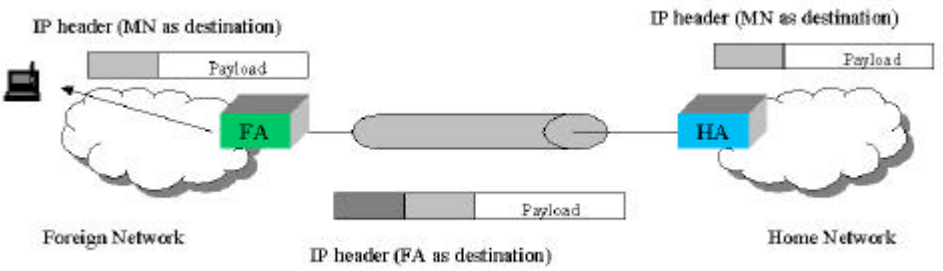


Figura 5: Tunneling

- i datagrammi nella direzione opposta, inviati cioè dal Mobile Node, sono instradati nel modo classico attraverso Internet e seguiranno un percorso diverso.

Come previsto in [1], quando l'Home Agent invia un datagramma verso il care-of address, i router intermedi prendono in considerazione solamente l'header "esterno" del datagramma, contenente il care-of address, e non quello interno, contenente l'home address del Mobile Node.

Si è inoltre specificato che l'Home Agent deve poter intercettare i datagrammi che sono destinati a tutti i Mobile Node da lui registrati. Tale funzione viene svolta in maniera diversa a seconda che l'Home Agent sia o meno l'unico router di accesso alla Home Network; nel secondo caso si vedrà che l'Home Agent farà uso di opportune procedure:
proxy ARP (Address Resolution Protocol) e *gratuitous ARP*.
La figura 6 riassume tutti i concetti ora esposti:

1. un datagramma inviato al Mobile Node giunge all'Home Network tramite il classico instradamento;
2. il datagramma è intercettato dall'Home Agent e tramite tunneling inviato verso il care-of address;
3. il datagramma è decapsulato e consegnato al Mobile Node;

4. i datagrammi inviati dal Mobile Node subiscono il classico instradamento. In figura è mostrato il caso in cui Foreign Agent svolge anche la funzione di default router per il Mobile Node.

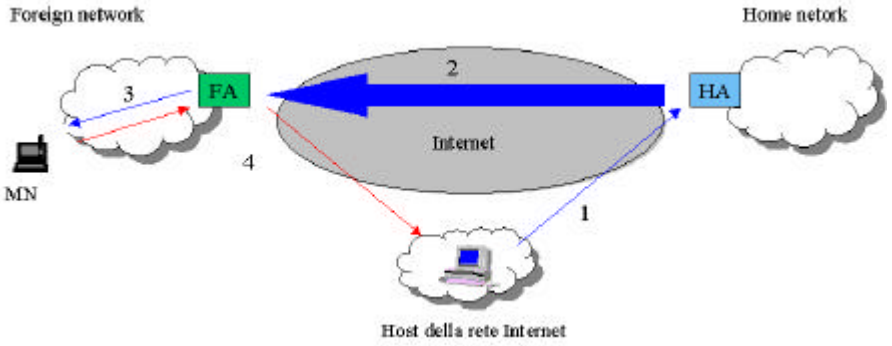


Figura 6: Instradamento

1.5 Formato dei messaggi ed estensione dei protocolli

Per attuare la procedura di Registrazione, sono stati introdotti un'insieme di messaggi di controllo trasmessi tramite il protocollo UDP (User Datagram Protocol) utilizzando il numero di porta 434.
Tali messaggi prendono il nome di:

- ***Registration Request Message***
- ***Registration Reply Message***

Inoltre la procedura di Agent Discovery si basa sull'utilizzo degli esistenti ***Router Advertisement*** e ***Router Sollecitation Message*** definiti nel protocollo denominato ICMP (Internet Control Message Protocol) Router Discovery [4].

Mobile IP consente un meccanismo di estensione di protocolli che permette di inserire informazioni opzionali nei messaggi di controllo o negli ICMP Router Discovery Message. Tali estensioni seguono il "corpo" dei messaggi

sopra definiti e sono identificabili attraverso l'analisi di opportuni campi contenuti nei messaggi.
I due gruppi di estensioni sono mantenuti separati:

- estensioni applicabili ai messaggi di controllo (*Mobile-Home Autentication Extension*; *Mobile-Foreign Autentication Extension*; *Foreign-Home Autentication Extension*);
- estensioni applicabili ai messaggi ICMP Router Discovery (*Mobility Agent Advertisement Extension*; *One-byte Padding Extension*; *Prefix Lengths Extension*).

Ciascun messaggio di controllo e ciascuna estensione viene univocamente identificata fornendogli un Type Number [5].

1.6 Internet Control Message Protocol

Dato che il protocollo IP fornisce un servizio non affidabile, se un router non riesce ad instradare o a consegnare un datagramma o se riscontra situazioni anomale (tra cui congestione di rete) deve poter notificare tali eventi al mittente del datagramma, affinchè siano attuate opportune operazioni per correggere il problema [2].

Per poter consentire ai sistemi coinvolti di scambiarsi informazioni circa tali situazioni, è stato definito un apposito protocollo. Tale protocollo, denominato Internet Control Message Protocol, è una parte integrante di IP e deve essere incluso in ogni implementazione standard di IP. Da sottolineare che la funzione di ICMP è solo di notifica degli errori al sistema di origine, ICMP non specifica le azioni che devono essere prese per rimediare agli errori ed ai malfunzionamenti. Sarà poi il sistema di origine a porre in relazione il particolare errore con il relativo programma applicativo ed a decidere cosa fare per risolvere il problema.

I messaggi ICMP, costituiti da una intestazione e da una parte dati, sono incapsulati nei datagrammi IP e subiscono il classico instradamento di Internet. L'intestazione prevede la presenza di un campo *Type* per identificare il messaggio, di un campo *Code* per fornire ulteriori informazioni sul tipo di messaggio e di un campo *Checksum*. Dato che ogni messaggio ICMP è relativo ad uno specifico datagramma (essendo IP un servizio senza connessione) la parte dati del messaggio dovrà contenere, tra le altre informazioni, un identificativo del particolare datagramma che ha generato l'errore o la situazione anomala.
Pur non volendo descrivere in dettaglio l'Internet Control Message Protocol occorre sottolineare i due seguenti concetti [6]:

- ICMP notifica eventuali errori solo al sistema che ha originato il datagramma e non ai sistemi intermedi lungo il percorso attraversato dal datagramma stesso; questo perchè il sistema d'indirizzamento di Internet è tale che, quando un datagramma arriva ad un determinato sistema, quest'ultimo non ha modo di sapere il percorso del datagramma, ma solo da chi è stato inviato;

- la procedura di gestione dei datagrammi prevede un'unica differenza tra i datagrammi che trasportano i messaggi ICMP e gli altri: non sono generati messaggi ICMP in seguito ad errori causati da datagrammi che trasportano messaggi ICMP, ciò serve ad evitare messaggi di errore relativi a messaggi di errore.

Esempi di messaggi ICMP sono:

- *Source Quench*

  Inviato dal destinatario, interrompe l'emissione d'unità informative da parte del mittente.

- *Redirect*

Il destinatario segnala al mittente di re-instradare una particolare unità informativa verso un altro sistema.

- *Echo*

  Controlla se un possibile destinatario è attivo.

- *Destination Unreacheable*

  Notifica il mittente della non raggiungibilità di un sistema.

- *Router Solicitation Message* e *Router Advertisement Message*

  Permettono agli host di scoprire dinamicamente un default router.

Nel caso specifico di Mobile IP, assumono particolare importanza gli ultimi due tipi di messaggi che, come detto in precedenza, permettono di implementare la procedura di Agent Discovery.

1.6.1 ICMP Router Discovery

ICMP fornisce un meccanismo denominato Router Discovery che permette ad un host di determinare l'indirizzo di un router a cui inviare i datagrammi.
Altri protocolli permettono di ottenere un risultato analogo [2]: BOOTP (Bootstrap Protocol) e DHCP, se utilizzati, individuano l'indirizzo di un default router consultando un database gestito dall'amministratore della rete. Il limite di questi due protocolli è quello di fornire informazioni che potrebbero essere non aggiornate e quindi non rispecchiare l'attuale "configurazione della rete".
ICMP Router Discovery permette di risolvere il problema sopra esposto: il protocollo prevede che gli host acquisiscano informazioni dagli stessi router attraverso i Router Solicitation Message ed i Router Advertisement Message; inoltre utilizzando dei timer un host è in grado di stabilire fino a quando l'indirizzo del default router può essere considerato valido.
Un'analisi più dettagliata dei due tipi di messaggi è la seguente [4]:

Router Advertisement Message

Se il router e la rete supportano il multicasting, un router può inviare messaggi utilizzando l'indirizzo 224.0.0.1, altrimenti il router invierà il messaggio utilizzando un *limited broadcast address*, 255.255.255.255. Di seguito è mostrato il formato di un Router Advertisement Message (tra parentesi viene indicato il valore assunto dal relativo campo):

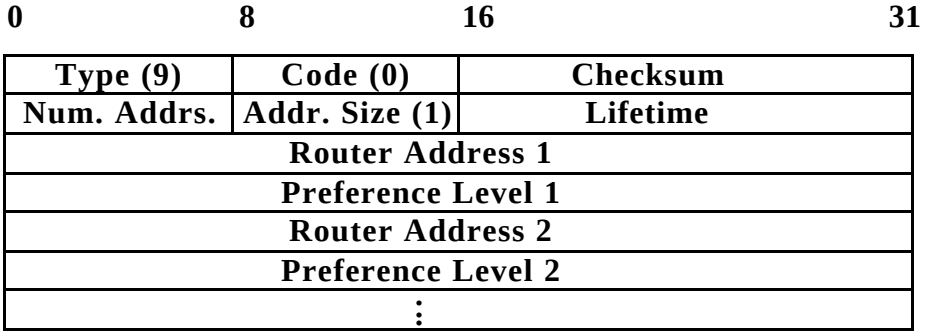


Figura 7: ICMP Router Advertisement Message

I campi *Type*, *Code* e *Checksum* sono comuni a tutti i messaggi ICMP. Il campo *Num. Addrs.* indica il numero d'indirizzi IP elencati mentre *Addr.Size* specifica la dimensione degli indirizzi espressa in unità di 32 bit (1 per IPv4). Si osservi che a ciascuno indirizzo viene associato un livello di preferenza. Infine il campo *Lifetime* indica l'intervallo di tempo per il quale gli indirizzi elencati possono essere considerati validi. Da sottolineare che ICMP specifica il periodo di trasmissione di tali messaggi, tale periodo è legato al valore indicato nel campo Lifetime.

Router Solicitation Message

ICMP permette ad un host di sollecitare l'emissione dei Router Advertisement Message attraverso l'invio dei Router Solicitation Message.
Anche in questo caso il messaggio può essere inviato utilizzando un *multicast address* o un *limited broadcast address*.

La struttura del messaggio è mostrata in figura e non richiede ulteriori considerazioni:

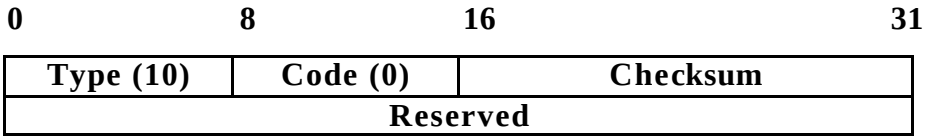


Figura 8: ICMP Router Solicitation Message

1.7 Agent Discovery

Attraverso la procedura denominata Agent Discovery, il Mobile Node è in grado di determinare se è connesso con la propria Home Network o con una Foreign Network, di acquisire il care-of address ed infine di gestire l' eventuale spostamento tra reti differenti.
Fondamentalmente la funzione di Agent Discovery impone ai mobility agent (Home Agent e Foreign Agent) di "pubblicizzare" in broadcast la loro disponibilità a fornire un servizio.

Come accennato precedentemente la funzione di Agent Discovery viene implementata facendo uso di due tipi di messaggi:

- ***Agent Advertisement Message***
- ***Agent Solicitation Message***

Occorre premettere che tutti i concetti che saranno esposti nel seguito partono dal presupposto che esiste una connettività a livello di collegamento (link-layer connection) tra il Mobile Node e la sotto-rete che fornisce accesso ad Internet. Inoltre, è opportuno precisare, che non è necessario fare uso delle procedure di Agent Advertisement e Agent Solicitation nel caso in cui la sotto-rete, alla quale è connesso il Mobile Node, permette di individuare il mobility agent a livello di collegamento.

Infine Mobile IP non prevede l' autenticazione dei messaggi sopra esposti, facoltativamente potrebbero essere autenticati tramite IP Autentication Header o altri meccanismi di cui non si entrerà in merito.

1.7.1 Agent Advertisement Message

Un Agent Advertisement Message risulta essere un ICMP Router Advertisement Message esteso in maniera tale da poter contenere un Mobility Agent Advertisement Extension ed, opzionalmente, un Prefix Lengths Extension un One-byte Extension o altre estensioni che potrebbero essere sviluppate per particolari applicazioni.

Prima di entrare in dettaglio nella spiegazione dei vari tipi di estensioni, occorre definire il contenuto di alcuni campi richiesti in corrispondenza dei diversi livelli della pila protocollare:

- ***Link-Layer Fields***
  - Destination Address: se l'advertisement è stato sollecitato da un Mobile Node, il link-layer addres del messaggio deve essere pari al source link-layer address dell'Agent Solicitation Message. Questa situazione rappresenta il solo caso in cui l'Agent Advertisement Message è inviato in unicast.
- ***IP Fields***
  - TTL (Time To Live): deve essere settato ad 1.
  - Destination Address: come specificato nel protocollo ICMP Router Discovery, è permesso utilizzare *all system multicast address* (224.0.0.1) oppure un *limited broadcast address* (255.255.255.255).
- ***ICMP Fields***
  - Code: se i mobility agent si comportano come dei router allora il campo Code assumerà il valore 0 altrimenti il valore 16. In

questo secondo caso, i mobility agent devono essere in grado di indirizzare i datagrammi ricevuti dal Mobile Node ad un router di default.

?? Lifetime: indica il periodo di tempo per il quale l'Advertisement deve essere considerato valido.

?? Router Address: tale campo può essere utilizzato dai mobility agent per comunicare gli indirizzi delle proprie interfacce di rete con i relativi livelli di preferenza.

Se spediti periodicamente, l'intervallo di tempo tra due Agent Advertisement dovrebbe essere pari ad un terzo del valore indicato nel campo Lifetime. In questo modo un Mobile Node può perdere fino a tre messaggi prima di eliminare il mobility agent dalla propria tabella (vedi paragrafo 1.7.4). Per evitare l'eventuale collisione tra diversi Agent Advertisement, il periodo di ritrasmissione deve essere leggermente modificato secondo un fattore casuale.

1.7.1.1 Mobility Agent Advertisement Extension

Tale estensione, utilizzata per indicare che un ICMP Router Advertisement Message è anche un Agent Advertisement Message, viene posta di seguito ai campi ICMP.
La struttura di tale estensione è mostrata in figura:

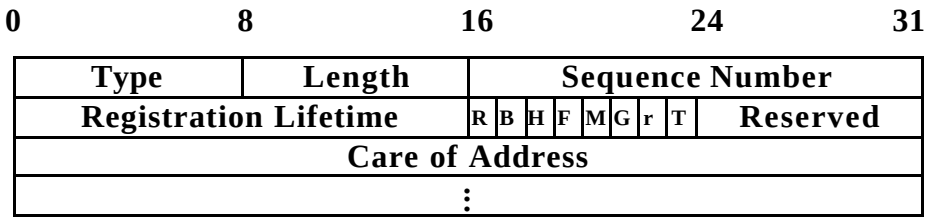


Figura 9: Mobility Agent Advertisement Extension

I diversi campi hanno il seguente significato:

- ***Type***

  Assume il valore 16.

- ***Length***

  Esprime la dimensione, in ottetti, dell'estensione escludendo i campi Type e Lenth. In particolare Length = 6+4^N dove 6 rappresenta il numero di byte necessari per i campi Sequence Number, Registration Lifetime, Flags e Reserved mentre N rappresenta il numero di care-of address segnalati.

- ***Sequence Number***

  Specifica il numero di sequenza del messaggio compreso in un determinato range di valori. Ciascun Advertisement, emesso dopo "l'inizializzazione" (booting) del mobility agent, sarà caratterizzato da un valore crescente del Sequence Number a partire da zero. Particolari accorgimenti vengono utilizzati per far sì che il Mobile Node possa distinguere un "crash" del mobility agent da una diminuizione del sequence number dovuta al fatto di aver ricoperto l'intero range di valori ammessi.

- ***Registration Lifetime***

  Specifica il periodo di tempo (espresso in secondi) per il quale il mobility agent è disposto a fornire il proprio servizio. Se il campo è costituito da tutti 1, il Lifetime sarà infinito.

- ***Flags***

  Sono utlizzati per caratterizzare il servizio offerto. In particolare:

  - *R: Registration Request.* E' settato per richiedere al Mobile Node di registrarsi tramite il Foreign Agent anche se utilizza un co-located care-of address.

?? *B: Busy.* E' settato quando il Foreign Agent è occupato e non è in grado di accettare nuove registrazioni. Da notare che il Foreign Agent, pur se occupato, deve continuare ad inviare gli advertisement per rendere nota la propria disponibilità ai Mobile Node precedentemente registrati.

?? *H: Home Agent.* E' settato quando il mobility agent svolge la funzione di Home Agent.

?? *F: Foreign Agent.* E' settato quando il mobility agent svolge la funzione di Foreign Agent.

?? *M,G.* Permettono di rendere noti i differenti tipi d'incapsulamento che il mobility agent è in grado di manipolare (*Minimal Encapsulation* [7]; *Gre Encapsulation* [8]). Da sottolineare che l'algoritmo di default, trattabile da tutti i mobility agent, è denominato *IP-within-IP* [9].

?? *r.* Viene ignorato in ricezione.

?? *T.* Se settato il Foreign Agent supporta la procedura di Reverse Tunneling [10].

✍✍ ***Reserved***

E' ignorato in ricezione.

✍✍ ***Care-of Address(es)***

Un Foreign Agent deve pubblicizzare almeno un care-of address. In presenza di più care-of address non è permesso associargli livelli di preferenza.

Per chiarire il formato complessivo di un Agent Advertisement Message può essere utile riferirsi alla seguente figura:

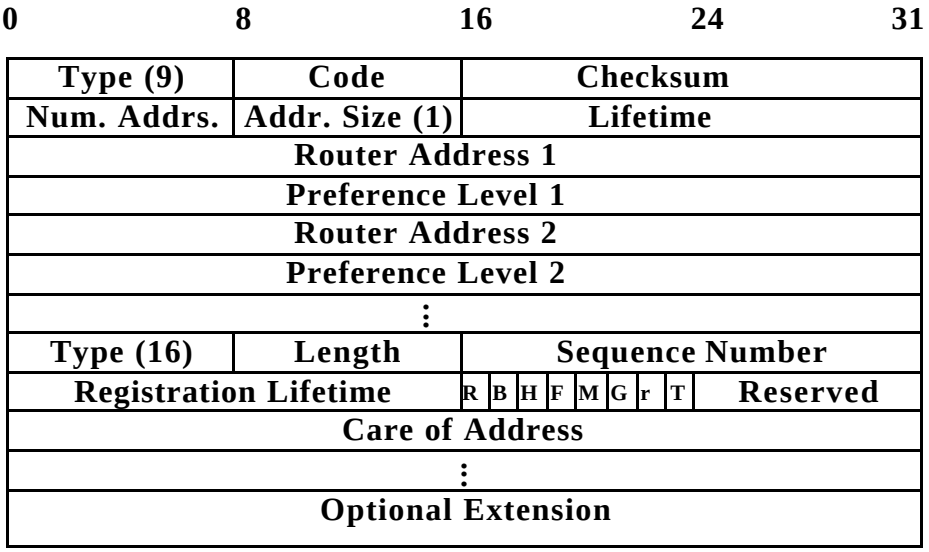


Figura 10: Esempio di un Agent Advertisement Message

1.7.1.2 Prefix-Length Extension

Nel caso in cui l'Agent Advertisement contenga una lista di indirizzi (specificati nell' ICMP fields), tale estensione permette al Mobile Node di apprendere la maschera necessaria per codificare il campo sub-net della Foreign Network.

Si vedrà in seguito, che tale conoscenza può essere utilizzata nella implementazione dell'algoritmo necessario per capire se il Mobile Node si è spostato da una sotto-rete ad un'altra.

Se presente, la Prefix-Length Extension deve seguire la Mobility Agent Advertisement Extension.

1.7.1.3 One-byte Padding Extension

E' una estensione di riempimento utilizzata da quelle implementazioni del protocollo IP che richiedono messaggi ICMP costituiti da un numero pari di byte. In [1] viene specificato che tale estensione, se presente, dovrebbe essere posta dopo tutte le altre estensioni.

1.7.2 Agent Solicitation Message

Attraverso questo messaggio un Mobile Node può sollecitare l'emissione di Agent Advertisement. Il formato di un Agent Solicitation Message è identico a quello di un ICMP Router Solicitation Message tranne per il fatto che il campo Time To Live deve essere impostato ad uno.

1.7.3 Comportamento delle entità architetturali

Sia i mobility agent che il Mobile Node devono rispettare delle regole che permettano di portare a buon fine la procedura di Agent Discovery:

- tutti i mobility agent dovrebbero rispondere ad un Agent Solicitation Message;
- i mobility agent devono regolare il tasso con cui inviano gli Agent Advertisement in maniera tale da non "consumare" una rilevante quota della larghezza di banda della rete;
- un mobility agent potrebbe essere configurato solamente per rispondere agli Agent Solicitation;
- se un mobility agent possiede più interfacce di rete, lo stesso può "apparire" in maniera differente nelle diverse sotto-reti a cui è allacciato. Ad esempio può comportarsi come Home Agent in una sotto-rete e come Foreign Agent in un'altra;
- tutti i Mobile Node devono poter inviare Agent Solicitation. Il tasso al quale un Mobile Node può inviare questi messaggi deve essere regolato dal Mobile Node stesso in accordo ad opportune regole;
- un Mobile Node deve essere in grado di elaborare gli Agent Advertisement. In particolare deve saper distingure un ICMP Router Discovery Message da un Agent Discovery Message.

1.7.4 Rilevamento della mobilità

Precedentemente, si è detto che attraverso la procedura di Agent Discovery un Mobile Node è in grado di stabilire se si è spostato da una sotto-rete ad un'altra. Nel caso venga rilevato uno spostamento, il Mobile Node dovrà procurarsi un nuovo care-of address, se la sotto-rete è una Foreign Network, altrimenti, se la sotto-rete è la Home Network (informazione ricavabile dal flag H dell' Agent Advertisement Message), il Mobile Node dovrà deregistrarsi dall'Home Agent.

Nello standard Mobile IP sono stati introdotti due meccanismi per il rilevamento della mobilità (anche se il protocollo non vieta l'utilizzo di altre procedure):

Algoritmo 1

Il primo metodo si basa sull'utilizzo del campo Lifetime contenuto nella porzione ICMP Router Advertisement dell' Agent Advertisement Message.
Il Mobile Node ogni volta che riceve un Advertisement memorizza le informazioni del mobility agent, ma soprattutto imposta un timer con scadenza temporale pari al Lifetime, aggiornandone il valore ad ogni ricezione di un Advertisement proveniente dallo stesso mobility agent. Se il Mobile Node non riceve Advertisement prima della scadenza del timer, rimuove le informazioni relative al mobility agent.

Ogni Mobile Node mantiene una tabella dei mobility agent da cui ha ricevuto Advertisement; questa tabella viene aggiornata periodicamente eliminando le entry scadute. Se una entry scade, il mobility agent dovrebbe essere considerato non raggiungibile.
Se non è più raggiungibile il mobility agent a cui fa riferimento il Mobile Node, il Mobile Node può avviare la procedura di Registrazione con uno dei mobility agent considerati validi; in alternativa il Mobile Node può inviare un Agent Solicitation Message.

Algoritmo 2

Il secondo metodo utilizza la Prefix-Length Extension, in questo modo il Mobile Node può determinare se i nuovi Agent Advertisement provengono da una nuova sotto-rete oppure no.
Occorre sottolineare che tale metodo dovrebbe essere utilizzato solamente quando il corrente ed il futuro mobility agent inseriscono la Prefix-Length Extension nei propri messaggi di Agent Advertisement.
Sostanzialmente tale metodo è applicabile quando il Mobile Node è in grado di stabilire il prefisso di rete della sotto-rete alla quale è attualmente connesso e di quella futura.

1.8 Procedura di Registrazione

La procedura di registrazione è un meccanismo flessibile che permette al Mobile Node di comunicare informazioni di raggiungibilità al proprio Home Agent. In particolare attraverso tale meccanismo il Mobile Node può richiedere un servizio di reinstradamento, quando si trova in una Foreign Network, può comunicare il care-of address, può rinnovare una registrazione ed infine può de-registrarsi quando torna nella propria Home Network.
Le funzioni sopra esposte costituiscono la base della procedura di registrazione, in aggiunta, tale meccanismo, consente al Mobile Node di:

- determinare il proprio home address e/o scoprire l'indirizzo di un Home Agent (nel caso in cui non sia configurato con tali informazioni);
- mantenere simultaneamente più registrazioni (e quindi disporre di più di un care-of address) per ricevere copie dello stesso datagramma. Tale funzione è utile quando la rete in cui si trova il Mobile Node è ad alto tasso d'errore;
- de-registrare uno specifico care-of address.

Quando un Home Agent accetta la richiesta di registrazione, associa l'home address del Mobile Node con il rispettivo care-of address e mantiene tale associazione per tutta la durata della registrazione. La tripletta costituita dall'home address, dal care-of address e dal lifetime della registrazione viene detta ***Mobility Binding***: una richiesta di registrazione può essere considerata come un aggiornamento del binding [11].

Lo standard Mobile IP, definisce due differenti procedure di registrazione a seconda che il Mobile Node utilizzi un Foreign Agent care-of address oppure un co-located care-of address.
In particolare se il Mobile Node utilizza un *Foreign Agent care-of ad*dress:

- il Mobile Node invia un messaggio di **Registration Request** al Foreign Agent;
- il Foreign Agent elabora la richiesta e la rilancia all'Home Agent;
- l'Home Agent invia un messaggio di **Registration Reply** al Foreign Agent indicando l'accettazione o il rifiuto della registrazione;
- il Foreign Agent elabora il messaggio e lo rilancia al Mobile Node per informarlo se la registrazione è andata a buon fine oppure no.

Nel caso in cui il Mobile Node utilizzi un *co-located care-of address* (ed il flag R dell'Agent Advertisement non è settato) lo scambio dei messaggi sopra menzionati avviene direttamente tra il Mobile Node e l'Home Agent.
Mobile IP prevede che i messaggi di Registration Request e Registration Reply siano trasmessi tramite il protocollo UDP utilizzando il numero di porta 434, inoltre lo standard incentiva l'utilizzo del campo Checksum contenuto nell'header del messaggio UDP.

Affinchè possa essere garantita l'autenticità dei messaggi di registrazione, [1] consente l'utilizzo di estensioni da applicare a tali messaggi. In particolare ogni coppia di entità architetturali (MN-HA, MN-FA, FA-HA) può condividere un *"**Mobility Security Association**"* cioè un insieme di "contesti" di sicurezza;

ogni contesto sarà caratterizzato da un algoritmo di autenticazione, da una chiave di decodifica delle informzioni trasmesse, etc. Da ciò deriva che ogni estensione, associata con una coppià di entità architetturali, conterrà una "parola di autenticazione" dipendente dal contesto di sicurezza utilizzato.
Il particolare contesto di sicurezza utilizzato verrà individuato tramite un ***Security Parameter Index*** (SPI), cioè un indice, contenuto nella estensione, attraverso il quale le due entità architetturali potranno risalire alla regola con la quale è stato autenticato il messaggio.
Come si vedrà in seguito, Mobile IP prevede che il Mobile Node debba condividere un Mobility Security Association con il proprio Home Agent e quindi ogni messaggio di registrazione dovrà contenere almeno un ***Mobile-Home Autentication Extension***.
Da tutto ciò deriva che la struttura di un messaggio di registrazione sarà la seguente:

Figura 11: Struttura del messaggio di registrazione

1.8.1 Registration Request Message

Un Registration Request Message permette al Mobile Node di "comunicare" con il proprio Home Agent, in maniera tale che quest'ultimo possa creare o aggiornare il Mobility Binding relativo al Mobile Node stesso. La registrazione può essere rilanciata dal Foreign Agent oppure può essere inviata all'Home Agent direttamente dal Mobile Node. Il messaggio di registrazione segue gli header IP e UDP ed è schematizzato di seguito:

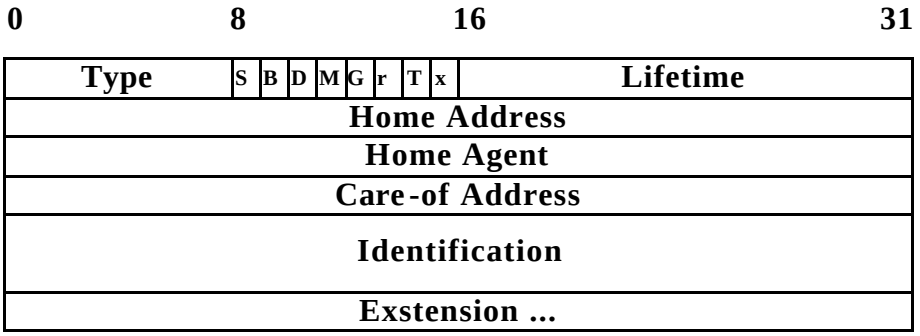


Figura 12: Registration Request Message

✍✍ ***Type***

Assume il valore 1

✍✍ ***Flags***

Permettono di caratterizzare la registrazione. In particolare:

?? *S: Simultaneous Binding.* Se settato, il Mobile Node richiede all'Home Agent di mantenere i precedenti binding. In questo modo il Mobile Node potrà ricevere più copie dello stesso datagramma.

?? *B: Broadcast Datagram.* Se settato il Mobile Node richiede all'Home Agent di inviargli i datagrammi di tipo broadcast ricevuti nell'Home Network. Se è richiesto questo servizio ed il Mobile Node utilizza un Foreign Agent care-of address, l'Home Agent dovrà prima incapsulare il broadcast datagram in un unicast datagram indirizzato all'home address del Mobile Node e poi inviarlo tramite tunneling al Foreign Agent.

?? *D: Decapsulation by Mobile Node.* Se settato sarà lo stesso Mobile Node a decapsulare i datagrammi provenienti dall'Home Agent. Questo significa che il Mobile Node utilizza un co-located care-of address.

?? *M,G: Minimal Encapsulation e Gre Encapsulation.* Permettono al Mobile Node di richiedere un particolare tipo d'incapsulamento. Questi flags possono essere settati solamente

quando il Mobile Node utilizza un co-located care-of address oppure quando il Foreign Agent implementa tali funzioni.

?? *r,x*. Vengono ignorati in ricezione.

?? *T*. Il Mobile Node richiede Reverse Tunneling.

✍✍ ***Lifetime***

Permette al Mobile Node di specificare la durata, in secondi, della registrazione. Un campo costituito da tutti 1 indica infinito, mentre se costituito da tutti 0 indica una richiesta di de-registrazione.

✍✍ ***Home Address, Home Agent e Care-of Address***

Indicano, rispettivamente, l'home address del Mobile Node, l'indirizzo dell'Home Agent ed il care-of address del Mobile Node.

✍✍ ***Identification***

Campo di 64 bit utilizzato per scopi d'autenticazione. Il valore contenuto in questo campo cambia con ogni nuova registrazione e quindi permette di associare uno specifico messaggio di registrazione con il rispettivo messaggio di risposta. Mobile IP permette di utilizzare due modalità differenti per autenticare ogni singola procedura di registrazione (il tipo di modalità utilizzata dipende dal Mobility Security Association esistente tra il Mobile Node e l'Home Agent):

Utilizzo di un Timestamp

Il Mobile Node che desidera registrarsi invierà un Registration Request Message con il campo Identification contenente una "fotografia" dell'istante in cui invia il messaggio; in seguito alla ricezione di tale messaggio, l'Home Agent dovrà verificare che il campo Identification contenga un valore "simile" a quello indicato nel proprio orologio (Mobile IP consente una tollerenza di circa sette secondi). Se la verifica va a buon fine l'Home Agent copierà l'intero Identification Field nel Registration Request, altrimenti rifiuterà la

registrazione ed inserirà nel campo Identification del messaggio di risposta delle informazioni per sincronizzare il Mobile Node.

Utilizzo di un "pseudorandom number"

Il Mobile Node in corrispondenza di ogni messaggio di registrazione inserirà nei 32 bit meno significativi del campo Identification un valore generato casualmente e copierà nella restante parte i 32 bit più significativi del campo Identification contenuto nell'ultimo Registration Reply Message ricevuto. Dualmente si comporterà l'Home Agent, cioè in corrispondenza di ogni Registration Reply, inserirà nei 32 bit più significativi un valore generato casualmente e in quelli meno significativi copierà il valore contenuto nell'ultimo Registration Request Message ricevuto. Procedendo in questo modo entrambe le entità architetturali invieranno un valore che sarà controllato nel successivo messaggio ricevuto.

I campi sopra descritti caratterizzano le informazioni che devono essere necessariamente presenti in tutti i Registration Request Message. In aggiunta, come è stato sottolineato precedentemente, i messaggi di registrazione possono contenere delle estensioni che permettono di comunicare ulteriori informazioni.

1.8.2 Registration Reply Message

Tale messaggio permette di informare il Mobile Node circa l'esito della sua richiesta di registrazione. Come descritto nell'introduzione al capitolo, il messaggio può essere inviato al Mobile Node direttamente dall'Home Agent oppure tramite il Foreign Agent.
Anche il Registration Reply Message segue gli header IP e UDP e può contenere delle estensioni.
La figura seguente illustra il formato del messaggio, identificabile dal campo Type che assumerà il valore 3:

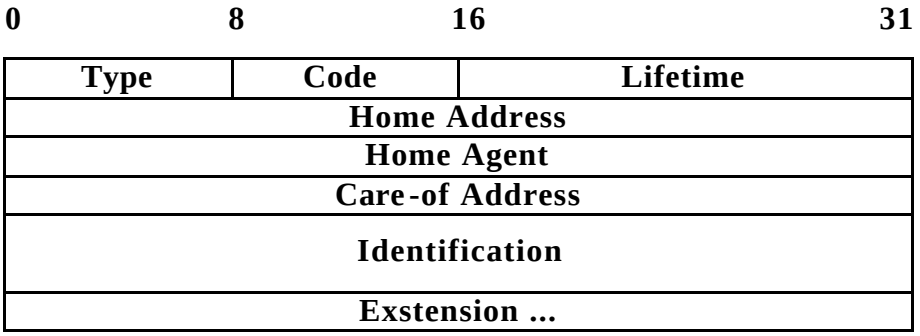


Figura 13: Registration Reply Message

Il campo ***Code*** indica l'esito della richiesta di registrazione; nel caso in cui il Mobile Node utilizzi un Foreign Agent care-of address tale richiesta può essere negata, oltre che dall'Home Agent, anche dal Foreign Agent. Di seguito vengono riportati alcuni dei valori che può assumere il campo Code:

Code	Registrazione accettata
0	Registration accepted
1	Registration accepted, but simultaneous mobility bindings unsopported

Tabella 1: Registrazione accettata

Code	Registrazione negata dal Foreign Agent
64	Reason unspecified
65	Administratively prohibited
66	Insufficient resources
67	Mobile Node failed authentication
⋮	⋮

Tabella 2: Registrazione negata dal Foreign Agent

Code	Registrazione negata dall'Home Agent
128	Reason unspecified
129	Administratively prohibited
130	Insufficient resources
131	Mobile Node failed authentication
⋮	⋮

Tabella 3: Registrazione negata dall'Home Agent

Se la richiesta di registrazione viene accettata il campo Lifetime indicherà per quanto tempo l'Home Agent considererà valida la registrazione. Tale durata può essere più breve di quella richiesta dal Mobile Node, ma non più elevata.
Se il campo Code indica che la richiesta non è stata accettata, il campo Lifetime dovrà essere ignorato in ricezione.

1.8.3 Estensioni

Mobile IP consente l'utilizzo di estensioni, particolare importanza assumono le estensioni di autenticità in quanto permettono di autenticare i messaggi di registrazione attraverso l'utilizzo di un contesto di sicurezza individuato dallo SPI. La regola utilizzata permetterà di elaborare un *Autenticator value* che dovrà tutelare il contenuto dei messaggi di richiesta o di risposta di registrazione, tutte le estensioni precedenti a quella in considerazione ed i campi Type, Lenght e SPI della estensione corrente. Sono esclusi da protezione l'header UDP e l'autenticator value stesso. Mobile IP prevede che l'algoritmo di default, utilizzato per elaborare il valore di autenticazione, sia *"The MD5 Message-Digest Algorithm"* [12].

Ogni coppia di entità architetturale, che condivide un Mobility Security Association, dovrà inserire un'opportuna estensione di autenticità in tutti i messaggi di registrazioneche si scambieranno.

1.8.3.1 Estensioni di autenticità

In [1] sono definiti tre tipi di estensioni di autenticità, ciascuna delle quali permette a due entità architetturali di condividere un Mobility Security Association. Come detto precedentemente, le due entità architetturali devono essere in grado di ricavare la regola di autenticità analizzando l'indicatore SPI contenuto nella estensione.

- **Mobile-home Autentication extension**

  Questa estensione deve essere presente in tutti i Registration Request e Registration Reply Message ed assume la seguente struttura:

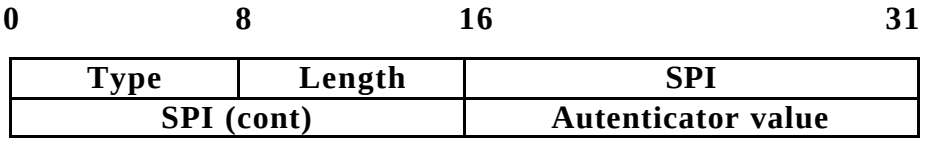


Figura 14: Mobile-Home Autenticator Extension

  Il campo Type assume il valore 3, Length esprime in byte la lunghezza dello SPI e del campo Autenticator Value, SPI è un campo di 4 byte descritto nei paragrafi precedenti mentre Autenticator Value è un campo di lunghezza variabile dipendente dal particolare algoritmo di autenticazione utilizzato.

- Gli altri due tipi di estensioni, associate con gli eventuali Mobility Security Association esistenti rispettivamente tra il Mobile Node ed il Foreign Agent ed il Foreign Agent e l'Home Agent, sono opzionali e prendono il nome di **Mobile-Foreign Autentication Extension** e **Foreign-Home Autentication Extension**. La struttura di queste due estensioni è identica a quella indicata in figura 14 ad eccezione del valore del campo Type.

Le estensioni descritte in questo paragrafo e quelle inerenti alla procedura di Agent Discovery rappresentano solamente un sottoinsieme delle possibili estensioni applicabili ai messaggi. In altre parole è consentito introdurne delle altre se una particolare applicazione ne richiede il bisogno. Proprio per questo motivo, in [1] sono state definite le regole che permettono di stabilire l'ordine secondo il quale estensioni di significato differente possono essere inserite in uno stesso messaggio.

1.8.4 Caratteristiche funzionali del Mobile Node

Un Mobile Node deve essere configurato con la net-mask della propria Home Network e con il Mobility Security Association da condividere con l'Home Agent. Opzionalmente potrebbe essere configurato con il proprio home address e con l'indirizzo IP di uno o più Home Agent; se il Mobile Node non possiede queste ultime informazioni, lo standard, precisato in [1], definisce le modalità con cui ricavarle:

- Per poter determinare l'indirizzo IP dell'Home Agent, il Mobile Node deve inviare un Registration Request Message con il campo Home Agent contenente un indirizzo broadcast per la propria Home Network. Per quanto riguarda il campo IP Destination Address (dell'header IP), se il Mobile Node si registra direttamente con l'Home Agent dovrà essere pari ad un indirizzo broadcast valido per la Home Network, altrimenti sarà pari all' indirizzo IP del foreigna agent.In seguito alla ricezione di questo messaggio, gli Home Agent, residenti nella Home Network, invieranno un Registration Reply Message nel quale, oltre a rifiutare la registrazione, indicheranno il proprio indirizzo IP (nel campo Home Agent) che potrà essere utilizzato dal Mobile Node per le successive registrazioni. La procedura appena descritta prende il nome di *Automatic Home Agent Discovery*.

- Per detrminare il proprio home address, il Mobile Node invierà una richiesta di registrazione contenente una particolare estensione denominata "**Mobile Node Network Access Identifier (NAI) Extension**" [13], descritta in un successivo capitolo, attraverso la quale il Foreign Agent sarà in grado di individuare la Home Network del Mobile Node. In aggiunta il Mobile Node dovrà inserire nel campo Home Address del Registration Request Message il valore 0.0.0.0 e dovrà essere in grado di "estrarre" il proprio home address dal Registration Reply Message.

Per tutte le richieste di registrazione in attesa di risposte, il Mobile Node deve mantenere una tabella contenente una serie di informazioni:

- L'indirizzo fisico del Foreign Agent al quale è stato inviato il Registration Request Message.
- L'indirizzo IP del destinatario del messaggio.
- Il care-of address che si vuole registrare.
- Il campo Identification contenuto nel messaggio di registrazione.
- Il valore del campo Lifetime del messaggio ed il rimanente lifetime della registrazione in attesa.

Affinchè la procedura di registrazione possa andare a buon fine, il Mobile Node deve essere in grado di generare opportuni messaggi di richiesta di registrazione e di elaborare i corrispondenti messaggi di risposta.
Per quanto riguarda i messaggi di richiesta di registrazione è opportuno sottolineare il contenuto che possono assumere i seguenti campi del messaggio:

- ***IP Field***
  - Source Address: se il Mobile Node utilizza un co-located care-of address dovrà indicare tale indirizzo, in tutte le altre circostanze utilizzerà il proprio home address.
  - Destination Address: se il Mobile Node si registra tramite un Foreign Agent dovrà indicare l'indirizzo di tale agent ricavato dall' IP Source Address dell' Agent Advertisement Message. Nelle reti che permettono di individuare il Foreign Agent a livello di collegamento e che quindi non forniscono l' indirizzo IP, il Mobile Node dovrà utilizzare l'indirizzo multicast "All Mobility Agent", 224.0.0.11. In entrambi i casi il Mobile Node

individuerà il corretto Foreign Agent attraverso l'indirizzo fisico dello stesso. Se il Mobile Node si registra direttamente con l'Home Agent ne indicherà il rispettivo indirizzo (eventualmente dopo averlo scoperto attraverso la procedura descritta nell'introduzione del paragrafo).

- Time To Live: se viene uilizzato l'indirizzo multicast il TTL deve essere impostato ad 1, altrimenti verrà scelto un valore adeguato all'applicazione.

✍✍ ***Registration Request Field***

- Lifetime: se il Mobile Node si registra tramite un Foreign Agent il Lifetime della registrazione non dovrebbe essere superiore al valore Registration Lifetime indicato nell' Agent Advertisement Message. Nei casi in cui il Mobile Node non conosca il Registration Lifetime, può essere utilizzato un valore di default pari a 1800 secondi. Se il Mobile Node vuole de-registrare un particolare care-of address invierà un messaggio di registrazione contenente il care-of address da de-registrare ed il Lifetime pari a zero. Infine se il Mobile Node vuole de-registrarsi completamente dall'Home Agent invierà un messaggio di registrazione con il campo care-of address contenente l'home address ed il Lifetime pari a zero.

In seguito alla ricezione di un Registration Reply Message, il Mobile Node deve, in primo luogo, verificare l'autenticità del messaggio, controllare cioè il cheksum nell'header UDP, la parola di identificazione e le estensioni di autenticazione presenti nel messaggio. Se il Mobile Node riscontra qualche problema dovrà scartare il messaggio e possibilmente registrare tale evento come un *"Security Exception"*. Nel caso in cui il controllo va a buon fine, ed il messaggio di risposta indica che la registrazione è stata accettata, il Mobile Node dovrà memorizzare le caratteristiche della registrazione aggiornandone eventualmente il Lifetime (dovrà diminuire il Lifetime residuo della

registrazione attraverso la differenza tra il Lifetime originario e quello indicato nel Registration Reply Message).

1.8.5 Caratteristiche funzionali del Foreign Agent

Come più volte sottolineato, il Foreign Agent è necessario quando il Mobile Node utilizza un Foreign Agent care-of address. Nella procedura di registrazione il suo ruolo è quello di intermediario tra il Mobile Node e l'Home Agent: rilancia i messaggi di richiesta e di risposta rispettivamente all'Home Agent ed al Mobile Node. L'unica circostanza, per la quale il Foreign Agent può inviare autonomamente un Registration Reply Message, è quando non è in grado di soddisfare le richieste del Mobile Node.

Il Foreign Agent per ogni Mobile Node registrato e per ogni richiesta di registrazione in attesa di risposta, deve memorizzare le seguenti informazioni:

- Indirizzo fisico del Mobile Node
- Home address del Mobile Node
- Indirizzo IP dell'Home Agent
- Campo Identification
- Lifetime originario della registrazione ed il valore rimanente

Lo standard Mobile IP specifica il comportamento del Foreign Agent in seguito alla ricezione di un messaggio di registrazione:
deve verificare l'autenticità del messaggio; se rilancia il messaggio ad un'entità architetturale con la quale condivide un Mobility Security Association deve inserire nel messaggio un'opportuna estensione d'autenticità; se riceve una richiesta di de-registrazione deve eliminare il Mobile Node dalla propria lista solamente se tale richiesta viene accettata dall'Home Agent; per ogni richiesta di registrazione che rilancia all'Home Agent (utilizzando come IP Source

Address l'indirizzo IP dell'interfaccia di rete dalla quale invia il messaggio) deve mantenere un temporizzatore settato al valore del Lifetime, se il Lifetime scade prima della ricezione del messaggio di risposta deve eliminare il Mobile Node dalla propria lista; ogni qual volta una richiesta di registrazione viene accettata dall'Home Agent, il Foreign Agent deve aggiornare le informazioni relative al Mobile Node contenute nella propria "Visited List", in particolare deve impostare il Lifetime della registrazione con il valore contenuto nel Registration Reply Message; etc.

Per comunicare con il Mobile Node, il Foreign Agent utilizzerà l'home address dello stesso e quindi, non potendo utilizzare il protocollo ARP (dato che l'home address non è uno degli indirizzi della Foreign Network), è essenziale che il Foreign Agent conosca il "Link-Layer Address" del Mobile Node.

1.8.6 Caratteristiche funzionali dell'Home Agent

A differenza del Foreign Agent, l'Home Agent è un'entità architetturale indispensabile per la procedura di registrazione. L'Home Agent riceve richieste di registrazione da parte del Mobile Node, aggiorna il Mobility Binding del Mobile Node ed accetta o rifiuta le richieste di registrazione.
Ciscun Home Agent deve essere configurato con un'indirizzo IP, con la net-mask dell'Home Network e con il Mobility Security Association condiviso con il Mobile Node. Inoltre per ciascun Mobile Node registrato deve mantenere le seguenti informazioni:

- Home address.
- Care-of address.
- Valore del campo Identification.
- Lifetime rimanente della registrazione.

Descrivere ogni singola azione svolta dall'Home Agent significherebbe effettuare un riepilogo di cose già dette, per questo motivo ritengo che sia più rilevante fornire degli esempi della procedura di registrazione che rispecchiano alcuni scenari di lavoro:

Registrazione tramite un Foreign Agent

Il Mobile Node riceve un Agent Advertisement da un Foreign Agent e desidera effettuare la registrazione del care-of address, vuole utilizzare lo schema d'incapsulamento standard (IP-within-IP), non vuole broadcast e non desidera simultaneous mobility binding:

- ***IP Fields***
  - Source Address: home address del Mobile Node.
  - Destination Address: copiato dall'IP source address dell' Agent Advertisement.
  - Time To Live: 1.
- ***UDP Fields***
  - Source Port : qualunque.
  - Destination Port : 434.
- ***Registration Request Fields***
  - Type : 1.
  - Flags : tutti settati a zero.
  - Lifetime: valore pari al Lifetime contento nel Mobility Agent Advertisement Message.
  - Home Address: home address del Mobile Node.
  - Home Agent: indirizzo IP dell'Home Agent
  - Care-of Address: valore copiato dall'omonimo campo del Mobility Agent Advretisement Message.
  - Identification: vedi paragrafo 1.8.1.
  - Extension: Mobile-Home Autentication Extension.

Registrazione di un co-located care-of address

Il Mobile Node accede ad una sotto-rete che non contempla un Foreign Agent e tramite il protocollo DHCP ottiene un co-located care-of address. Il Mobile

Node supporta tutte le forme d'incapsulamento, desidera una copia dei datagrammi broadcast inviati nella Home Network e non desidera simultaneous mobility binding:

- ***IP Fields***
  - Source Address: care-of address ottenuto dal DHCP Server.
  - Destination Address: indirizzo IP dell'Home Agent.
  - Time To Live: 64.
- ***UDP Fields***
  - Source Port : qualunque.
  - Destination Port : 434.
- ***Registration Request Fields***
  - Type : 1.
  - Flags : S=0; B=1; D=1; M=1; G=1.
  - Lifetime: 1800 sec.
  - Home Address: home address del Mobile Node.
  - Home Agent: indirizzo IP dell'Home Agent.
  - Care-of Address: indirizzo ottenuto dal DHCP Server.
  - Identification: vedi paragrafo 1.8.1.
  - Extension: Mobile-Home Autentication Extension.

De-registrazione

Il Mobile Node fa ritorno alla propria Home Network e desidera de-registrare tutti i carte-of address dall'Home Agent:

- ***IP Fields***
  - Source Address: home address del Mobile Node.
  - Destination Address: indirizzo IP dell'Home Agent.
  - Time To Live: 1.
- ***UDP Fields***
  - Source Port : qualunque.
  - Destination Port : 434.
- ***Registration Request Fields***
  - Type : 1.
  - Flags : tutti settati a zero.
  - Lifetime: 0 sec.

- ?? Home Address: home address del Mobile Node.
- ?? Home Agent: indirizzo IP dell'Home Agent.
- ?? Care-of Address: home address del Mobile Node.
- ?? Identification: vedi paragrafo 1.8.1.
- ?? Extension: Mobile-Home Autentication Extension.

1.9 Routing

Quando il Mobile Node accede ad Internet dalla propria Home Network opera senza l'ausilio del protocollo Mobile IP, viene quindi considerato come un qualsiasi host fisso. Quando invece è connesso ad una Foreign Network le tre entità architetturali (Home Agent, Foreign Agent e Mobile Node) devono cooperare fra di loro per garantire la corretta consegna dei datagrammi. In particolare:

- ✍✍ Sia l'Home Agent che il Foreign Agent devono supportare il tunneling dei datagrammi tramite la modalità IP-within-IP, inoltre se il Mobile Node utilizza un co-located care-of address, la stessa funzionalità deve essere svolta dal Mobile Node. Opzionalmente possono essere utilizzate altre forme d'incapsulamento.

- ✍✍ Se il Mobile Node si registra tramite un Foreign Agent care-of address, può utilizzare come router di default lo stesso Foreign Agent scoprendone l'indirizzo attraverso l'Agent Advertisement. Se invece viene caratterizzato attraverso un co-located care-of address, il router di default può essere determinato tramite i messaggi ICMP Router Discovery. In questo caso il protocollo Mobile IP non specifica come determinare l'indirizzo fisico del router, vieta però l'utilizzo del protocollo ARP.

- ✍✍ L'Home Agent deve essere in grado di intercettare, nella Home Network, i datagrammi destinati al Mobile Node per poi inviarli al care-of address (tramite tunneling). Se il datagramma intercettato

risulta essere incapsulato, l'Home Agent deve controllare sia l'header esterno che quello interno per verificarne il corretto contenuto.

- Mobile IP consente due modalità differenti attraverso le quali un Mobile Node, presente in una Foreign Network, può legarsi ad un Multicast Group:
  - Attraverso un multicast router presente nella Foreign Network, utilizzando come Source Address dei messaggi IGMP (Internet Group Management Protocol) l'home address oppure il co-located care-of address.
  - Attraverso un tunnel bi-direzionale con il proprio Home Agent, il Mobile Node invia messaggi IGMP all'Home Agent il quale a sua volta invierà i datagrammi multicast al Mobile Node. In questo caso il Mobile Node deve essere in grado di trattare datagrammi incapsulati a prescindere dal fatto che utilizzi un co-located care-of address.

1.9.1 IP encapsulation within IP

IP encapsulation within IP (brevemente IP-overIP) è l'algoritmo standard utilizzato da Mobile IP per incapsulare i datagrammi. E' opportuno sottolinere che tale tecnica è di validità generale in quanto utilizzata in molteplici applicazioni: multicasting, policy routing, privacy, etc.
Nel presente paragrafo si vuole fornire una descrizione sommaria dell'algoritmo, focalizzando l'attenzione nel suo uso in Mobile IP.
L'incapsulamento si ottiene inserendo, prima del datagramma originario, un nuovo header IP [9]:

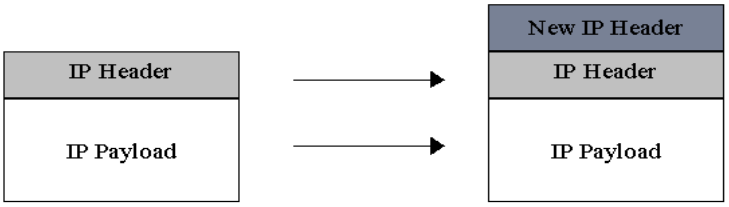


Figura 15: IP-within-IP Encapsulation

Ad eccezione del campo TTL che viene decrementato di una unità, l'header interno non subisce nessun tipo di modifica. Per quanto riguarda gli indirizzi IP presenti nell'header esterno questi rispecchieranno il mittente ed il destinatario del datagramma (generalmente Home Agent e Foreign Agent). Infine un datagramma incapsulato viene riconosciuto tramite il campo Protocol dell'header esterno che indicherà il protocollo IP (Protocol Field=4).

Dopo aver inviato un datagramma incapsulato, l'Home Agent potrebbe ricevere un ICMP Message dal destinatario del datagramma (ad esempio dal Foreign Agent) o da uno dei router intermedi che costituiscono il tunnel. In queste circostanze l'Home Agent dovrà notificare l'errore al mittente del datagramma originario. Dato che il messaggio ICMP identifica il datagramma utilizzando otto byte, tale informazione potrebbe non contenere l'header interno e quindi potrebbe non consentire l'identificazione del mittente.

Per questo motivo l'Home Agent manterrà dei parametri caratterizzanti lo stato del tunnel, *"Soft State of the Tunnel"* [3]. Esempi di tali parametri sono il Time To Live necessario al datagramma incapsulato, la Maximun Trasmission Unit (MTU) del tunnel ed informazioni sulla raggiungibilità del Foreign Agent.

Attraverso queste informazioni l'Home Agent, prima di incapsulare il datagramma, potrà controllare lo stato del tunnel ed inviare tempestivamente un appropriato messaggio ICMP al mittente. E' stata utilizzata la parola "appropriato" per sottolineare che i messaggi ICMP inviati al mittente potrebbero non rispecchiare la situazione reale. Ad esempio, se il soft state indica che la rete di destinazione non è raggiungibile, l'Home Agent non invierà il messaggio ICMP "*Network Unreachable*", ma il messaggio "*Host*

Unreachable" dato che il mittente del datagramma, presumibilmente, non è a conoscenza dell'esistenza del tunnel.

1.9.2 ARP, Proxy ARP e Gratuitous ARP

Oltre ad utilizzare il protocollo ARP, Mobile IP deve far uso di due varianti dello stesso denominate *Proxy ARP* e *Gratuitous ARP*:

- Un Proxy ARP è un ARP Reply inviato da un nodo al posto di un altro nodo quando quest'ultimo non può o non vuole rispondere alle ARP Request [14].
- Un Gratuitos ARP è un pacchetto ARP inviato in broadcast da un nodo per forzare l'aggiornamento delle tabelle ARP degli altri nodi della sotto-rete [14].

Quando un Mobile Node si trova nell'Home Network e si comporta quindi come un qualsiasi host fisso, l'unico meccanismo utilizzato per la risoluzione degli indirizzi è il protocollo ARP.
Proxy ARP e Gratuitos ARP intervengono quando il Mobile Node vuole registrarsi in una Foreign Network oppure quando decide di tornare nella Home Network.
Per chiarire i concetti ora esposti e quindi stabilire l'ordine temporale secondo il quale devono essere utilizzati i diversi protocolli, è utile considerare le due seguenti situazioni:

Il Mobile Node lascia la Home Network e decide di registrarsi con un Foreign Agent

Prima di inviare un messaggio di Registration Request, il Mobile Node disabilita l'elaborazione dei messaggi ARP che potrebbe ricevere o inviare nella Foreign Network.

Se l'Home Agent accetta la registrazione, utilizzerà Gratuitos ARP per aggiornare le tabelle ARP degli altri nodi della Home Network, associando l'home address del Mobile Node con il proprio indirizzo fisico. Inoltre attraverso Proxy ARP risponderà alle ARP Request, che richiedono la risoluzione dell'home address del Mobile Node, fornendo il proprio indirizzo fisico.

Il Mobile Nodo fa ritorno nella Home Network

Prima di inviare un messaggio di Registration Request al proprio Home Agent (per de-registrarsi), il Mobile Node deve compiere le due seguenti azioni:

- Riabilitare l'elaborazione dei messaggi ARP.
- Utilizzare Gratuitos ARP per aggiornare nuovamente le tabelle degli atri nodi della Home Network.

Se l'Home Agent accetta la de-registrazione, disabilita Proxy ARP ed implementa Gratuitos ARP con lo stesso scopo del Mobile Node. La procedura Gratuitos ARP viene svolta sia dall'Home Agent che dal Mobile Node dato che, nel caso di "Wireless Network Interface", l'area di copertura delle due entità architetturali può essere differente.

2 Tecniche di ottimizzazione del protocollo

Il protocollo Mobile IP, definito in [1] e descritto nel precedente capitolo, può essere considerato come l'insieme delle regole basilari che devono essere soddisfatte per gestire in modo semplice la mobilità degli host.

Un'analisi attenta del protocollo evidenzia la possibilità di introdurre dei meccanismi che consentano di migliorarne l'efficienza. Le procedure proposte per raggiungere tale obiettivo sono molte; personalmente ritengo opportuno presentare solamente quelle tecniche che offrono delle soluzioni atte a risolvere i seguenti problemi:

- ***Gestione non efficiente del routing***

  I datagrammi inviati al Mobile Node da un correspondent node (cioè da un qualsiasi dispositivo in comunicazione con il Mobile Node) devono transitare preliminarmente per l'Home Network.

- ***Gestione non efficiente degli handoff***

  I datagrammi inviati ad un Mobile Node impegnato in un handoff (cioè in un cambio del punto di accesso ad Internet) sono persi con una probabilità molto elevata.

- ***Gestione non efficiente della procedura di registrazione***

  Ogni qual volta il Mobile Node acquisisce un nuovo care-of address o necessita di rinnovare il Lifetime della registrazione deve comunicare con il proprio Home Agent.

2.1 Route Optimization

Come si è avuto modo di sottolineare più volte, il protocollo Mobile IP permette di gestire la mobilità degli host attraverso l'utilizzo di due indirizzi.
In particolare, il mantenimento di un home address consente al Mobile Node di essere raggiungibile da un qualsiasi correspondent host indipendentemente dal proprio punto d'accesso ad Internet.
Tale schema richiede che tutti i pacchetti destinati al Mobile Node transitino preliminarmente per la Home Network, provocando così:

- Un carico addizionale nella Home Network.
- Un ritardo nella consegna dei pacchetti destinati al Mobile Node.

A sua volta i pacchetti inviati dal Mobile Node, tranne in particolari circostanze definite in [10], saranno consegnati al destinatario in maniera diretta, cioè attraverso il classico instradamento implementata da IP.
Questo tipo di routing assimetrico, denominato *Triangle Routing* e schematicamente mostrato in figura, manifesta tutti i suoi limiti quando il correspondent node è situato nella stessa Foreign Network che rispecchia la posizione attuale del Mobile Node:

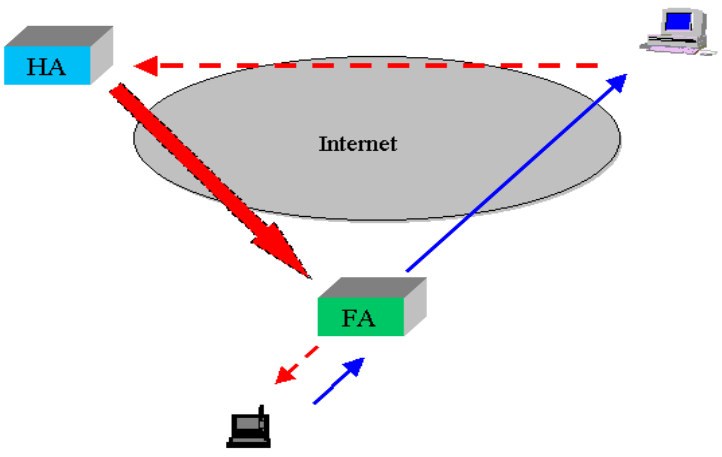


Figura 16: Triangle Routing

Per i motivi sopra esposti, il "Mobile IP Workgroup" esistente all'interno dell'IETF, ha proposto una possibile soluzione denominata ***Route Optimization*** e definita in [15], attraverso la quale il correspondent node è in grado di acquisire il care-of address in maniera tale da poterlo utilizzare come "Destination Address" dei pacchetti inviati al Mobile Node (evitando così il "passaggio" di tali pacchetti per la Home Network).
I vantaggi derivanti dall'utilizzo di Route Optimization sono evidenti, esistono però anche degli svantaggi, in quanto tale meccanismo richiede di introdurre delle informazioni aggiuntive ai dispositivi che desiderano comunicare con il Mobile Node. E' intuibile infatti la necessità di "istruire" il correspondent node poichè dovrà essere in grado, non solo di riconoscere particolari messaggi che verranno spiegati in seguito, ma anche d'implementare la procedura di tunneling.

2.1.1 Analisi della procedura

Nel presente paragrafo si vuole fornire una visione generale della procedura di Route Optimization traendo spunto, non solo da [15], ma anche da una serie di altri documenti ([3], [16], [17]).

Il concetto alla base della procedura di Route Optimization è quello di consentire agli host, che desiderano "colloquiare" con un Mobile Node, di mantenere una tabella nella quale poter memorizzare il care-of address. In altre parole, ciascuna entry della tabella conterrà il "binding" esistente tra l'home address del Mobile Node e l'attuale care-of address dello stesso.

Nell'introduzione al capitolo si è effettuata una netta distinzione tra la gestione non corretta del routing e quella legata all'handoff del Mobile Node. In realtà i due problemi sono legati fra di loro, nel senso che, come si vedrà in seguito, la procedura Route Optimization può essere applicata, oltre che per ottimizzare il routing, anche per consentire una migliore gestione degli handoff.

Senza dilungarsi ulteriormente, Route Optimization può essere considerato come un protocollo la cui implementazione richiede l'adempimento delle seguenti regole:

- Un messaggio di controllo, denominato ***Binding Warning Message***. può essere inviato all'Home Agent per indicare che un correspondent node non è a conoscenza del care-of address di un particolare Mobile Node.

- Quando un correspondent node necessità di rinnovare un "binding", può inviare all'Home Agent un ***Binding Request Message*** per richiedere il care-of address del Mobile Node.

- Per notificare un care-of address, l'Home Agent può inviare un ***Binding Update Message***. Quando si analizzerà l'applicabilità di Route Optimization per ottenere una migliore gestione degli "handoff", si vedrà che tale messaggio potrà essere inviato anche dal Mobile Node.

L'introduzione di tali messaggi consente di descrivere la procedura di Route Optimization attraverso degli esempi che rispecchiano delle situazioni riscontrabili nella realtà.

Esempio 1

Come descritto nel precedente capitolo, in seguito alla ricezione di un datagramma destinato al Mobile Node, l'Home Agent, dopo averlo incapsulato, lo rilancerà al Foreign Agent.
In aggiunta l'Home Agent potrà inviare un *Binding Update Message* al mittente del pacchetto per notificargli l'attuale care-of address del Mobile Node.
In seguito alla ricezione del Binding Update Message, il correspondent node sarà in grado di inviare i pacchetti destinati al Mobile Node direttamente al care-of address dello stesso utilizzando il meccanismo di tunneling.
La procedura ora esposta è mostrata in figura 17 nella quale si evidenzia come il primo pacchetto inviato dal correspondent node ed intercettato dall'Home Agent provochi la trasmissione del Binding Update Message :

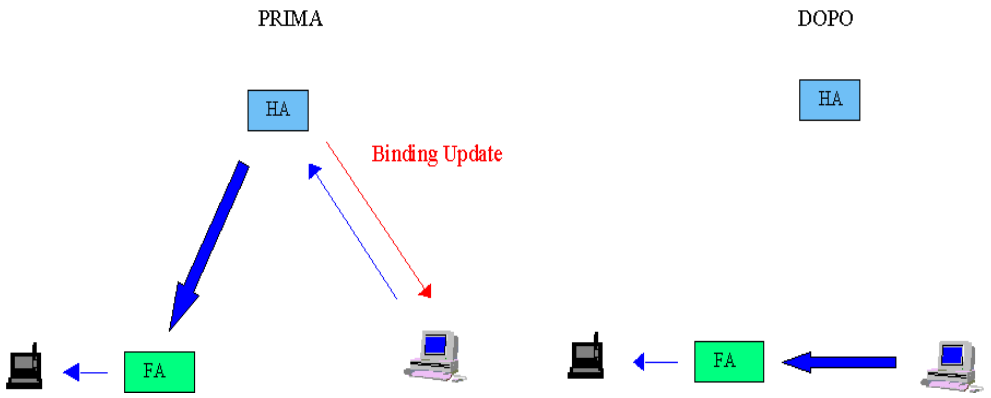


Figura 17: Route Optimization

Esempio 2

Se il correspondent node dispone di un binding non più aggiornato, i pacchetti da lui inviati saranno consegnati ad un Foreign Agent che non fornisce servizio al Mobile Node.

In questa circostanza il Foreign Agent potrà inviare un *Binding Warning Message* all'Home Agent il quale, a sua volta, attraverso un *Binding Update Message* comunicherà il corretto care-of address del Mobile Node al correspondent host.

La stessa situazione può essere gestita in maniera più efficiente attraverso l'utilizzo di uno ***Special Tunnel*** descritto in [18]. Il Foreign Agent, invece di inviare un Binding Warning Message, potrà rilanciare il pacchetto ricevuto all'Home Agent attraverso la procedura di tunneling. In altre parole il Foreign Agent dovrà settare sia il campo Destination Address dell'header esterno, che lo stesso dell'header interno, con l'home address del Mobile Node (informazione ricavabile esaminando l'header interno del pacchetto ricevuto). Il datagramma così incapsulato verrà inviato verso l'Home Network del Mobile Node ed intercettato dall'Home Agent il quale lo rilancierà all'attuale Foreign Agent del Mobile Node (tramite il consueto tunnel) ed invierà un *Binding Update Message* al correspondent node come descritto nell'esempio 1.

La procedura ora esaminata è schematizzata in figura. Si noti che il correspondent node non è in grado di indirizzare correttamente il pacchetto a causa dell'handoff implementato dal Mobile Node:

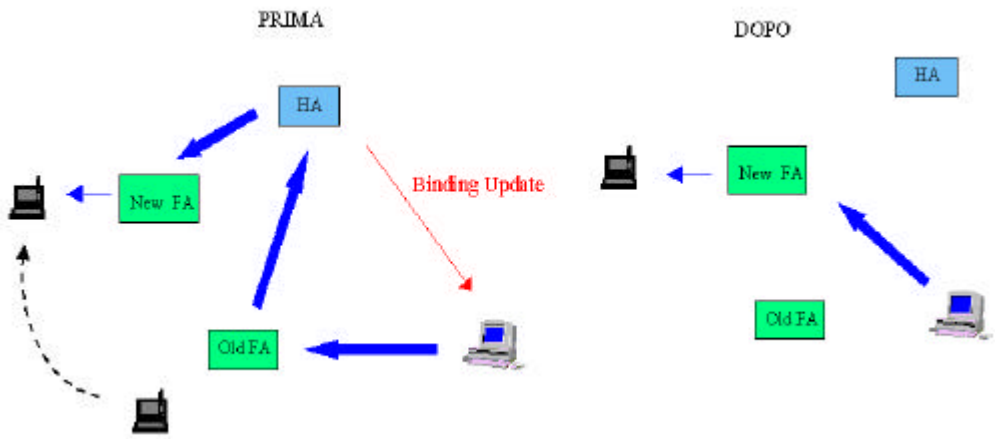


Figura 18: Route Optimization e Special Tunnel

2.1.2 Formato dei messaggi

Nel presente paragrafo si fornirà una descrizione della struttura dei messagi di controllo definiti in [15] ed il cui utilizzo è stato evidenziato negli esempi sopra citati.

Binding Warning Message

0	8	31
Type (16)	**Reserved**	
Mobile Node Home address		
Target Node Address		
…		

Figura 19: Binding Warning Message

Il campo Type assume il valore 16, Reserved è ignorato in ricezione, Mobile Home Address identifica il Mobile Node al quale il messaggio si riferisce mentre il campo Target Node Address conterrà l'indirizzo di uno o più correspondent node ai quali dovrà essere inviato un Binding Update Message.

Occorre sottolineare che gli esempi descritti nel precedente paragrafo non rappresentano tutte le possibili situazioni contemplate in [15]. Da ciò deriva che il Binding Warning Message potrà essere inviato, ad esempio, anche da un Mobile Node che fa ritorno nella propria Home Network. In questo modo il correspondent node, attraverso il Binding Update Message inviatogli dall'Home Agent, potrà eliminare, dalla propria tabella, l'entry relativa al Mobile Node.

Binding Request Message

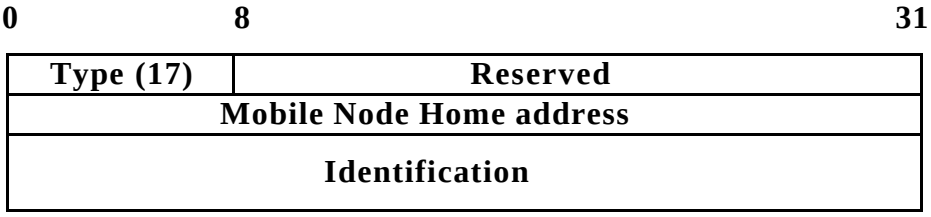


Figura 20: Binding Warning Message

Senza ripetere cose già dette, è necessario specificare che Identification rappresenta una parola di 64 bit che consente di associare il Binding Request Message, inviato dal correspondent node, con il seguente Binding Update Message Generato dall'Home Agent.

Binding Update Message

Il formato del messaggio è mostrato in figura:

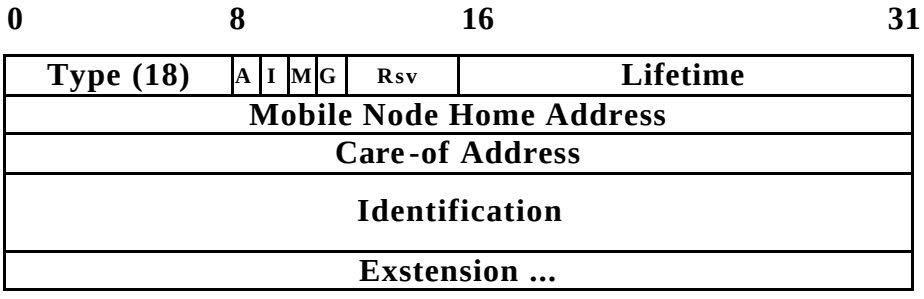


Figura 21: Binding Update Message

Tralasciando la descrizione di Type, Mobile Node Home Address, Identification e Care-of address, il significato assunto dagli altri campi è il seguente:

- ***Flags***

  Permettono di notificare particolari informazioni:

  - *A: Acknowledge*. Viene settato quando il dispositivo che invia il messaggio richiede un acknwledge in risposta.
  - *I: Identification*. Viene settato per notificare che il messaggio contiene il Campo Identification. Ad esempio se il Binding Update Message viene inviato in risposta ad un Binding Request Message, il campo Identification dovrà essere necesseriamente presente.
  - *M,G*. Permettono di comunicare il tipo d'incapsulamento che dovrà essere utilizzato per inviare i datagrammi al Mobile Node.

- ***Lifetime***

  Specifica la durata della validità del binding (care-of address e home address). Un valore nullo permette di richiedere l'eliminazione, dalla tabella del correspondent node (o di quella del Foreign Agent, se la tecnica di Route Optimization viene utilizzata per ottimizzare la gestione degli handoff), delle entry relative al Mobile Node (indicato nel campo Mobile Node Home Address).

Per consentire l'autenticazione del Binding Update Message è utilizzato lo stesso meccanismo implementato per i messaggi di registrazione definiti in [1]. In altre parole sono impiegate delle estensioni d'autenticazione.
Nel caso che si sta prendendo in considerazione, il destinatario di un Binding Update Message risulta un correspondent node; da ciò deriva che si dovrà prevedere un meccanismo che consenta di instaurare un "Security Association" tra l'Home Agent ed il correspondent node stesso.

A causa delle carenze del protocollo IPv4, per quanto riguarda gli aspetti legati alla sicurezza ed all'implementazione di procedure per la distribuzione di chiavi d'autenticazione, l'applicabilità di Route Optimization richiede una particolare attenzione. E' intuibile infatti la difficoltà, dovuta al motivo che si è appena esposto, di prevedere l'instaurazione di un "Security Association" tra l'Home Agent e tutti i possibili correspondent node della rete Internet. Tale problema è risolvibile attraverso l'instaurazione di accordi, stabiliti in anticipo, tra i domini in cui risiedono i correspondent node e quello d'appartenenza dell'Home Agent.

2.2 Smooth Handoff

La procedura denominata *Smooth Handoff*, e definita ancora in [15], consente di limitare la perdita di pacchetti destinati ad un Mobile Node impegnato in un handoff. Tale obiettivo verrà raggiunto notificando al "vecchio" Foreign Agent, che gestiva il Mobile Node, l' attuale care-of address acquisito dallo stesso.

Sostanzialmente il Mobile Node dovrà "istruire" il nuovo Foreign Agent ad inviare un Binding Update Message al vecchio Foreign Agent in maniera tale che quest'ultimo sia in grado di creare una entry (proprio come faceva il correspondent node) relativa al Mobile Node.

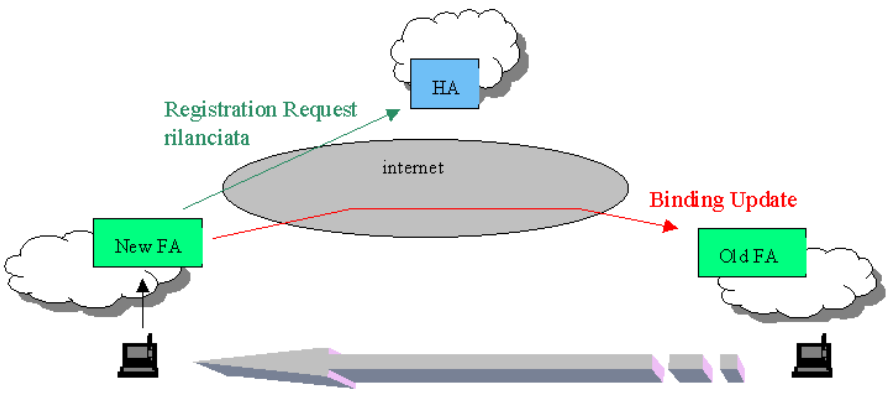


Figura 22: Smooth Handoff

Nella figura 22 è mostrato tale scambio d'informazione; per snellire tutta l'operazione il Mobile Node comunicherà al nuovo Foreign Agent la necessità di inviare un Binding Update Message nell'ambito della procedura di registrazione. In particolare attraverso l'introduzione di una nuova estensione da applicare al messaggio di registrazione, il Mobile Node potrà notificare al Foreign Agent tutte le informazioni necessarie per l'elaborazione, da parte di quest'ultimo, del Binding Update Message (care-of address del vecchio Foreign Agent, informazioni necessarie per l'estensione di autenticità, etc.):

Anche in questo caso riveste un ruolo molto importante l' autenticazione del binding da parte del vecchio Foreign Agent. Il protocollo Mobile IP, definito in [1], impone l' esistenza di un conteso di sicurezza solamente tra l'Home Agent ed il Mobile Node. Per questo motivo, considerando le stesse limitazioni introdotte nel precedente paragrafo, è opportuno rimarcare la necessità di meccanismi che consentano di instaurare un "Security Association" tra il Mobile Node ed il Foreign Agent (maggiori dettagli possono essere trovati in [18]).

In figura 23 viene riproposto l' esempio 2 descritto nel precedente paragrafo considerando però anche i vantaggi derivanti dall' utilizzo della procedura Smooth Handoff:

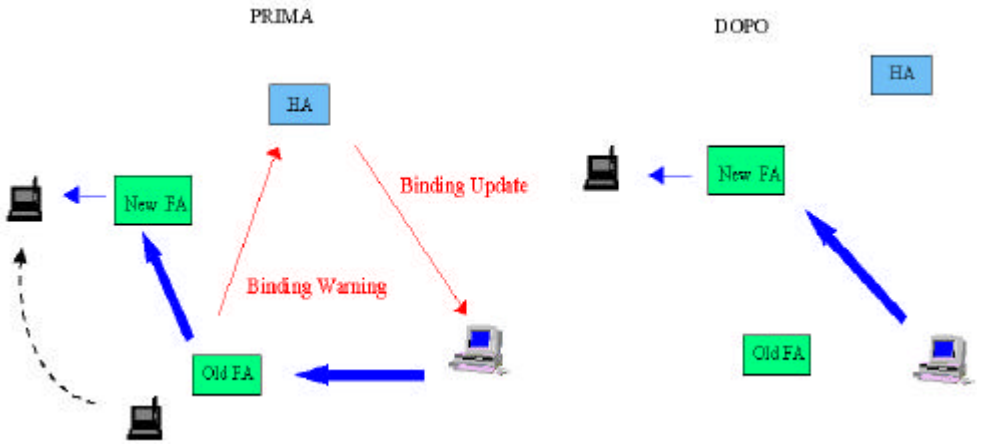


Figura 23: Route Optimization e Smooth Handoff

il “vecchio" Foreign Agent, in seguito alla ricezione di un pacchetto inviato da un correspondent node, sarà in grado, consultando la entry relativa al Mobile Node, di rilanciarlo direttamente alla attuale posizione del Mobile Node. Per consentire un aggiornamento del binding posseduto dal correspondent node, il Foreign Agent potrà inviare un Binding Warning Message all’Home Agent. In seguito alla ricezione di tale messaggio, l’Home Agent invierà Binding Update Message al correspondent node.

2.3 Regionalized Registration

Come specificato nel protocollo Mobile IP, un Mobile Node è costretto a registrarsi con il proprio Home Agent ogni qual volta acquisisce un nuovo care-of address. Se la distanza tra la Foreign Network e la Home Network è notevole, il ritardo introdotto dalla procedura di registrazione può causare dei problemi.

Una soluzione per eliminare tale problema è stata proposta in [20] e consiste nell’ implementare la procedura di registrazione all’ interno dello stesso dominio “visitato” dal Mobile Node, cioè effettuando un tipo di registrazione denominata *Regionalized Registration*.

Per poter realizzare una registrazione locale, il dominio visitato dal Mobile Node (cioè l’ insieme di un certo numero di Foreign Network controllate da uno stesso amministratore) deve essere organizzato in maniera tale da presentare una gerachia di Foreign Agent. In altre parole i diversi Foreign Agent dovranno costituire una struttura ad albero:

la radice dell’albero rappresenterà l’unico Foreign Agent in grado di comunicare con l’Home Agent mentre, tutti i Foreign Agent di livello inferiori, saranno interessati nell’ ambito della registrazione locale del Mobile Node.

Una descrizione dettagliata della procedura di Regionalized Registration esula dagli scopi della tesi, per questo motivo se ne forniranno i principi di funzionamento attraverso l’analisi della figura 24:

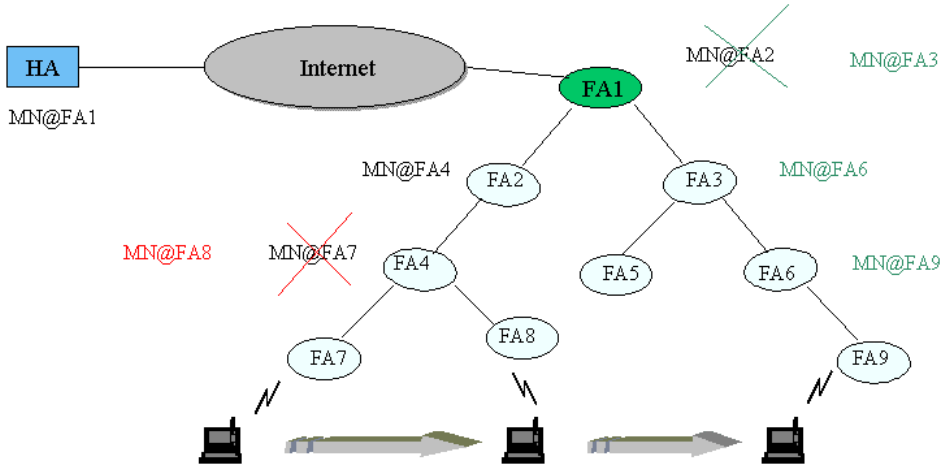


Figura 24: Regionalized Registration

- Quando il Mobile Node accede al dominio, riceverà gli Advertisement Message dal Foreign Agent FA7 il quale notificherà non solo il proprio care-of address, ma anche quello dei Foreign Agent FA1,FA2 e FA4. Nello schema proposto in figura la radice dell'albero è FA1, da ciò deriva che il Mobile Node registrerà, con il proprio Home Agent, il care-of address di tale nodo. Sostanzialmente fino a questo punto non ci sono variazioni dalla classica procedura di registrazione implementata nel modello basilare del protocollo Mobile IP.

- Grazie al fatto di aver registrato il care-of address del Foreign Agent gerarchicamente superiore rispetto a tutti gli altri, il Mobile Node non dovrà più contattare l'Home Agent in seguito ai successivi spostamenti che effettuerà all'interno del dominio. In altre parole l'Home Agent potrà rilanciare i pacchetti destinati al Mobile Node servendosi del care-of address caratterizzante FA1.

- In seguito a questa prima registrazione, le informazioni a disposizione delle diverse entità architetturali conducono alle seguenti osservazioni:

  HA "crede" che il Mobile Node sia localizzato al care-of address FA1

  FA1 "crede" che il Mobile Node sia localizzato al care-of address FA2

.....

- Se il Mobile Node si muove verso il Foreign Agent FA8, attraverso l' analisi dei care-of address avvisati da quest' ultimo (FA1, FA2, FA4, FA8), sarà in grado di inviare una richiesta di *Registrazione Locale* al Foreign Agent FA4 senza dover "interpellare" l' Home Agent e gli altri Foreign Agent dell' albero. Analogamente, nel caso in cui il Foreign Agent si dovesse spostare da FA8 a FA9, la richiesta di registrazione locale verrà inviata a FA1. Questo significa che in seguito ad ogni spostamento effettuato all'interno del dominio, il Mobile Node dovrà registrarsi solamente con il nodo di livello superiore che risulta comune sia al vecchio che al nuovo Foreign Agent. In figura sono riportate le informazioni registrate dai diversi Foreign Agent in seguito agli spostamenti del Mobile Node.

- Tenendo presente le informazioni mantenute da ciascuna entità architetturale occorre precisare che il generico datagramma rilanciato dall'Home Agent verso il Mobile Node dovrà subire un "trattamento" differente da quello definito in [1]. E' chiaro infatti che il pacchetto dovrà essere incapsulato e decapsulato più volte: HA dovrà rilanciare il datagramma originario verso FA1; FA1 dovrà rilanciarlo verso il Foreign Agent di livello inferiore; ..... Tale procedura dovrà essere ripetuta fino alla consegna del pacchetto al Foreign Agent di livello più basso che lo potrà così consegnare al Mobile Node.

3 Mobile IPv6

Nei precedenti capitoli si è fornita una visione generale delle caratteristiche del protocollo Mobile IP e dei meccanismi necessari per migliorarne l'efficienza.
Nell'analisi effettuata si è sempre sottointeso che il protocollo alla base della rete Internet fosse IPv4, in altre parole non si è mai menzionata l'applicabilità di Mobile IP in previsione di ciò che costituirà l'ossatura della futura rete Internet, cioè di IPv6.

Come sarà descritto in seguito, Mobile IP potrà essere considerato, in un certo senso, come parte integrante di IPv6 in quanto interagirà con esso per sfruttarne le potenzialità e migliorare così le proprie funzionalità.
Il seguito del capitolo è suddiviso in due parti: inizialmente sarà fornita una visione generale delle caratteristiche principali del protocollo IPv6 (tratte da [21], [2] e [22]) in maniera tale da evidenziare, nella seconda parte, le differenze salienti tra Mobile IPv4 e Mobile IPv6.

3.1 IPv6

Le caratteristiche del protocollo IPv4 hanno facilitato la grande diffusione di Internet, ma, anche a causa di quest'enorme diffusione, IPv4 appare non essere più adeguato a soddisfare le esigenze degli utenti. In particolare, la principale motivazione che sta conducendo alla graduale sostituzione di Ipv4 con Ipv6 è la necessità di uno spazio d'indirizzamento più ampio.

Una volta riconosciuta la necessità di cambiare il protocollo di rete, l'IETF si è posta il problema di individuare quali caratteristiche di IPv4 mantenere, quali eliminare e quali modificare. L'obiettivo è quello di dotare IPv6 di quei requisiti che IPv4 non è in grado di soddisfare come, ad esempio, la possibilità di garantire una determinata qualità di servizio per le applicazioni multimediali.

Di seguito sono analizzate le caratteristiche principali del protocollo IPv6.

3.1.1 Soluzione al problema della scarsità di indirizzi IPv4

All'inizio degli anni '90 è diventato evidente che gli indirizzi IP erano destinati ad esaurirsi, e così sarebbe stato se non si fossero adottate delle tecniche che hanno consentito di prolungare la vita del protocollo IPv4. Tra queste ricordiamo l'introduzione del CIDR (Clasless Interdomain Routing) che ha permesso di superare la rigidità dovuta alla suddivisione degli indirizzi in tre sole classi.

Nel protocollo IPv6 il problema legato alla scarsità del numero di indirizzi è stato risolto alla base: sono stati tutti concordi nel definire uno spazio di indirizzamento che non sia più soggetto, in futuro, ad esaurimento. Per questo motivo la lunghezza di un indirizzo IPv6 è stata fissata in 128 bit contro i 32 di IPv4.

La maggiore dimensionalità dello spazio degli indirizzi consente di introdurre una gerarchia più articolata rispetto a quella di IPv4 e quindi di facilitare le operazioni di instradamento. Sono previsti indirizzi di tipo globale, locale ed indirizzi che identificano un singolo "link". Gli indirizzi *globali* sono quelli con significatività nell'intera rete Internet, quelli *locali* sono usati per nodi interni alle intranet (sostanzialmente possono essere considerati come gli indirizzi privati di IPv4), mentre quelli di *link* consentono a due nodi di comunicare attraverso una singola sotto-rete fisica. Un esempio d'utilizzo dei "link-address" è quello per l'implementazione della procedura denominata ***Neighbor Discovery*** che permette ad un nodo IPv6 di:

- scoprire quali sono i nodi che risiedono nel suo medesimo link;
- determinare qual è il link-address dei nodi vicini e la validità di quelli contenuti in eventuali cache (da ciò deriva che IPv6 non fa uso del protocollo ARP per la risoluzione degli indirizi). Per attivare la procedura di risoluzione degli indirizzi un nodo trasmetterà in multicast (tramite il protocollo ICMPv6) un pacchetto denominato

Neighbour Solicitation attraverso il quale richiederà al nodo “target” di restituire il proprio link-addresss. Il nodo in questione risponderà attraverso un Neighbour Advertisement Message nel quale inserirà l’informazione richiesta;

- tenere traccia di quali vicini sono raggiungibili e quali no;
- etc.

Nell’allocazione degli indirizzi IPv6 sono state tenute in considerazione anche le necessità relative all’integrazione con diversi tipi di rete già esistente ed il supporto per diversi tipi di indirizzi. In particolare sono stati identificati tre tipi di indirizzi:

- **Unicast**

  E’ l’indirizzo di una singola interfaccia. Un pacchetto inviato ad un indirizzo unicast è recapitato unicamente all’interfaccia identificata da quell’indirizzo.

- **Multicast**

  E’ l’indirizzo di un insieme di interfacce che tipicamente appartengono a nodi diversi. Un pacchetto inviato ad un indirizzo multicast è recapitato a tutte le interfacce appartenenti all’insieme.

- **Anycast**

  Rappresenta un’innovazione rispetto ad IPv4; è l’indirizzo di un insieme di interfacce che tipicamente appartengono a nodi diversi. Un pacchetto inviato ad un indirizzo anycast è recapitato ad una sola interfaccia dell’insieme (la più vicina al nodo mittente, coerentemente con le metriche di routing).

3.1.2 Configurazione dei nodi IPv6

Per sopperire ai problemi dovuti alla configurazione di un host connesso ad Internet (ad esempio l'acquisizione dell'indirizzo IP, della maschera di sotto-rete, del default router, etc.), IPv6 ha introdotto dei meccanismi di auto-configurazione che snelliscono drasticamente le operazioni sopra citate.
A titolo di esempio può essere menzionata la procedura denominata ***Stateless Address Autoconfiguration*** progettata in maniera tale da non richiedere nessuna forma di configurazione manuale prima di collegare un host IPv6 alla rete. Quando un'interfaccia viene attivata, l'host, per prima cosa, genera un link address derivandolo da quello fisico (ad esempio, nel caso di rete Ethernet, tale indirizzo sarà derivato da quello MAC). L'indirizzo così generato non è assegnato immediatamente all'interfaccia, ma viene posto in uno stato detto di "tentative" fino a quando non si è certi, attraverso l'impiego di opportune procedure, della sua univocità. Se la procedura non conferma l'univocità dell'indirizzo, esso non viene assegnato all'interfaccia ed è richiesta una configurazione manuale. Il passo successivo consiste nell'invio di Router Solicitation Message in risposta del quale l'host riceverà un Router Advertisement Message dal quale sarà in grado di "estrarre" le informazioni necessarie (ad esempio l'indirizzo unicast).
Per completezza è opportuno citare che, in alcune circostanze, la configurazione dell'host avverrà attraverso procedure più "comuni" come ad esempio l'impiego di un DHCP Server (***Stateful Address Autoconfiguration***).

3.1.3 Formato del datagramma

Una delle innovazioni più evidenti introdotte da IPv6 è la struttura del datagramma in quanto risulta composto da una parte base e da una parte opzionale.
L'intestazione base (denominata *header IP*) è di lunghezza fissa, è presente in tutti i datagrammi ed è stata strutturata in maniera tale da consentire una maggiore efficienza di processamento da parte dei router.

Per rendere altamente flessibile il protocollo e consentire l'implementazione di eventuali opzioni, il datagramma può essere esteso in maniera tale da contenere, oltre all'header IP, anche una o più *extension headers*. Il principio alla base degli extension header è che la maggior parte dei pacchetti necessitano di un trattamento molto semplice per cui sono sufficienti i campi previsti nell'header IPv6. I pacchetti che necessitano di informazioni aggiuntive possono codificare tali informazioni in header addizionali che saranno collocati tra l'header IPv6 ed il payload.

Con un tale formato dei pacchetti il tempo di elaborazione degli stessi da parte dei router sarà notevolmente ridotto rispetto a quello degli header IPv4: la maggior parte dei pacchetti transiterà molto velocemente e solo quelli che hanno richiesto particolari funzioni subiranno un trattamento più complesso che prevede l'analisi degli extension header. In ogni caso molti degli extension header riguardano funzionalità end-to-end e quindi non devono essere elaborati dai router, ma solo dai nodi mittente e destinatatario.

3.1.3.1 Header IPv6

L'header IPv6 è stato considerevolmente semplificato rispetto a quello IPv4: è costituito da 40 byte di cui 32 sono usati per gli indirizzi ed i rimanenti 8 byte da campi addizionali.
Il formato dell'header è rappresentato in figura:

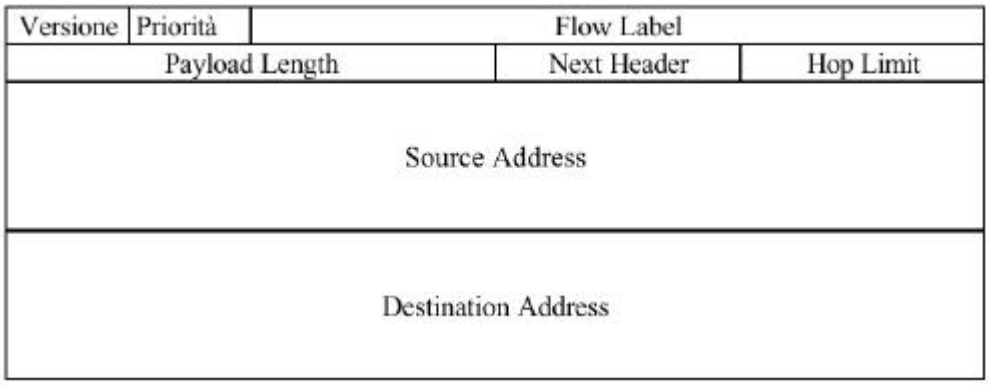


Figura 25: Header IPv6

Il significato dei diversi campi è il seguente:

- ***Versione*** **(4 bit)**

  Indica la versione del protocollo, è possibile la coesistenza di più versioni di IP.

- ***Priorità*** **(4 bit)**

  Consente al nodo mittente di differenziare i pacchetti da esso generati associando loro una proprietà di consegna diverse. Al momento sono definite due classi di priorità: *Congestion Controlled Traffic* (ad esempio traffico TCP) e *Noncongestion Controlled Traffic* (ad esempio traffico UDP).

- ***Flow Label*** **(24 bit)**

  Può essere utilizzato dal nodo sorgente per contraddistinguere un insieme di pacchetti appartenenti allo stesso flusso. I flussi sono univocamente identificati dall'indirizzo del mittente e da una Flow Label diversa da zero. I pacchetti appartenenti ad uno stesso flusso devono essere trattati in modo coerente dai router IPv6. Come trattare pacchetti appartenenti ad uno stesso flusso può essere specificato, ad esempio, tramite il protocollo RSVP (Resource Reservation Protocol). Appare evidente come il campo Flow Label consenta di introdurre il concetto di qualità del servizio: pacchetti appartenenti a flussi differenti possono aver bisogno di una qualità differente.

- ***Payload Length*** **(16 bit)**

  Contiene la lunghezza del payload, cioè del campo dati che segue l'header IPv6, espressa in ottetti. Poichè il campo è di 16 bit la lunghezza massima del payload di un pacchetto IPv6 può essere di 64 Kbyte. Per poter utilizzare un campo dati di dimensione superiore si può ricorrere all'opzione *Jumbo Payload* disponibile nell'extension header che prende il nome di *Hop-by-Hop Options*.

- ***Next Header*** **(8 bit)**

  Indica il tipo dell'Extension Header successivo, se ne esiste uno, oppure il protocollo di strato superiore al quale il pacchetto deve essere consegnato.

- ***Hop Limit*** **(8 bit)**

  Viene decrementato di un'unità ogni qual volta che un nodo (tipicamente un router) trasmette il pacchetto. Se il campo Hop Limit viene ad assumere il valore zero, il pacchetto è scartato. Scopo principale di questo campo è di individuare e scartare pacchetti che siano entrati in condizione di loop.

Infine ***Source Address*** e ***Destination Address*** rappresentano, rispettivamente, l'indirizzo del nodo sorgente e di quello di destinazione. Se il pacchetto contiene una Routing Header Extension, il Destination Address può non essere l'indirizzo del destinatario finale.

3.1.3.2 Extension Header

Come detto precedentemente gli Extension Header, compresi tra l'header IP ed il campo payload, consentono di inviare informazioni addizionali alla destinazione o ai sistemi intermedi. La concatenazione tra i diversi Extension Header avviene tramite il campo Next Header presente in tutti gli header.
Da ciò deriva che la struttura generale di un datagramma IPv6 è la seguente:

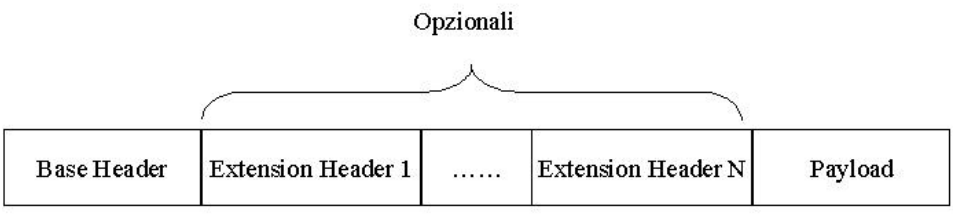


Figura 26: Struttura generale di un datagramma IPv6

Gli Extension Header devono essere elaborati nell'ordine in cui compaiono nel pacchetto, inoltre tale ordine non può essere casuale ma deve rispettare delle regole ben precise.
Di seguito è fornita una visione generale delle caratteristiche dei diversi Hextension Header:

- **Hop-by-Hop Header**

  Consente di trasportare informazioni addizionali che devono essere elaborate da ogni nodo lungo il percorso dei pacchetti.

- **Routing Header**

  Svolge una funzione simile a quella del Source Route Option di IPv4, permette quindi di specificare una lista dei nodi intermedi che il pacchetto dovrà attraversare durante il suo percorso verso il nodo di destinazione. In questo caso l'indirizzo indicato nell'header IP non è quello del destinatario, bensì rappresenta l'indirizzo del prossimo router elencato nella lista.

- **Fragment Header**

  Contiene informazioni per la frammentazione e la riorganizzazione delle unità informative. E' importante sottolineare che in IPv6 tutte le operazioni di segmentazione e di aggregazione sono svolte da estremo a estremo e non coinvolgono i router intermedi.

- **Authentication Header**

  Contiene informazioni necessarie per autenticare il datagramma. Permette di verificare che non sia stato alterato durante il transito in rete e che sia stato emesso effettivamente dal mittente indicato nel datagramma. In analogia alle estensioni di autenticità, definite nel protocollo Mobile IP, si fa uso di Security Association e di un Security Parameter Index.

- **Encapsulated Security Payload Header**

  Anche questo header viene utilizzato per risolvere problemi legati alla sicurezza in rete. L'obiettivo è di proteggere i pacchetti da "ascolti" non desiderati.

- **Destination Option Header**

  Consente di trasportare informazioni addizionali che debbono essere elaborate solamente dal nodo o dai nodi di destinazione.

3.2 Visione generale del protocollo Mobile IPv6

Il protocollo Mobile IPv4 non può essere semplicemente implementato in IPv6 modificando la lunghezza degli indirizzi da 32 a 128 bit; le differenze tra IPv4 ed IPv6 richiedono che le specifiche di MIPv4 siano adattate alle caratteristiche funzionali di IPv6.

L'analisi di MIPv6 evidenzierà la grande flessibilità del protocollo IPv6, in particolare consentirà di mostrare come alcune delle sue proprietà siano direttamente estendibili per gestire in maniera efficiente la mobilità degli host.

Alla base di Mobile IPv6 vi sono gli stessi concetti che hanno condotto allo sviluppo di MIPv4: viene mantenuta l'idea di una Home Network, di un Home Agent e dell'uso di un tunnel per consegnare i datagrammi dalla Home Network alla posizione corrente del Mobile Node.

Come in MIPv4, il Mobile Node dovrà acquisire un care-of address, però non sarà più necessaria la presenza del Foreign Agent nella Foreign Network; da ciò deriva che il Mobile Node, sfruttando le funzionalità dei protocolli Stateless Address Autoconfiguration o Stateful Address Autoconfiguration, acquisirà un co-locate care-of address.

Come sarà descritto in maniera più dettagliata, Mobile IPv6 necessità dell'introduzione di nuove opzioni inseribili nel Destination Option Header [23]:

- **Binding Update**
- **Binding Acknowledgement**
- **Binding Request**
- **Home Address Option**

Tali opzioni sostituiscono i messaggi di controllo propri di Mobile IPv4 (Registration Request, Registration Reply, etc.) e quindi, potendo sfruttare un'extension header, non esiste più la necessità di ricorrere al protocollo UDP per la loro trasmissione.

Un'ulteriore caratteristica di MIPv6 consiste nell'integrazione delle procedure d'ottimizzazione del routing con le caratteristiche funzionali dello stesso protocollo; in altre parole, come si è detto nel secondo capitolo, una migliore efficienza di MIPv4 può essere ottenuta modificando opportunamente il protocollo, mentre in MIPv6 l'applicabilità delle tecniche d'ottimizzazione è un requisito obbligatorio.

In figura è rappresentato il routing dei pacchetti nel protocollo MIPv6:

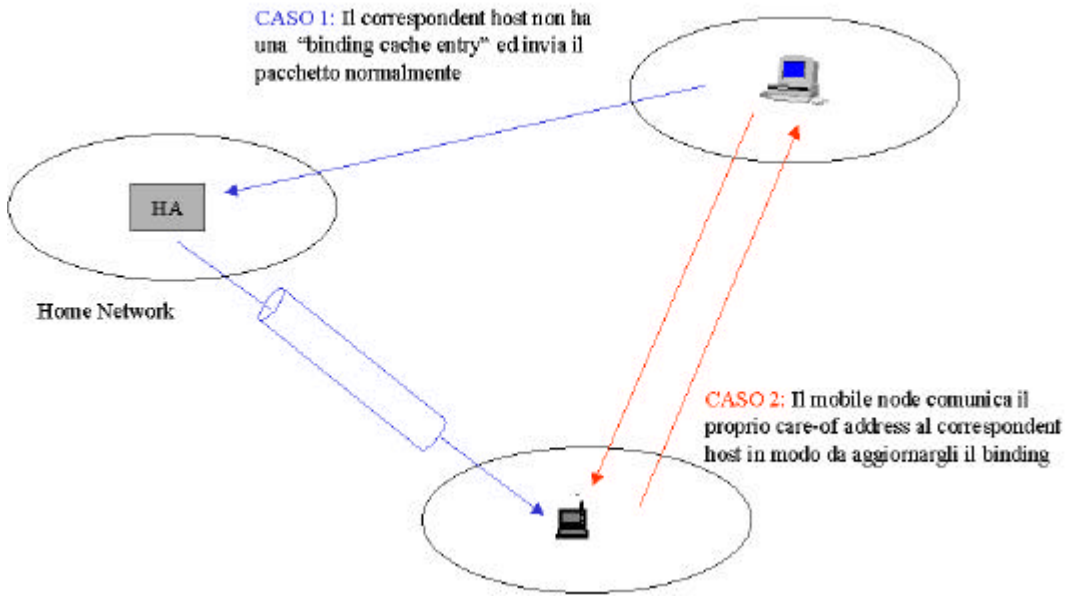


Figura 27: Consegna dei datagrammi in MIPv6

I correspondent node devono possedere una tabella denominata “binding cache” nella quale mantenere il binding (associazione tra home address, care-of address e lifetime) dei Mobile Node con cui comunicano.
Ogni qual volta il correspondent node necessita di inviare un datagramma al Mobile Node consulterà tale tabella: se non esiste il binding il pacchetto sarà instradato verso la Home Network, intercettato dall’Home Agent, attraverso un meccanismo denominato *Proxy Neighbor Discovery*, e da questo inviato verso il Mobile Node mediante tunneling.
In seguito alla ricezione di tale datagramma il Mobile Node comunicherà, attraverso le opzioni del Destination Option Header sopra menzionate, il care-of address al correspondent node. Tutti i successivi pacchetti saranno inviati dal correspondent node direttamente al Mobile Node. Si noti che in questo caso non è utilizzato il meccanismo di tunneling in quanto si sfrutta il Routing Header Extension di IPv6. Il campo Destination Address dell’header IPv6 conterrà il care-of address del Mobile Node mentre, all’interno del Routing Header Extension, sarà inserito l’Home Address dello stesso [24]. Il Mobile Node, una volta ricevuto il datagramma, consulterà il Routing Header Extension ed invierà il pacchetto verso l’indirizzo indicato. Dato che tale indirizzo corrisponde all’Home Address il pacchetto sarà “looped back” e quindi, in effetti, non sarà trasmesso verso la Home Network.

3.3 Messaggi del protocollo MIPv6

Come accennato in precedenza il protocollo Mobile IPv6 richiede l’introduzione di nuove opzioni inseribili nel Destination Option Header Extension.
Più precisamente sono state introdotte quattro opzioni il cui significato è il seguente:

- **Binding Update**

  Il Binding Update è utilizzato da un Mobile Node per comunicare all’Home Agent (o ad un correspondent host) il care-of address

acquisito. Può essere quindi associato al Registration Request Message di MIPv4.

Nello stesso datagramma deve essere presente anche l'opzione denominata Home Address.

- **Binding acknowledgement**

  Il Mobile Node può richiedere un acknowledgement in risposta ad un Binding Update.

- **Binding Request**

  Tale opzione è utilizzata da un correspondent node per richiedere al Mobile Node l'invio di un Binding Update in maniera tale da creare (o aggiornare) l'entry nella binding cache.

- **Home Address**

  Deve essere presente in tutti i Binding Update ed in tutti i pacchetti che il Mobile Node invia quando si trova in una Foreign Network. Tale opzione consente al destinatario di stabilire il vero mittente del datagramma: il Mobile Node inserirà il care-of address nel campo Source Address dell'header IPv6 mentre nell'opzione in questione inserirà il proprio Home Address.

3.4 Dynamic Home Agent Discovery

Analogamente a quanto accade nel protocollo MIPv4, quando il Mobile Node varia punto d'accesso alla rete Internet (informazione reperibile, ad esempio, attraverso gli ICMPv6 Router Advertisement Message emessi dai router della Foreign Network) deve avviare una procedura di registrazione con l'Home Agent ed eventualmente aggiornare il binding di un correspondent node.

Ripetere tutte le fasi della procedura di registrazione è inutile, in questo contesto si vuole solamente evidenziare come in MIPv6 sia stata migliorata la procedura, denominata Dynamic Home Agent Discovery, attraverso la quale il

Mobile Node è in grado di acquisire dinamicamente l'indirizzo dell'Home Agent.

A tale scopo sono stati introdotti due nuovi messaggi ICMPv6, denominati *ICMP Home Agent Address Discovery Request Message* e *ICMP Home Agent Address Discovery Reply Message.*

Se il Mobile Node necessita di ottenere dinamicamente l'Home Address, invierà un ICMP Home Agent Address Discovery Request all'indirizzo anycast "Mobile IPv6 Home Agents". In questo modo il messaggio suddetto (che dovrà contenere anche un Home Address Option) verrà ricevuto da tutti gli Home Agent presenti nella Home Network.

In risposta a tale messaggio gli Home Agent invieranno, al Mobile Node, un ICMP Home Agent Address Discovery Reply contente sia il proprio indirizzo che una lista contenente gli indirizzi di tutti gli Home Agent presenti nella Home Network

Attraverso tali informazioni il Mobile Node sarà in grado di individuare un Home Agent disponibile ad accettare la richiesta di registrazione.

3.5 Sicurezza nel protocollo Mobile IPv6

Un aspetto molto importante del protocollo Mobile IP, sia nel caso di IPv4 che in IPv6, è quello legato alla sicurezza delle informazioni trasmesse.

Trattare con dettaglio tale argomento non rientra negli obiettivi della tesi, è necessario però delineare quali potrebbero essere le conseguenze dovute ad una non corretta protezione dei messaggi.

Un esempio può essere fornito dall'impiego delle procedure di tunneling. Dato che i tunnel sono creati, "rediretti" e distrutti attraverso dei Binding Update (o tramite dei Registration Request Message) è chiaro che l'invio da parte di nodi non autorizzati di tali messaggi possa causare dei seri problemi. Nel caso più semplice, si può creare una situazione nella quale il tunnel venga rediretto verso il nodo non autorizzato il quale potrà così assumere le "sembianze" del Mobile Node. Inoltre a causa dei cosiddetti "man-in-the-middle attack" si possono verificare delle situazioni paradossali: un nodo non

autorizzato potrebbe redirigere il tunnel su se stesso e comportarsi, nei confronti del Mobile Node, come l'Home Agent.

Nel primo capitolo si è evidenziata la tecnica utilizzata dal protocollo MIPv4 per proteggere i messaggi scambiati: sono stati introdotti i concetti di estensioni di autentictà.

Nel caso di MIPv6 sono sfruttate le caratteristiche del datagramma IPv6, in altre parole i pacchetti contenenti Binding Update o Binding Acknowledgement devono comprendere anche gli header utilizzati per scopi di sicurezza, vale a dire l'Authentication Header Extension e Encapsulated Security Payload Header Extension. Inoltre una maggiore protezione può essere ottenuta impiegando dei protocolli specifici (come ad esempio il Protocol Security Architecture, IPSec) a riguardo dei quali non si entrerà in merito.

4 Cellular IP

Lo standard Mobile IP, proposto in [1], è stato sviluppato con l' obiettivo di risolvere problemi legati alla "macro" mobilità (o mobilità globale) degli host, non è quindi ottimizzato per gestire la mobilità all' interno delle singole sotto-reti che forniscono l' accesso ad Internet (denominata "micro" mobilità o mobilità locale). Il motivo per cui si evidenzia una differenza fra i due tipi di mobilità è legato al fatto che nella "micro-mobility" la frequenza con la quale si manifestano gli "handoff" dei Mobile Node (variazioni del punto d'accesso caratterizzate dal mantenimento delle eventuali connessioni) può essere molto elevata. Da ciò deriva il limite di Mobile IP: in corrispondenza di ciascun handoff, Mobile IP richiede l'invio di messaggi di aggiornamento all'Home Agent (presumibilmente collocato in una zona distante dall'attuale posizione del Mobile Node) provocando così un ritardo nella gestione dell' handoff e la conseguente perdita di pacchetti.

Nel presente capitolo sarà descritto *Cellular IP* [25], un protocollo per la gestione della mobilità degli host, ottimizzato per reti di accesso di tipo wireless ed in grado di controllare adeguatamente i frequenti spostamenti del Mobile Node. Una visione globale, della struttura della rete mobile che si prenderà in considerazione, è mostrata in figura:

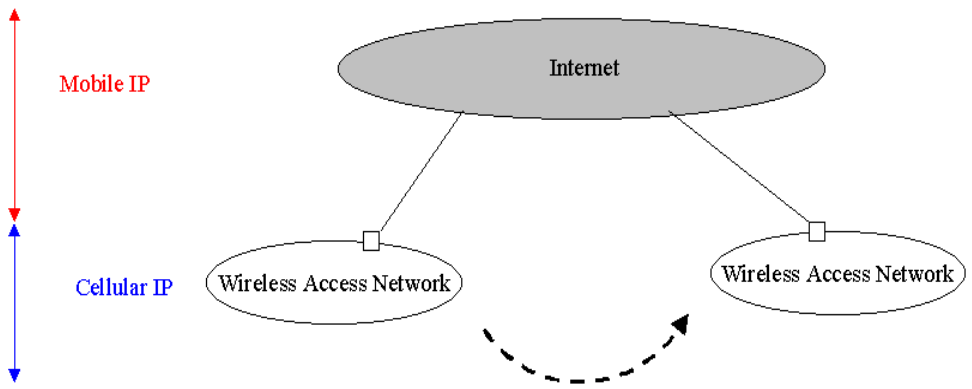


Figura 28: Cellular IP e Mobile IP

all' interno di ciascuna W*ireless Access Network* la micro mobilità degli host è gestita tramite il protocollo Cellular IP il quale dovrà cooperare con Mobile IP per consentire al Mobile Node di muoversi tra le diverse reti d' accesso. Il vantaggio di aver separato la gestione della mobilità locale da quella globale risiede nel fatto che non sarà necessario informare l'Home Agent degli spostamenti compiuti dall'host all'interno di una rete d'accesso, ma solamente di quelli compiuti per muoversi da una rete all'altra.

4.1 Caratteristiche generali

Il protocollo Cellular IP consente di gestire in maniera semplice ed efficiente la mobilità degli host all' interno delle wireless access network. Tale obiettivo è stato raggiunto mantenendo una piena compatibilità con il protocollo IP e sfruttando alcuni vantaggi dei sistemi di telefonia cellulare.
In particolare, in analogia con i sistemi cellulari, un mobile host connesso ad una *Cellular IP Network* (cioè ad una rete d'accesso wireless implementante Cellular IP) può trovarsi in due stati differenti:
se il mobile host invia o riceve pacchetti IP viene classificato come *host attivo*, nel caso opposto verrà considerato come *host passivo*.
Aver distinto in maniera netta lo stato in cui può trovarsi il Mobile Node consente al protocollo di gestire la mobilità degli stessi con modalità differenti:

- nel caso degli host attivi, questi devono poter continuare a ricevere o inviare pacchetti durante il loro spostamento all'interno della rete d'accesso e quindi, in corrispondenza di ciascun handoff locale, si dovranno implementare delle procedure per consentire l'immediata localizzazione dell'host;

- nel caso degli host passivi non è necessario monitorare attentamente il loro spostamento, la conoscenza della loro posizione da parte della rete è solo approssimata. In seguito all'arrivo di un pacchetto

destinato all'host, sarà effettuata una ricerca per individuare la posizione attuale dello stesso;

Nei paragrafi successivi i concetti sopra esposti verranno ulteriormente chiariti, per il momento si vuole evidenziare come la gestione differenziata degli host permetta di alleggerire notevolmente il carico della rete dovuto ai messaggi di controllo. Questa caratteristica si riflette sulla scalabilità del protocollo in quanto consente di gestire un numero molto elevato di utenti.

Ulteriori vantaggi di Cellular IP possono essere ricercati nella facilità con cui controlla gli handoff degli host e nella possibilità di poter implementare, tale protocollo, sia su piccole LAN che su reti con vasta area di copertura, cioè su ambienti architetturali molto differenti tra di loro.
Altre caratteristiche generali del protocollo possono essere ricercate in [26], [27] e [28]; in particolare è importante sottolineare che Cellular IP è un protocollo di tipo distribuito, in quanto:

- i nodi non sono a conoscenza della topologia della rete;
- non vi sono dispositivi centralizzati;
- aumentare l'area di copertura della rete non significa aumentare la complessità dei dispositivi che ne costituiscono la struttura.

4.2 Struttura architetturale della Cellular IP Network

Una Cellular IP Network è costituita essenzialmente da *Cellular IP Node* interconnessi fra di loro; tali nodi istradano i pacchetti all' interno della rete ed alcuni di essi comunicano con i mobile host attraverso delle interfacce wireless. In particolare, i Cellular IP Node dotati di tali interfacce sono chiamati *Base Station*.
La rete è connessa ad Internet attraverso un *Gateway Router* provvisto quindi di un indirizzo IP; con riferimento a Mobile IP, che come sottolineato

precedentemente viene utilizzato per implementare la mobilità degli host a livello globale, il Gateway Router svolge la funzione di Foreign Agent per i Mobile Node connessi alla Cellular IP Network. Per tale motivo il care-of address, acquisito da tali Mobile Node, sarà proprio l'indirizzo IP del gateway. E' intuitivo che il gateway potrà svolgere anche la funzione di Home Agent per quei Mobile Node la cui rete di appartenenza è proprio la Wireless Access Network "interfacciata" ad Internet tramite il suddetto router.

In figura 29 è mostrata l' architettura di rete appena descritta, inoltre, per completezza, viene mostrata anche l'area di copertura fornita da ciascuna Base Station. In un successivo paragrafo si descriverà un'ottimizzazione del protocollo che, sfruttando l'eventuale sovrapposizione di tali aree, consentirà una migliorare gestione degli handoff.

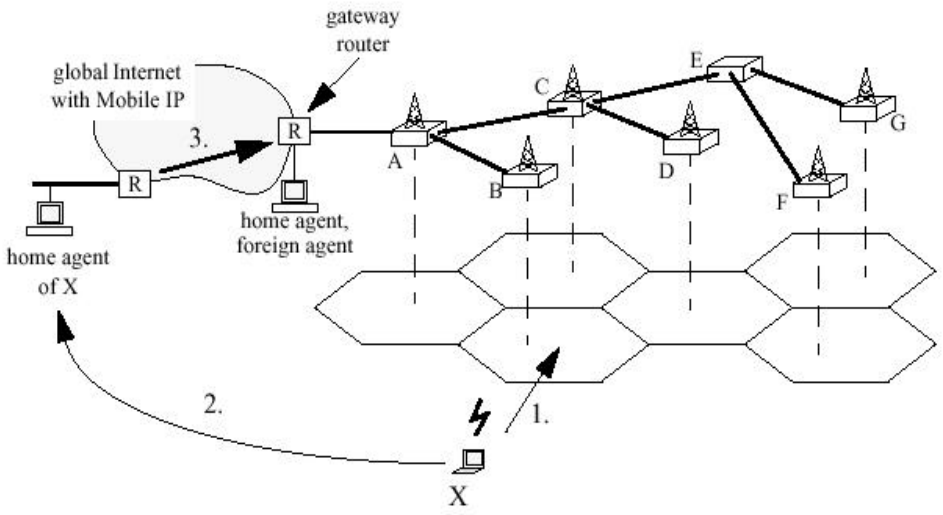


Figura 29: Struttura di una Cellular IP Network

Nella figura sono state indicate anche le azioni che occorre svolgere per rispettare il protocollo Mobile IP. In particolare:
in seguito all' ingresso nella rete (step 1) il Mobile Node X dovrà registrarsi con l' Home Agent (step2) il quale invierà, tramite tunneling, i pacchetti destinati ad X al Foreign Agent (step 3). Infine, attraverso un meccanismo che sarà descritto in seguito, il pacchetto sarà consegnato al Mobile Node. I

successivi spostamenti dell'host all'interno della rete saranno trasparenti, come già detto, all' Home Agent e quindi saranno gestiti completamente dal protocollo Cellular IP.

4.3 Proprietà del Cellular IP Protocol

Come si è avuto modo di sottolineare precedentemente, nessuno dei Cellular IP node conosce l' esatta posizione di un Mobile Node. Per questo motivo il criterio utilizzato per consegnare un pacchetto destinato al Mobile Node sarà identico a quello utilizzato nella rete IP:
ciascun nodo è in grado di individuare solamente verso quale porta rilanciare il pacchetto e quindi il cammino complessivo dal gateway alla Base Station (*downlink*) verrà "elaborato" passo dopo passo (*hop-by-hop*). Ovviamente lo stesso meccanismo sarà implementato anche per determinare il cammino che va dalla Base Station che controlla il Mobile Node al gateway (*uplink*).
Da ciò deriva che ogni nodo manterrà una tabella in cui ciascuna entry conterrà:

- identificativo del Mobile Node (generalmente l'home address);
- identificativo della porta verso la quale rilanciare il pacchetto;
- in aggiunta ciascuna entry conterrà, oltre ad una parola di autenticazione, anche il lifetime dell'associazione.

Per aggiornare e creare le entry necessarie per l'individuazione del downlink, i Cellular IP Node coinvolti dovranno monitorare i pacchetti inviati dal Mobile Node, mentre per stabilire l'uplink verranno utilizzati appositi pacchetti di controllo inviati in broadcast dal gateway:

- nel primo caso i nodi coinvolti saranno in grado di acquisire, oltre alle informazioni del Mobile Node (home address, parola di

autenticazione,etc), anche l' identificativo della *downlink-port* (cioè della porta collegata alla *uplink-port* di un nodo adiacente).;

- nel secondo caso tutti i nodi della rete saranno in grado di stabilire quale delle proprie uplink- port deve essere utilizzata per rilanciare un pacchetto verso il gateway;

E' intuibile che la gestione di tali tabelle dovrà essere differenziata a seconda dello stato del Mobile Node: i tempi di aggiornamento di una tabella relativa ad un host attivo dovranno essere necessariamente più brevi di quelli relativi ad un host passivo. Per risolvere tale problema il protocollo Cellular IP contempla l'utilizzo di due tabelle:

- tutti i nodi dovranno mantenere una *Routing Cache (RC)* relativa agli host attivi;

- alcuni nodi della rete dovranno mantenere anche una *Paging Cache (PC)* necessaria per monitorare gli host passivi. In aggiunta in [28] viene introdotto il concetto di *Paging Area*: normalmente un host passivo deve inviare pacchetti di controllo, necessari per aggiornare la PC, ogni qual volta si sposta sotto l'area di copertura di una nuova Base Station. Alcuni operatori di rete potrebbero alleggerire il carico di rete dovuto a tali messaggi raggruppando celle adiacenti in Paging-Area. In questo modo i messaggi di cui sopra saranno inviati solamente ad ogni passaggio in una nuova Paging Area;

In figura 30 viene evidenziata la relazione tra Paging Cache e Routing Cache:
un host passivo invia messaggi di aggiornamento con bassa frequenza (step 1). Quando un pacchetto deve essere inviato a tale host, le Paging Cache verranno utilizzate per poterlo individuare (step 2). In seguito l'host passerà nello stato attivo e terrà aggiornate le Routing Cache attraverso i pacchetti dati da lui inviati o attraverso l'utilizzo di appositi pachetti di controllo (step 3). Per tutto

il tempo in cui l'host rimarrà nello stato attivo, le routing cache permetteranno di localizzare la posizione del Mobile Node (step 4).

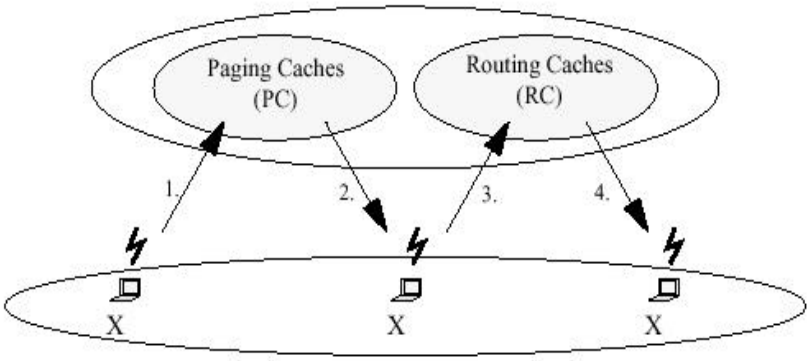


Figura 30: Paging e Routing Cache

4.4 Paging

In questo paragrafo verranno approfonditi i concetti legati al monitoraggio del Mobile Node e quindi alla gestione delle tabelle sopra introdotte.
Un host passa dallo stato attivo a quello passivo se nell'ambito di un certo intervallo di tempo definito *Active-State Timeout* non riceve e non invia nessun pacchetto. Entrato nello stato passivo, il Mobile Node invierà, ad intervalli regolari, pacchetti di controllo definiti P*aging-Update Packets* (attraverso il protocollo ICMP e destinati al gateway) che permetteranno di tenere aggiornate le PC. Una volta giunto al gateway il pacchetto verrà riconosciuto e scartato, non verrà quindi rilanciato verso la rete Internet globale.

Come già detto le paging cache sono caratterizzate dal fatto che ciascuna entry avrà un lifetime, denominato *paging-timeout*, maggiore di quello delle routing cache, *route-timeout.* E' intuibile la grande importanza dovuta alla corretta scelta della temporizzazione che lega il timeout delle tabelle con il periodo di invio dei pacchetti di aggiornamento: in entrambi i casi fornire dei valori elevati alleggerisce il carico della rete dovuto ai messaggi di controllo però estende la permanenza delle entry non più valide all' interno delle tabelle.

Nella tabella 4 vengono riportati i valori indicativi che dovrebbero assumere i diversi “temporizzatori” proposti in [28]:

Nome	Significato	Valore Tipico
Route Update Time	Tempo di inter-arrivo massimo dei pacchetti che aggiornano la RC	1 sec.
Route Timeout	Validità della entry nella RC	3 sec.
Paging Update Time	Tempo di inter-arrivo massimo dei pacchetti che aggiornano la PC	1 min.
Paging Timeout	Validità della entry nella PC	3 min.
Active State Timeout	Intervallo di tempo per il quale il mobile host rimane nello stato attivo senza ricevere dati	5 sec.

Tabella 4: Temporizzazione

Un’ ulteriore differenza tra le due tabelle è da ricercare nel fatto che le Paging Cache conteranno indicazioni anche nei confronti di quei Mobile Node indicati nelle Routing Cache, in altre parole le paging cache verranno aggiornate non solo dai Paging-Update Packet ma anche dai pacchetti inviati da un host attivo. Infine è importante sottolineare che i pacchetti dati inviati da un host attivo potranno solamente aggiornare le entry delle routing cache, mentre per crearne delle nuove il Mobile Node dovrà inviare pacchetti di controllo, denominati *Routing Update,* contenenti informazioni necessarie per l’autenticazione (per chiarezza è opportuno precisare che tali informazioni saranno contenute anche nei Paging Update Packets).
Nella tabella riportata in figura vengono sommariamente riassunte le operazioni necessarie per gestire le paging e routing cache:

	Paging Cache	Route Cache
Refreshed by	Pacchetti dati, Paging Update Packet, Route Update Packet	Pacchetti dati e Route Update Packet
Update by	Paging Update Packet, Route Update Packet	Route Update Packet
Update When	Movimento dell'host in una Paging Area o in seguito ad un Paging Update Time	Movimento dell'host in una nuova cella o in seguito ad un Route Update Time
Scope	Mantiene entry sia per host attivi che passivi	Mantiene entry solo per host attivi
Purpose	Instrada "downlink packet" se non vi sono entry nelle RC	Instrda "Downlink Packet"

Tabella 5: Gestione delle Paging e Routing Cache

4.4.1 Esempio

Per chiarire ulteriormente i diversi concetti relativi al "paging" è utile riferisi al seguente esempio tratto da [25] e suddiviso in diversi passi successivi. Per semplicità non verrà considerata la suddivisione della Cellular IP Nertwork in Paging-Area:

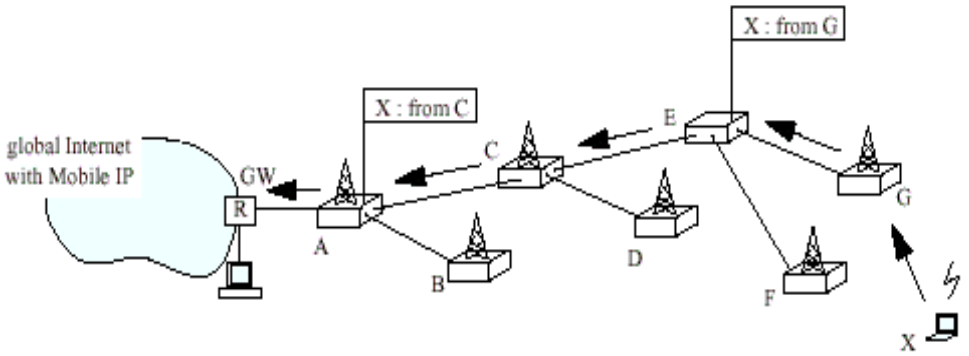


Figura 31: Mantenimento delle Paging Cache

la figura 31 mostra la situazione iniziale nel quale l'host passivo X, sotto il controllo della Base Station G, invia paging-update packet. Tali pacchetti giungeranno al gateway attraverso i nodi G, E, C ed A. Nell' esempio solamente i nodi E ed A contengono Paging Cache, quindi il nodo C non farà altro che

rilanciare il pacchetto verso il gateway sfruttando la propria up-link port determinata tramite il meccanismo descritto in precedenza. Infine i nodi A ed E terranno aggiornate le entry delle proprie PC associando, rispettivamente, l'host X con la porta C e la porta G.

In seguito ad un movimento dell'host le diverse PC dovranno subire degli aggiornamenti.

Si supponga quindi che l'host X si sposti nell'area di copertura offerta dalla Base Station F (tale informazione sarà acquisita da X in un modo molto simile a quello utilizzato in Mobile IP, cioè attraverso l'impiego di segnalazioni emesse dalle Base Station e denominate *Beacon Signals*). Per aggiornare le PC, il Mobile Node invierà un Paging Update Message attraverso F. Si noti che, a causa dei temporizzatori presenti nel nodo E, si avranno, per un certo periodo, due differenti mappaggi per X, come indicato in figura 32:

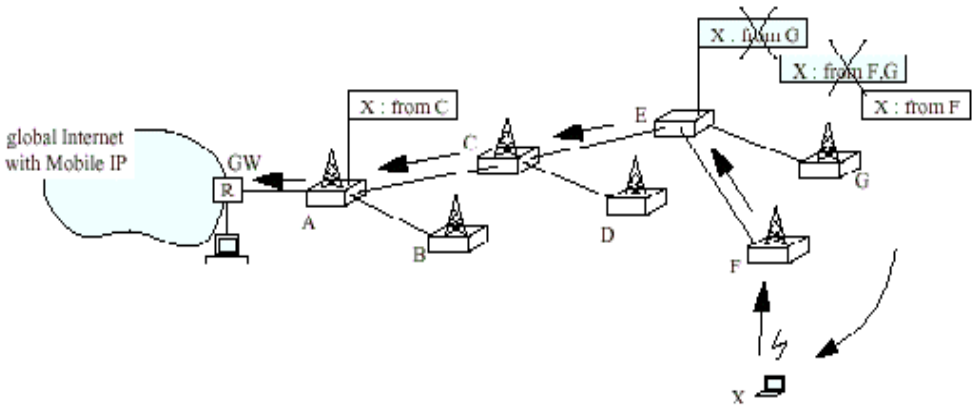


Figura 32: Aggiornamento delle Paging Cache

Quando un pacchetto indirizzato al Mobile Node giunge al gateway, le Paging Table verranno utilizzate per localizzarne la posizione:

il gateway genera un *Paging Packet*, contenente l' identificativo del Mobile Node che rilancerà all' appropriato nodo, della Cellular IP Network, consultando la propria PC. Tutti i nodi contenente una PC ripeteranno la stessa operazione mentre quelli sprovvisti di tale tabella rilanceranno il pacchetto verso tutte le proprie porte d' uscita.

Ritornando all'esempio, il gateway rilancerà il Paging Packet verso il nodo A il quale a sua volta, consultando la propria PC, lo invierà a C. Tale nodo, non possedendo la tabella, lo consegnerà sia a D che a E, etc. Infine come ultimo passo, la Base Station F rilancerà il pacchetto al Mobile Node (figura 33).

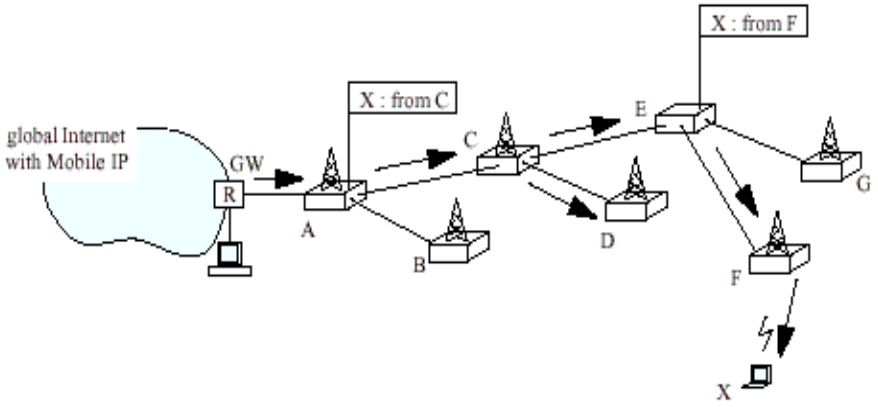


Figura 33: Instrdamento di un Paging Packet

In seguito alla ricezione del Paging Packet il Mobile Node genera un RouteUpdate Packet che, attraverso F, lo invierà al gateway in maniera da creare la entry necessaria nelle routing cache.
Uno svantaggio del meccanismo ora descritto è quello di ritardare la consegna del primo pacchetto in quanto il gateway sarà costretto a memorizzarlo fino a quando i diversi nodi della rete non avranno aggiornato le routing cache. Ovviamente tale procedura non dovrà essere ripetuta per consegnare gli altri pacchetti.

4.5 Handoff

Come si è avuto modo di intuire dalla precedente discussione, nel protocollo Cellular IP gli handoff, sono inizializzati dallo stesso Mobile Node, il quale, dopo essersi spostato in una nuova cella, provocherà l'aggiornamento delle informazioni contenute nei diversi nodi della rete attraverso l'invio di un

pacchetto di controllo. Si è anche sottolineato che per una certa durata il Mobile Node sarà caratterizzato dal possedere due diversi “mappaggi”, uno relativo alla vecchia Base Station ed uno relativo a quella nuova.

Lo scenario complessivo di un handoff è rappresentato in figura:

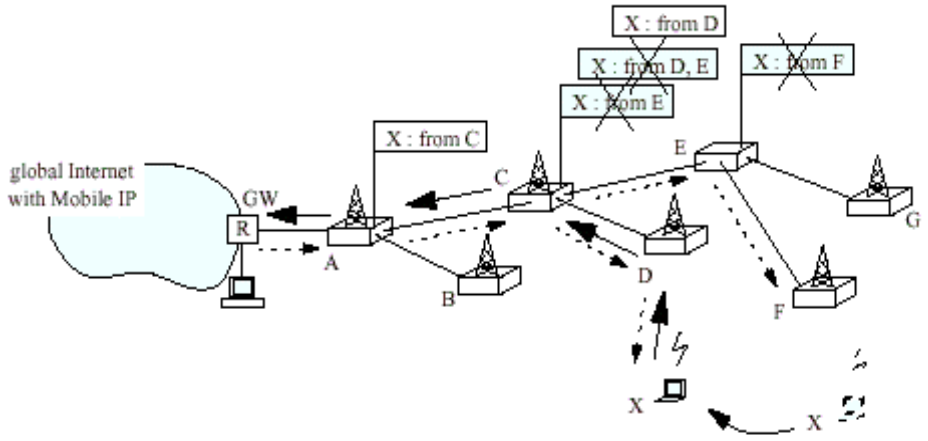


Figura 34: Handoff

l’host attivo X, dopo essersi spostato dalla cella F alla cella D, invierà un Routing Update Packet che provocherà l’aggiornamento delle Routing Table. Come indicato dalle frecce tratteggiate, per un certo periodo i pacchetti destinati al Mobile Node saranno rilanciati sia verso la Base Station D che verso la F.

Si è voluto rimarcare il meccanismo che gestisce l’handoff non per ripetere cose già dette, bensì per introdurre un’ottimizzazione dello stesso denominata *Semi-soft Handoff* applicabile quando il Mobile Node pur spostandosi sotto l’area di copertura offerta da una nuova Base Station, è in grado di “sintonizzarsi” anche con quella vecchia; sostanzialmente questo è possibile quando le due œlle si sovrappongono. In [28] tale procedura è descritta in dettaglio, nell’ambito dello studio che si sta effettuando, ritengo sia importante solamente sottolinearne il vantaggio:

il Semi-soft Handoff consente di ridurre al minimo la perdita di pacchetti che si manifesta quando il Mobile Node è in transito da una Base Station all’ altra.

4.6 Considerazioni conclusive

Per concludere la descrizione di Cellular IP è necessario sottolineare alcuni aspetti in maniera tale da fornire un quadro complessivo, se pur non dettagliato, del protocollo.

4.6.1 Sicurezza

I pacchetti di controllo (Paging Update e Routing Update) che permettono di modificare le informazioni contenute nelle tabelle, devono poter essere autenticati. A tale scopo tutti i nodi della rete sono provvisti di una chiave di autenticazione (chiave di rete), caratterizzante la rete e tenuta all'oscuro dai diversi Mobile Node. Nasce quindi il problema di fornire al Mobile Node una chiave, differente dalla precedente, da poter utilizzare per elaborare la parola di autenticazione contenuta nei pacchetti sopra menzionati. A tale scopo, il gateway, dopo aver autenticato (con tecniche che si anarizzerranno in seguito) il Mobile Node che richiede di accedere alla rete, fornirà allo stesso un PID (*Protocol IDentifier*), ottenuto concatenando (con opportune regole) la chiave della rete con l'home address. Tale PID verrà utilizzato dal Mobile Node come parola di autenticazione dato che ciascun nodo sarà in grado di interpretarlo attraverso l' utilizzo della chiave di rete.
E' importante menzionare anche la necessità di meccanismi di sicurezza da utilizzare per i W*ireless Link* esistenti tra il Mobile Node e la Base Station.

4.6.2 Identificativo del Mobile Node

All' interno di una Cellular IP Network, l'indirizzo IP del Mobile Node non ha una particolare importanza in quanto non permette di individuare l'esatta posizione dello stesso. Più precisamente, come è stato ampliamente detto, i diversi nodi della rete hanno bisogno solamente di un identificativo che consenta di "indicizzare" il particolare host.
Per questo motivo si è scelto di utilizzare come identificativo l'home address del Mobile Node solamente per semplificare le cose: in questo modo non c'è

bisogno di implementare tunneling o conversioni d'indirizzo. Un pacchetto destinato al Mobile Node sarà decapsulato dal gateway (come richiede Mobile IP) e "consegnato" alla rete senza compiere particolari operazioni.

4.6.3 Stati del Mobile Node

Si è avuto modo di distinguere i due stati in cui può trovarsi il Mobile Node: stato attivo e stato passivo.
In figura 35 viene mostrato un diagramma di stato che chiarisce la modalità con la quale avviene la transizione da uno stato all'altro:

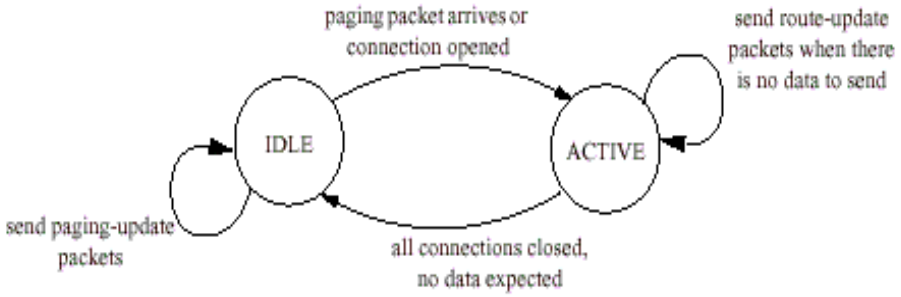


Figura 35: Transizioni di Stato

- nello stato passivo (*Idle State*) il Mobile Node invia Paging Update Packet con un periodo che dipende dalla temporizzazione utilizzata. Sicuramente dovrà emettere tale messaggio in corrispondenza d'ogni handoff (o di ogni cambiamento di paging area);

- il Mobile Node passa nello stato attivo (*Active State*) in seguito alla ricezione di un pacchetto o all'instaurazione di una connessione;

- nello stato attivo il Mobile Node invierà Routing Update Pachet in seguito ad ogni handoff oppure per mantenere aggiornate le tabelle dei nodi quando non ha dati da inviare ma necessita di essere raggiungibile;

- infine il Mobile Node tornerà nello stato passivo una volta che avrà terminato di inviare o ricevere dati.

5 Interworking dei sistemi GPRS/UMTS con il protocollo Mobile IP

Negli ultimi anni si è assistito ad uno sviluppo senza precedenti del settore delle telecomunicazioni, in particolare gran parte degli sforzi sono stati rivolti verso la fornitura di servizi dati su rete mobile.
Le motivazioni principali che stanno spingendo all'innovazione del settore, sono:

- l'impressionante crescita degli utenti della telefonia mobile e di *Internet*. Circa 400 milioni di persone nel mondo utilizzano sistemi radiomobili con la previsione di raggiungere un miliardo d'utenti entro il 2003. Sul fronte *Internet*, d'altro canto, ogni mese si registrano 18 milioni di nuovi utenti, con un traffico dati che raddoppia ogni sei mesi circa;
- l'esigenza di conciliare la mobilità dell'utente con la crescente domanda di comunicazione multimediale ed in particolare di un accesso wireless ad alte prestazioni ad *Internet*;
- il parallelo sviluppo dei servizi e delle applicazioni dell'*Information Technology*.

D'altro canto però, allo stato attuale, la crescente domanda di un mercato di massa dei servizi dati su mobile si scontra con i limiti fisici e funzionali tipici del GSM (*Global System for Mobile communications*). È una realtà che gli esistenti servizi dati per cellulari non soddisfino le necessità degli utenti. La causa di ciò può essere individuata nei seguenti fattori: basse velocità di

trasferimento dei dati, procedure di connessione complicate, tempi di *set up* della connessione troppo lunghi ed infine costi eccessivi.

In questa direzione, per le reti GSM è in corso un processo d'aggiornamento che faciliterà l'introduzione di servizi dati e multimediali. Questo processo, che ha portato alla standardizzazione dei cosiddetti sistemi di generazione "2+" o "2.5", si sta sviluppando su diversi livelli e presenta le seguenti soluzioni:

- *High Speed Circuit Switched Data* (HSCSD).
- ***General Packet Radio Service* (GPRS)**.
- *Enhanced data rates for GSM and TDMA Evolution* (EDGE).

In particolare il servizio GPRS è lo standard, definito in ambito ETSI (European Telecommunications Standards Institute), che permette l'introduzione della trasmissione dei dati a pacchetto nel sistema GSM e può essere considerato il primo reale passo verso "*mobile internet*".
Con l'introduzione del GPRS nella rete GSM, l'operatore può offrire un accesso radio efficiente alle reti esterne basate su IP o X.25, come *Internet* e le *Intranet* aziendali.
Il valore aggiunto offerto dal GPRS non sarà tanto la velocità di trasferimento dei dati, comunque superiore ai tradizionali 9.6 Kbit/s del GSM CSD (*Circuit Switched Data*), quanto piuttosto tutti i vantaggi che offre la tecnologia a commutazione di pacchetto nell'accesso alle risorse del *web*. Lo scambio dei dati su *Internet* è caratterizzato da brevi e frequenti trasmissioni bidirezionali (traffico a *"burst"*) fra le quali vi sono moltissime pause. È evidente che in un tale contesto una tecnologia che consenta un accesso rapido alla rete, la possibilità di essere sempre *on-line* (*always on*) e una nuova concezione della tariffazione non più basata sul tempo di connessione bensì sul volume di dati scambiati, risulti assolutamente ottimale.
Infine il GPRS getterà le basi per l'evoluzione dai sistemi radiomobili di "seconda generazione" a quelli di "terza generazione" come l'UMTS (Universal Mobile Telecommunications System). Progettato in modo altamente flessibile,

l'UMTS, fornirà un'ampia gamma di applicazioni in una molteplicità di ambienti, attraverso un sistema universale che sfrutti appieno le potenzialità del mercato mondiale delle telecomunicazioni. Nell'ambito dei servizi dati avrà caratteristiche assolutamente innovative rispetto al GSM, estendendo all'utenza mobile tutti i servizi attualmente offerti su *Internet* all'utenza fissa. Questo sarà reso possibile fornendo un accesso wireless, con tecnologia a pacchetto, ai servizi dati con velocità di trasferimento fino a 2 Mbit/s.

Nel panorama sopra descritto è intuibile la notevole importanza che potrà assumere il protocollo Mobile IP: consentirà all'utente una completa mobilità in ambito Internet; si potrà spostare liberamente da una wireless LAN (Local Area Netork) ad un sistema GPRS senza dover abbattere le eventuali sessioni Internet.

Ovviamente per raggiungere tale obiettivo non solo si dovrà dotare l'utente di un terminale compatibile con le diverse tecnologie ma si dovrà anche lavorare per rendere compatibili i diversi protocolli che gestiscono le reti d'accesso ad Internet.

Nel presente capitolo si fornirà una descrizione generale del sistema GPRS in maniera tale da poter presentare le modalità che consentiranno di "affiancare" le caratteristiche proprie del protocollo Mobile IP con quelle del sistema GPRS (ed il futuro UMTS).

5.1 Aspetti innovativi del sistema GPRS

Il GPRS è un nuovo servizio portante per il GSM, definito in ambito ETSI, che permette di trasmettere e ricevere dati con una modalità a pacchetto sia sull'interfaccia radio, sia sull'interfaccia di rete, senza impegnare risorse a commutazione di circuito.

Per capire come funziona il GPRS è necessario innanzi tutto riassumere il funzionamento della tradizionale trasmissione dati CSD (*Circuit Switch Data*) sul GSM. Questa gestisce le risorse radio con il principio della commutazione di circuito in maniera analoga alle normali conversazioni telefoniche nelle quali, una volta stabilita una connessione fisica fra due utenti, la "linea virtuale

radio" viene interamente e totalmente dedicata ad essi fino a che non viene richiesto il rilascio della connessione, tutto ciò indipendentemente dal fatto che i due utenti si scambino dati durante tale periodo [29].
In condizioni ottimali il CSD garantisce una connessione "costante" e bidirezionale a 9,6 Kbps, tuttavia queste peculiarità non rivestono particolare importanza per le moderne trasmissioni dati interattive via *Internet*, perché queste ultime non necessitano di una reale trasmissione continua, ma semmai di brevi e frequenti trasmissioni bidirezionali (traffico a *"burst"*) fra le quali vi sono moltissime pause. Ad esempio quando un utente digita sul proprio *browser* l'indirizzo (URL) di una pagina *web*, invia una richiesta al *server* sul quale è localizzata tale pagina. Una volta che la richiesta è arrivata a destinazione, il *server* trasmetterà di ritorno i contenuti della pagina (testo, grafica, audio,…). Successivamente, quando l'utente sta consultando la pagina, la rete non trasmette alcun dato significativo, pertanto finché non verrà richiesto al sistema di inviare altre informazioni, la linea virtuale radio non viene, di fatto, sfruttata, e quindi potrebbe essere utilizzata da un altro utente che necessita di trasmettere dati in quel momento.

Il GPRS essendo un servizio portante basato sulla commutazione a pacchetto sfrutta il principio della multiplazione statistica permettendo a più utenti di condividere lo stesso canale fisico. Questo sarà allocato all'utente soltanto quando effettivamente necessario, e rilasciato immediatamente dopo.
In altre parole il GPRS consentirà all'operatore GSM di "sospendere" provvisoriamente il canale dati ad un utente quando non ne ha bisogno in modo da risparmiare risorse e di assegnarle a chi nello stesso momento ha la reale necessità di trasmettere o ricevere dati.

5.1.1 Gestione delle risorse radio

Come accennato nel paragrafo precedente, l'allocazione delle risorse radio nel GPRS è differente rispetto al GSM.
Il GPRS permette ad una singola stazione mobile di trasmettere su *time slots* multipli della stessa trama TDMA (Time Division Multiple Access), allocando i

canali solo quando ci sono dati da trasmettere o ricevere, rilasciandoli dopo la trasmissione. Con questo principio, una molteplicità di utenti può condividere lo stesso canale fisico permettendo un'allocazione dei canali molto flessibile, nonché una maggiore efficienza nell'utilizzazione delle "scarse" risorse radio in caso soprattutto di traffico a *burst*. [30].

Le risorse in Uplink e Downlink sono allocate separatamente, il che permette di supportare in modo efficiente un traffico dati asimmetrico (e.g. navigazione nel web).

In una cella i canali fisici dedicati al GPRS, denominati PDCH (Packet Data Channel), sono presi dall'insieme comune dei canali previsti nell'interfaccia GSM. Considerando il fatto che in una cella possono trovarsi a condividere le risorse radio sia utenti GPRS che GSM si avrà, di conseguenza, un'allocazione di canali fisici sia per servizi a commutazione di circuito (GSM voce o dati), sia per servizi a commutazione di pacchetto (GPRS). Questa allocazione sarà fatta dinamicamente in accordo al principio della *"Capacity on Demand*". In base a questo principio, in contrapposizione a quello della *"Resources Reservation"* tipico della commutazione di circuito, l'allocazione di capacità per il GPRS può essere basata, ad esempio, sull'attuale necessità di trasferimento di pacchetti, sul carico di traffico, etc. Il numero di PDCH allocati in una cella può quindi essere incrementato o decrementato in funzione della domanda di risorse.

Per consentire sviluppi futuri del sistema GPRS (vedi UMTS) si è mantenuta una stretta separazione tra l'architettura di rete interna e quella dell'interfaccia radio, tale principio consentirà di modificare l'interfaccia wireless d'accesso senza intervenire sulle caratteristiche della "core network".

5.1.2 Vantaggi del sistema GPRS

Come è noto nel GSM quando si effettua una comune telefonata o ci si connette ad *Internet* in modalità CSD si utilizza un solo time slot. Nel caso di trasmissione dati questo time slot dispone di una capacità pari a 9,6 Kbps. La pratica dimostra che questa capacità può bastare per applicazioni fax o per leggere e-mail, ma per quanto riguarda la navigazione nel web con immagini o

la trasmissione di file, porta a dei tempi di attesa inaccettabili. A ciò si deve aggiungere il fatto che soprattutto durante le ore di congestione, in cui il flusso dei dati può addirittura arrestarsi per lunghi periodi, si continua sempre a sostenere i normali costi di traffico.

Nel GPRS, come accennato nel precedente paragrafo, è possibile allocare più di un canale per un singolo utente, raggiungendo capacità teoriche di 171,2 Kbps. In realtà tale capacità non potrà essere raggiunta in quanto i valori reali si attestano, in condizioni ottimali, intorno ai 40 Kbps.

Da ciò deriva che il valore aggiunto offerto agli utenti GPRS sarà fornito, come accennato nell'introduzione al capitolo, dai vantaggi intrinseci della tecnologia di trasmissione a commutazione di pacchetto.

In definitiva il GPRS dovrebbe portare i seguenti benefici pratici:

- **Accesso istantaneo alla rete**

  Sarà notevolmente ridotto, rispetto al CSD, il tempo di set up della connessione.

- **Always on**

  L'utente avrà la possibilità di essere sempre connesso ad Internet negli stessi luoghi dove oggi può essere può essere usato il GSM.

- **Tariffazione non a tempo**

  Nei servizi dati a commutazione di circuito l'utente deve pagare per tutto il tempo che sta "on-line" compresi i periodi di inattività in cui non vengono trasmessi pacchetti (per esempio la consultazione di pagine Web). Tutto ciò è evidentemente inadatto per applicazioni con traffico a burst. Di conseguenza nei servizi a commutazione di pacchetto la tariffazzione sarà effettuata sulla quantità di dati trasmessi permettendo cosi all'utente di stare "on-line" per lunghi periodi di tempo con costi molto inferiori rispetto alla situazione attuale.

5.2 Architettura della rete GPRS

Il GPRS rappresenta un esempio d'integrazione tra funzioni a circuito e modalità a pacchetto. Il principale problema che si è dovuto risolvere in questo sistema è legato proprio alla compatibilità tra un ambiente fortemente orientato alla commutazione a circuito (quello usato nella rete di accesso GSM) ed i requisiti tipici della commutazione a pacchetto.
Per superare questo problema, il GPRS è stato definito sia attraverso l'introduzione di nuovi elementi di rete (Gateway Support Node – GSN), sia attraverso l'aggiornamento degli esistenti nodi GSM [31].
Di seguito viene riportata l'architettura logica delle rete GPRS:

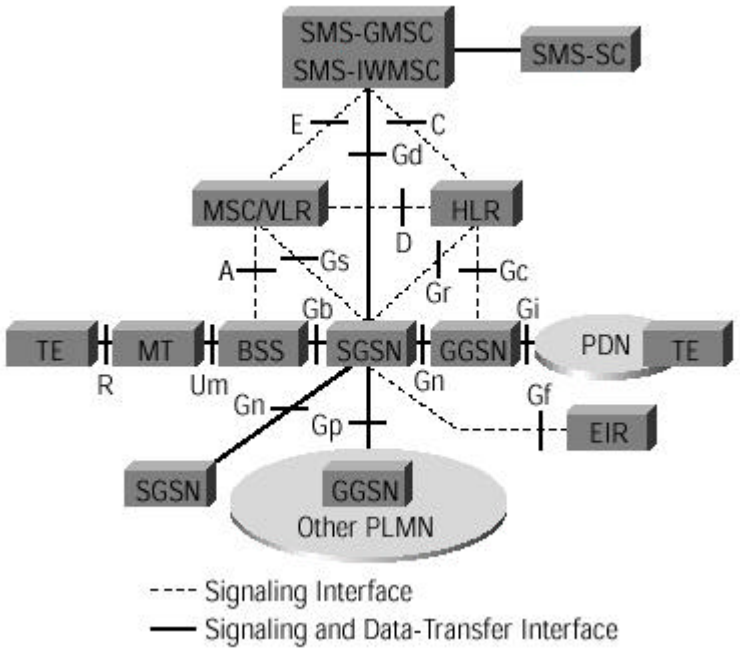


Figura 36: Architettura logica della rete GPRS

Fornire una descrizione dettagliata dell'architettura della rete GPRS esula dagli scopi della tesi, si cercherà quindi di caratterizzarne solamente gli aspetti più generali, evidenziando le innovazioni rispetto al sistema GSM. Per una maggiore comprensione delle funzionalità di tutte le entità architetturali ed

interfacce di rete rappresentate in figura si rimanda a [30], [31], [32] oltre che, ovviamente, alle reference ETSI sull'argomento.

5.2.1 Aggiornamento della rete GSM

Tutti i segnali radio sono trasmessi e ricevuti dal BSS (Base Station Subsystem) che dovrà far condividere le risorse tra un sistema GSM, a commutazione di circuito, e un sistema GPRS a commutazione di pacchetto.
Il BSS sarà aggiornato con delle funzionalità idonee a trattare un traffico dati a pacchetto. Queste includeranno: gestione di dati a pacchetto, diffusione di informazioni GPRS, gestione delle risorse ed una nuova interfaccia con il nodo SGSN.
In particolare i sotto-sistemi che costiuiscono il BSS, il BTS (Base Transceiver Station) ed il BSC (Base Station Controller), dovranno subire le seguenti modifiche:

- **Base Transceiver Station**

  Dovrà subire un aggiornamento software, ma probabilmente non hardware. Quando i segnali radio sono ricevuti dal BTS, questo separa dati/voce GSM a commutazione di circuito da dati a pacchetto GPRS ed inoltra entrambe le categorie al BSC.

- **Base Station Controller**

  Ciascun BSC dovrà essere equipaggiato con nuovi elementi hardware e richiederà un aggiornamento software. In termini di hardware sul BSC saranno installate una o più **PCU** (*Packet Control Unit*) per gestire i pacchetti GPRS. La PCU fornisce un'interfaccia logica e fisica alla BSS gestendo il trasferimento dei pacchetti dati d'utente dalla stazione mobile all'SGSN.

Occorre infine ricordare che tutti i dispositivi che costituiscono la rete GSM, cioè l'HLR (Home Location Register), l'MSC (Mobile Switching Center), il

VLR (Visited Location Register), etc. dovranno subire un aggiornamento software per poter gestire le funzionalità introdotte dal sistema GPRS.

5.2.2 Innovazioni introdotte dal sistema GPRS

La rete GSM classica non fornisce funzionalità adeguate per l'instradamento dei dati a pacchetto. Per questa ragione la struttura convenzionale GSM è stata estesa con l'introduzione di una nuova classe di entità logiche di rete denominate GSN (*GPRS Support Node*).

Questi nuovi nodi sono il GGSN (*Gateway GPRS Support Node*) e l'SGSN (*Serving GPRS Support Node*) e sono connessi mediante una rete backbone GPRS basata sul protocollo IP. Costituiscono l'interfaccia tra il sistema radio e le reti fisse per servizi a commutazione di pacchetto. Esiste una relazione many-to-many tra SGSN e GGSN nel senso che un GGSN è l'interfaccia con una PDN (Packet Data Network) per una pluralità di SGSN, mentre un SGSN può inviare i suoi pacchetti verso una pluralità di GGSN.
Questi nodi svolgono tutte le funzioni necessarie per gestire la trasmissione dei pacchetti da e verso la MS (Mobile Station). In particolare si occupano di: gestione dell'utenza, tassazione e sicurezza, gestione della mobilità, trasmissione dei pacchetti, etc.

Saranno infine necessari anche dei nuovi terminali, in quanto gli esistenti telefoni GSM non sono in grado di gestire servizi a commutazione di pacchetto.

5.2.2.1 Serving GPRS Support Node

Questo nodo è responsabile per il trasporto dei pacchetti dati da e verso la stazione mobile entro la sua area di servizio (area SGSN). L'area SGSN è la parte di rete servita da un SGSN.
In generale i compiti dell'SGSN includono:

- monitoraggio della posizione dei terminali all'interno della propria area di servizio;

- individuazione di nuovi terminali GPRS all'interno dell'area di servizio;
- funzioni di controllo di accesso per i terminali GPRS,
- trasferimento ed instradamento dei pacchetti (in entrambe le direzioni tra uno o più GGSN e il BSS);
- gestione della mobilità (attach/deattach);
- funzioni di charging e autenticazione.

5.2.2.2 Gateway GPRS Support Node

Il GGSN agisce come un'interfaccia tra la rete backbone GPRS e le reti dati a pacchetto esterne. Svolge anche la funzione d'instradamento in entrambe le direzioni tra queste reti esterne e uno o più SGSN.
In particolare converte i pacchetti GPRS che arrivano dall'SGSN in un formato appropriato per essere spediti alle reti dati esterne (e.g. IP o X.25). Nell'altra direzione gli indirizzi PDP (Packet Data Protocol) dei pacchetti dati entranti (ad esempio indirizzo IPv4) sono convertiti nell'indirizzo GSM dell'utente destinatario. I pacchetti re-indirizzati sono spediti all'SGSN responsabile. A questo scopo il GGSN memorizza l'indirizzo IP dell'SGSN a cui è correntemente registrato l'utente (si ricordi infatti che i nodi GPRS sono connessi tra di loro mediante una rete IP e quindi saranno identificabili attraverso indirizzi IP).
Come l'SGSN, anche il GGSN svolge funzioni di autenticazione e charging.

5.2.2.3 Rete Backbone GPRS

Tutti i nodi GSN sono connessi attraverso una rete backbone GPRS basata sul protocollo IP. Entro questa rete backbone, i GSN incapsulano i pacchetti delle reti dati e li trasmettono (Tunnel) usando il GPRS Tunneling Protocol (GTP).

Esistono due tipi di rete Backbone (vedi figura 37):

- **Rete Backbone INTRA-PLMN**

  E' la rete IP che interconnette i GSN situati entro la stessa PLMN (Public Land Mobile Network).

- **Rete Backbone INTER-PLMN**

  È la rete IP che interconnette i GSN e le reti backbone intra-PLMN, in differenti PLMN.

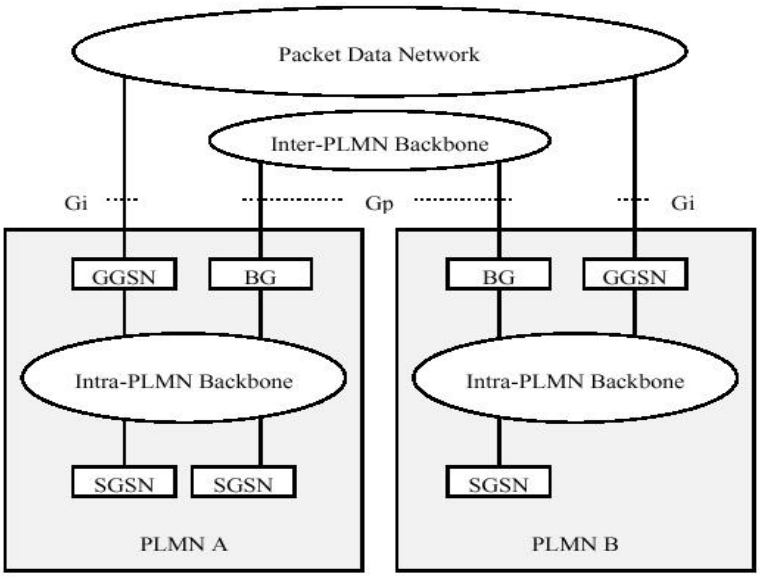


Figura 37: Reti Backbone intra e inter PLMN

Ogni rete backbone intra-PLMN è una rete IP privata concepita esclusivamente per dati e segnalazione GPRS. Una rete IP privata è una rete IP alla quale è applicato un certo meccanismo di controllo di accesso per garantire un richiesto livello di sicurezza.

Due reti backbone intra-PLMN sono connesse attraverso l'interfaccia Gp usando dei **Border Gateway (GP)** e una rete backbone inter-PLMN. Quest'ultima è selezionata da un accordo di roaming che include i BG (i quali

forniscono l'appropriato livello di sicurezza per proteggere la PLMN ed i suoi abbonati).

5.2.2.4 Mobile Station (MS)

La stazione mobile (MS) consiste dell'attrezzatura fisica usata dall'utente della PLMN e comprende il Mobile Equipment (ME) e la SIM (Subscriber Identity Module).
A sua volta l'ME comprende il Mobile Termination (MT) il quale, in funzione delle applicazioni e dei servizi, potrebbe supportare varie combinazioni di gruppi funzionali distribuiti sul Terminal Adapter (TA) e sul Terminal Equipment (TE).
Bisogna notare che l'MT e il TE potrebbero essere situati nello stesso equipaggiamento o in dispositivi separati come ad esempio un telefono GPRS collegato ad un computer (anche portatile):

- il TE è il computer terminale che spedisce e riceve i dati a pacchetto dell'utente. Da un suo punto di vista l'MT funziona come un modem che lo connette, tramite il sistema GPRS, ai servizi Internet-Intranet;
- l'MT comunica sul canale radio con il BTS e deve essere dotato di specifici software ed hardware per accedere al sistema GPRS.

Con lo scopo di soddisfare i bisogni di diversi segmenti di mercato sono stati definiti, nello standard GPRS tre diversi tipi di terminali:

- **Terminala di Classe A**

  Supporta in maniera simultanea le funzionalità del sistema GPRS e quelle più convenzionali del sistema GSM. Allo stato attuale, sembra impossibile che questo tipo di terminali venga realizzato nel breve periodo a causa della loro complessità e dell'alto consumo di potenza.

- **Terminali di Classe B**

L'MS è collegato ad entrambe i servizi GPRS e GSM, ma può operare soltanto su un servizio alla volta. Questo significa che non può inviare e ricevere simultaneamente il traffico nelle due modalità.

- **Terminali di Classe C**

  L'MS è collegato o al servizio GPRS o al servizio GSM. È quindi possibile soltanto un uso alternativo dei due.

5.3 Caratteristiche funzionali del sistema GPRS

Prima che un terminale mobile possa accedere ai servizi GPRS, deve informare la rete della propria presenza, eseguendo una procedura di registrazione (***GPRS Attach***) verso il nodo SGSN. Questa procedura di *Attach* è analoga alla procedura corrispondente nel mondo a circuito (***IMSI Attach***) e comprende: l'aggiornamento delle informazioni di localizzazione nell'HLR; il trasferimento delle informazioni fra il vecchio SGSN, nel quale il mobile era registrato in precedenza, e il nuovo SGSN e la cancellazione dei dati dal vecchio SGSN (e dal vecchio VLR se il mobile era anche registrato, per i servizi a commutazione di circuito, con la rete GSM).
A sua volta la disconnessione dalla rete GPRS è denominata ***GPRS Detach*** e può essere inizializzata sia dal Mobile Station che dalla rete.

Una volta eseguito un GPRS Attach, devono essere avviate delle procedure di Mobility Management che permettano di tener traccia della posizione attuale del terminale. Le funzioni svolte saranno differenti a seconda dello stato assunto dal terminale.
Nella figura 38 sono indicati sia i possibili stati del Mobile Station sia le diverse motivazioni che causano la transizione di stato:

- nello stato IDLE, la rete non ha bisogno di conoscere la posizione del terminale in quanto quest'ultimo non è registrato con la rete GPRS;

- nello stato Ready il MS può inviare e ricevere pacchetti, da ciò deriva che la posizione dello stesso deve essere monitorizzata con estrema cura;

- infine nello stato STANDBY, nel quale il terminale non invia e non riceve dati, verranno attivate funzioni di Mobility Management solamente in seguito alla variazione di una Routing Area (cioè di un raggruppamento opportuno di celle) da parte del terminale;

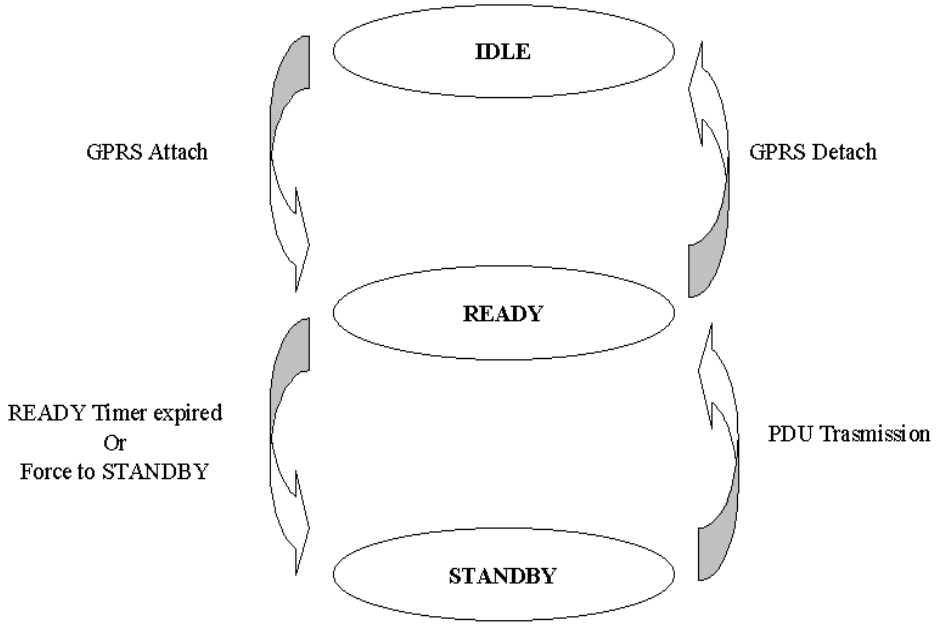


Figura 38: Modello a stati di un GPRS Mobile Station

In seguito ad un GPRS Attach, il Mobile Station per poter ricevere e trasmettere dati deve attivare un contesto PDP (*PDP Context*) che descrive le caratteristiche della connessione verso la rete dati esterna come: il tipo di rete, l'indirizzo del destinatario, l'indirizzo del GGSN da utilizzare e le caratteristiche di qualità del servizio (QoS).
Una descrizione sommaria della procedura d'attivazione di un PDP Context è la seguente:

- il terminale mobile richiede l'attivazione del contesto PDP, specificando alcuni parametri tra cui l'assegnazione di un indirizzo statico o dinamico e la qualità del servizio richiesta;
- il nodo SGSN convalida la richiesta in base ai dati di sottoscrizione ricevuti dal registro HLR al momento della registrazione;
- il nodo SGSN determina l'indirizzo del nodo GGSN in base alle informazioni fornite dal terminale mobile;
- viene creata una connessione logica tra SGSN e GGSN (Tunnel GTP);
- il nodo SGSN chiede al nodo GGSN di allocare un indirizzo IP e quindi lo trasferisce al terminale mobile;
- a questo punto può cominciare la comunicazione tra il terminale mobile e la rete dati esterna.

In generale la procedura di attivazione di un contesto può essere iniziata sia dal MS che dalla rete, di seguito viene mostrata la procedura dell'attivazione di un contesto da parte del MS:

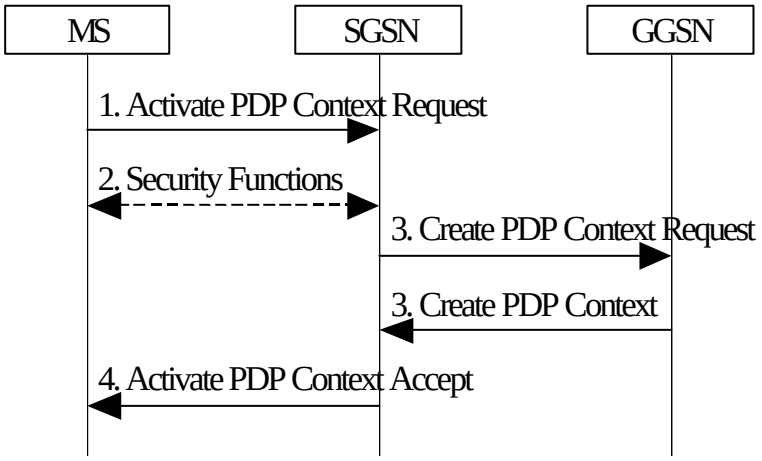


Figura 39: Attivazione di un PDP Context

L'MS invia un messaggio **Activate PDP Context Request** specificando le caratteristiche che dovrà possedere il contesto (ad esempio può richiedere l'allocazione di un indirizzo dinamico oppure no; può selezionare attraverso un particolare campo del messaggio, denominato APN, Access Point Name, la rete dati esterna alla quale connettersi, etc.). In questa fase possono essere svolte anche opportune procedure di sicurezza. L'SGSN, dopo aver validato la richiesta di attivazione del contesto, invierà un **Create PDP Context Request** al GGSN. Quest'ultimo dopo aver creato una entry nella propria tabella dei contesti rilancerà il messaggio **Create PDP Context** al SGSN il quale completerà la procedura informando il MS attraverso un **Activate PDP Context Accept.**

Per concludere questa visione generale del sistema GPRS può essere utile osservare la seguente figura nella quale sono rappresentati tre differenti schemi d'instradamento dei pacchetti: il cammino 1 rappresenta il caso in cui il terminale invia messaggi; il cammino 2 rappresenta la situazione opposta (un host della rete Internet invia pacchetti al terminale) mentre il cammino 3 rappresenta la situazione nella quale il MS si è spostato nella rete GPRS di un altro operatore.

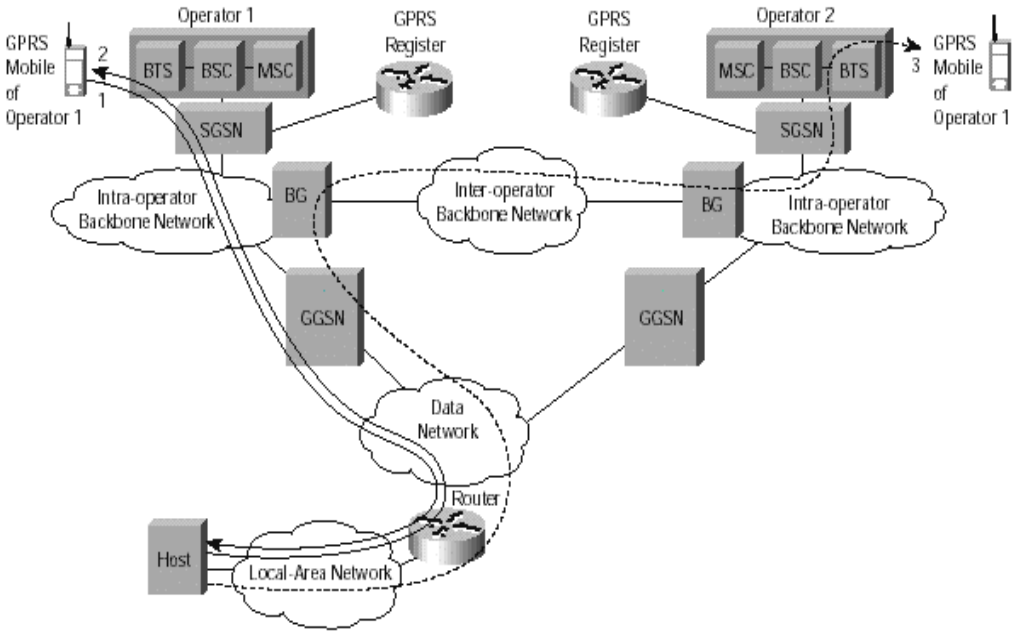


Figura 40: Routing dei pacchetti dati

5.4 Mobile IP over GPRS/UMTS

Come si è avuto modo di sottolineare più volte, la possibilità di fornire un accesso ad Internet, indipendente dalla posizione dell'utente e dalle caratteristiche della rete d'accesso, rappresenta uno dei maggiori impulsi allo sviluppo del settore delle telecomunicazioni.
Considerando inoltre l'espansione sempre più massiccia del sistema GPRS (e del futuro UMTS) come rete d'accesso wireless, appare evidente come l'introduzione del protocollo Mobile IP, in tali sistemi, rappresenti una notevole spinta verso il raggiungimento dell'obiettivo sopra delineato.

Secondo quanto riportato in [33] e [34] l'introduzione del protocollo Mobile IP dovrà avvenire in maniera graduale, in particolare si prevede un'evoluzione basata su tre fasi successive:

- **Fase 1**

  Rappresenta la minima configurazione necessaria per consentire ad un operatore di rete di usufruire delle caratteristiche del protocollo Mobile IP.

- **Fase 2**

  Verranno introdotte delle soluzioni per consentire una migliore gestione del routing dei pacchetti.

- **Fase 3**

  L'architettura di rete verrà modificata in maniera tale da consentire una completa applicabilità del protocollo Mobile IP.

Prima di descrivere in dettaglio l'evoluzione della rete GPRS, è opportuno evidenziare alcuni aspetti di validità generale che dovranno essere soddisfatti a prescindere dallo stadio raggiunto:

- per consentire di salvaguardare le risorse radio è consigliabile la presenza del Foreign Agent (e quindi l'utilizzo di un Foreign Agent care-of address). In questa circostanza l'end point del tunnel sarà il Foreign Agent e non il dispositivo mobile, ciò significa che l'interfaccia radio non dovrà subire il carico dovuto al "trasporto" di pacchetti incapsulati;

- sempre per raggiungere l'obiettivo di non sovraccaricare le risorse radio si dovranno determinare delle procedure che consentiranno al Foreign Agent di non inviare in broadcast gli Agent Advertisement;

- come nel normale funzionamento del sistema GPRS vi saranno delle procedure d'attivazione di contesti PDP. Dato che la rete dovrà essere in grado di gestire richieste provenienti sia da terminali dotati delle funzionalità Mobile IP sia da quelli privi di tali caratteristiche, si dovrà prevedere un meccanismo che consenta alla rete di gestire in maniera adeguata le differenti richieste. In tal senso può essere sfruttato il campo APN del messaggio Activate PDP Context Request inviato dal MS. Tale campo risulta suddiviso in due parti: Network ID e Operator ID, la prima identifica la rete esterna alla quale il MS vuole accedere mentre la seconda caratterizza l'operatore. In aggiunta, poichè la parte Network ID può essere utilizzata anche per specificare un particolare servizio, verrà sfruttata per consentire al MS di richiedere il servizio Mobile IP;

- come verrà descritto in maniera dettagliata nei prossimi capitoli, il sistema GPRS dovrà essere in grado di interagire con le infrastrutture AAA in maniera tale da verificare le credenziali dell'utente nell' Home Domain e procedere all'accounting dello stesso.

5.4.1 Fase 1: Introduzione del servizio Mobile IP

In questa fase le caratteristiche del protocollo Mobile IP verranno sovrapposte a quelle del sistema GPRS integrando le funzionalità del Foreign Agent con quelle del GGSN.
In figura è mostrata la struttura di rete (la parte indicata con il nome UTRAN rappresenta l'interfaccia radio utilizzata nella rete UMTS mentre filter caratterizza la presenza di eventuali funzionalità di controllo sui pacchetti entranti ed uscenti dalla rete):

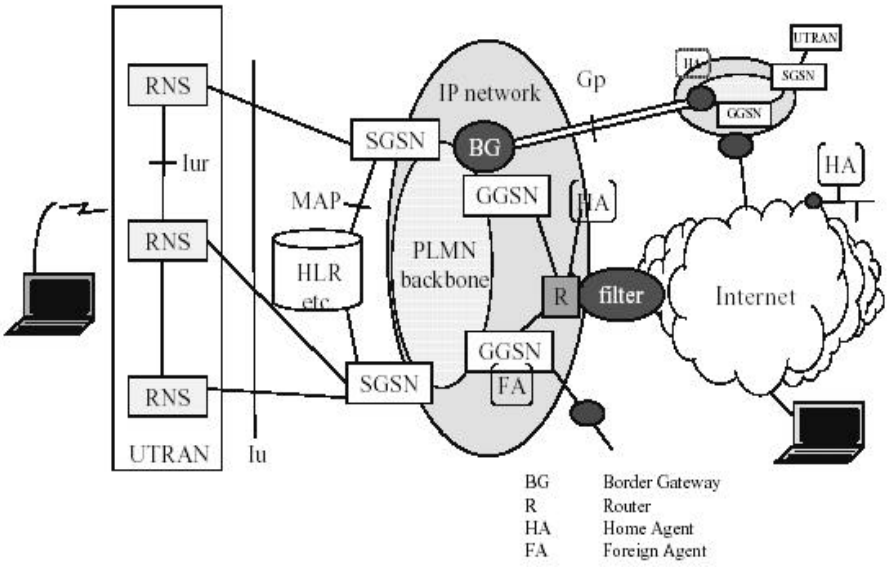


Figura 41: Rete GPRS con funzionalità Mobile IP di fase 1

L'impatto provocato da Mobile IP al sistema GPRS sarà minimo: la mobilità all'interno della rete PLMN sarà gestita dalle caratteristiche proprie del GPRS mentre Mobile IP potrà essere impiegato per gestire la mobilità tra due PLMN che supportano GGSN/FA. Nel caso in cui la rete d'arrivo non offra il servizio Mobile IP, il terminale mobile dovrà mantenere il GGSN/FA presente nella rete di partenza. Ciò significa che, in tale circostanza, il routing dei pacchetti tra le due reti sarà gestito come previsto dal sistema GPRS e quindi attraverso i Border Gateway e le caratteristiche funzionali dell'interfaccia Gp.

In questo primo stadio dell'evoluzione della rete GPRS il Mobile Node non potrà variare GGSN/FA nell'ambito di una stessa sessione, da ciò deriva che, per tutta la durata di un conteso PDP, il terminale mobile dovrà mantenere lo stesso Foreign Agent anche in caso di roaming tra due PLMN che supportano la funzionalità Mobile IP.

Come rappresentato in figura, è sufficiente che un solo nodo GGSN di una PLMN sia configurato con funzionalità di Foreign Agent, è essenziale però che in tale nodo vi sia il mappaggio tra indirizzo IP del terminale (Home Address) e l'indirizzo locale dello stesso denominato TID (*GPRS Tunnel ID*). E' chiaro, infatti, che il GGSN/FA, una volta ricevuto un datagramma destinato al Mobile Node, lo invierà allo stesso sfruttando il protocollo *GPRS Tunneling Protocol*.

Per descrivere la procedura d'attivazione di un contesto PDP e la seguente registrazione del terminale mobile con il rispettivo Home Agent si può far riferimento allo schema rappresentato in figura:

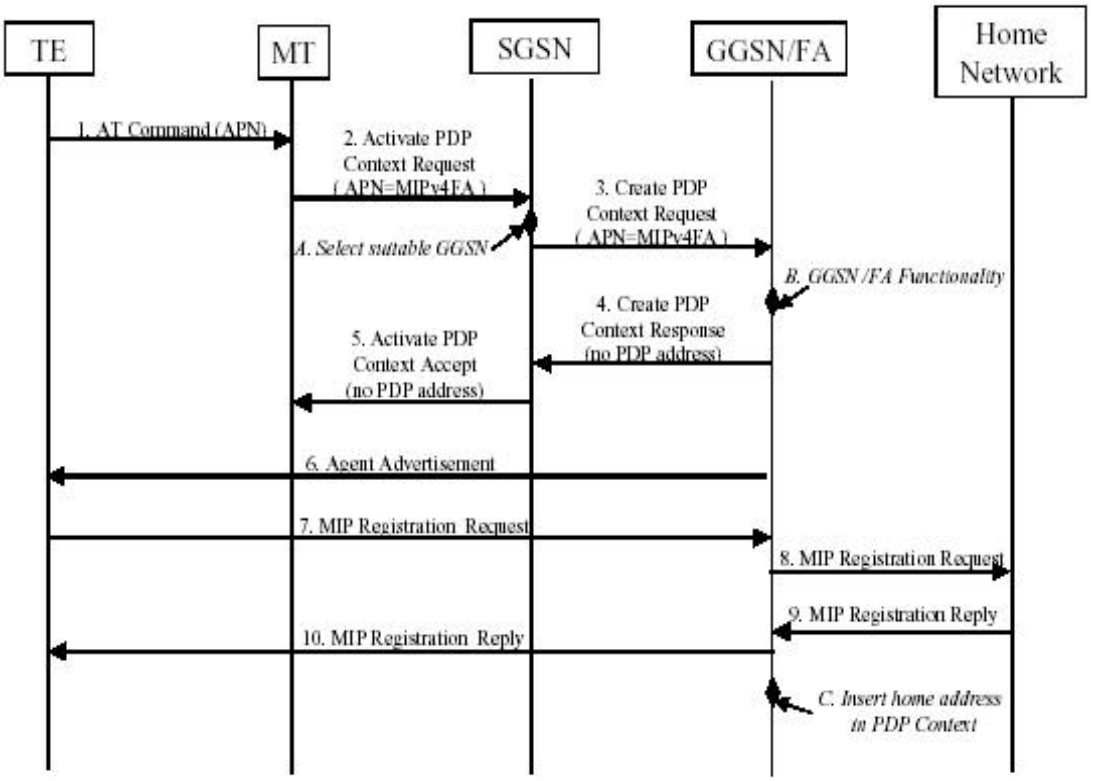


Figura 42: Attivazione di un contesto PDP e registrazione del MN

Come si è avuto modo di descrivere in un precedente paragrafo il MS può essere considerato suddiviso in due parti: il TE e l'MT. Il TE, attraverso comandi AT (Attention Command), trasferirà parametri al MS; tra questi vi sarà l'APN che potrà essere utilizzato per richiede il servizio Mobile IP. In seguito alla ricezione di tali comandi, l'MT invierà un Activate PDP Context Request all'SGSN, il quale, dopo aver selezionato un GGSN/FA gli trasmetterà un Create PDP Context Request. Le fasi successive d'attivazione del contesto procedono in maniera analoga a quanto visto precedentemente. Un'unica considerazione è obbligatoria: nell'attivazione di un conteso PDP il MS non deve richiedere l'assegnazione di un PDP Address.
Una volta completata l'instaurazione del PDP Context, il GGSN sarà in grado di inviare un Agent Advertisement direttamente al MS (utilizzando il TID) riducendo cosi il traffico di messaggi broadcast sull'interfaccia radio.
In seguito alla ricezione dell'Advertisement, il MS avvierà la procedura di registrazione del care-of address, fornito dal GGSN, con l'Home Agent.
Attraverso i messaggi di registrazione il GGSN sarà in grado di creare l'associazione, sopra menzionata, tra Home Address e PID (in altre parole, dato che l'MS non ha richiesto l'assegnazione di un PDP Address, il GGSN inserirà un'entry, nella tabella dei contesti, associando l'Home Address del Mobile Node con il PID dello stesso).

5.4.2 Fase 2: Ottimizzazione del Routing

Durante una sessione, il Mobile Node può effettuare diversi *SGSN handover* provocando un degradamento del routing dei pacchetti se il nuovo SGSN è sotto il controllo di un differente GGSN/FA. Si presenta, in pratica, un problema molto simile a quello studiato in un precedente capitolo e denominato *triangle routing.*
Per questo motivo l'obiettivo che si vuole raggiungere in questo secondo stadio dello sviluppo è quello di consentire al terminale mobile di variare GGSN/FA nell'ambito di una stessa sessione. Occorre precisare però che il cambio di

GGSN/FA sarà effettuabile solamente quando il MS non invia o riceve pacchetti (Idle State).

La struttura che assumerà la rete è mostrata in figura, si noti come, a differenza del caso precedente, vi siano più GGSN/FA in una stessa PLMN:

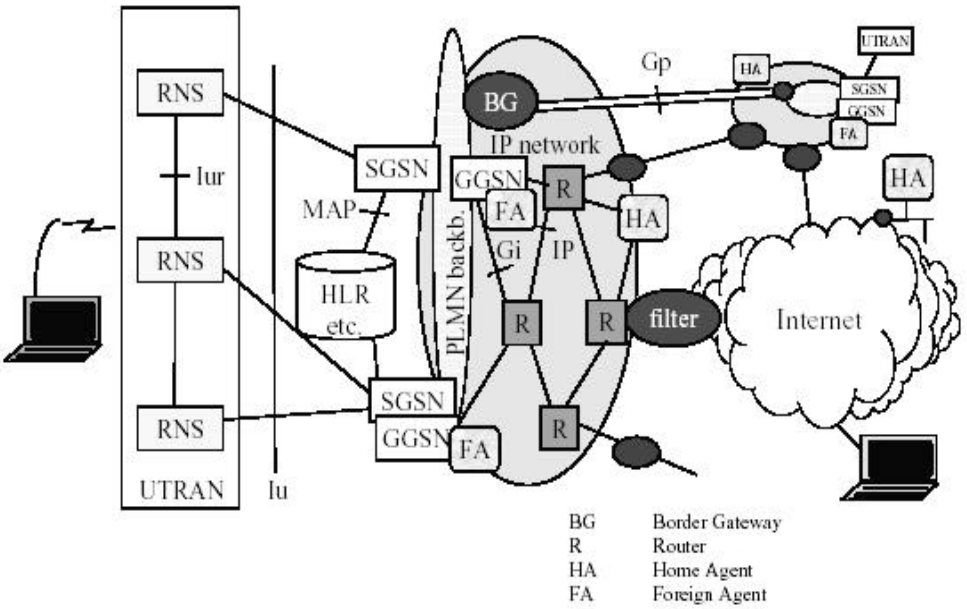


Figura 43: Rete GPRS con funzionalità Mobile IP di fase 2

Sia in questa fase dello sviluppo che in quella successiva si dovranno mantenere le funzionalità del Border Gateway e dell'interfaccia Gp che consentiranno di gestire il routing dei pacchetti nel caso di roaming del Mobile Node in una PLMN che non supporta funzionalità Mobile IP

La procedura d'attivazione di un contesto PDP e la seguente registrazione del Mobile Node è analoga al caso precedente. Più interessante è lo studio del diagramma di segnalazione che consente di effettuare una variazione del GGSN/FA nell'ambito di un stessa sessione. In altre parole occorre mostrare il meccanismo che consente di "spostare" il PDP Context dal "vecchio" GGSN/FA a quello "nuovo".

Si possono presentare le seguenti situazioni:

✍✍ **Il nuovo GGSN/FA accetta il PDP Context**

Come mostrato in figura, il cambio del GGSN/FA è controllato dall'SGSN attraverso l'invio del messaggio Create PDP Context Request (punto A in figura); per evitare la perdita di pacchetti verrà mantenuto, per un certo periodo, un tunnel tra il vecchio GGSN/FA e l'SGSN, in altre parole verrà inizializzato un timer (punto B) allo scadere del quale l'SGSN invierà un Delete PDP Context Request:

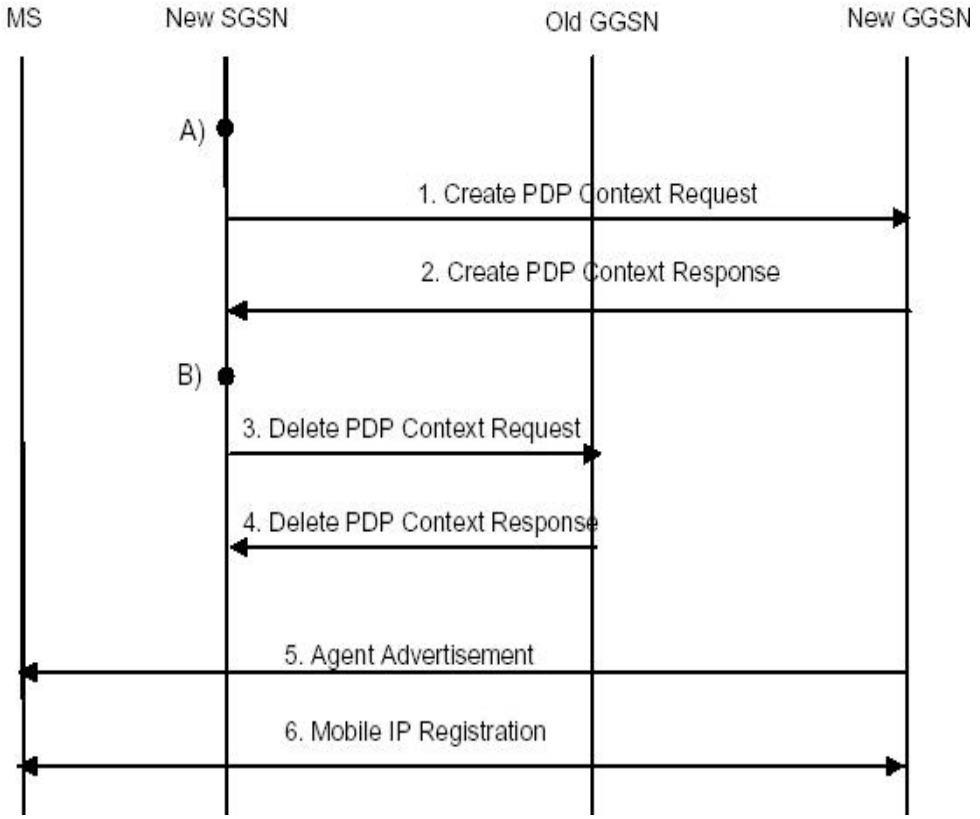


Figura 44: GGSN/FA Handover

✍✍ **Il nuovo GGSN/FA rifiuta la registrazione del Mobile Node**

In seguito al rifiuto della registrazione del terminale (punto A di figura 45), il "nuovo" GGSN/FA notificherà all'SGSN la cancellazione del PDP Context attraverso il messaggio Delete PDP Context. A sua volta l'SGSN determinerà la possibilità di re-instradare

tutto il traffico al vecchio GGSN/FA (punto B). In figura il Mobile Node è stato indicato con il termine User Equipment.

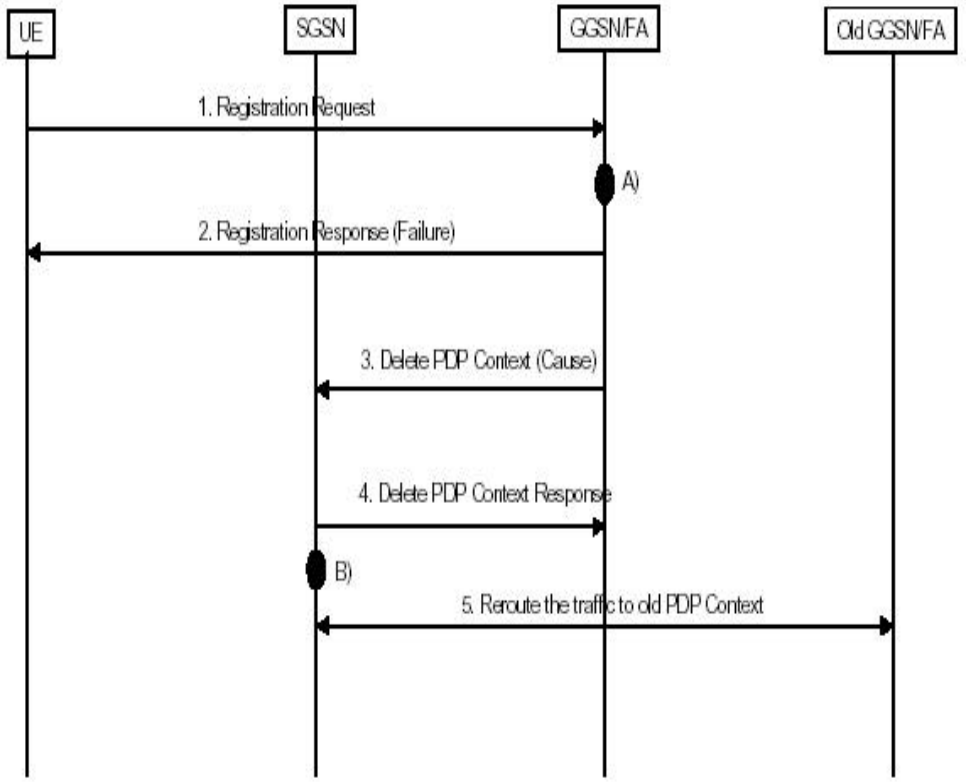


Figura 45: GGSN/FA rifiuta il servizio

Infine può capitare il caso in cui l'SGSN decidi di non trascurare il motivo che ha provocato la negazione del servizio da parte del nuovo GGSN/FA (ad esempio a causa di un rifiuto della registrazione da parte dell'Home Agent). Tale circostanza viene mostrata in figura 46 in cui si evidenzia la richiesta da parte dell'SGSN di eliminare l'eventuale PDP Context esistente con il vecchio GGSN/FA:

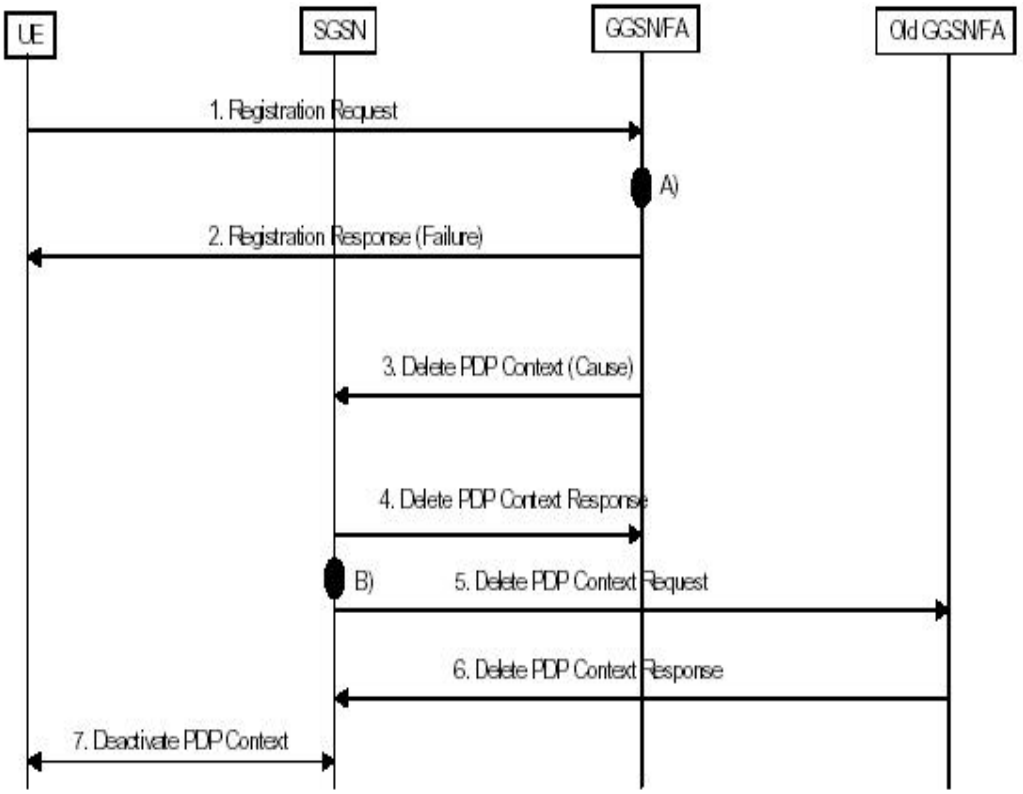


Figura 46: Eliminazione di tutti i PDP Context

5.4.3 Fase 3: Target Architecture

Lo sviluppo del sistema GPRS/UMTS condurrà ad un'architettura nella quale il protocollo Mobile IP verrà utilizzato per gestire sia la mobilità all'interno della PLMN sia quella tra PLMN differenti. Per raggiungere tale obiettivo le caratteristiche del sistema GPRS dovranno essere modificate in maniera tale da combinare in un unico nodo denominato IGSN (Internet GPRS Support Node) sia le funzionalità del SGSN che quelle del GGSN.
La struttura che assumerà la rete è rappresentata in figura:

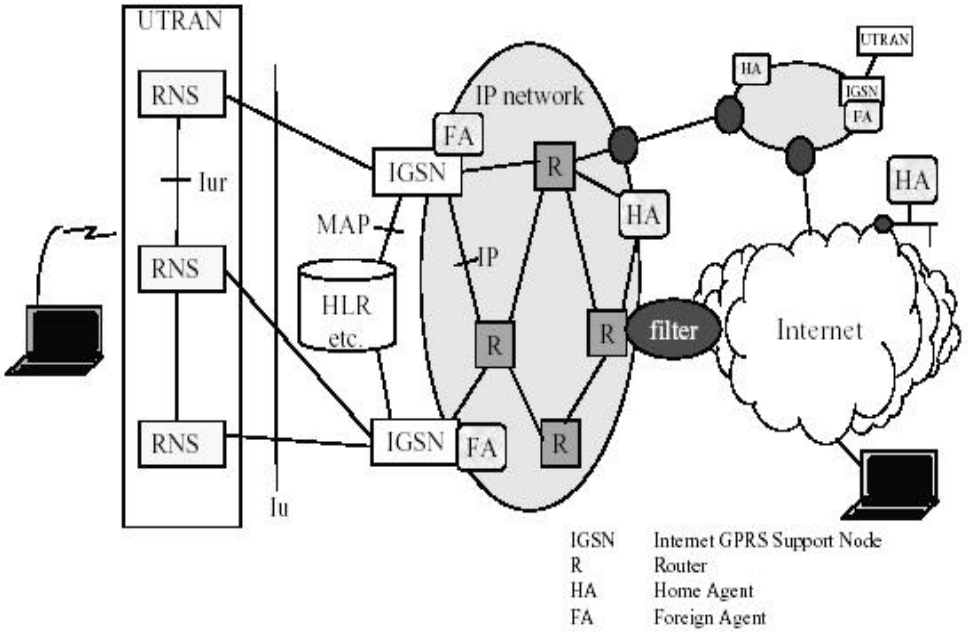


Figura 47: Target Architecture

Tutti i diagrammi di segnalazione descritti nei precedenti paragrafi dovranno essere modificati in maniera tale da rispettare la nuova architettura di rete; concettualmente la differenza più evidente sarà che lo scambio dei messaggi avverrà direttamente tra l'MS e l'IGSN.

Per concludere la descrizione di quest'ultimo stadio dello sviluppo, vengono mostrati i diagrammi temporali che caratterizzano la consegna di pacchetti IP tra un host della rete Internet (Correspondent Host) ed l'MS collegato al sistema GPRS. In figura 13 è rappresentato il caso in cui il datagramma inviato dal CH è intercettato dall'Home Agent prima di essere inviato all'IGSN, mentre in figura 14 il CH, attraverso la procedura Route Optimization descritta nel secondo capitolo, è in grado d'inviare il pacchetto direttamente all''IGSN. Per completezza sono mostrati anche i messaggi di paging necessari per individuare l'esatta posizione del MS all'interno della rete.

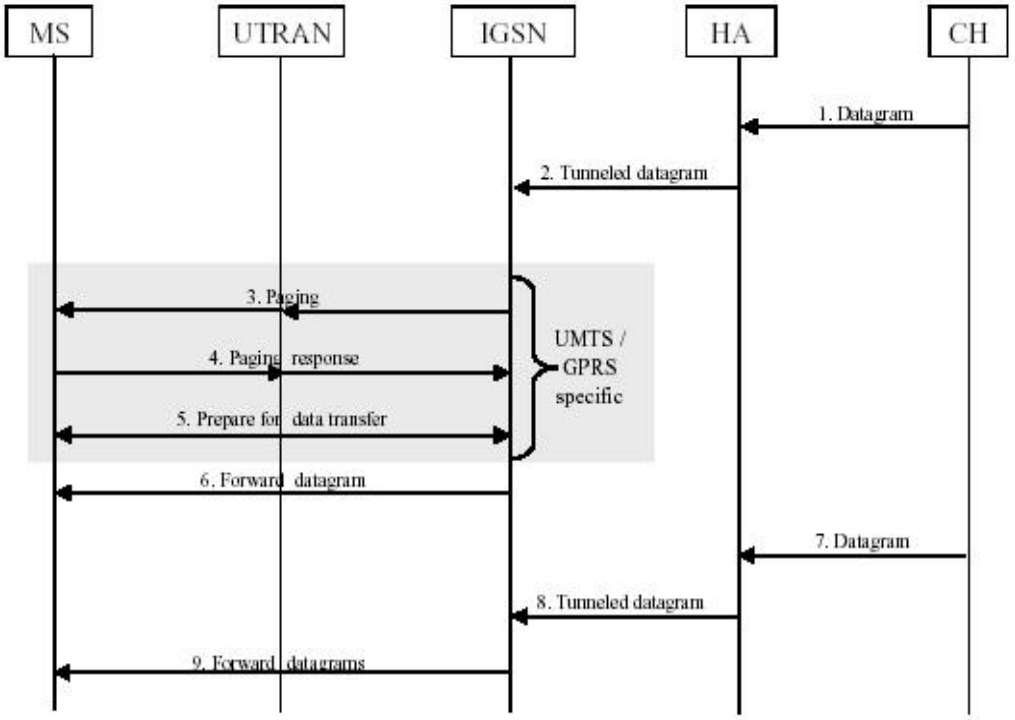


Figura 48:Consegna di pacchetti IP senza Router Optimization

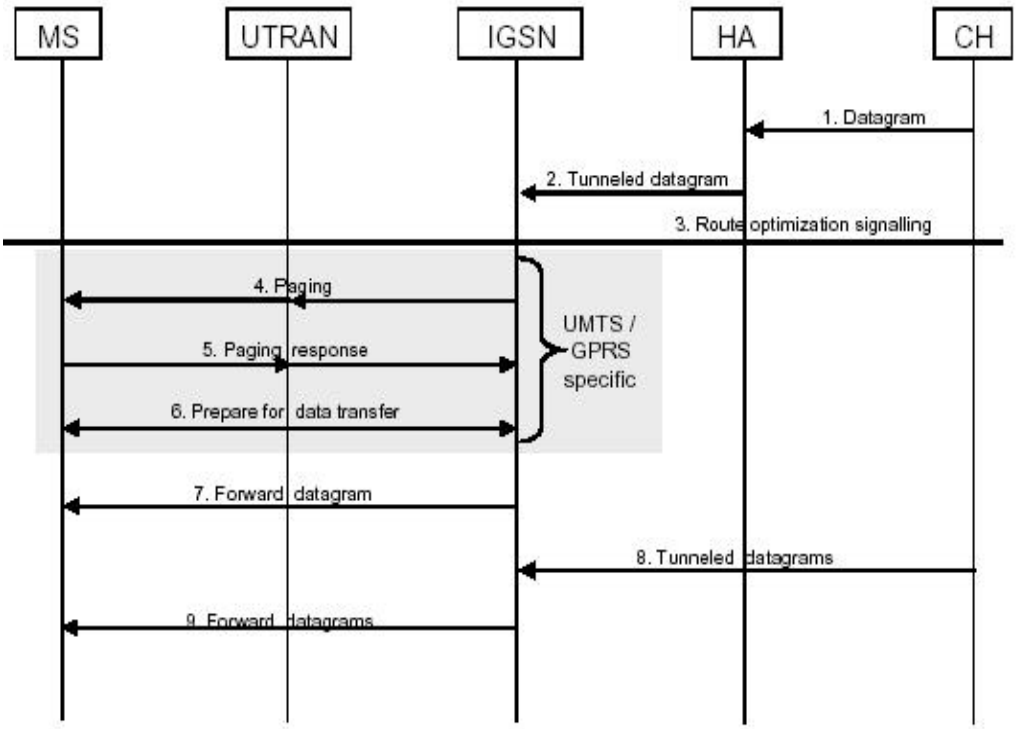


Figura 49: Consegna di pacchetti IP con l'utilizzo di Route Optimization

6 Internet Accounting

Attualmente, a causa del grande sviluppo della rete Internet e delle molteplici applicazioni usufruibili dall'utente (*video on demand, video conferecing, Internet radio, IP telephony, electronics commerce,* etc.), ha assunto un ruolo molto importante lo studio dell'Accounting Management. A dimostrazione del grande interesse nei confronti di tale settore è menzionabile il fatto che, all'interno dell'Internet Engineering Task Force, sia stato creato uno specifico Working Group denominato "*Authentication, Authorization and Accounting working group*".

Nel seguito del capitolo si fornirà una visione di tutte le problematiche e di tutti i diversi aspetti legati al concetto di accounting.

In particolare tra i diversi obiettivi dell'*Accounting Management*, si analizzeranno, con maggior dettaglio, le tematiche legate all'utilizzo dei dati di accounting per finalità di *billing*.

Si cercherà così di rispondere alle domande più comuni di tale settore:

Quali informazioni devono essere memorizzate? Quali sono le entità coinvolte nello scambio di tali informazioni? Cosa si deve pagare?

Infine, nell'ultima parte del capitolo, si individuerà un'architettura di accounting che possa soddisfare i requisiti del protocollo Mobile IP.

6.1 Generalità e terminologia

Come descritto in [35], l'obiettivo dell'Accounting Management è di monitorizzare il consumo delle risorse di rete per scopi di *Capacity and Trend Analysis, Auditing, Billing,* etc.:

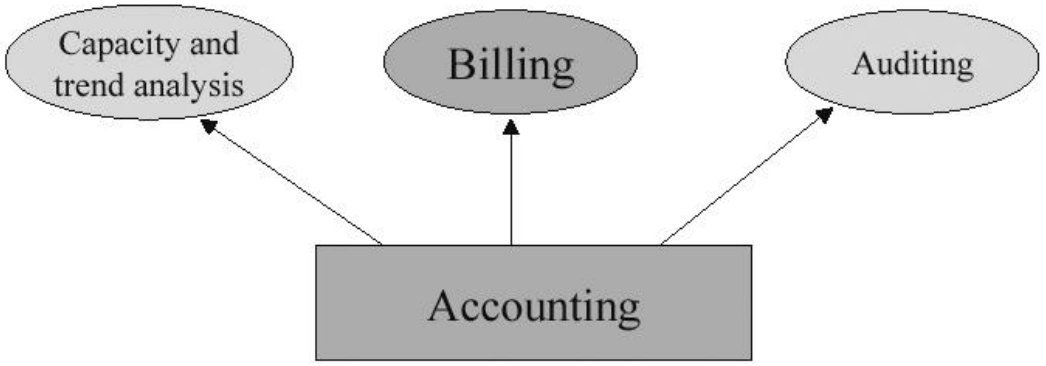


Figura 50: Finalità dell'Accounting Management

Con il termine *Capacity and Trend Analysis* si intende la capacità di sfruttare i dati di accounting per poter pianificare operazioni future, effettuare previsioni sull'utilizzo delle risorse.

Auditing rappresenta l'insieme delle operazioni svolte per verificare la correttezza di una certa procedura e quindi il rispetto di opportune regole. Per fornire un esempio si può ricordare che le procedure di Auditing sono normalmente incluse nei Service Level Agreement, cioè nelle specifiche che caratterizzano un contratto di servizio stipulato tra un Service Provider ed un utente (utente inteso in senso molto lato in quanto può essere un ulteriore Service Provider, un Content Provider oppure un utente finale). Infine le procedure di *Billing* sfruttano i dati di accounting per poter richiedere il pagamento di un servizio fornito all'utente.

In termini molto generali un'architettura di Accounting Management richiede l'iterazione tra dispositivi di rete, Accounting Server e Billing Server. Scopo dei dispositivi di rete è di "raccogliere" informazioni sul consumo delle risorse e di aggregarle secondo opportune regole. Tali informazioni dovranno poi essere elaborate da un Accounting server il cui obiettivo sarà quello di eliminare eventuali dati non necessari e generare dei *Session Record,* vale a dire effettuare un'ulteriore compattazione e suddivisione dei dati (ad esempio potrebbero essere creati dei Session Record che consentano di distinguere un traffico locale da quello che coinvolge domini differenti). Il ciclo si conclude con la "manipolazione", da parte di un Billing Server, dei Session Record. Si

noti che in questo contesto un Billing Server deve essere considerato come un'entità in grado di raggiungere le finalità sopra delineate e quindi potrà svolgere non solo le procedure di Billing, ma anche quelle di Auditing e Trend Analysis.

In questa visione generale del processo di accounting è necessario effettuare una distinzione tra i protocolli di Authentication, Authorization and Accounting (*AAA protocol*) ed i *Monitoring Tool*.

I protocolli AAA saranno analizzati nei prossimi capitoli quindi è sufficiente accennare che, attraverso il loro impiego, è possibile gestire la comunicazione tra server che amministrano informazioni di autenticazione, autorizzazione ed accounting. Per quanto riguarda l'accounting tali protocolli consentono di trasmettere un sotto-gruppo di tutti i possibili dati di accounting. In altre parole sono stati standardizzati per poter trasmettere informazioni come il numero di pacchetti inviati o ricevuti da un utente, ma non informazioni quali, ad esempio, il numero di e-mail inviate o ricevute dallo stesso utente (tale argomento sarà approfondito quando si analizzerà il concetto di Internet Protocol Data Record).

Scopo dei Monitoring Tool è di "analizzare" l'utilizzo delle risorse di una rete. A tale riguardo credo che sia interessante descrivere brevemente l'architettura proposta in [36]. Essa è composta da quattro entità (figura 51):

- *Meter*

  Ha il compito di suddividere i pacchetti che transitano (nella parte di rete da loro "gestita") in maniera tale da classificarli in flussi differenti.

- *Meter Reader*

  Memorizza e trasferisce le informazioni dei flussi tra il Meter e le Analysis Application.

- *Manager*

  Configura e controlla le attività di uno o più Meter e Meter Reader. Si basa sulle richieste delle applicazioni che fanno uso dei dati di accounting.

✍✍ *Analysis Application*

Rappresenta l'applicazione che necessità dei dati di accounting.

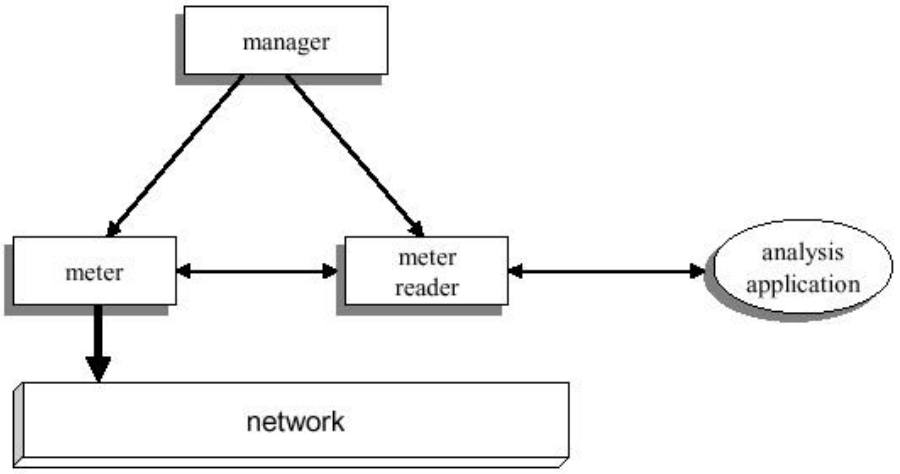


Figura 51: RTFM Architecture

L'architettura sopra descritta prende il nome di *Real-Time Traffic Flow Measurement* e si basa sul concetto di flusso di dati. Il Meter deve essere in grado di separare i pacchetti appartenenti a flussi differenti:
tutti i pacchetti appartenenti ad uno specifico flusso devono soddisfare un set di attributi forniti al Meter dal Manager. L'esempio più immediato è quello di suddividere i flussi in base ai campi Source Address e Destination Address dell'header IP.
Alcune ottimizzazioni dell'architettura sopra citata prevedono la suddivisione dei pacchetti, in flussi differenti, attraverso l'utilizzo del protocollo Resource Reservation Protocol (RSVP) di cui non si entrerà in merito [37].

Con riferimento all'utilizzo dei dati di accounting per finalità di billing si può cercare di chiarire ulteriormente le fasi che costituiscono un processo di accounting:

- *Metering*

  Rappresenta il processo di monitorizzazione del consumo delle risorse di rete da parte di un utente.

- *Pricing*

  Processo che consente di definire un costo per unità, permette quindi di assegnare un prezzo all'unità di misura prescelta per quantificare l'utilizzo delle risorse.

- *Charcing*

  Processo che quantifica l'intero utilizzo delle risorse attraverso l'informazione pervenutagli dal processo di Pricing.

Infine il processo di billing utilizzando le informazioni di charging e quelle relative ad eventuali accordi tra il fornitore del servizio e l'utente (agevolazioni, sconti, etc.) permetterà di "fatturare" l'utente stesso. In letteratura la definizione del processo di billing è la seguente: "*The act of preparing an invoice*".

6.2 Classificazione del processo di accounting

Nel precedente paragrafo si è cercato di fornire una visione globale del concetto di accounting e nello stesso tempo si è riusciti ad individuare un primo gruppo di entità architetturali coinvolte nello scambio dei dati di accounting.

Si è utilizzato il termine "dati di accounting" per poter mantenere un certo livello di astrazione in maniera tale da affrontare, in questa sede, il problema legato alla classificazione degli stessi.

Il quesito iniziale "Cosa si deve pagare ?" consente di effettuare la seguente distinzione [38]:

- *Content/Service Accounting*

  L'utente deve pagare il servizio da lui richiesto. Questo significa che i parametri che devono essere considerati sono quelli legati al "tipo" di richiesta effettuata dall'utente. Esempi possono essere video clips, contenuti di pagine web, servizi di e-mail, etc.

- *Trasport Accounting*

  L'utente deve sostenere le spese legate alla consegna del servizio richiesto. E' quindi necessario verificare l'utilizzo delle risorse di rete. Inoltre, in previsione della possibilità di consentire ad un utente di scegliere la qualità con cui ottenere il servizio, sarà essenziale monetizzare in maniera differente tale qualità.

A prima vista la classificazione introdotta può apparire superflua in quanto i parametri legati al Transport Acounting potrebbero essere inglobati in quelli relativi al Content/Service Accounting. In realtà tale visione è sbagliata e per capirne il motivo si faccia riferimento alla figura 52 nella quale sono rappresentati un utente, il relativo Internet Service Provider (ISP), dei Backobone Provider che consentono il trasferimento di informazioni tra più ISP ed un Content Provider che può essere considerato come il proprietario del servizio:

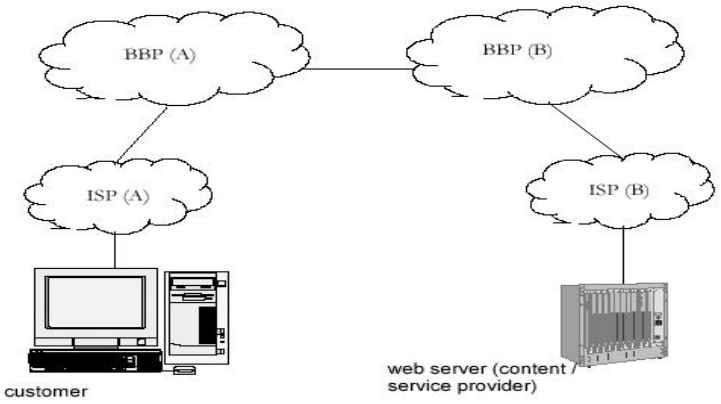


Figura 52: Entità coinvolte nella fornitura di un servizio

Inglobare i parametri relativi al Transport Accounting con quelli del Content/Service Accounting significherebbe non prendere in considerazione, ad esempio, eventuali *free content*: si consideri la situazione nella quale il Content Provider metta a disposizione un servizio gratuito, è chiaro che gli ISP ed i BBP coinvolti valuterebbero in maniera antieconomica la fornitura di tale servizio al customer.

6.3 Transport Accounting

Dopo aver specificato il significato del concetto di *Transport Accounting* è necessario individuare l'insieme dei parametri che caratterizzano l'utilizzo delle risorse di rete.
A tale scopo è utile considerare due differenti tipi di approccio [39]:

- *Botton-up Approach*

  Tenendo presente gli attuali protocolli e tecnologie di rete, quali variabili occorre misurare?

- *Top-down Approach*

  Date le differenti strategie di prezzo applicabili, quali variabili occorre misurare?

6.3.1 Botton-up Approach

Considerando il protocollo IP è intuibile che i parametri utilizzabili per scopi di accounting possono essere ricercati all'interno dei stessi pacchetti IP.
In particolare si può effettuare un'analisi dei campi che costituisco l'header del datagramma, distinguendo il protocollo IPv4 da quello IPv6.

6.3.1.1 Parametri basati sui campi dell'header IPv4

Il formato dell'header IPv4 è mostrato in figura:

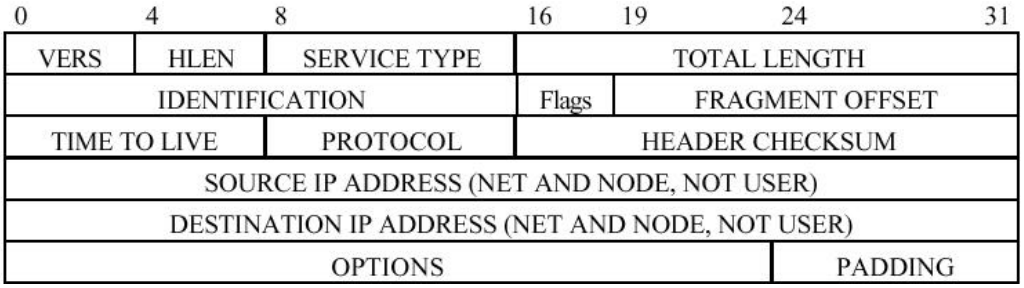


Figura 53:Header IPv4

L'obiettivo è di individuare quali campi "contengono" informazioni utili ai fini del processo di accounting:

- Version

  Attualmente vi sono due versioni del protocollo (IPv4 e IPv6) e quindi può essere utile distinguerli in maniera netta. Ad esempio un ISP, che desidera migrare da IPv4 a IPv6, potrebbe adottare tariffe differenti a seconda del protocollo.

- Header Length

  In combinazione con il campo Total Length consente di determinare la lunghezza totale del pacchetto permettendo così di fornire dati di accounting basati sul numero totale di byte trasferiti.

- Type of Service

  Tale campo può essere sfruttato per introdurre il concetto di qualità del servizio e quindi ai fini dell'accounting risulta molto importante.

- Identification

  Tale campo, come del resto il Time To Live, il Fragmentation offset e l'Header Checksum, non contiene informazioni utili al processo di accounting.

- Flags

  Sono utilizzati per gestire la frammentazione di un datagramma: indicano se il pacchetto contiene un frammento oppure se il pacchetto non può essere frammentato.

  Teoricamente tale conoscenza può essere sfruttata per scopi di accounting: un ISP può decidere, ad esempio, di fornire un "peso" maggiore (in termini monetari) ad un pacchetto non frammentabile.

- Protocol

  Indica il protocollo di livello superiore a cui consegnare il datagramma: protocolli differenti possono essere considerati, dal punto di vista dell'accounting, in maniera differente.

- Source Address e Destination Address

  A differenza della rete telefonica non è possibile implementare un criterio di tariffazione in grado di distinguere: traffico locale, traffico regionale, traffico nazionale e traffico internazionale.

  Attraverso le informazioni contenute nelle tabelle di routing è però fattibile la differenziazione tra traffico locale (nell'ambito cioè di uno stesso ISP) e traffico non locale, che coinvolge quindi più ISP:

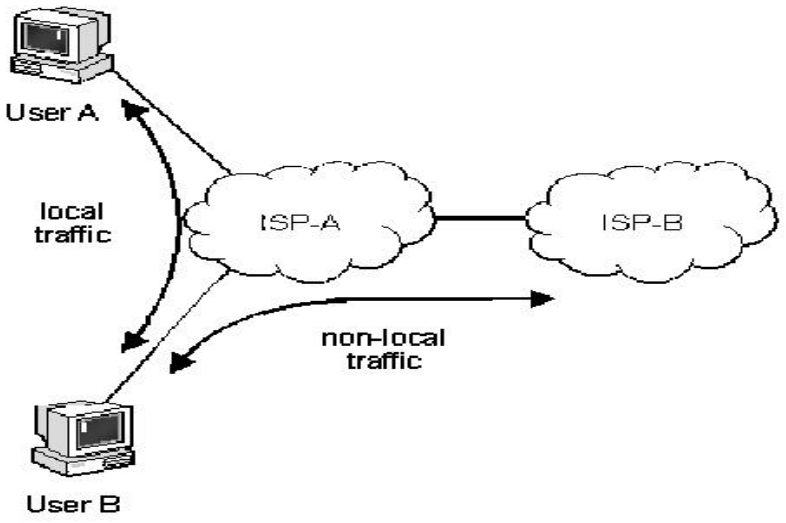


Figura 54: Traffico locale e non locale

La possibilità o meno di impiegare i vari campi che costituiscono l'Header del pacchetto IP per scopi di accounting è riassunta nella seguente tabella:

IP Header Filed	Parametro per accounting
Version	SI
Header Length	SI
Type of Service	SI
Total Length	SI
Identification	NO
Flags	SI
Fragmentation offset	NO
Time To Live	NO
Protocol	SI
Header Checksum	NO
Src and Dst Address	SI
Option	Non preso in considerazione

Tabella 6: Parametri per accounting basati sull'Header IPv4

6.3.1.2 Parametri basati sui campi dell'header IPv6

Per non ripetere le stesse considerazioni effettuate nel precedente paragrafo è sufficiente notare come, l'analisi dei vari campi che costituiscono l'Header del datagramma IPv6 (svolta nel capitolo 3), consenta di escludere come dato di accounting il solo campo Hop Limit.
Schematicamente si può riportare la seguente tabella:

IP Header Filed	Parametro per accounting
Versione	SI
Priorità	SI
Flow Label	SI
Payload Length	SI
Next Header	SI
Hop Limit	NO
Src and Dst Address	SI

Tabella 7: Parametri per accounting basati sull'Header IPv6

6.3.2 Top-down Approach

Come menzionato precedentemente si vogliono determinare i parametri utilizzabili, per scopi di accounting, considerando come punto di partenza le diverse strategie di prezzo applicabili dai fornitori di servizio.
Nonostante esistano molti *pricing scheme,* tutti possono essere considerati come la combinazione di due schemi basilari:

- *Flat Rate*
- *Usage Based*

Lo shema Flat Rate è suddivisible in *Pure Flat Rate* ed in *Restricted Flat Rate,* mentre lo schema Usage Based può essere utilizzato con una modalità di prezzo costante (*Static Pricing*) oppure no (*Dynamic Pricing*):

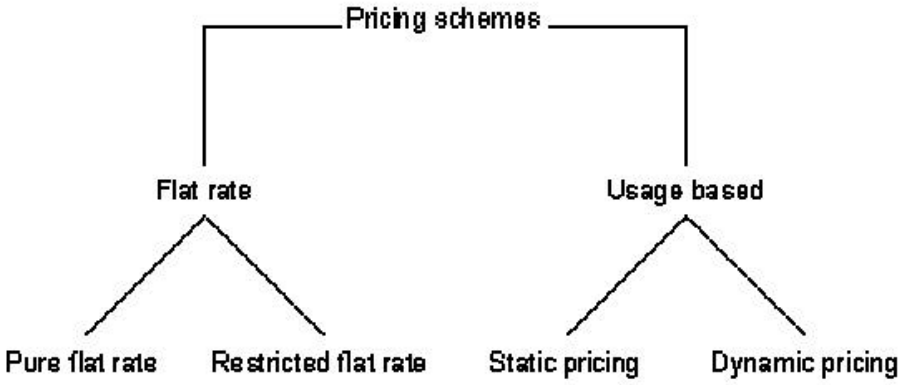


Figura 55: Pricing Schemes

Con lo schema **Flat Rate** l'utente paga una somma stabilita per la durata di un certo periodo.
In particolare nel caso di **Pure Flat Rate** non ci sono restrizioni o limiti sull'utilizzo delle risorse. Da ciò deriva che non sono necessari dati di accounting per finalità di billing.

Il modello **Restricted Flat Rate** richiede che tra utente e fornitore del servizio vi sia una "relazione" più stretta: l'utente può richiedere un servizio con delle limitazioni stabilite a priori. Un esempio di restrizione può essere quella in cui l'utente può sfruttare le linee d'accesso, messe a disposizione dall'ISP, solamente per un certo numero di giorni nell'ambito di un mese. Nel caso in cui l'utente ecceda tale limite, il fornitore del servizio può:

- negare l'accesso;
- addebitare all'utente un costo aggiuntivo;
- aggiornare il contratto;
- non prendere nessun tipo di provvedimento.

Si noti che il secondo ed il terzo caso sono una combinazione degli schemi Flat Rate e Usage Based, mentre il quarto caso rispecchia la modalità Pure Flat Rate (non ci sono restrizioni)..
Dalla descrizione effettuata deriva che lo schema Restricted Flat Rate richiede il controllo delle risorse per due motivi differenti:

- verificare che l'utente ecceda o no quanto stabilito nel contratto;
- monitorizzare lo sfruttamento delle risorse per prendere dei provvedimenti nel caso in cui l'utente superi il limite.

I parametri che dovranno essere presi in considerazione sono, in linea di principio, gli stessi di quelli che saranno considerati nel caso del modello Usage Based.
Lo schema **Usage Based** incentiva l'utente a "comportarsi" in un modo tale da non provocare aggravi eccessivi alla rete, evitare ad esempio delle situazioni di congestione.

E' possibile utilizzare la modalità Usage Based con prezzo per unità di consumo fisso oppure dinamico. Nel primo caso il prezzo è stabilito a priori mentre nel secondo caso può subire degli aggiornamenti in base, ad esempio, al carico della rete.
Un insieme di possibili dati di accounting utilizzabile sono:
volume, durata, distanza, larghezza di banda, qualità del servizio, orario della giornata.

6.3.2.1 Volume

Basare il processo di Billing sul parametro volume (ad esempio numero di pacchetti) consente, in un certo senso, di limitare la quantità di dati trasferiti dall'utente.
Vi è solo una questione ancora irrisolta: l'eventuale ritrasmissione del pacchetto deve essere addebitata all'utente oppure no?
Inoltre, la monitorizzazione di tale parametro deve essere effettuata in un punto della rete nella quale vi sia una stretta "relazione" tra utente e fornitore del servizio come ad esempio nei router d'accesso di un ISP o nei border router di una backbone network.

6.3.2.2 Durata

Dato che la rete Internet sfrutta il principio della commutazione a pacchetto e non quello a circuito, come nel caso della rete telefonica, il concetto di durata non deve essere legato a quello di durata temporale di una connessione, ma a quello di "flusso" di pacchetti.
I moderni router sono in grado di aggregare i pacchetti, da loro gestiti, in flussi differenti, associando ad un flusso l'insieme dei pacchetti che "viaggiano" tra due stessi endpoint della rete.
In tal senso può essere quantifica la durata di un flusso in maniera tale da addebitare all'utente solamente l'effettivo periodo di tempo in cui invia o riceve dati.

Anche in questo caso i dispositivi interessati sono i boreder router ed i router d'accesso.

6.3.2.3 Distanza

Si è già discusso di tale parametro, quindi è sufficiente ricordare la possibilità di sfruttare come dato di accounting la circostanza di considerare un traffico locale oppure no "individuabile" dai border router.

6.3.2.4 Larghezza di banda

E' possibile attribuire ad un utente costi differenti a seconda della capacità della loro connessione ad Internet.
Ad esempio un parametro utilizzabile potrebbe essere il *peak-bandwith* sostenibile dalla linea d'accesso.

6.3.2.5 Qualità del servizio

L'attuale tendenza della rete Internet è di individuare dei meccanismi che consentano di affiancare alla caratteristica *Best Effort* la fornitura di servizi con differenti livelli di qualità.
Per evitare che tutti gli utenti scelgano la classe di servizio con qualità maggiore, è necessario introdurre una differenziazione delle tariffe che tenga conto della qualità richiesta dall'utente.
Come nel caso degli altri parametri, i dispositivi in grado di individuare la classe di servizio dovranno essere situati sia nei router d'accesso che nei boreder router.

6.3.2.6 Orario della giornata

Infine se la congestione della rete occorre in periodi di tempo regolari ed identificabili, è possibile introdurre delle tariffe che incoraggino gli utenti ad occupare risorse di rete nelle ore più "scariche".

6.4 Internet Protocol Data Record

Nei precedenti paragrafi si è focalizzata l'attenzione sull'individuazione delle entità architetturali e sui possibili parametri caratterizzanti lo sfruttamento delle risorse.

In una visione globale, è intuibile che il processo di accounting debba agire su delle informazioni completamente differenti fra di loro.

In altre parole, occorre tener presente, la necessità di manipolare dati di accounting provenienti, ad esempio, da un *Mail Server*, da un *Content Delivery*, da un *Web Server*, da un Server in grado di dialogare tramite i protocolli AAA (ad esempio un *Radius Server*), etc.

Questo significa che in un ambiente reale è possibile effettuare accounting su delle risorse che presentano caratteristiche disomogenee fra di loro.

Una possibile soluzione a tale problema è di standardizzare il formato dei dati accounting, lavoro che, all'interno dell'organizzazione denominata *ipdr.org*, sta conducendo allo sviluppo di un Internet Protocol Data Record [40].

Il modello che caratterizza lo scambio di informazioni, denominato **IPDR Reference Model**, è concettualmente suddivisibile in tre strati:

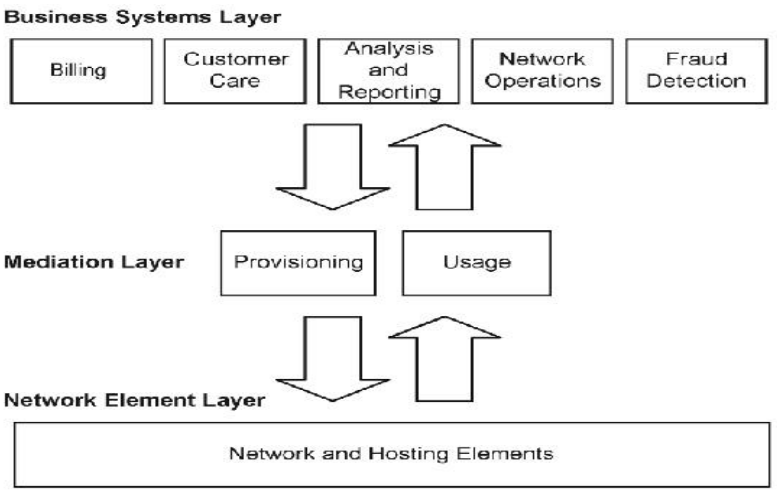


Figura 56: IPDR Reference Model

- *Network and service element layer (NSE)*

  Consiste in tutti gli elementi di rete e risorse di rete utili ai fini dell'acquisizione di dati di accounting.

- *Mediation Layer*

  Svolge un duplice compito:
  in termini di *Usage Collection* deve prelevare dal Network and service element layer le informazioni richieste dal Business System Layer; inoltre deve essere in grado di trasferire *provisioning information* dal BSS al NSE (un esempio d'informazione di provisioning può essere l'account di un utente che necessita di essere inserito in un mail-server).

- *Business support system (BSS) layer*

  Comprende tutti i sistemi impiegati da un fornitore di servizio per svolgere *business operation.*

Con specifico interesse all'Internet Protocol Data Record il flusso che si andrà a particolareggiare è quello precedentemente denominato Usage Collection.
Nella figura successiva è mostrata l'architettura relativa a tale flusso, si osservi come il Mediation Layer aggreghi le informazioni provenienti dai diversi dispositivi in maniera tale da fornire al BSS layer una struttura dati compatta e caratterizzata da un set di informazioni standard.
Le informazioni contenute nell'IPDR saranno tali da poter descrivere, in maniera particolareggiata, l'utilizzo della risorsa. Vi saranno informazioni circa "l'identità" dell'utente, il periodo temporale caratterizzante l'utilizzo della risorsa, che tipo di parametri si vuole trasferire, il tipo di risorsa utilizzata ed infine il motivo per cui i dispositivi necessitano di comunicare informazioni.

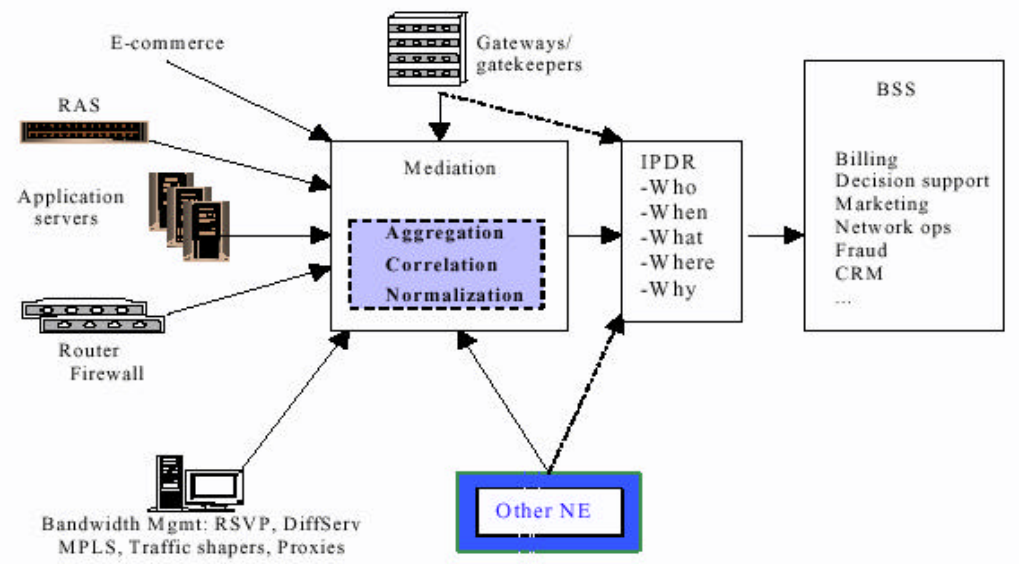


Figura 57: IPDR Record flow

6.4.1 IPDR Interface

Un'analisi più approfondita del Mediation Layer richiede l'introduzione di nuove entità architetturali e di interfacce che consentano lo scambio di informazio ni.

Di seguito è riportato uno schema più dettagliato del Mediation Layer; per completezza, anche se non si fornirà una descrizione degli strati protocollari, sono rappresentate, mediante lettere, le interfacce poste tra le rispettive entità.

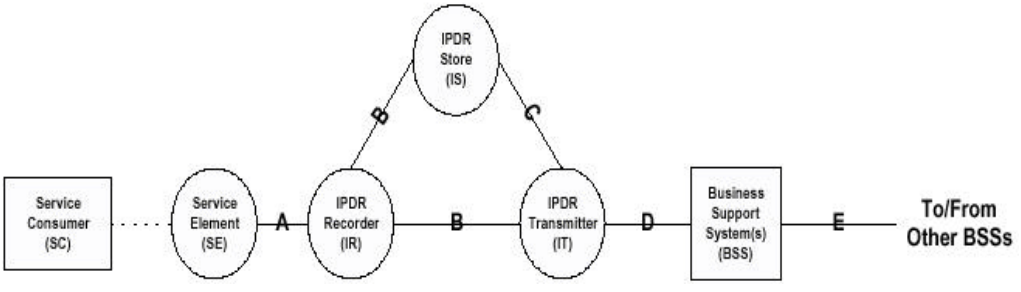


Figura 58: Modello dettagliato del Mediation Layer

Il compito svolto dalle diverse entità è il seguente:

- *Service Consumer*

  Rappresenta l'utente finale di un servizio.

- *Service Element*

  Forniscono accesso alle risorse richieste dall'utente ed effettuano la monitorizzazione delle stesse.

- *IPDR Record*

  Preleva informazioni dal Service Element e le compatta in Internet Protocol Data Record.

- *IPDR Trasmitter*

  Consegna le IPDR al Business Support System.

- *IPDR Store*

  Consente di mantenere in memorie non volatili le IPDR.

6.5 Accounting Architecture

Attualmente non vi sono delle architetture standardizzate per scopi di accounting, è però possibile descrivere le proposte fornite dal gruppo di ricerca denominato *Internet Next Generation*.
In particolare, si può prendere in considerazione l'architettura denominata ***Provider Based Accounting Architecture (PBA)*** [41] ottimizzata per consentire il pagamento e la consegna di un *content*. Da ciò deriva che lo scopo di tale architettura è di implementare *Accounting for content*, con la caratteristica che il pagamento del content sarà effettuata dall'Internet Service Provider dell'utente. E' chiaro che periodicamente l'ISP eseguirà dei *financial balance* sia nei confronti dell'utente che in quelli del Content Provider.
In figura è schematizzata l'architettura PBA, o meglio è rappresentato lo scambio di informazioni tra le differenti entità:

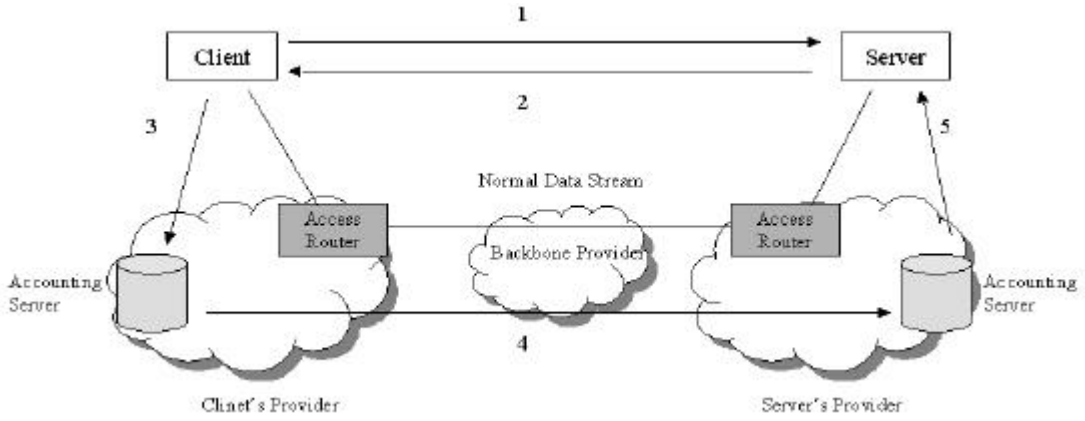


Figura 59: Provider Based Accounting Architecture

L'architettura prevede un *client* connesso ad un ISP ed un *server* (facente parte di un'organizzazione proprietaria del content) connesso ad un altro ISP. Tra i due fornitori di servizio vi possono essere uno o più Backbone Provider.
Il processo inizia con la richiesta, da parte del client, della "consegna" di un content (1). A sua volta il server invierà un *accounting request message* (2) nel quale richiederà il pagamento del content e specificherà le caratteristiche del content. In particolare il messaggio potrà contenere i seguenti parametri:

- *Server Information*

  Consiste nell'insieme delle informazioni necessarie per identificare il proprietario del server e per svolgere operazioni di autenticazione nei riguardi dei successivi messaggi.

- *Price*

  Specifica la metrica utilizzabile per stabilire il prezzo del content.

- *Content Type*

  Caratterizza il content che sarà consegnato.

- *Accounting Server Information*

Consente di specificare l'indirizzo dell'Accounting Server che risiede nel *Server's Provider* ed il meccanismo di autenticazione da utilizzare con lo stesso.

Se il client decide di accettare le richieste del server rilancerà le informazioni sopra descritte all'Accounting Server del proprio Internet Service Provider (3). Il server aggiornerà il bilancio del'utente e invierà un *accounting accepted message* (4).
Infine la trasmissione del content avrà inizio non appena il server riceve un messaggio di conferma da parte dell'Accounting Server.
Anche se non specificato, vi dovranno essere dei meccanismi che consentano ai due ISP di essere remunerati per le risorse di rete occupate nel trasferimento del content, e quindi saranno attuate delle procedure di Transport Accounting.
Come accennato in un precedente paragrafo, vi può essere la situazione nella quale il Content Provider decida di fornire, ad un qualsiasi utente della rete Internet, un servizio gratuito con la condizione di non "caricare" su se stesso le spese di trasporto.
In tal caso si parla di *Reverse Charging* :
il client, che desidera ricevere il content, dovrà sostenere le spese di trasporto dell'Internt Service Provider che controlla il Content Provider.
L'architettura attraverso la quale è possibile implementare la procedura Reverse Charging è molto simile a quella descritta sopra; per completezza si riporta il seguente schema, tratto da [42], in cui si evidenzia una entità denominata *Trusted Third Party* (che teoricamente potrebbe essere una banca) che svolge il compito di verificare il corretto svolgimento dei *financial balance* tra gli ISP coinvolti. La differenza rispetto al caso precedente consiste nella circostanza che le diverse entità coinvolte devono essere a conoscenza che il trasferimento del content sarà del tipo reverse charging, in particolare, il Server ISP deve poter implementare la procedura Transport Accounting nei confronti del Client e non del Server. Per questo motivo, i router d'accesso dovranno essere configurati in maniera tale da disporre delle informazioni necessarie per individuare i pacchetti relativi al *reversed traffic*.

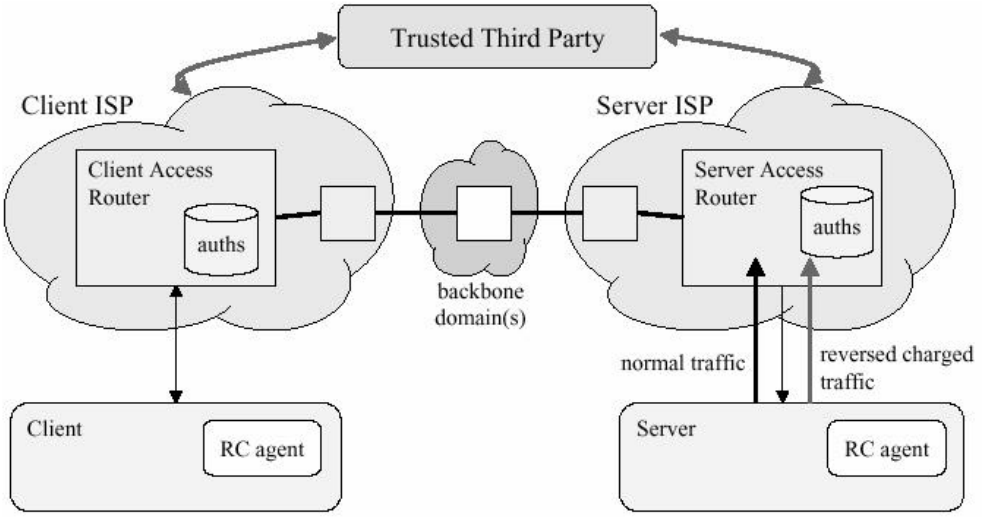


Figura 60: Reverse Charging Architecture

6.6 Accounting Architecture for Mobile IP

Lo sviluppo del protocollo Mobile IP richiede di apportare delle modifiche alle architetture analizzate precedentemente.

E' intuibile la necessità di coinvolgere, nelle procedure di accounting, non solo l'ISP con il quale il Mobile Node ha stipulato una forma di contratto (*Home ISP*), ma anche il fornitore di servizio che mette a disposizione le proprie risorse in caso di *roaming* del Mobile Node (*Foreign ISP*).

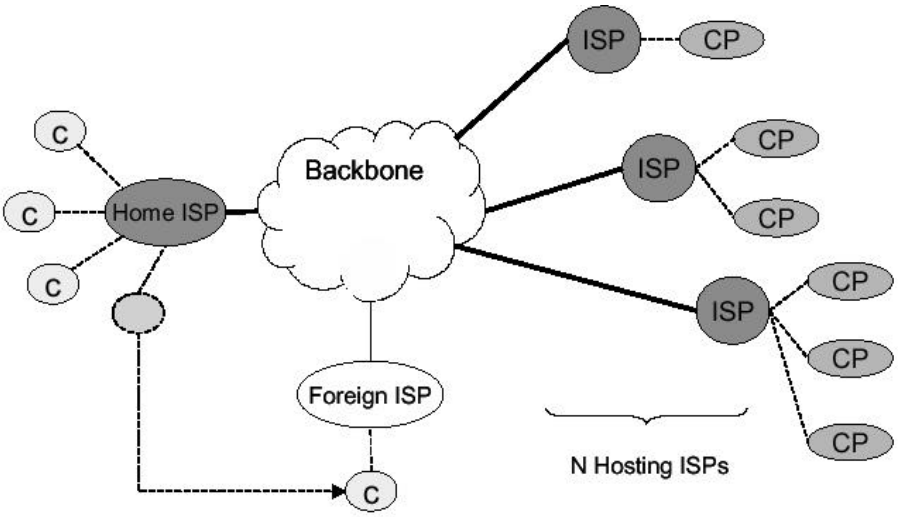


Figura 61: Home ISP a Foreign ISP

Per questo motivo si vuole estendere la Provider Based Accounting Architecture in maniera tale da poter contemplare la mobilità degli host.
Sono possibili due tipi di soluzione [43]:

- *Centralized Accounting*

  Tutti i messaggi di richiesta di pagamento di un content (*Payment Request*) inviati da un Content Provider al Mobile Node ed i relativi *Payment Acknowledgement* devono transitare per l'Home ISP. In questo scenario l'Home ISP si incarica di remunerare (sempre tramite dei *financial bilance*) sia l'ISP che controlla il Content Provider sia il Foreign ISP che fornisce accesso al Mobile Node.

- *Accounting by Delegation*

  L'Home ISP delega al Foreign ISP la gestione dei messaggi sopra menzionati. Al termine della sessione (o di un periodo temporale definito a priori) il Foreign ISP invierà un *accounting records* all'home ISP dettagliando tutti i costi sostenuti per soddisfare le richieste del Mobile Node.

Una descrizione più dettagliata delle soluzioni proposte può essere effettuata attraverso l'analisi di diagrammi temporali che caratterizzano il flusso dei *Payment Request Message* e dei *Payment Acknowledgement Message.*
Per ciascuna soluzione saranno prese in considerazione due categorie differenti:

- analisi del solo processo di *Content Accounting*;

- generalizzazione del processo attraverso l'inclusione dell'accounting di eventuali servizi di valore aggiunto (*Integrated Accounting*) come ad esempio: funzionalità svolte dal Foreign Agent (decapsulamento e rilancio di pacchetti IP, tunneling, etc.), qualità del content, etc.

6.6.1 Centralized Accounting

La figura 62 illustra il flusso di messaggi relativi al solo *Content Accounting.*

Il diagramma presuppone il precedente scambio di messaggi di richiesta del content tra il Mobile Node (Client) ed il Content Provider.

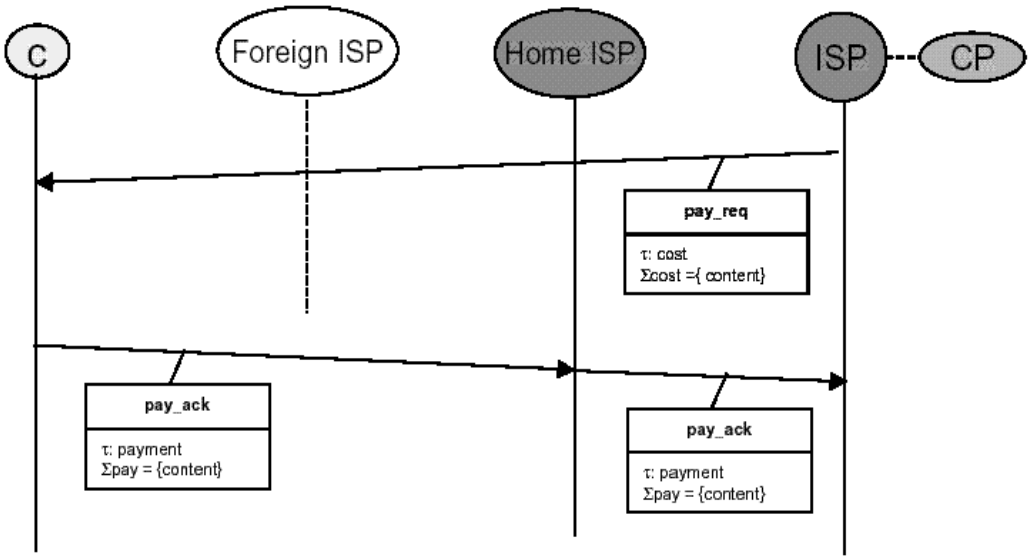


Figura 62: Centralized Accounting: Content Accounting only

Descrizione:

1? Il Content Provider invia un Payment Request al Mobile Node.

2? Il Mobile Node accetta le richieste del Content Provider ed invia un Payment Acknowledgement all'Home ISP.

3? L'Home ISP conclude la transizione rilanciando il messaggio al Content Provider

Nel caso di *Integrated Accounting* il flusso è rappresentato in figura 14: rappresenta la situazione più completa, il Payment Request che giungerà al Mobile Node non conterrà solamente le indicazione circa il prezzo del content, ma anche quelle relative al valore aggiunto del content e del Foreign ISP.

In questa circostanza l'Home ISP dovrà inviare due Payment Acknowledgement Message: uno per il Content Provider ed uno per il Foreign ISP.

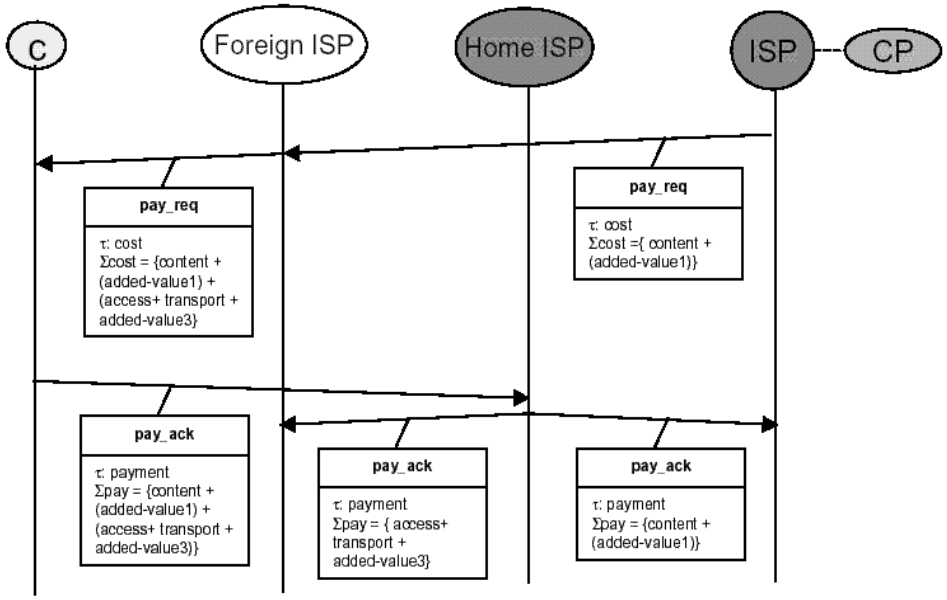


Figura 63: Centralized Accounting: Integrated Accounting

6.6.2 Accounting by Delegation

Di seguito sono riportati i diagrammi temporali relativi al solo *Content Accounting* ed all'*Integrated Accounting*.

La descrizione dei due schemi è superflua, è però necessario sottolineare l'importanza dei protocolli AAA:

il Foreign ISP si assumerà la responsabilità di autorizzare la consegna di un content solamente dopo aver verificato, con l'Home ISP, le credenziali del Mobile Node.

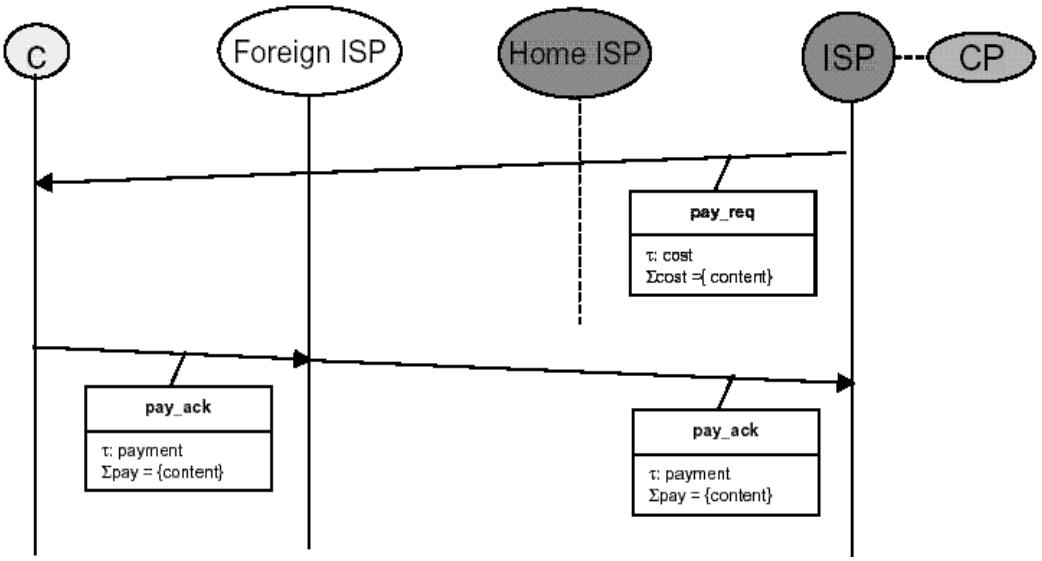


Figura 64: Accounting by Delegation: Content Accounting only

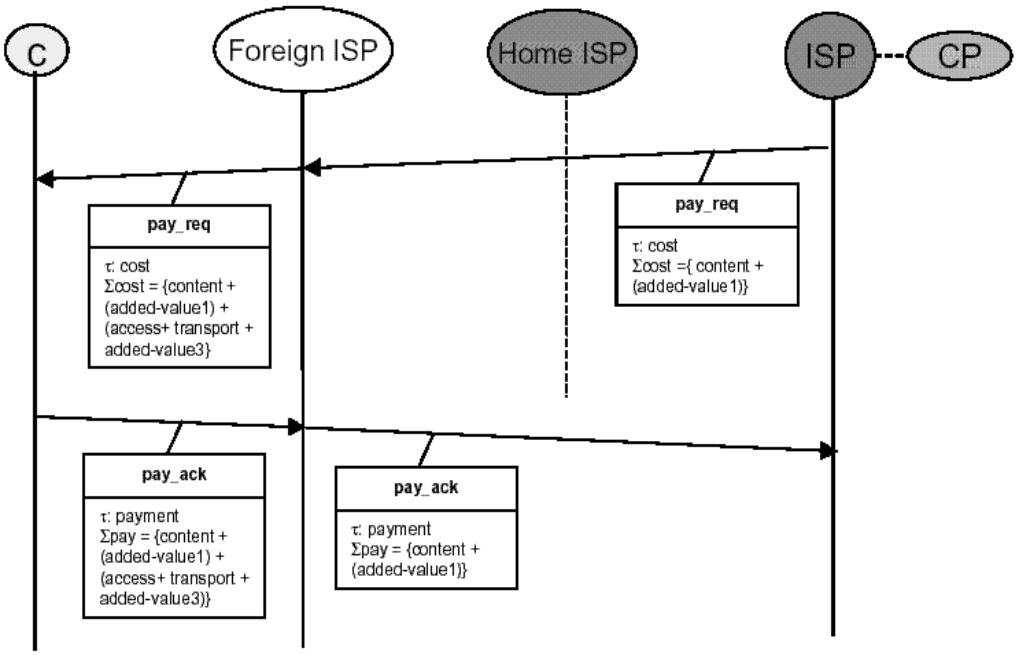


Figura 65: Accounting by Delegation: Integrated Accounting

7 Mobile IP e le procedure AAA

Molti degli attuali operatori di telefonia cellulare ed Internet Service Provider (ISP) autorizzano un utente ad usufruire delle proprie infrastrutture solamente dopo averlo autenticato; una volta verificatene le "credenziali", possono eseguire un monitoraggio dello sfruttamento delle risorse con lo scopo, ad esempio, di richiedere un eventuale pagamento del servizio offerto.
E' intuibile la necessità di rendere lo standard Mobile IP, precisato in [1], compatibile con il meccanismo sopra definito e generalmente denominato servizio di **Authentication, Authorizatione Accounting (AAA)**.
Vi sono diverse implementazioni dei servizi AAA, nel presente capitolo si fornirà una descrizione del protocollo Radius (che in un certo senso può essere considerato come uno standard tra i diversi ISP) ed una visione di ciò che rappresenta la naturale evoluzione di Radius, cioè il protocollo Diameter.
L'obiettivo sarà quello di introdurre un modello AAA utilizzabile da Mobile IP e sarà raggiunto descrivendo in maniera graduale le seguenti specifiche:

- specifiche basilari del modello;
- specifiche legate alle esigenze di connettività proprie del protocollo IP;
- specifiche legate alle particolari richieste del protocollo Mobile IP.

7.1 Radius

Radius è l'acronimo di Remote Authentication Dial In User Service e rappresenta il protocollo più diffuso per l'implementazione del servizio AAA [44]. Consente di autenticare le credenziali di un utente, autorizzare l'utente ad

instaurare una connessione ed eventualmente procedere all'accounting dello stesso.
Il protocollo si basa sul paradigma client/server:

- un *Network Access Server* (NAS) opera come un client di Radius: riceve le richieste di connessione da parte dell'utente e fornisce al Radius Server le informazioni che consentono l'autenticazione dello stesso;
- un *Radius Server*, attraverso la consultazione di un database, verificherà le credenziali dell'utente e fornirà al NAS le informazioni necessarie per soddisfare o meno la richiesta di connessione. Inoltre il Radius server può agire come un proxy client verso altri Radius server o altri tipi di server di autenticazione.

Le transazioni tra client e Radius server sono autenticate attraverso l'uso di meccanismi di crittografia. Inoltre ogni password d'utente è scambiata in modalità criptata tra client e server.

Il Radius server può supportare molti metodi di autenticazione utente. Quando l'utente fornisce username e password può supportare PAP (*Password Authentication Protocol Challenge*), CHAP (*Handshake Authentication Protocol*) ed altri meccanismi di autenticazione.

7.1.1 Operazioni

L'insieme delle operazioni che vanno dalla richiesta di connessione da parte dell'utente fino all'eventuale fornitura del servizio possono essere riassunte come segue:

- l'utente che desidera instaurare una connessione deve fornire al client (NAS) le informazioni necessarie per l'autenticazione. Tale obiettivo

può essere raggiunto attraverso l'utilizzo di un *login prompt*, nel quale l'utente inserirà user-name e password, oppure attraverso l'impiego di protocolli di collegamento, come il *Point to Point Protocol* (PPP), che consentono di determinare le informazioni sopra esposte nella fase di negoziazione dei parametri;

- una volta ottenute queste informazioni, il client invierà un messaggio di **Access Request** al Radius server. Tale messaggio conterrà una serie di attributi (*Attribute Value Pair*) che permetteranno di comunicare user-name e password dell'utente, l'identificativo del NAS che ha generato la richiesta ed ulteriori informazioni che consentiranno di caratterizzare il servizio da offrire all'utente. Il formato di un Access Request Message è mostrato in figura:

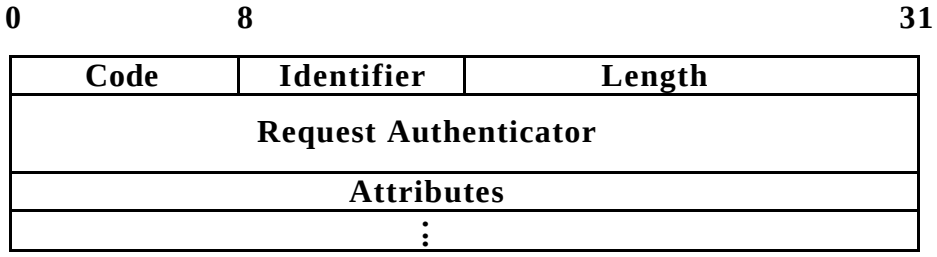


Figura 66: Access Request Message

Il campo *Code* consentirà di distinguere il tipo di messaggio, *Identifier* e *Request Autehnticator* sono utilizzati per scopi di autenticazione delle informazioni scambiate tra NAS e Server.
Infine la struttura degli attributi risulta:

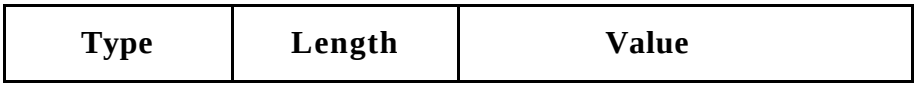


Figura 67: Attribute Value Pair

dove *Type* indica il tipo di attributo e *Value* contiene l'informazione tra trasferire;

- il Radius server, dopo aver verificato l'autenticità del NAS, consulterà un database di utenti alla ricerca della entry relativa all'utente che ha richiesto la connessione. In particolare il server cercherà di verificare le informazioni ricevute, con il messaggio di Access Request, con quelle memorizzate nel database. In alcune circostanze, il Radius server può anche girare la richiesta di autenticazione ad altri server, nel qual caso agisce come client;

- se le informazioni contenute nel database non rispecchiano quelle fornite dal client, il Radius server invierà un messaggio di **Access Reject** al NAS il quale a sua volta negherà la connessione all'utente;

- in alcuni casi il Radius Server potrà decidere di "interrogare " l'utente per acquisire ulteriori conferme circa l'autenticità dello stesso. In questi casi il server invierà un messaggio di **Access Challenge** al client, il quale lo presenterà all'utente. Tale messaggio potrà contenere, ad esempio, un valore numerico che l'utente dovrà essere in grado di associare con un altro valore. Normalmente l'utente sarà equipaggiato con un particolare software o con una smart card appositamente progettati per rispondere al challenge del server. In seguito il client invierà un ulteriore messaggio di Access Request al Radius server il quale potrà rispondere con un messaggio di Access Reject, Access Challenge o Access Accept;

- infine, se tutte le informazioni subiscono un riscontro positivo, il Radius server invierà un messaggio di **Access Accept** al client il quale potrà così instaurare la connessione. Tale messaggio conterrà tutte le informazioni necessarie per caratterizzare il servizio (ad esempio indirizzo IP da assegnare all'utente, maschera di sotto-rete, protocollo da utilizzare, etc).

In figura sono schematizzate le funzionalità sopra esposte ed è evidenziato il paradigma client/server tra NAS e Radius server e tra l'utente ed il NAS (è intuibile, infatti, che l'utente si comporti come un client del Network Access Server):

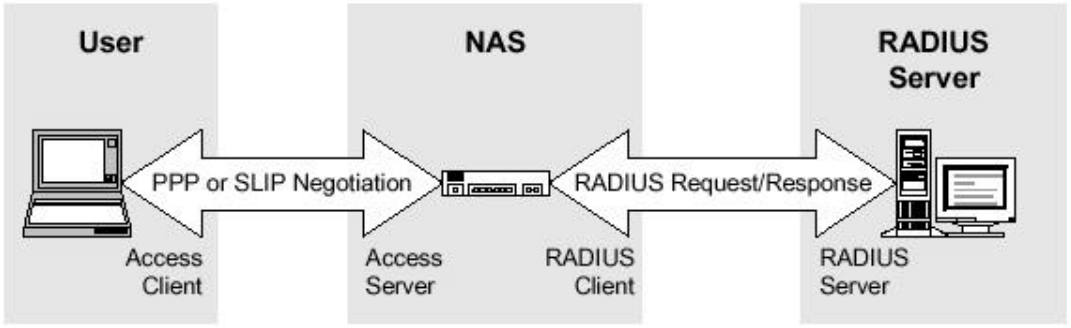


Figura 68: Scambio di dati tra utente, NAS e Radius server

Come si era brevemente accennato, un ulteriore caratteristica del protocollo Radius è quella di poter procedere all'Accounting [45] dell'utente.
Se un client è configurato per gestire l'accounting, in concomitanza con l'instaurazione di una connessione, invierà un messaggio di **Accounting Start** al Radius server indicando l'identificativo dell'utente e tutte le necessarie informazioni per caratterizzare il servizio offerto. In risposta il server invierà un **Acknowledgement Message**.
Al termine del servizio, il client trasmetterà al server un messaggio denominato **Accounting Stop** attraverso il quale potrà comunicare, ad esempio, la durata della connessione, il numero di byte inviati e ricevuti dall'utente, etc. Anche in questo caso il server dovrà confermare l'avvenuta ricezione del messaggio attraverso l'invio di un Acknowledgement.

7.1.2 Utilizzo di PAP e CHAP

Spesso il protocollo di comunicazione tra NAS e utente è il Point-to-Point Protocol (PPP) il quale utilizza dei meccanismi di protezione delle informazioni

di autenticazione come *Password Authentication Protocol* (PAP) e *Challenge Handshake Authentication Protocol* (CHAP).

PAP è un metodo di convalida di base in cui l'utente invia un'username ed una password al NAS, il quale confronta tali informazioni con quelle contenute in un database per trovare una corrispondenza. Tuttavia, nonostante le password sul server possano essere cifrate, esse vengono trasmesse dall'utente al server in chiaro. Ovviamente, questo schema di autenticazione non è molto sicuro.
Il NAS prende il PAP ID e la password inviati dall'utente e li inserisce in un pacchetto di Access Request rispettivamente come User-Name e User-Password.

CHAP è un metodo di autenticazione più sicuro rispetto a PAP in quanto non viene mai inviata sul collegamento la password in chiaro.
Il NAS genera una "challenge" casuale e la invia all'utente che risponderà con una CHAP response insieme con un CHAP ID ed un CHAP username. Il NAS invierà allora un pacchetto di Access Request al Radius server con CHAP username come User-Name e CHAP ID e CHAP response come CHAP-Password.

7.1.3 Proxy Radius

Un Radius server funziona come proxy Radius quando riceve una richiesta di autenticazione da un Radius client, rilancia la richiesta ad un Radius server remoto, riceve la risposta da quest'ultimo e la inoltra al client. Un utilizzo comune per il proxy Radius è il roaming.
Un Radius server può funzionare sia come forwarding server sia come server remoto, operando come forwarding server per alcune reti e come server remoto di autenticazione per altre reti.
Un forwarding server può rilanciare le richieste di autenticazione per un qualunque numero di server remoti.

Infine un forwarding server può rilanciare la richiesta di autenticazione ad un altro forwarding server creando così una catena di proxy.

7.2 Caratteristiche generali del protocollo Diameter

Diameter è un protocollo ancora in fase di standardizzazione che rappresenta un'evoluzione di Radius.
Si è resa necessaria tale migrazione per diversi motivi, in particolare per [46]:

- *sopperire al "limitato" numero di AVP inseribili in un pacchetto Radius.* Radius contempla l'esistenza di 256 AVP differenti, mentre Diameter è stato progettato in maniera tale da poter prevedere milioni di attributi. E' chiara, quindi, la grande scalabilità del protocollo;

- *consentire al Server AAA di inviare unsoliceted message.* Diameter, come del resto Radius, è un protocollo basato su di un modello di tipo Client-Server. A differenza di Radius, in cui la comunicazione può essere inizializzata solamente dal Client, Diameter permette al Server di inviare dei messaggi senza un'esplicita richiesta. Tale comportamento è utile in diverse applicazioni, come ad esempio nel caso di Mobile IP.

Concettualmente il protocollo è stato progettato in maniera tale da poterlo suddividere in due blocchi distinti:
un insieme di messaggi e di meccanismi di trasporto comune a tutte le applicazioni che richiedono servizi AAA, *Diameter Base Protocol*, e delle estensioni che caratterizzano la particolare applicazione. Ad esempio, nel caso di Mobile IP, l'estensione, che prende il nome di *Diameter Mobile IPv4 Extension*, rispetterà tutte le specifiche descritte nel paragrafo 7.7.
Di seguito sono riportati alcuni dei problemi di Radius risolti dal protocollo Diameter:

- *inefficcient retransmission algorithm*: entrambi i protocolli operano su UDP e quindi su di un servizio senza ri-trasmissioni. Diameter prevede degli schemi per regolare il flusso dei pacchetti UDP (*Windowing Scheme*);

- *silent discarding of packets*: nel caso del protocollo Radius, un pacchetto può essere eliminato dal Server senza avvertire il Client il quale, non potrà fare altro che ri-trasmettere il messaggo. Diameter prevede la possibilità che il Server notifichi il tipo di problema al Client;

- *hop-by-hop Security*: Radius implementa meccanismi di protezione dei messaggi di tipo Hop-by-hop e non End-to-end utili, ad esempio, nel caso dei forwarding server.

7.3 Modello basilare

Come descritto nell'introduzione al capitolo, l'obiettivo di fornire un modello di compatibilità tra Mobile IP ed il servizio AAA sarà raggiunto in maniera graduale [47]. Per il momento si vogliono evidenziare le specifiche basilari del modello, legate alla verifica dell'autenticità di un utente mobile nell'ambito della rete Internet.
Un host mobile (*client*), autenticabile all'interno del proprio dominio d'appartenenza (*home domain*), può avere l'esigenza di usufruire delle risorse di un dominio (*foreign domain*) diverso dal proprio. All'interno del foreign domain, descrivibile anche come un *local domain* dato che rispecchia l'attuale posizione dell'host, vi può essere un dispositivo, denominato *attendant*, il cui scopo è quello di verificare le credenziale dell'host prima di fornirgli l'acceso alle infrastrutture del sistema. Molto probabilmente l'attendant non sarà in grado di autenticare l'utente e quindi dovrà consultare un AAA server, appartenete al suo stesso dominio (*AAA Local Authority*), il quale, a sua volta, richiederà conferma delle credenziali dell'host all'AAA server che gestisce l'home domain (*AAA Home Authority*).

Per chiarire il concetto ora esposto si può far riferimento alla figura, nella quale sono evidenziate le entità sopra definite e le iterazioni fra le stesse:

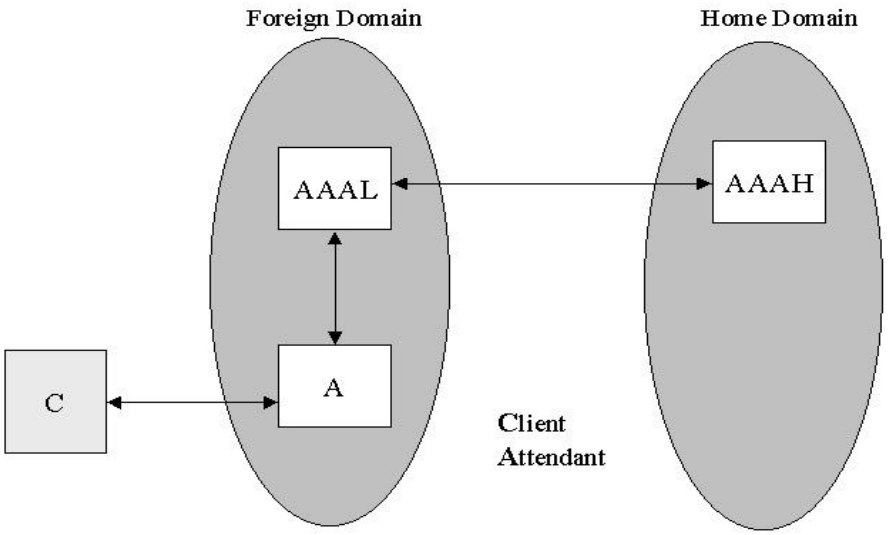


Figura 69: AAA Server nel Foreign e Home Domain

In seguito alla ricezione delle necessarie informazioni di autenticità fornite da AAAH, l'autorità locale AAAL comunicherà all'attendant l'esito della verifica e quindi la disponibilità o meno ad accettare la richiesta dell'host mobile.

La procedura sopra descritta richiede uno scambio di informazioni tra diverse entità, sono quindi necessari dei contesti di sicurezza (*Security Association*) in maniera da poter salvaguardare, attraverso l'utilizzo di appositi algoritmi di autenticazione e chiavi di decodifica, tali informazioni.
In particolare, come indicato nella figura 70, si può evidenziare la necessità di tre contesti di sicurezza ciascuno dei quali dovrà essere condiviso da una coppia di entità. In primo luogo è naturale assumere la presenza di tali contesti tra l'host mobile ed il server AAAH (indicato in figura con SA1) e tra l'attendant ed il server AAAL (SA2), inoltre, affinchè i due server possano scambiarsi informazioni protette, dovrà esistere un contesto anche tra AAAL e AAAH (SA3):

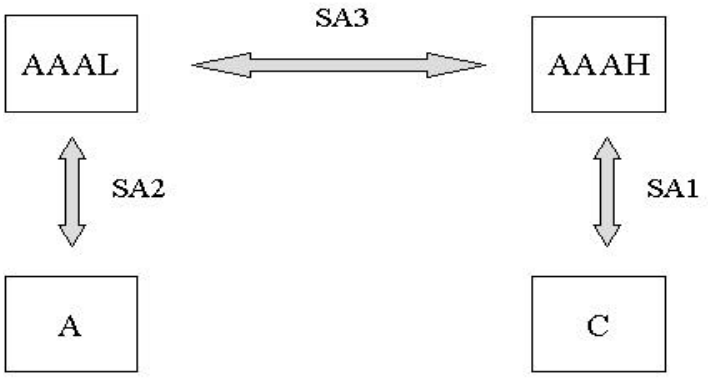


Figura 70: Security Association

Infine, in aggiunta alle considerazioni sopra esposte, occorre enunciare dei requisiti che permettano di ottimizzare l'autenticazione del client:

- il client deve essere in grado di fornire tutte le proprie credenziali senza dover interagire con l'home domain. Nel successivo paragrafo si descriverà un particolare tipo di identificativo che permetterà di soddisfare tale richiesta;
- l'attendant deve mantenere la richiesta di accesso fornita dal client per tutta la durata della procedura di autenticazione. Inoltre deve essere in grado di gestire più richieste contemporaneamente.

7.4 Specifiche legate al protocollo IP

Il modello definito nel precedente paragrafo descrive l'iterazione tra diverse entità senza prendere in considerazione un aspetto legato alle esigenze del client. In particolare molti host, sia fissi che mobili, possono avere la necessità di ricevere delle informazioni di configurazione nel momento in cui cercano di connettersi ad Internet.
Da ciò deriva che, con riferimento al tipo di analisi che si stà svolgendo, occorre sottolineare un ulteriore requisito che gli AAA server devono essere in

grado di soddisfare: devono poter allocare un indirizzo IP al client nel caso in cui questo ne effettui la richiesta.
Prendendo in considerazione le caratteristiche di Mobile IP, questa specifica è molto importante in quanto si riflette nella procedura di assegnazione di un home address, ed eventualmente anche nell'identificazione di un indirizzo dell'Home Agent.
Il problema ora esposto, si ricollega alla ricerca di un identificativo dell'host mobile che permetta di individuare univocamente il suo dominio d'appartenenza e che sia ovviamente differente dall'indirizzo IP dello stesso.
L'identificativo considerato più valido è il Network Access Identifier [48] la cui forma è la seguente *NAI= username@realm*. Attraverso quest'identificativo gli AAA server saranno in grado di stabilire la provenienza del client attraverso l'analisi del campo realm. E' importante rilevare che, tramite l'utilizzo della NAI, si ha la coincidenza tra identificativo dell'host e dell'utente.
Affinchè tale identificativo possa essere utilizzato anche da un Mobile Node, l'IETF ha introdotto una particolare estensione da associare al messaggio di registrazione denominata *Network Access Identifier Extension* la cui struttura e indicata in figura:

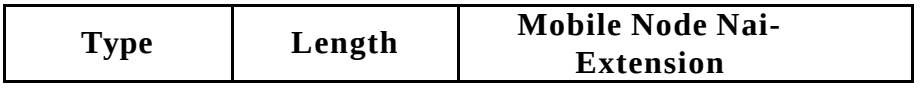


Figura 71: Mobile Node Network Access Identifier Extension

Il campo *Type* assumerà il valore 131, *Lenght* indicherà la lunghezza in byte della NAI mentre il campo *Mobile Node NAI* conterrà la stringa di caratteri rappresentate l'identificativo.

7.5 Specifiche legate alle richieste di Mobile IP

Per completare la descrizione, è necessario particolareggiare tutti i concetti sopra esposti in base alle caratteristiche dello standard Mobile IP [49].

Con riferimento alle entità architetturali di Mobile IP, il Foreign Agent svolgerà le funzioni eseguite dall'attendant mentre il client sarà identificato dal Mobile Node. E' intuibile che, una volta terminate le operazioni di autenticazione, il Mobile Node dovrà continuare ad interagire con il Foreign Agent, secondo quanto ampliamente descritto in un precedente capitolo, e quindi senza richiedere ulteriori interventi da parte degli AAA server (tranne nel caso in cui si necessiti di un servizio di accounting).

Affinchè le operazioni di autenticazione non ritardino la procedura di registrazione del Mobile Node, una prima importante specifica è quella di consentire che tali servizi (autenticazione e registrazione) siano implementati simultaneamente. Dato che nella procedura di registrazione entrano in gioco le funzioni svolte dall'Home Agent, per raggiungere l'obiettivo di simultaneità dei servizi, sarà necessario un "colloquio " tra il server AAAH e l'Home Agent stesso.

Da questa prima analisi deriva che il modello descritto in figura 69 dovrà essere modificato in quello rappresentato nella figura successiva.

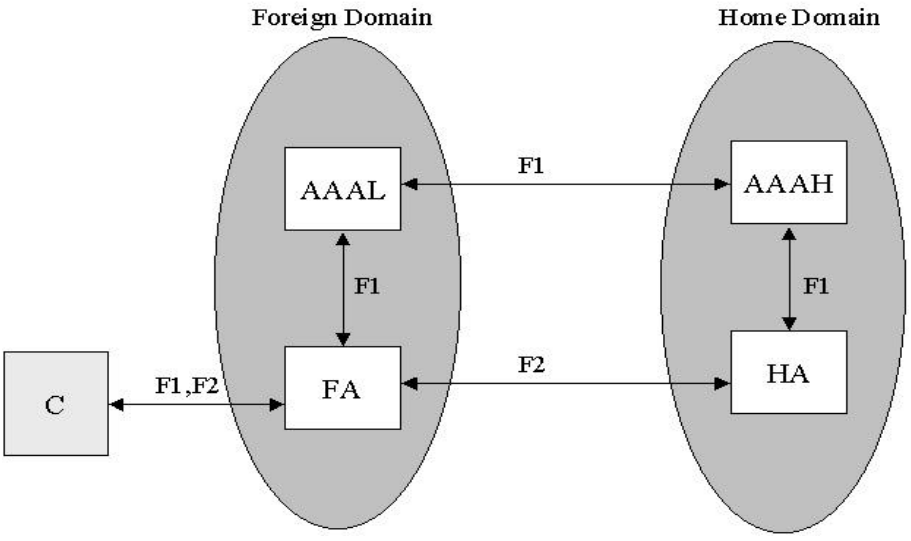


Figura 72: AAA Server e Mobile IP

Oltre all'introduzione dell'Home Agent, si evidenzia una prima fase (F1) nella quale si procede all'autenticazione ed all'instaurazione della procedura di

registrazione del Mobile Node ed una seconda fase (F2) nella quale si conclude la registrazione e si implementano le funzioni proprie di Mobile IP. Ciascuna fase è caratterizzata dallo scambio di informazione tra le entità corrispondenti (notare che il server AAAL è stato indicato con la sigla AAAF per mantenere la nomenclatura di Mobile IP e quindi, lo si chiamerà AAAForeign server).

7.5.1 Configurazione del Mobile Node

Come accennato precedentemente, un Mobile Node (oltre ad un care-of address) potrebbe aver bisogno di particolari informazioni prima di accedere ad Internet. Al limite, potrebbe richiedere l'intero insieme d'informazioni utili per lavorare:
Home address; Indirizzo IP dell' Home Agent; Security Association con Home Agent ed eventualmente con il Foreign Agent; Indirizzo IP del server AAAH.
Occorre sottolineare che la non conoscenza dei parametri enunciati non è uno svantaggio, infatti consente di alleggerire notevolmente la configurazione del Mobile Node dato che dovrà disporre solamente del NAI, di una password per poter essere autenticato dal proprio AAAH e di un contesto di sicurezza con lo stesso AAAH.
E' importante rimarcare che grazie al NAI, il server AAAF potrà risalire all'entità AAAH, alla quale sarà demandato il compito di procurare tutte le necessarie informazioni al Mobile Node.

7.6 Utilizzo di un "broker"

Nel paragrafo 7.3 si è assunto l'esistenza di un contesto di sicurezza tra il server AAAF e l'analoga entità residente nell'home domain del Mobile Node.
E' intuibile che tale richiesta rende il modello poco scalabile in quanto non è fattibile la circostanza per la quale un AAAF sia in grado di mantenere contesti di sicurezza con tutti i possibili home domain.
Per questo motivo può essere introdotta un'entità intermediaria, denominata *broker*, in grado di condividere contesti di sicurezza con un elevato numero di

domini. Da notare che l'introduzione di tale dispositivi non preclude l'eventuale esistenza di associazioni di sicurezza tra entità AAA..
In altre parole il compito del broker sarà quello di mettere in comunicazione i server AAA (appartenenti a domini differenti) consentendo loro di scambiarsi informazioni protette e richiedendo, come unica condizione, che ciascuno di essi condivida un security association con il broker stesso.

7.7 Descrizione generale del protocollo

Dopo aver descritto i requisiti che devono essere soddisfatti per consentire una compatibilità del servizio AAA con lo standard Mobile IP, si vogliono fornire le basi attraverso le quali sia possibile implementare un protocollo in grado di gestire lo scambio di informazioni tra le diverse entità.
Si noti che l'estensione Mobile IP del protocollo Diameter è stata introdotta proprio per raggiungere tale obiettivo; la sequenza delle operazioni da eseguire sono:

- il Mobile Node (MN) invia un messaggio di Registration Request al Foreign Agent (FA) secondo quanto definito nello standard Mobile IP;
- il Foreign Agent rilancia la richiesta al foreign AAA (AAAF) il quale, dopo aver individuato il dominio di appartenenza del Mobile Node, si metterà in contatto con un broker;
- il broker invierà la richiesta al server AAA appartenente all'home domain del Mobile Node (AAAH) il quale identificherà gli eventuali parametri necessari al Mobile Node (home address, Home Agent, etc.) ed autenticherà l'utente. In seguito rilancerà le informazioni di autenticazione ed il Registration Reply Message al server AAAF (sempre tramite il broker);

- infine il server AAAF comunicherà al Foreign Agent l'esito della verifica dell' autenticità del Mobile Node ed, in caso di riscontro positivo, sarà conclusa la procedura di registrazione.

7.7.1 Desrizione della procedura "Registration Request"

Per consentire al Foreign Agent di stabilire se nuove richieste di registrazione provengono da uno stesso Mobile Node ed inoltre per migliorare l'aspetto legato alla sicurezza dello standard Mobile IP, l'IETF ha introdotto un'estensione da applicare ai messaggi di Agent Advertisement ed ai Registration Request Message denominata *Challenge/Response Extension* rappresentata in figura:

Type	Length	Challenge/Respose Extension

Figura 73: Formato della Challenge/Response Extension

Il valore assunto da *Type* varierà a seconda se l'estensione sia utilizzata in un Agent Advertisement oppure in un messaggio di registrazione, *Length* indica la lunghezza in byte del campo, *Challenge* rappresentante un valore casuale di almeno 32 bit.

Nell'ambito dello studio che si sta effettuando non è necessario caratterizzare in dettaglio le modalità secondo le quali tale estensione può essere utilizzata (argomento descritto in [50]), basta sottolineare che il suo scopo è quello di permettere una maggiore autenticazione del Mobile Node. Sostanzialmente il Foreign Agent inserirà una Challenge Extension in tutti gli Advertisements da lui emessi, a sua volta il Mobile Node inserirà il valore, prelevato nel campo Challenge, nella Response Extension che assocerà con la propria richiesta di registrazione.

Avendo introdotto tale estensione si può procedere ad una descrizione più dettagliata della procedura di registrazione seguendo lo schema rappresentato in figura:

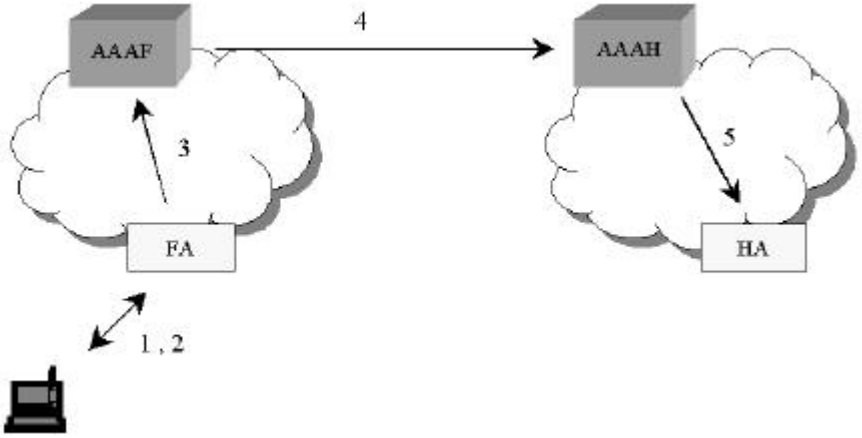


Figura 74: Mobile IP/AAA Registration Request

Il significato dei vari passi è il seguente:

1. il Foreign Agent pubblicizza la propria presenza tramite gli Agent Advertisements nei quali inserirà una Challenge Extension;
2. il Mobile Node invia un messaggio di Registration Request inserendo una NAI Extension, una Challenge Response Extension, etc;
3. il Foreign Agent invia la richiesta al server AAAF;
4. AAAF tramite la NAI individua il server AAAH cui rilanciare il messaggio (eventualmente tramite un broker);
5. il server AAAH autentica il Mobile Node e, se necessario, alloca un Home Agent ed un home address.

Come menzionato più volte un aspetto molto importante riguarda la sicurezza delle informazioni inviate in rete. Nel caso di mobile IP le tre entità architetturali (Mobile Node, Home Agent, Foreign Agent) devono poter condividere un contesto di sicurezza quindi, nella circostanza in cui tali entità

non siano configurate con le necessarie informazioni di sicurezza, si deve prevedere un meccanismo che permetta di distribuirle.
Assumendo l'esistenza di contesti di sicurezza tra le seguenti entità:

- AAAH e Mobile Node (SA1)
- AAAH e Home Agent (SA2)
- AAAH e AAAF (SA3)
- AAAF e Foreign Agent (SA4)

il server AAAH deve essere in grado di identificare e distribuire contesti di sicurezza condivisibili tra:

- Mobile Node e Home Agent;
- Mobile Node e Foreign Agent;
- Foreign Agent e Home Agent.

Più precisamente il server dovrà generare e distribuire delle "chiavi " che permetteranno alle entità sopra definite di interpretare le estensioni di sicurezza che accompagneranno il Registration Reply Message (MN-HA Authentication Extension, MN-FA Authentication Exstension, HA-FA Authentication Extension). Le chiavi saranno contenute in apposite estensioni (associate ancora al messaggio Registration Reply) definite in [51] che dovranno ovviamente precedere quelle di sicurezza. Infine dato che le chiavi saranno utilizzate nell'ambito di un certo algoritmo di autenticazione individuato dal Security Parameter Index (SPI), contenuto nelle estensioni di sicurezza, le entità architetturali dovranno essere in grado di implementare l'algoritmo richiesto.
Per chiarire i concetti ora esposti occorre descrivere la seconda fase del protocollo di registrazione, cioè la procedura di "Registration Reply".

7.7.2 Descrizione della procedura di “Registration Reply”

La prima fase del protocollo, descritta nel precedente paragrafo, si è conclusa con la generazione, da parte del server AAAH, di tre chiavi di codifica:

- K1 condivisa tra MN – FA
- K2 condivisa tra MN – HA
- K3 condivisa tra FA – HA

Si deve ora procedere alla distribuzione di tali chiavi alle diverse entità ed alla conclusione della registrazione del Mobile Node. E’ importante sottolineare che per consentire una distribuzione protetta delle chiavi, queste saranno codificate in accordo ai contesti di sicurezza disponibili dal server AAAH. In particolare AAAH dovrà codificare ciascuna chiave due volte, infatti, considerando i contesti di sicurezza introdotti nel precedente paragrafo:

- K1 e K2 saranno consegnate al Mobile Node codificandole attraverso SA1;
- K1 e K3 saranno consegnate al Foreign Agent codificandole attraverso SA3;
- K2 e K3 saranno consegnate all’Home Agent codificandole attraverso SA2.

Tenendo presente tale concetto si possono esaminare i diversi passi che caratterizzano la procedura di Registration Reply indicata in figura 75 (si assume che la verifica del Mobile Node vada a buon fine):

6. il server AAAH invia la richiesta di registrazione all’Home Agent comunicandogli le chiavi K2 e K3 e codificandole attraverso SA2;

7. HA elabora un messaggio di Registration Reply inserendo le estensioni di sicurezza (HA-FA Authentication Extension e HA-MN Authentication Extension). In seguito invia tale messaggio al server AAAH;
8. AAAH rilancia il messaggio ad AAAF inserendo tutte le chiavi;
9. AAAF decodifica le chiavi K1 e K3 attraverso SA3 e dopo averle codificate attraverso SA4 le invia al Foreign Agent insieme alla chiave K2 (ancora codificata attraverso SA1) ed al messaggio Registration Reply
10. il FA decodefica K1 e K3 attraverso SA4 e verifica l'autenticità del messaggio Registration Reply controllando la HA-FA Authentication Extension attraverso la chiave K3. In seguito rilancia il messaggio di registrazione al Mobile Node inserendovi una FA-MN Authentication Extension. Il Mobile Node decodifica le chiavi K1 e K2 attraverso SA1 e verifica l'autenticità del messaggio controllando la HA-MN Authentication Extension attraverso la chiave K2 e la FA-MN Authentication Extension attraverso K1.

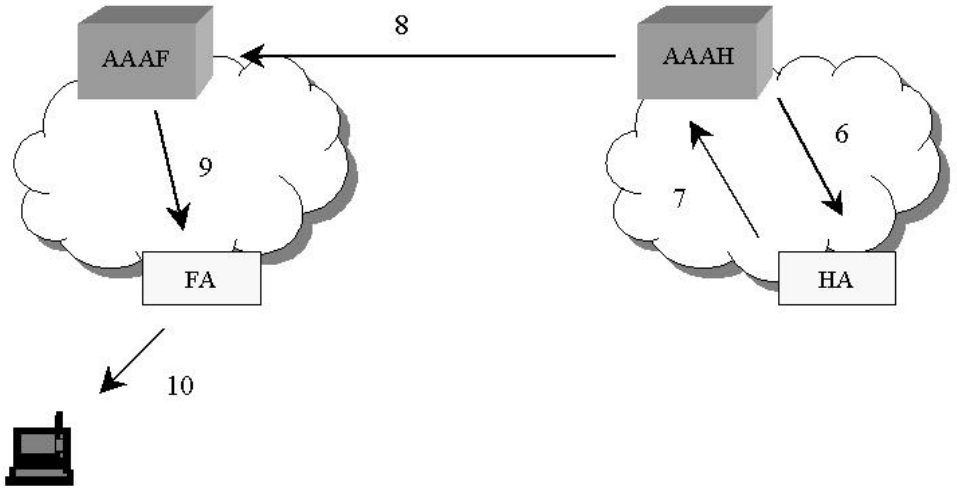


Figura 75: Mobile IP/AAA Registrtion Reply

8 Progettazione di un sistema AAA basato sul protocollo RADIUS

Il lavoro compiuto nel corso di questa tesi è stato sviluppato nell'ambito delle attività di ricerca svolte allo IASI-CNR (Istituto per l'Analisi dei Sistemi Informatici del Consiglio Nazionale delle Ricerche) ed in particolare nell'ambito del progetto NetLab (Network Laboratory).
A causa della grande importanza che sta assumendo negli ultimi anni il concetto comunemente definito *Mobile Internet*, si è deciso di avviare una serie di ricerche con lo scopo di analizzare i diversi aspetti legati a tale settore.
In particolare, come si è avuto modo di descrivere nei precedenti capitoli, riveste una grande importanza, in caso di *roaming* di un utente, l'analisi delle procedure AAA.
In conformità a queste considerazioni è stato deciso di progettare ed implementare un sistema AAA per Mobile IP tenendo ben presente le attuali tecnologie di cui si dispone.
Un'attenta analisi di mercato ha permesso di costatare che:

- attualmente gli Internet Service Provider basano la propria architettura AAA sul protocollo Radius, la migrazione verso Diameter avverrà in tempi piuttosto lunghi;
- i software Mobile IP, reperibili nelle comunità scientifiche, non supportano le caratteristiche designate nel precedente capitolo.

Da tali considerazioni deriva che il lavoro svolto deve essere inserito in un contesto ben definito, nel quale sarà molto importante tener presente le specifiche funzionali del protocollo Radius e del software Mobile IP.

8.1 Obiettivo

Nei precedenti capitoli, si è cercato di porre in risalto l'importanza di introdurre tecniche che consentano da un lato di verificare le credenziali di un utente e dall'altro di procedere all'accounting dello stesso.
E' chiaro, infatti, che lo sviluppo di nuove tecnologie, pur se efficienti e risolutive di diversi problemi, devono scontrarsi con le reali caratteristiche di mercato. Un fornitore di servizio sarà propenso ad accettare tali tecnologie solamente se può trarne dei benefici in termini monetari.
In tale contesto deve essere inquadrato l'obiettivo della tesi:
sviluppare un'architettura che fornisca i mezzi per inserire in un *Business System* il servizio Mobile IP.

In fase di progettazione di un sistema, un requisito fondamentale è quello di delineare il problema da risolvere. In altre parole, volendo sviluppare un sistema AAA per Mobile IP, di quali mezzi si può disporre?
Per rispondere a tale domanda, si è resa necessaria una ricerca di mercato in grado di fornire riscontri circa l'attuale stato dell'arte delle tecnologie richieste. In particolare, è stato necessario individuare un'implementazione di Mobile IP e stabilire il tipo di protocollo AAA utilizzabile. In base alla scelta effettuata si è potuto circoscrivere il problema e quindi individuare un gruppo di specifiche che il progetto dovrà soddisfare.

Dalla ricerca svolta è emerso che il protocollo AAA attualmente più diffuso risulta Radius.
Questo significa che gli attuali Internet Service Provider saranno favorevoli all'introduzione di un nuovo servizio, quale ad esempio Mobile IP, se questo non richieda, almeno nel breve periodo, una completa revisione delle infrastrutture di rete.
In una visione più ampia, la scelta del protocollo Radius è motivabile considerando che, attualmente, non è disponibile un'implementazione del protocollo Diameter che includa le estensioni per Mobile IP.

In definitiva, dalle considerazioni svolte, si delinea maggiormente l'obiettivo da raggiungere:
progettare un'architettura nella quale le procedure di Autenticazione, Autorizzazione ed Accounting siano basate sul protocollo RADIUS.
Tale architettura sarà poi inserita in un contesto più vasto, in cui si prenderà in considerazione l'iterazione con un eventuale sistema di Billing.

8.2 Requisiti di progetto

In questo paragrafo si cercherà di individuare, in maniera esauriente, l'intero insieme di requisiti che il progetto dovrà soddisfare.
Per una maggiore comprensione, ritengo che sia importante effettuarne una classificazione attraverso l'analisi dei seguenti aspetti:

- **Scelta del software**

  La fase di progettazione del sistema dovrà porre le basi per l'effettiva implementazione dello stesso, da ciò deriva la necessità di individuare un'implementazione del protocollo Mobile IP e del protocollo RADIUS.

- **Authentication and Authorization**

  Un Internet Service Provider consentirà ad un Mobile Node di usufruire delle proprie risorse solamente dopo averne verificato le "credenziali". E' importante, quindi, delineare con precisione le azioni da svolgere per il corretto conseguimento di tale obiettivo.

- **Accounting**

  Dal punto di vista dell'ISP, le procedure di accounting sono il mezzo con cui ricevere un pagamento per il servizio offerto. Si dovranno cosi individuare i parametri più significativi per ciò che concerne l'utilizzo delle risorse da parte del Mobile Node.

Di seguito è fornita una descrizione dettagliata delle componenti sopra delineate.

8.2.1 Scelta del software

Data la grande diffusione di RADIUS, esistono diverse implementazioni del protocollo e molte di queste sono reperibili via Internet.
Di notevole importanza riveste l'implementazione denominata **Merit Radius Server** sviluppata dalla *University of Michigan*. Oltre a soddisfare le specifiche delle RFC, è adatta all'implementazione del sistema che sarà proposto poichè consente di emulare il comportamento del NAS Server.
Inoltre, prevede la possibilità di configurare il funzionamento *Proxy Server*, requisito essenziale in caso di roaming di un utente. E' evidente, infatti, la necessità da parte di un Internet Service Provider di rilanciare, la richiesta d'autenticazione, ad un opportuno AAA Server nel caso in cui il Mobile Node non faccia parte della "lista" degli utenti da lui gestiti. Per raggiungere tale obiettivo sarà necessario utilizzare l'informazione contenuta nella Network Access Identifier fornita al NAS dal terminale mobile.

Molte sono le società impegnate nello sviluppo del protocollo Mobile IP, convinte che questo sarà di notevole importanza nel prossimo futuro.
In particolare, sono le Università i centri in cui si concentra il maggior sforzo nella ricerca delle soluzioni migliori da adottare.
Di seguito e fornita una descrizione schematica di alcune implementazioni di Mobile IP.

- **SUN**

  Risulta un'implementazione piuttosto datata poichè risale al 1999. A parte un limitato numero di eccezioni, soddisfa le specifiche dettate dalla prima versione della RFC 2002.

Una caratteristica di tale software è individuabile nell'implementazione di meccanismi in grado di istaurare una *Virtual Private Network* tra il Mobile Node e la Home Network.
Il software è disponibile on-line.

✍✍ **Carnegie Mellon University**

All'interno di tale Università vi è un gruppo di ricerca denominato *CMU Monarch Project* interamente dedicato allo studio del protocollo Mobile IP.
La prima versione del software risale al 1997 e da allora sono stati rilasciati diversi aggiornamenti.
Una particolarità di tale software è la possibilità di istaurare un tunnel, per motivi di sicurezza, tra il Foreign Agent e l'Home Agent (*reverse tunneling*).
Il software è disponibile on-line.

✍✍ **Stanford University**

Il gruppo *Mosquito Net Mobile Computing* si occupa dello sviluppo di un'implementazione adattabile al protocollo IPv6. Tale circostanza implica che il software non prevede l'utilizzo del Foreign Agent.
Il software è disponibile on-line.

✍✍ **CISCO**

Nelle versioni più recenti dei router CISCO è prevista la possibilità di configurare le funzionalità svolte dal Foreign Agent e dall'Home Agent.
L'implementazione è pienamente compatibile con le specifiche dettate dalla rfc 2002.

✍✍ **Birdstep Tecnhnology**

L'azienda, nell'Aprile 2001, ha rilasciato quella che può essere considerata la prima implementazione del protocollo Mobile IP a livello commerciale. Più precisamente, la *Birdstep Tecnhnology* si è occupata di porre nel mercato un prodotto in grado di implementare le

funzionalità del Mobile Node, dichiarando la completa compatibilità con i router CISCO. E' prevista, inoltre, la possibilità di attivare procedure di Route Optimization.

La tabella seguente riassume le caratteristiche delle diverse implementazioni prese in considerazione:

COMPANY	*PIATTAFORMA*	*RFC*	*ENTITA'*	*LIMITI*
SUN	Solaris 2.5.1 o superiore Linux	rfc 2002 rfc 2003 rfc 2356	Home Agent Foreign Agent Mobile Node	·No reverse tunneling ·No unicast advertisements ·Security association solo tra HA e MN ·Solo IP in IP encapsulation
Carnegie Mellon University	NetBSD 1.1 FreeBSD 2.2.2	rfc 2002 rfc 2003 rfc 2004	Home Agent Foreign Agent Mobile Node	·No route optmization ·No reverse tunneling
Stanford University	RedHat 6.0 o superiore	rfc 2002 rfc 2003	Home Agent Mobile Node	·Solo IP in IP encapsulation ·Solo time-stamp based reply attack
CISCO	Router cisco	rfc 2002 rfc 2003 rfc 2006	Home Agent Foreign Agent	·Non dichiarati
BIRDSTEP Technology	Windows 2000 Windows 98 Windows ME Windows CE Linux EPOC	rfc 2002 rfc 2344 Supporterà route optimization	Mobile Node	·Non dichiarati

Tabella 8: Implementazioni di Mobile IP

Nell'elenco precedente non è stato inclusa l'implementazione che sarà utilizzata nello sviluppo dell'architettura AAA proposta in questa tesi.
Sarà impiegato un software sviluppato presso la *Helsinki University of Technology* denominato **Dynamics-HUT Mobile IP**.
Le motivazione che hanno condotto a tale scelta sono:

- importanza data al software dalla comunità scientifica. Le caratteristiche di Dynamics-HUT Mobile IP sono state presentate in diversi meeting, ad esempio:
  Sixth IEEE International Workshop on Mobile Multimedia Communications (MoMuC'99), IP based Cellular Networks (IPCN2000*) conference*.
- interesse mostrato dal gruppo di lavoro attraverso il mantenimento di mailing list ed il continuo sviluppo del software;
- disponibilità di una documentazione esauriente;
- facilità di configurazione del software;
- disponibilità del codice sorgente.

Il software, riveste un'ulteriore importanza poichè è compatibile con reti d'accesso di tipo wireless ed inoltre consente di implementare la tecnica descritta in un precedente capitolo e denominata *Regionalized Registration*.
Lo sviluppo dei prodotti sopra menzionati è caratterizzato dalla ricerca di determinare la soluzione migliore che consenta di soddisfare i requisiti propri del protocollo Mobile IP.
Solamente nelle ultime settimane sta affiorando, all'interno della mailing list inerente *Dynamics-HUT Mobile IP*, la necessità di affrontare le problematiche relative ai sistemi di Autenticazione, Autorizzazione ed Accounting.
Da tale considerazione deriva che, nella progettazione del sistema che si vuole proporre, non occorre soddisfare delle condizioni inerenti le procedure AAA e derivanti dalla particolare implementazione del protocollo Mobile IP.

Infine è importante rilevare che il software prescelto richiede che il Mobile Node sia configurato, a priori, con:

- indirizzo IP dell'Home Agent;
- Home Address;
- Security Associtione Condivisa con l'Home Agent ed, eventualmente, con il Foreign Agent.

8.2.2 Authentication and Authorization

In linea di principio, sia per le procedure di Authentication ed Authorization che per quelle di Accounting, è necessario effettuare un'analisi separata a seconda che:

- il Mobile Node risieda nel proprio dominio;
- il Mobile Node sia in roaming.

In realtà il primo caso non riveste grande interesse poiché è indipendente dal servizio Mobile IP, quindi la concentrazione sarà rivolta verso l'individuazione dei requisiti necessari per un corretto svolgimento delle procedure AAA in caso di roaming del terminale.

Si possono verificare le seguenti situazioni:

- **il Mobile Node richiede di accedere alle risorse di un *Foreign ISP***

  Prima di gestire la richiesta di registrazione sarà necessario verificarne l'autenticità attraverso uno scambio di informazioni tra il server AAA locale e quello residente nell'*Home Domain*.

Solo in caso di riscontro positivo il Foreign Agent sarà abilitato alla gestione del *Registration Request Message*.

Nel caso in cui la richiesta di registrazione venga negata, si dovrà procedere nuovamente all'autenticazione del terminale.

- **il Mobile Node risiede nel Foreign ISP e richiede di rinnovare la richiesta di registrazione**

  Nel caso in cui si verifichi tale situazione il terminale è stato precedentemente autenticato dall'Home ISP.

  Si può quindi prevedere un meccanismo che consenta di effettuare un'autenticazione locale del Mobile Node.

  Occorre precisare che nel caso in cui il terminale "abbandoni" il Foreign ISP per poi tornarci in un secondo tempo, l'autenticazione dovrà essere eseguita nuovamente dal Server AAA residente nell'Home ISP.

- **il Mobile Node fa ritorno nell'Home ISP**

  Sarà necessario attuare le classiche procedure di autenticazione applicate nei confronti di tutti gli utenti amministrati dal fornitore di servizio.

8.2.3 Accounting

Nella fase di accounting riveste particolare importanza l'individuazione dei parametri significativi ai fini della valutazione dell'utilizzo delle risorse.
Inoltre, è importante stabilire l'esatta temporizzazione con cui devono essere inviati i messaggi di Accounting.

- **Parametri**

  L'architettura che sarà proposta consentirà di implementare ciò che in un precedente capitolo è stato indicato come *Trasport Accounting*.

Sarà quindi necessario monitorizzare lo sfruttamento delle risorse attraverso l'impiego di parametri quali:

- *numero pacchetti inviati*;
- *numero pacchetti ricevuti;*
- *numero byte inviati;*
- *numero byte ricevuti;*
- *durata.*

✍✍ **Messaggistica**

I messaggi che saranno presi in considerazione sono:

- *Accounting Start*: sarà inviato solamente in seguito alla registrazione del Mobile Node;
- *Accounting Stop*: sarà inviato in seguito all'abbandono del Mobile Node del Foreign ISP;
- *Interim Accounting*: consente di inviare al RADIUS Server delle "fotografie" circa l'attuale utilizzo delle risorse. In altre parole, durante l'intero periodo in cui il Mobile Node risiede nel Foreign ISP sarà inviato, periodicamente, tale messaggio.

Anche se non esplicitamente menzionato, tutti i messaggi sopra individuati conterranno il valore assunto dai parametri di accounting.

8.2.4 Riepilogo

Data l'importanza dei requisiti di progetto, nella tabella seguente sono riportati i risultati ai quali si è giunti.

	REQUISITI
Software	?? Merit Radius Server ?? Dynamics HUT Mobile IP
Authentication and Authorization	?? Se il Mobile Node richiede i servizi di un Foreign ISP: rilanciare la richiesta di autenticazione al Server AAA che amministra l'Home Domain ?? Se l'autenticazione del Mobile Node non va a buon fine, attendere una nuova richiesta di registrazione e ripetere il passo precedente ?? Se la registrazione del Mobile Node è negata, riprocedere con l'autenticazione dello stesso ?? Nell'ambito di una stessa sessione effettuare autenticazioni locali ?? Se il Mobile Node fa ritorno nell'Home ISP effettuare la classica procedura di autenticazione
Accounting	?? Parametri di Accounting: pacchetti inviati, pacchetti ricevuti, byte inviati, byte ricevuti, durata ?? Accounting Start inviato dopo l'effettiva registrazione del Mobile Node ?? Accounting Stop inviato in seguito all'abbandono del Foreign ISP da parte del Mobile Node ?? Interim Accounting inviati periodicamente nell'ambito della sessione

Tabella 9: Requisiti progettuali

8.3 Architettura di sistema

Dall'analisi effettuata nel precedente paragrafo si è riusciti ad individuare una serie di requisiti che consentiranno di "guidare" la progettazione del sistema.

Un primo problema nasce dalla necessità di consentire al protocollo Mobile IP di poter "dialogare" con RADIUS:

è stato necessario sviluppare un'interfaccia, indicata con l'acronimo **RMI** (**Radius Mobility Interface**) in grado di gestire lo scambio d'informazione tra i due protocolli.

Tabella 10: Radius Mobility Interface

Nel seguito del capitolo le caratteristiche della Radius Mobility Interface saranno esplorate in dettaglio, per il momento ritengo opportuno delinearne il comportamento ad alto livello evidenziando le iterazioni con i due protocolli:

- **Lato Mobile IP**
  - Acquisirà informazioni sul Mobile Node che desidera usufruire delle risorse del Foreign ISP
  - Sarà informata dell'arrivo di nuovi Mobile Node e della "partenza" di quelli precedentemente autenticati
  - Fornirà informazioni circa l'esito delle procedure di autenticazione
  - Manterrà informazioni nei confronti dei Mobile Node autenticati in maniera da poter consentire le successive autenticazioni locali. In altre parole, ogni qual volta il Mobile Node richiederà di rinnovare la registrazione, dovrà ricevere informazioni inerenti il terminale e procedere all'autenticazione dello stesso senza usufruire dei servigi del RADIUS Server

- **Lato protocollo RADIUS**
  - Nei confronti Radius Server svolgerà i stessi compiti del Network Access Server: gestirà lo scambio dei messaggi di autenticazione (*Access Request*, *Access Response*), invierà i messaggi di accounting (*Accounting Start*, *Accounting Stop*, *Interim Accounting*)

Tutte le informazioni di autenticità, scambiate tre le differenti, entità dovranno essere "protette" attraverso meccanismi di sicurezza (ad esempio tramite algoritmi di criptazione).
Da questo primo esame, deriva che un ostacolo che si dovrà superare sarà rappresentato dalla necessità di temporizzare in maniera adeguata lo scambio delle informazioni.

L'introduzione della Radius Mobility Interface consente di schematizzare il modello architetturale che si prenderà in considerazione.
Per semplicità, si è mantenuta la nomenclatura del protocollo Mobile IP in maniera tale da distinguere con le sigle **F**oreign e **H**ome le entità appartenenti, rispettivamente, al Foreign ISP o al Home ISP.
In figura sono indicate tutte le entità architettuali che dovranno essere prese in considerazione; per completezza è stato rappresentato anche un AAA Server di livello superiore in grado di rendere il modello più scalabile:

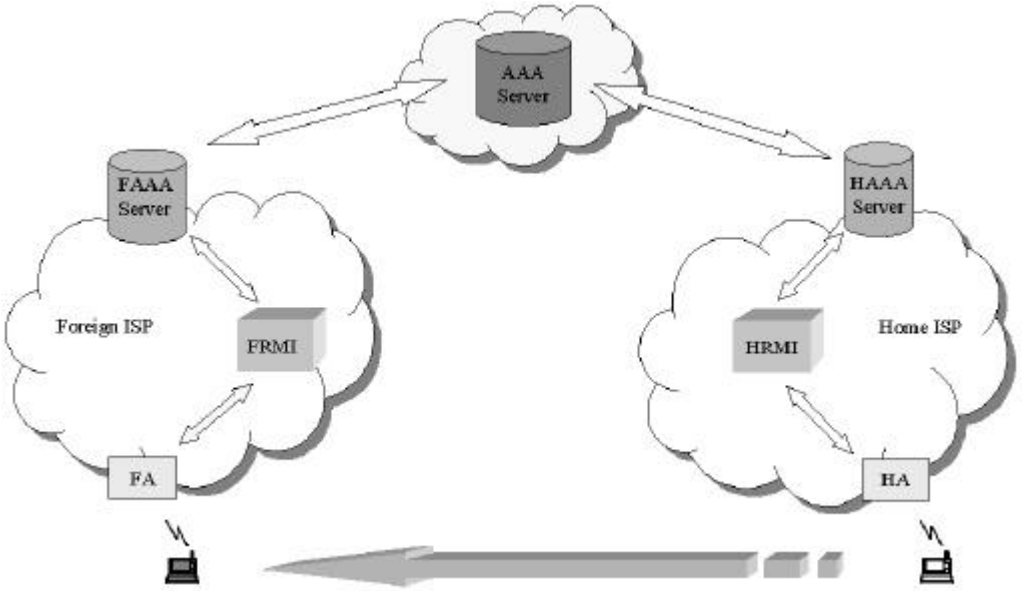


Figura 76: Architettura di sistema

se il Server *FAAA* non è configurato con le informazioni necessarie per individuare il Server *HAAA*, rilancerà la richiesta di autenticazione al Server Radius di livello superiore (*AAA Server*) istaurando cosi una catena di Proxy Radius.
Da ciò deriva che il compito di tale Server non sarà quello di autenticare l'utente, ma di mantenere rapporti di roaming con diversi Internet Service Provider consentendogli così di poter "dialogare".

Si è detto che la Radius Mobility Interface deve scambiare informazioni con un Server Radius.
In un ambiente reale si deve prevedere un procedimento che consenta di salvaguardarsi da eventuali situazione di mal funzionamento del Server (reboot, crash, etc). A tale scopo all'interno di un Internet Service Provider vi sarà un'ulteriore Radius Server che entrerà in azione nel caso in cui si verifichino tali situazioni.
Da ciò deriva che, nella circostanza in cui il Server "primario" non risponda alle richieste di autenticazione o di accounting, la RMI dovrà rilanciare le richieste verso il Server alternativo.

Il meccanismo più semplice per raggiungere tale obiettivo è di numerare i messaggi inviati, superato un certo limite superiore, la RMI rilancerà lo stesso messaggio al Server “secondario”.

Per descrivere in dettaglio l’architettura proposta è opportuno procedere come nel caso del paragrafo precedente:
saranno analizzate separatamente le funzionalità relative alle procedure di Autorizzazione ed Autenticazione da quelle di Accounting.

8.4 Architettura di Authentication and Authorization

Personalmente ritengo che lo schema migliore per delineare il comportamento delle entità architetturali sopra introdotte sia quella di utilizzare i diagrammi temporali.
Tale scelta è motivabile considerando che, attraverso questa rappresentazione, è possibile individuare sia il flusso dei messaggi scambiati tra le entità che la corretta sequenza temporale con cui devono essere trasmessi.

Nella descrizione della procedura di autenticazione si analizzeranno, separatamente, le diverse situazioni che si possono presentare e che rientrano nelle specifiche di progetto.

8.4.1 Autenticazione iniziale del Mobile Node

Tale situazione deve essere ulteriormente suddivisa in base all’esito della richiesta di autenticazione e della richiesta di registrazione.
Per semplicità, nei diagrammi che seguono non è considerata l’iterazione con il Radius Server di livello superiore:
si suppone che tra il Foreign ISP e l’Home ISP esista un contratto di roaming e che quindi il FAAA Server sarà configurato con le informazioni necessarie per individuare l’HAAA Server.

Esito positivo di entrambe le richiste

Il diagramma rappresentato in figura fa riferimento alla prima richiesta di registrazione inviata dal Mobile Node.

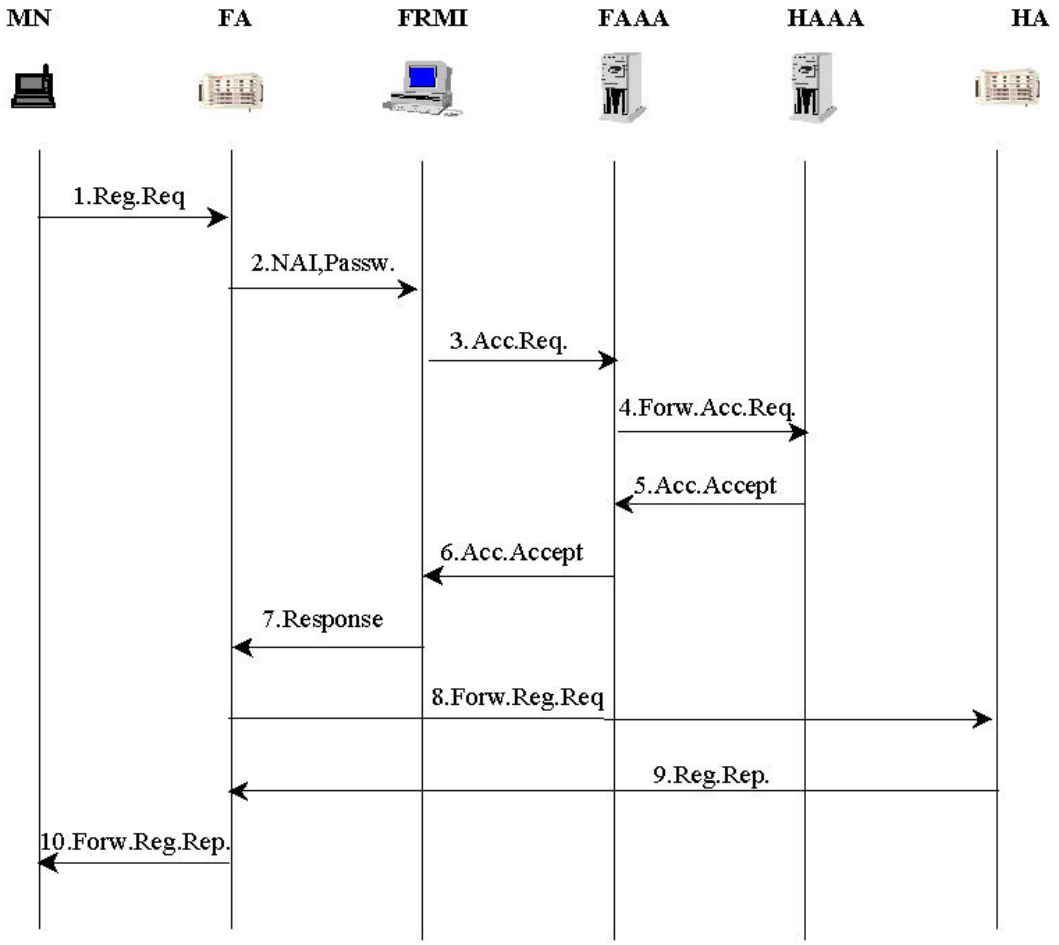


Figura 77: Autenticazione e richiesta di registrazione accettata

In seguito alla ricezione del *Registration Request Message*, il Foreign Agent "contatterà" la FRMI per comunicargli:

- Network Access Identifier del Mobile Node;
- password che il Mobile Node condivide con l'HAAA.

Attraverso tali informazioni la Radius Mobilty Interface sarà in grado di inviare al FAAA un *Access Request Message*. A sua volta il Server, non potendo autenticare autonomamente il Mobile Node, rilancerà la richiesta all'HAAA.
Effettuata l'autenticazione, l'HAAA invierà un *Access Accept Message* che seguirà il percorso a ritroso fino alla Foreign Radius Mobility Interface.
Quest'ultima comunicherà l'esito dell'autenticazione al Foerign Agent che potrà così rilanciare il messaggio di registrazione all'Home Agent.
Il tutto si conclude con le operazioni classiche del protocollo Mobile IP: generazione da parte dell'Home Agent di un Registration Reply Message, invio di tale messaggio al Foreign Agent e successiva consegna al Mobile Node.

La procedura di autenticazione non da esito positivo

Nel caso in cui si verifichi tale situazione il Foreign Agent dovrà negare la richiesta di registrazione e comunicare al Mobile Node la causa per cui non gli è consentito di accedere alle risorse del Foreign ISP.
Se il Mobile Node è in grado di prendere provvedimenti potrà inviare un nuovo *Registration Request Message* che causerà l'avvio di una nuova procedura d'autenticazione.
Tale procedura dovrà soddisfare lo scambio di messaggi rappresentato nel diagramma precedente.

La richiesta di registrazione è negata

Il protocollo Mobile IP prevede che la richiesta di registrazione possa essere negata sia dal Foreign Agent che dall'Home Agent.
In entrambi i casi, il Mobile Node può re-inizializzare la procedura con l'invio di un nuovo *Registration Request Message*.
Anche in questo caso la ricezione del nuovo messaggio di registrazione da parte del Foreign Agent provocherà l'inizializzzione delle operazioni d'autenticazione.

A differenza delle situazioni precedenti, non sarà necessario autenticare il Mobile Node nell'Home ISP.
Si consideri il diagramma seguente:

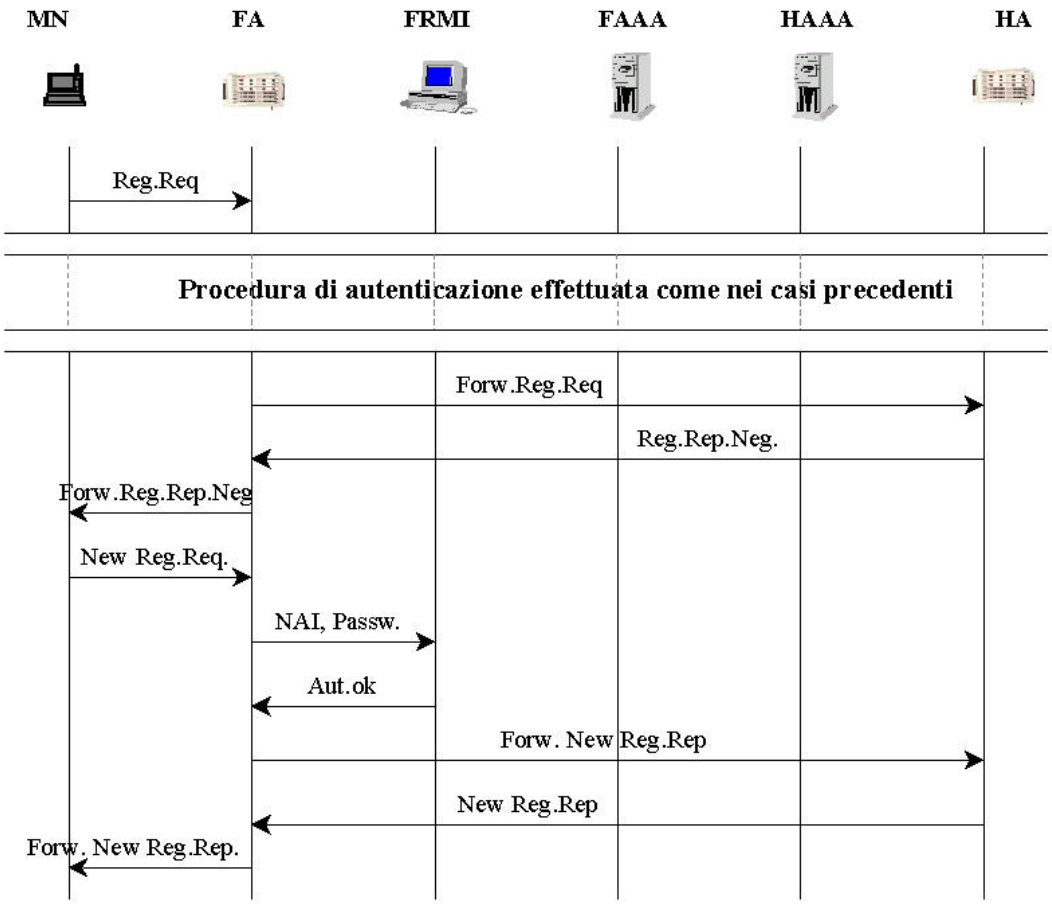


Figura 78: Richiesta di registrazione negata

In figura è indicato il primo Registration Request Message inviato dal Mobile Node. Per semplicità è stata omessa la sequenza inerente l'iniziale procedura di autenticazione che rispecchia il diagramma di figura 77.
Completata questa prima fase con esito positivo, il Foreign Agent rilancerà il messaggio di registrazione all'Home Agent.
Si supponga che l'Home Agent neghi la richiesta di registrazione e che quindi giunga al Mobile Node un Registration Reply Message che notifichi tale rifiuto.

In base alle specifiche del protocollo Mobile IP, il Mobile Node è normalmente in grado di individuare il motivo che ha condotto al rifiuto e di prendere così dei provvedimenti. Sarà quindi in grado di generare una nuova richiesta di registrazione che invierà al Foreign Agent.
Il Foreign Agent dovrà chiedere nuovamente conferma delle credenziali del Mobile Node e quindi comunicherà alla FRMI la NAI e la password dello stesso.
Conseguentemente all'iniziale procedura di autenticazione, la Radius Mobility Interface dovrà essere in grado di autenticare il Mobile Node senza richiedere la "partecipazione" dei Server Radius.
Effettua, quindi, una autenticazione locale che permette di migliorare l'efficienza dell'intero sistema.
Affinchè tale requisito possa essere soddisfatto, la RMI dovrà mantenere una sorte di database in maniera da poter conservare delle informazioni inerenti a ciscun Mobile Node precedentemente autorizzato.
E' chiaro che tale entry non potrà avere una durata indeterminata in quanto se il Mobile Node abbandona il Foreign ISP per poi tornare in un secondo tempo dovrà sostenere nuovamente la procedura di autenticazione descritta nel diagramma di figura 77.

8.4.2 Autenticazione nell'ambito di una stessa sessione

Si è voluto separare tale situazione solamente per evidenziare un ulteriore aspetto del sistema che si sta progettando.
Il protocollo Mobile IP richiede che il Mobile Node, durante il periodo in cui "risiede" in un Foreign ISP (sessione), rinnovi periodicamente la registrazione attraverso l'invio di Registration Request Message.
In corrispondenza di ciascun messaggio il sistema deve consentire l'autenticazione del Mobile Node:
è chiaro che tale compito sarà svolto dalla Radius Mobility Interface senza l'intervento dei Server AAA.

Si effettuerà quindi, come nel caso precedente, una autenticazione locale che permetterà di velocizzare l'intera procedura.

8.4.3 Autenticazione del Mobile Node nell'Home ISP

Un ultimo aspetto che occorre menzionare è inerente la procedura di autenticazione del Mobile Node effettuata nell'Home ISP.
Più precisamente, si può considerare il caso in cui il Mobile Node torni nell'Home ISP e richieda all'Home Agent di de-registrarsi:
prima di svolgere tale compito, l'Home Agent dovrà verificare l'autenticità dell'utente.
In questo caso le entità architetturali che interverranno saranno solamente quelle locali, come indicato nel diagramma che segue.

Data l'analogia concettuale con i casi precedenti, non è necessario descrivere in dettaglio la sequenza temporale dei diversi messaggi.

Per semplicità si è rappresentato il caso in cui entrambe le richieste vadano a buon fine (autenticazione e de-registrazione), se ciò non avvenisse si deve procedere nuovamente all'autenticazione del Mobile Node:
tramite l'ausilio dei Server nel caso in cui sia negata l'autenticazione, locale nel caso opposto.

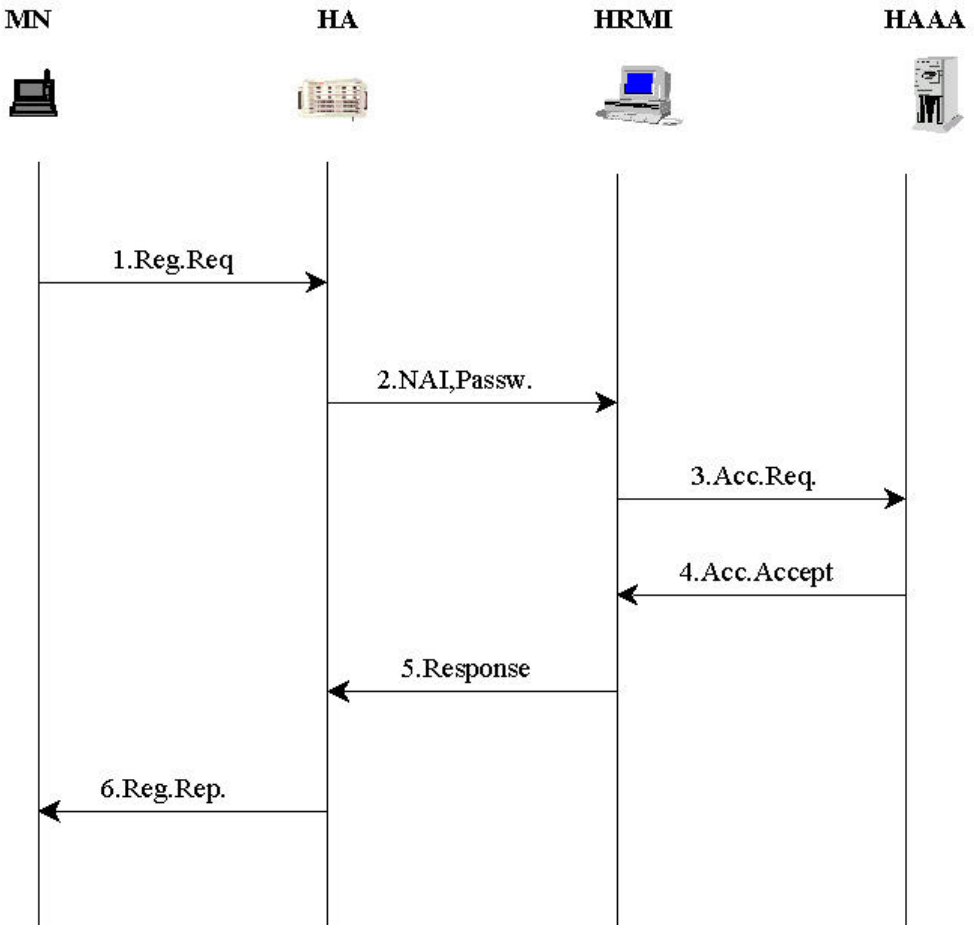


Figura 79: Autenticazione nell'Home ISP

Occorre precisare che la Home Radius Mobility Interface dovrà conservare i dati di autenticazione del Mobile Node, necessari per l'autenticazione locale, solamente per il tempo necessario al completamento della fase di de-registrazione.
Infatti, il protocollo Mobile IP specifica che qualora il Mobile Node risieda nell'Home ISP, dovrà operare come un qualsiasi altro utente e quindi senza la necessità dei servizi dell'Home Agent.

8.5 Architettura di Accounting

Effettuata l'autenticazione e la successiva registrazione del Mobile Node si dovrà procedere con le operazioni di Accounting.

In un precedente paragrafo sono stati specificati i parametri in grado di fornire informazioni utili circa l'utilizzo delle risorse:

- pacchetti inviati;
- pacchetti ricevuti;
- byte inviati;
- byte ricevuti;
- durata.

Sia il software Mobile IP che il protocollo Radius non contemplano delle applicazioni attraverso le quali sia possibile ottenere i parametri sopra delineati: in fase di implementazione del progetto si forniranno i mezzi per poter superare tale problema.

Il protocollo Radius prevede che l'inizio e la fine delle operazioni di Accounting siano delineate attraverso i messaggi *Accounting Start* ed *Accounting Stop*.
Nel sistema che si sta proponendo tali informazioni saranno generate dalla Radius Mobility Interface, è quindi necessario inglobare tali messaggi in una contesto più ampio che tenga conto delle caratteristiche del protocollo Mobile IP.

A tale scopo, si consideri il diagramma rappresentato in figura nel quale si presuppone che il Mobile Node sia stato autenticato e che la richiesta di registrazione sia andata a buon fine.

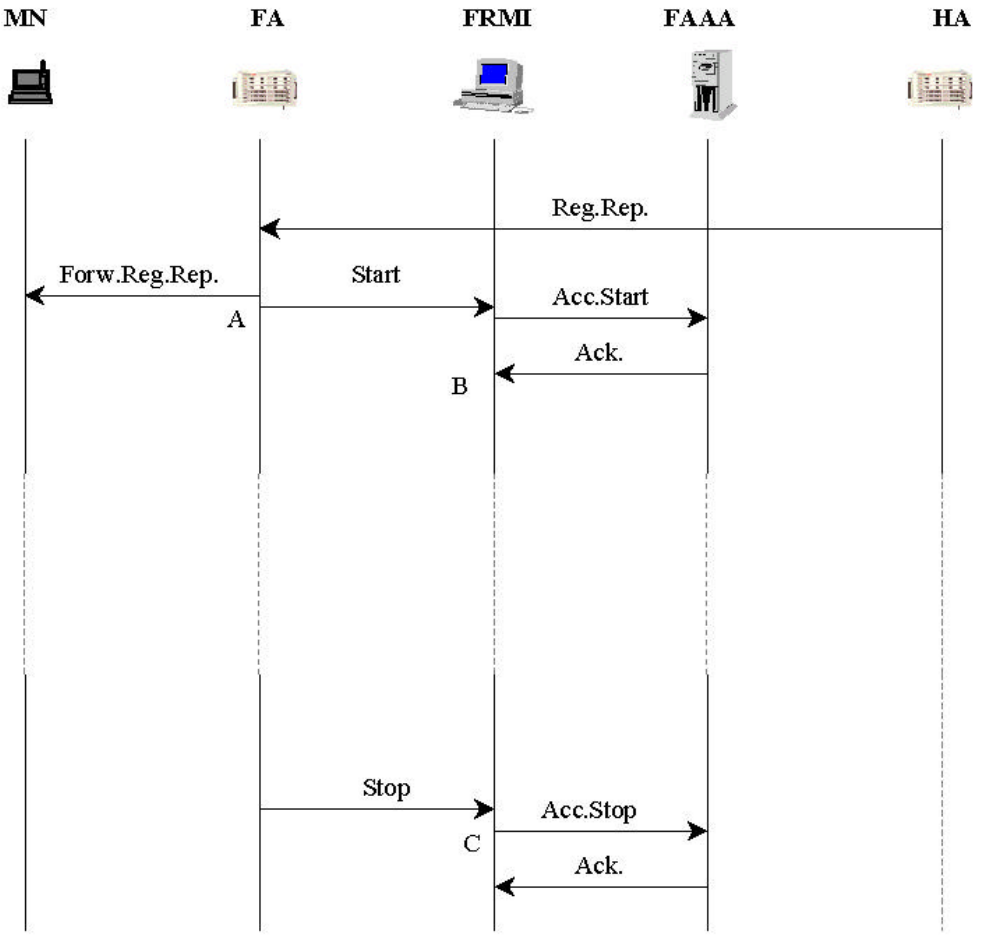


Figura 80: Inizio e fine del processo di Accounting

Avvio della procedura di Accounting

In seguito alla ricezione del Registration Reply Message, il Foreign Agent dovrà (punto A):

- rilanciare tale messaggio al Mobile Node;
- comunicare alla Radius Mobilityt Interface di avviare la procedura di Acounting.

A sua volta la RMI invierà un *Accounting Start Message* al Server FAAA; ricevuto il riscontro dovrà avviare il meccanismo che consente di monitorare i parametri sopra introdotti (punto B).

Conclusione della procedura di Accounting

Durante la permanenza del Mobile Node nella Foreign Network il processo di misurazione delle risorse di rete non sarà interrotto.
Le caratteristiche del protocollo Mobile IP consentono al Foreign Agent di stabilire quando il Mobile Node abbandona la rete.
Da ciò deriva che quando tale situazione si verifica, il Foreign Agent dovrà comunicare alla RMI di interrompere la procedura di Accounting.
Nel messaggio *Accounting Stop,* diretto al FAAA, la RMI dovrà inserire i parametri d'utilizzo della rete (punto C):
sarà necessario interrompere il processo di misurazione ed acquisire tali parametri.
La procedura di Accounting termina con la ricezione, da parte della RMI, di un Acknowledgement inviato dal Server Radius.
Anche se non indicato nel diagramma, si può prevedere che i parametri complessivi di accounting, oltre che inviati al FAAA, siano rilanciati anche all'HAAA. Tali informazioni possono essere utilizzate dall'Internet Service Provider sia per scopi di billing, sia per stime sull'utilizzo delle risorse compiuto dai propri abbonati.

Nei precedenti paragrafi si è parlato di inviare degli *Interim Accounting Message* che consentano al Radius Server di mantenere informazioni parziali circa il valore assunto dai parametri di Accounting.
Poter disporre di informazioni parziali, permette al Foreign ISP di implementare le procedure di Billing, nei confronti del Mobile Node, anche in presenza di situazioni anomale:
crash, reboot della RMI, problemi di rete, etc

La figura seguente completa il diagramma sopra descritto includendo gli Interim Accounting Message.

E' chiaro, che l'invio di tali messaggi comporta una maggiore iterazione tra la Radius Mobility Interface ed il sistema che consente la misurazione dei parametri.

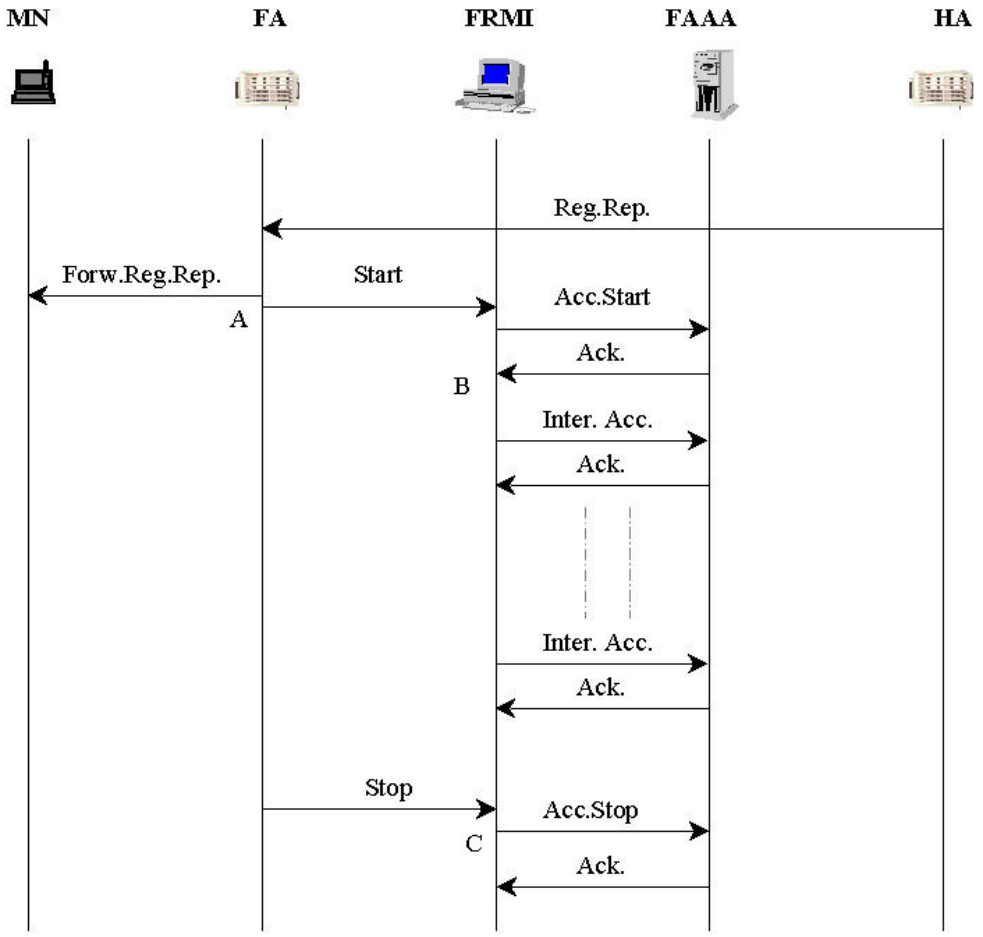


Figura 81: Interim Accounting

8.6 Business System

L'architettura AAA descritta nei precedenti paragrafi può essere inserita in un contesto più vasto nel quale, l'obiettivo, è quello di sfruttare i dati di Accounting per finalità di Billing.

Occorre precisare che in tale visione, i parametri individuati (pacchetti inviati, ricevuti, etc) costituiscono solamente un sottoinsieme delle possibili informazioni utilizzabili.
In altre parole, un sistema di Billing riceverà come input, non solo i parametri provenienti dal Server Radius, ma anche informazioni di valore aggiunto:

- indicazione delle funzioni svolte dal Foreign Agent:
  - realizzazione delle procedure di registrazione del Mobile Node;
  - decapsulamento e rilancio dei pacchetti IP destinati al Mobile Node;
  - etc.
- eventuali servizi richiesti dal terminale (ad esempio invio o ricezione di e-mail)
- eventuali agevolazioni che il Foreign ISP può applicare nei confronti dell'Home ISP
- etc.

E' prevedibile, inoltre, la presenza di un sistema di *Mediation*, in grado di fornire al *Billing Server* delle informazioni compatte e con un formato standard. Come indicato in figura, il Mediation System agirà su dei parametri "fisici", mentre il Billing Server sfrutterà l'intero insieme dei dati di Accounting. Si osservi che il parametro indicato con il termine "Funzioni Foreign Agent" è stato inviato come input al Billing Server in quanto può essere considerato come un dato globale e stabilito a priori.

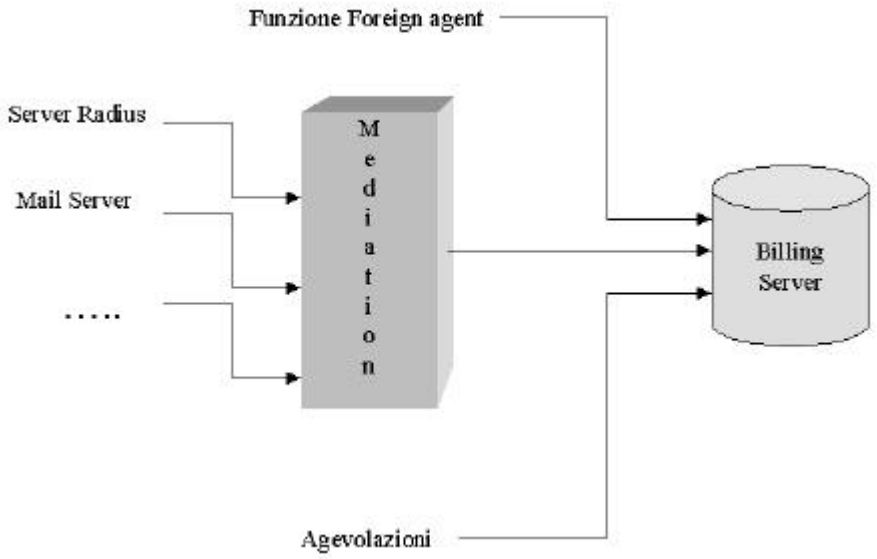


Figura 82: Mediation System and Billing Server

L'introduzione del Billing Server e del Mediation System non completa la visione generale dell'architettura, poichè non si è presa in considerazione l'iterazione tra il Foreign ISP e l'Home ISP.
L'obiettivo finale di tutto il sistema è di addebitare al terminale i servizi di cui ha usufruito. Tale procedura può essere suddivisa in due fasi:

- il Foreign ISP richiede il pagamento all'Home ISP;
- l'Home ISP richiede il pagamento al Mobile Node.

Occorre precisare che le due fasi sono scorrelate, periodicamente vi saranno dei *financial balance* tra i due fornitori di servizio e tra l'Home ISP e l'utente.

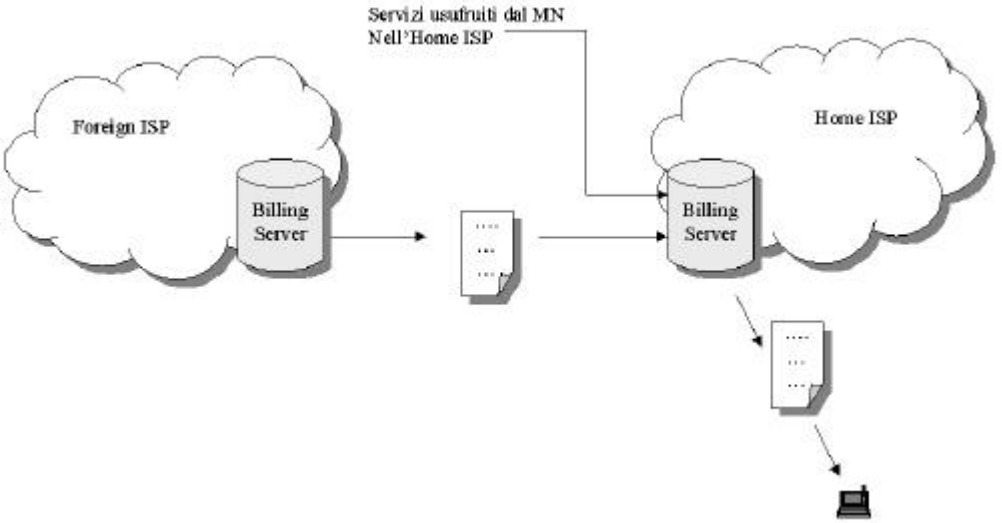


Figura 83: Business System

9 Realizzazione del sistema proposto

Nel presente capitolo saranno illustrate le soluzioni adottate per l'effettiva implementazione dell'architettura AAA, per Mobile IP, basata sul protocollo Radius.

In primo luogo è stato necessario effettuare uno studio delle risorse disponibili, all'interno del laboratorio NetLab, che ha permesso di individuare la dislocazione delle diverse entità architetturali coinvolte:

Radius Server, Foreign Agent, Home Agent e Mobile Node.

Si è poi passati alla fase d'istallazione dei software Dynamic-Hut Mobile IP e Merit Radius ed alla loro corretta configurazione. Entrambi i prodotti si basano sul sistema operativo Unix-Linux, in particolare, l'istallazione di Dynamic-Hut Mobile IP, ha richiesto una preventiva compilazione del Kernel ed il caricamento di moduli aggiuntivi.

Lo sviluppo dell'interfaccia denominata Radius Mobility Interface ha richiesto un'attenta analisi del codice sorgente del software Dynamic-Hut Mobile IP in quanto, come evidenziato in sede di progettazione, l'interfaccia necessita di interagire non solo con Radius, ma anche con il protocollo Mobile IP. Dal lato Radius si è riusciti ad ottenere una completa indipendenza dalla particolare implementazione del protocollo, mentre, nei confronti di Mobile IP, si sono dovute apportare delle modifiche al software scelto. E' importante rilevare che le soluzioni adottate, per consentire lo scambio d'informazioni tra la RMI ed il software Mobile IP, si basano su caratteristiche che derivano dalle specifiche dello standard e che quindi devono essere soddisfatte da tutte le diverse implementazioni. In tal senso, anche dal lato Mobile IP, si è riusciti ad ottenere un alto livello d'indipendenza.

9.1 Ambiente di lavoro

L'implementazione dell'architettura proposta ha richiesto l'utilizzo delle risorse disponibili nel laboratorio NetLab, presente nei locali dell'Istituto per l'Analisi dei Sistemi Informatici (IASI).

In figura è fornita una schematizzazione della rete interna di tale laboratorio, più precisamente sono rappresentate:

le sotto-reti necessarie alla realizzazione del sistema e le macchine che saranno utilizzate.

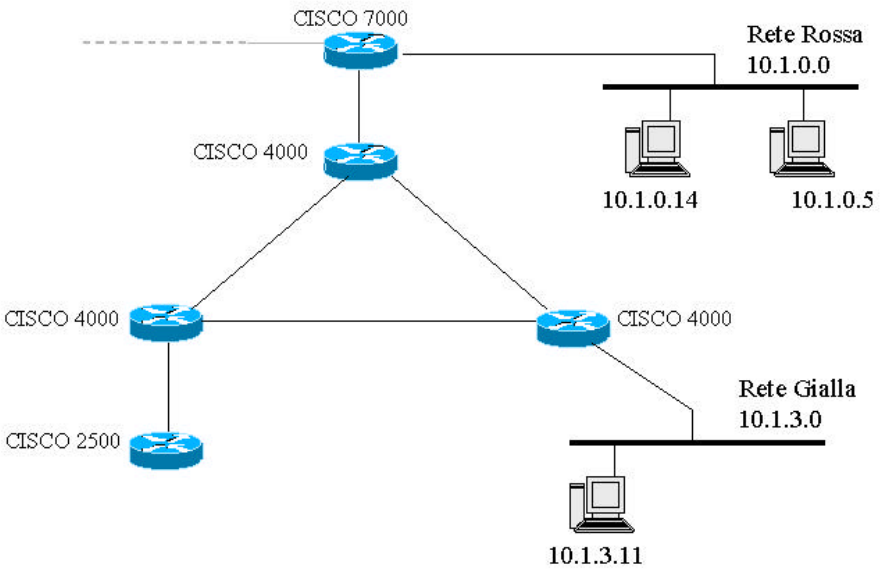


Figura 84: Rete Interna

Con riferimento all'analisi svolta nel precedente capitolo si può effettuare la seguente associazione:

- **Rete Rossa**

  Rappresenterà il dominio di appartenenza del Mobile Node, lo si potrà così identificare con l'Home Internet Service Provider.

- **Rete Gialla**

  Costituisce il dominio alle cui risorse vuole accedere il Mobile Node, è associabile con il Foreign Internet Service Provider.

Tra le diverse sotto-reti disponibili, la scelta è ricaduta su quelle rappresentate in figura in quanto i terminali indicati sono caratterizzati da prese Ethernet fisicamente vicine:
il sistema che si vuole implementare, basandosi sul protocollo Mobile IP, richiede che un host vari la propria ubicazione fisica quindi, non disponendo d'interfacce di tipo *wireless,* è stato necessario utilizzare delle macchine opportunamente dislocate all'interno del laboratorio.

Tutti gli host indicati in figura sono configurati con il sistema operativo *Linux Mandrake versione 7.2* e sono identificabili, all'interno del laboratorio, da un nome logico risolto tramite un Server DNS (Domain Name System).

Per terminare, è necessario caratterizzare, nell'ambito del sistema che si vuole realizzare, la funzione svolta da ciascuna macchina:

- **pc-server.rossa.netlab.it**

  Rappresenta la macchina con indirizzo 10.1.0.5 e svolgerà le funzioni del Mobile Node.

- **pc-linux.rossa.netlab.it**

  Rappresenta la macchina con indirizzo 10.1.0.14 e svolgerà le funzioni di:

  - Home Agent
  - Server Radius dell'Home Internet Service Provider (Home AAA Server)

- **pc-linux2.gialla.netlab.it**

  Rappresenta la macchina con indirizzo 10.1.3.11 e svolgerà le funzioni di:

  - Foreign Agent
  - Server Radius del Foreign Internet Service Provider (Foreign AAA Server)

9.2 Istallazione del software

I software utilizzati per implementare il sistema, denominati **Dynamic-Hut Mobile IP** e **Merit Radius Server**, sono freeware e disponibili in rete.
In particolare:

- Dynamic-Hut Mobile IP è reperibile all'indirizzo *http://www.cs.hut.fi/Research/Dynamics*;
- Merit Radius Server è reperibile all'indirizzo *http://www.interlinknetworks.com/downloads.*

Nel seguito del paragrafo si presterà particolare attenzione alla corretta configurazione dei prodotti, necessaria per strutturare in maniera adeguata l'ambiente di lavoro descritto precedentemente.

9.2.1 Dynamic-Hut Mobile IP

Il software è distribuito sia nella versione binaria (pacchetto RPM) che in quella sorgente. Ovviamente, per lo sviluppo della Radius Mobility Interface, è stato necessario prelevare il codice sorgente e quindi procedere alla compilazione dello stesso per l'effettiva istallazione.
Occorre precisare che, per consentire il corretto funzionamento del software, si è dovuto configurare opportunamente il kernel del sistema operativo.

Fortunatamente la documentazione allegata, sia nella forma di *Howto* che in quella di *Man-Pages,* ha facilitato tale operazione.

Dynamic-Hut Mobile IP consiste di tre *daemon* eseguibili indipendentemente, ***dynfad***, ***dynhad***, ***dynmnd*** che svolgono, rispettivamente, le funzionalità del Foreign Agent, dell'Home Agent e del Mobile Node.
Ciascun *daemon* può essere eseguito in modalità *foreground* in maniera tale da monitorarne il funzionamento attraverso messaggi di *debug*.
Sono forniti inoltre dei *tool*, ***dynfad_tool***, ***dynhad_tool*** e ***dynmn_tool*** che consentono di interagire con il Foreign Agent, Home Agent e Mobile Node.
Di seguito è rappresentata l'interfaccia a linea di comando di *dynmn_tool*:

```
[root@pcserver tools]# ./dynmn_tool
Dynamics Mobile Agent Control Tool v0.6.2
Using agent path "/var/run/dynamics_mn_admin"
> update
Trying to use the default interface address.
Location updated.
> status
Mobile status:
        state           Connected
        local addr      10.1.0.5
        co-addr         10.1.3.11
        FA-addr         10.1.3.11
        HA-addr         10.1.0.14
        Home addr       10.1.0.5
        tunnel is       up
        lifetime left   271
        tunneling mode  1
        last request    Wed Sep 26 15:45:36 2001
        last reply      Wed Sep 26 15:45:36 2001
        reply code      0 - registration accepted
        info text       connection established
        active devices 1
>
```

E' possibile interagire attraverso l'utilizzo di diversi comandi, nell'esempio sono evidenziati:

- *update*

  Consente di inviare un Agent Solicitation Message;

✍✍ *status*

Visualizza le caratteristiche del Mobile Node. Le informazioni sopra riportate permettono di stabilire che:

?? il Mobile Node 10.1.0.5, relativo all'Home Agent 10.1.0.14, è attualmente connesso al Foreign Agent 10.1.3.11;

?? il tunnel tra Home Agent e Foreign Agent è attivo;

?? il Lifetime della registrazione risulta di 271 sec.;

?? etc.

Per configurare opportunamente le macchine del laboratorio, si sono utilizzati dei files (forniti con il software ed installati di default nella direttori */usr/local/etc*) contenenti delle informazioni lette dai *daemon* in seguito alla loro esecuzione.

Tali files prendono il nome di ***dynfad.conf***, ***dynhad.conf*** e ***dynmnd.conf*** e permettono di configurare, rispettivamente, il Foreign Agent, l'Home Agent ed il Mobile Node.

Per completezza si riporta parte del contenuto del file *dynhad.conf* opportunamente modificato per rispecchiare la topologia del laboratorio descritta nel precedente paragrafo:

Configurazione dell'Home Agent: **macchina 10.1.0.14**

```
# : dynhad.conf,v 1.29
# Home Agent configuration file
#
# Dynamic hierarchial IP tunnel
# Copyright (C) 1998-99, Dynamics group
#
# Home Agent IP Address
HAIPAddress 10.1.0.14
# UDP port to listen for registration requests
# The default is 434
UDPPort 434
# MaxBindings can be used to restrict the maximum number of Mobile Nodes
# that are concurrently attached to this Home Agent.
# The default is 20.
MaxBindings 20
# The default tunnel lifetime is suggested also by the HA.
```

```
# The default lifetime is 500.
HADefaultTunnelLifetime 600
# The interval with which the Home Agent will send agent advertisement
# messages
AdvertisementInterval 30
AUTHORIZEDLIST_BEGIN
# SPI           IP
1000             10.1.0.5
AUTHORIZEDLIST_END
# The Home Agents needs a security association for each authorized Mobile
# Node. The association includes following information.
#
# SPI (Security Parameter Index)
#
# Authentication Algorithm: 1: keyed-MD5
#
# Replay Protection Method:
#    0: none
#    1: timestamps
#    2: nonces
#
# The maximum lifetime for the binding is given in seconds.
#
# Shared Secret:
#
# The SPI is the key identificator for the rest of the security parameters
# on the same line. SPI number ranges may be assigned the same security
# parameters.
#
SECURITY_BEGIN
#       auth.   replay  timestamp       max             shared
# SPI   alg.    meth.   tolerance       lifetime        secret
1000      1       1      120              600            "test"
SECURITY_END
#
```

9.2.2 Merit Radius Server

La caratteristica principale di questa implementazione del protocollo RADIUS è di consentire l'emulazione del Network Access Server:
è disponibile un comando, denominato ***radpwtst***, che consente di inviare *Access Request Message* ed *Accounting Request Message* al Radius Server.
Inoltre è possibile configurare il software per eseguire le funzionalità di *Proxy Server*, requisito basilare per lo sviluppo dell'architettura proposta in questa tesi.

L'esecuzione del comando ***radiusd –p 1645 –q 1646*** attiva il Server e permette di specificare il numero di porta, del protocollo UDP, nel quale il Server aspetta di ricevere, rispettivamente, richieste di autenticazione e di accounting:

```
[root@pc-linux etc]# ./radiusd -p 1645 -q 1646
Merit AAA server Version 3.6B , licensed software
COPYRIGHT 1992, 1993, 1994, 1995, 1996, 1997, 1998
THE REGENTS OF THE UNIVERSITY OF MICHIGAN
ALL RIGHTS RESERVED
```

La configurazione del Server avviene attraverso l'utilizzo di tre distinti files istallati di default nella direttori */usr/private/etc/raddb*:

- ***users***

  Consente di specificare gli utenti gestiti dal Server ed altre informazioni a loro pertinenti (ad esempio la password).

- ***clients***

  Contiene la lista dei Client che sono autorizzati ad inviare richieste al Server.

- ***authfile***

  Gli utenti possono essere identificati, all'interno del file *users*, attraverso la Network Access Idetifier e quindi nella forma *username@realm*. Per consentire di risolvere il campo realm, che rappresenta il dominio d'appartenenza dell'utente, è utilizzato il file *authfile*. E' evidente che, in caso di *Proxy Server*, è necessario impiegare tale file.

Nella configurazione del funzionamento Proxy Server si sono incontrate delle difficoltà in quanto la documentazione a riguardo non è esauriente.
Dopo diversi tentativi si è riusciti ad implementare tale funzionamento e quindi a realizzare la seguente procedura:

- il Mobile Node 10.1.0.5@pc-server.rossa.netlab.it è autenticabile dal Server pc-linux.rossa.netlab.it (Home AAA Server);

- il Server pc-linux2.gialla.netlab.it (Foreign AAA Server), ricevuta la richiesta di autenticazione dalla Radius Mobility Interface (non indicata in figura), consulterà il file *authfile* ed individuerà il Server a cui rilanciare la richiesta:

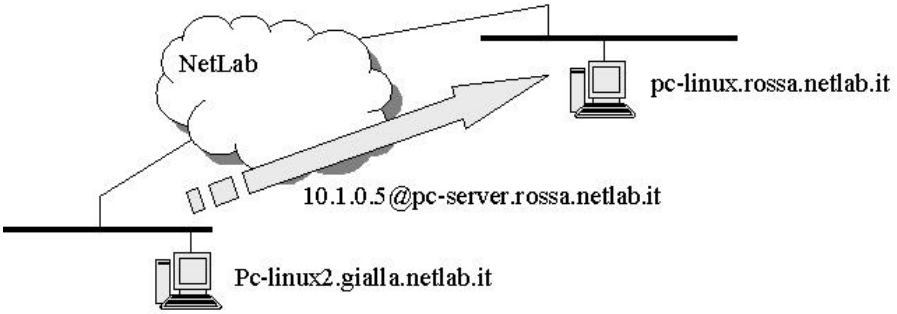


Figura 85: Proxy Radius-Fase 1

- Infine il Server pc-linux.rossa.netlab.it, eseguita l'autenticazione del Mobile Node, comunicherà l'esito al Foreign AAA Server:

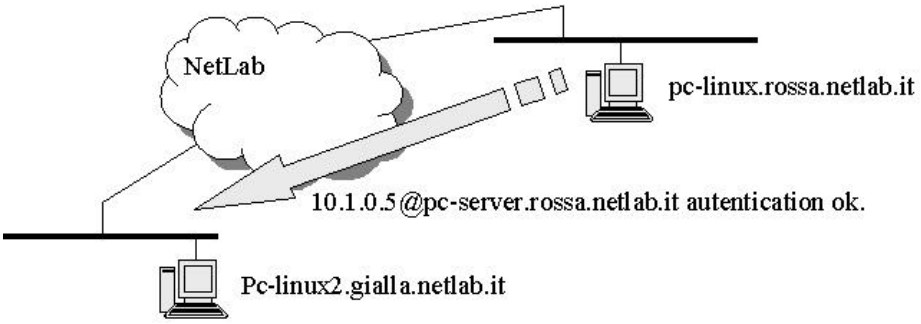


Figura 86: Proxy Radius-Fase 2

9.3 Radius Mobility Interface

Nel precedente capitolo, sono state individuate le funzioni che la Radius Mobility Interface deve eseguire per consentire il colloquio tra il protocollo Mobile IP e RADIUS.
Si deve ora procedere all'implementazione della stessa, attraverso l'utilizzo di metodologie che consentano di soddisfare i requisiti di progetto.
Il lavoro ha richiesto un'attenta analisi del codice sorgente, del software Dynamic-Hut Mobile IP, che ha permesso di individuare le diverse "zone" in cui intervenire.
Il software è stata realizzato utilizzando il linguaggio di programmazione C e strutturando opportunamente il programma attraverso l'utilizzo dei *makefile.*

Personalmente ho ritenuto opportuno sviluppare la RMI attraverso due approcci differenti tra loro:

- la parte relativa alle procedure di autenticazione ed autorizzazione è stata implementata utilizzando il linguaggio C e quindi creando delle funzioni specifiche ed inserendo i "prototipi" di tali funzioni negli opportuni makefile del software Dynamic-Hut Mobile IP. Il legame tra le diverse funzioni è stato poi ottenuto grazie al meccanismo di inclusione;

- la parte relativa alle procedure di accounting è stata sviluppata attraverso uno Script Shell e quindi sfruttando le potenzialità messe a disposizione dalla Shell Bash del sistema operativo Linux. Il legame con le funzioni sviluppate in C è stato possibile utilizzando il comando *system* contenuto nella libreria indicata dal file header *unistd.h*.

Quanto è stato appena menzionato potrebbe sembrare in contrasto con le caratteristiche della Radius Mobility Interface descritte nel precedente capitolo:

si era considerata la RMI come un'entità indipendente, nulla vieta, però, di inglobare le sue funzionalità all'interno del Foreign Agent.

E' importante rilevare che il principio seguito in fase di realizzazione del sistema è stato di non apportare nessun tipo di modifica al software Merit Radius e di interagire con l'implementazione di Mobile IP attraverso caratteristiche derivanti dalle specifiche dello stesso protocollo.
In tal modo la Radius Mobility Interface potrà "colloquiare" facilmente con software Mobile IP differenti da quello preso in considerazione.

Per fornire una descrizione esauriente del lavoro svolto, è preferibile procedere come in fase di progettazione e quindi analizzare, in maniera separata, le soluzioni adottate per sviluppare le funzionalità di autenticazione e quelle di accounting.

9.4 RMI: funzionalità di Autenticazione ed Autorizzazione

Le operazioni che la Radius Mobility Interface deve svolgere per consentire l'autenticazione del Mobile Node sono state ampliamente descritte nel precedente capitolo e non necessitano di ulteriore analisi. In questa sede si procederà per gradi, analizzando i diversi aspetti del progetto.

Una prima osservazione nasce dall'esigenza di fornire alla RMI le informazioni necessarie per inviare, tramite Proxy Server, un *Access Request Message* all'Home AAA Server:

- Network Access Indentifier
- password

Dall'analisi svolta precedentemente, si è potuto rilevare che il software Dynamic-Hut Mobile richiede che il Mobile Node sia configurato con:
home address, indirizzo IP dell'Home Agent e Security Associtaion da condividere con L'Home Agent.
Da ciò segue la necessità di "simulare" sia la NAI che la password.

- Per quanto riguarda la Network Access Identifier se ne è più volte delineata la struttura:
  NAI = Username@Realm.
  La soluzione adottata, per risolvere il problema, è stata di utilizzare come *Username* l'Home Address del Mobile Node (informazione reperibile dal Registration Request Message) e di effettuare una richiesta esplicita del campo *Realm*.
  Ad esempio, nel caso del Mobile Node 10.1.0.5, la Network Access Identifier risulterà:
  NAI = 10.1.0.5@pc-server.rossa.netlab.it.
- Analogamente, è richiesto all'utente di inserire la password che condivide con il Radius Server.

Ovviamente le soluzioni trovate derivano dall'assoluta necessita di disporre delle informazioni sopra descritte.
Si tenga presente che prelevare l'indirizzo IP del Mobile Node significa "ricavare" il Registration Request Message ed effettuare un'analisi dello stesso per individuare il campo Home Adress. Concettualmente tale operazione deve essere svolta anche in presenza di un Software Mobile IP che permetta di configurare il Mobile Node con NAI e password:
sarebbe in ogni caso necessario esaminare il messaggio di registrazione.

La realizzazione delle procedure di autenticazione ed autorizzazione del Mobile Node ha richiesto lo sviluppo di due differenti funzioni denominate *authentication_fase* e *delete_autorization*.

Per consentire l'inclusione di tali funzioni con il resto del software Dynamic-Hut Mobile IP è stato necessario creare i files *authentication.c* ed *elimina_entry.c*; a sua volta i prototipi delle funzioni sono stati inseriti nei file *authentication.h* ed *elimina_entry.h*.

In fase di progettazione si è rimarcata l'importanza di effettuare autenticazioni locali del Mobile Node:
il protocollo Mobile IP richiede che un MN, durante la sua permanenza in una Foreign Network, aggiorni il proprio *binding* attraverso l'invio di messaggi di registrazione.
Tali richieste non devono essere autenticate dall'Home AAA Server, ma dalla stessa Radius Mobility Interface in quanto presuppongono una precedente verifica del Mobile Node da parte del Server Radius presente nell'Home Internet Service Provider.
Da ciò deriva la necessità di gestire una sorta di tabella attraverso la quale la RMI potrà essere in grado di stabilire se il particolare Mobile Node, che ha inviato un Registration Request Message, è stato precedentemente autenticato dal Radius Server oppure no:
nel primo caso la tabella presenterà un entry contenente un identificativo del Mobile Node (Home Address).

L'introduzione di tale tabella, che non sarà altro che un'array di puntatori a stringhe di dimensione pari al massimo numero di Mobile Node gestibili dal Foerign Agent, richiede di risolvere un ulteriore problema:
l'entry non dovrà possedere una "vita" illimitata, ma dovrà rispecchiare la durata della permanenza del Mobile Node nella Foreign Network.

Per fornire una descrizione più dettagliata, si analizzeranno separatamente le due funzioni.

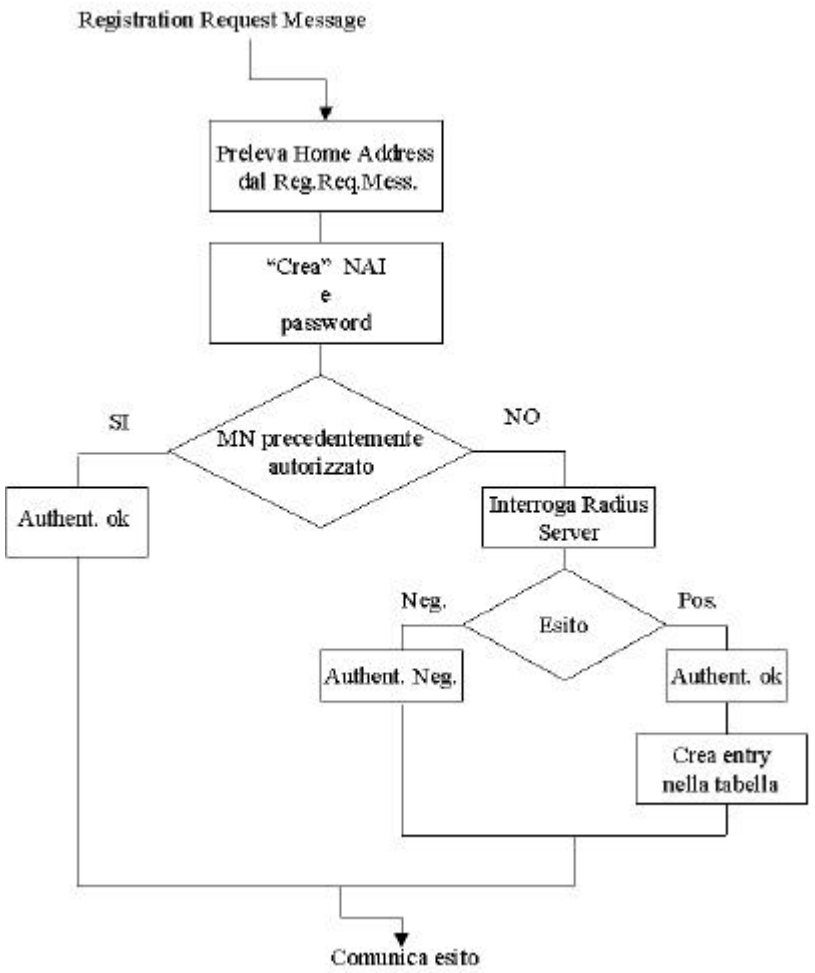
authentication_fase

Tale funzione interverrà in seguito alla ricezione di un Registration Request Message da parte del Mobile Node.

Riceverà in input l'intero messaggio di registrazione e restituirà una variabile indicante l'esito dell'autenticazione. In base al valore assunto da tale variabile il Foreign Agent sarà abilitato o meno al rilancio del messaggio di registrazione all'Home Agent.

L'autenticazione del Mobile Node sarà effettuata localmente o tramite il Server AAA residente nell'Home Domain a seconda dell'esistenza o meno di un entry nella tabella.

Il seguente diagramma di flusso illustra la sequenza delle operazioni:



E' chiaro che la entry relativa al Mobile Node dovrà essere inserita nella prima posizione disponibile della tabella.
Per completezza si riporta il comando che permette di effettuare la chiamata al Radius Server e quindi di emulare il comportamento del Network Access Server:

radpwts –p 1645 –s pc-lunx2.gialla.netlab.it –w *password Network Access Identifier*

L'opzione –p consente di specificare il numero della porta UDP, -s consente di specificare il Server al quale inviare l'*Access Request Message* (l'esempio fa riferimento al Foreign AAA Server), -w consente di specificare la password dell'utente ed infine il comando richiede di inserire la NAI.
Si tenga presente che per gestire più terminali, e quindi strutturare adeguatamente il comando radpwtst, è stato necessario effettuare una serie di concatenazione di stringhe attraverso l'utilizzo del comando *strcat* disponibile nella libreria indicata dal file header *string.h*.

delete_autorization

Per gestire l'eliminazione dei Mobile Node dalla tabella locale, è necessario introdurre una funzione che si occupi esclusivamente di tale compito.
Il problema non è stato quello di gestire l'effettiva eliminazione della entry, piuttosto quello di determinare il principio secondo il quale basare tale eliminazione.
La soluzione è stata individuata sfruttando una caratteristica del protocollo Mobile IP:
il Foreign Agent, per ciascun Mobile Node da lui gestito, deve mantenere un binding nel quale inserire:

- Home Address;

- indirizzo IP dell'Home Agent;
- Lifetime della registrazione.

E' chiaro, quindi, che anche il Foreign Agent dovrà gestire l'eliminazione dei *binding* non più validi.
Seguendo tale approccio, si è effettuato uno studio del software Dynamic-Hut Mobile IP allo scopo di individuare la parte del codice che si occupa di tale questione.
Una volta stabilito dove intervenire si è inserita la chiamata alla funzione.
La funzione riceverà come input l'Home Address del Mobile Node ed attraverso tale informazione sarà in grado di:

- eliminare la entry relativa;
- "riordinare" tutta la tabella.

Per concludere l'analisi, si riportano delle "fotografie", tratte dal *debug* del software, indicative delle operazioni sopra descritte:

invio di un Agent Advertisement da parte del Fereign Agent

```
sending agent advertisement
 * header, len=8
 * agentadv ext, len=12
 * Dynamics ext, len=8
 * total len: 28
send_agent_advs:next agentadv:1002543358.417100 diff=30168msec
```

ricezione del primo Registration Request Message da parte del Foreign Agent

```
Got UDP message(eth0)
Received 55 bytes from 10.1.0.5
        dst_addr=10.1.3.11
        TTL=255
Registration Request
        type 1, lifetime 300
        home_addr 10.1.0.5, ha_addr 10.1.0.14
```

```
        co_addr 10.1.3.11
```

autenticazione del Mobile Node effettuata dal Server Radius

```
INDIRIZZO IP DEL MOBILE NODE = 10.1.0.5
INDIRIZZO IP DELL' HOME AGENT= 10.1.0.14
FASE DI AUTENTICAZIONE
Merit AAA server Version 3.6B , licensed software
COPYRIGHT 1992, 1993, 1994, 1995, 1996, 1997, 1998
THE REGENTS OF THE UNIVERSITY OF MICHIGAN
ALL RIGHTS RESERVED

'10.1.0.5@pc-server.rossa.netlab.it' authentication OK
MOBILE NODE AUTORIZZATO
```

rilanco del messaggio di registrazione all'Home Agent

```
Handling request from MN 10.1.0.5
No binding for MN => making new binding
        unconfirmed binding
Adding unconfirmed request data
        assuming lowest FA (i.e. request from MN)
Forwarding request upwards
 * copying up to and including mh_auth (len ==> 55)
forward_request ==> HA 10.1.0.14
```

conclusione della procedura di registrazione

```
Got UDP message(eth0)
Received 199 bytes from 10.1.0.14
        dst_addr=10.1.3.11
        TTL=61
Registration Reply
        type 3, code 0, lifetime 300
        home_addr 10.1.0.5, ha_addr 10.1.0.14
Handling reply
create_tunnel_upwards: Highest FA - creating tunnel to HA
tunnel_add 10.1.0.14
        adding tunnel[TUNL0], remote=10.1.0.14, local=10.1.3.11
create_tunnel_upwards: connecting tunnel
Forwarding reply
 * copying up to and including mh_auth (len ==> 67)
 *  sending 92 bytes to 10.1.0.5:1025
```

autenticazioni successive del Mobile Node

```
Got UDP message(eth0)
Received 55 bytes from 10.1.0.5
        dst_addr=10.1.3.11
        TTL=255
Registration Request
        type 1, lifetime 300
        home_addr 10.1.0.5, ha_addr 10.1.0.14
        co_addr 10.1.3.11
INDIRIZZO DEL MOBILE NODE PRELEVATO NELLA RICHIESTA DI
REGISTRAZIONE=10.1.0.5
MOBILE NODE AUTORIZZATO PRECEDENTEMENTE
Handling request from MN 10.1.0.5
```

eliminazione della entry relativa al Mobile Node

```
check_bindings: binding expired
        binding->mn_addr = 10.1.0.5
INDIRIZZO DEL MOBILE NODE DA ELIMINARE =10.1.0.5
        binding->lower_addr = 10.1.0.5
        Highest FA - deleting tunnel to HA
tunnel_delete 10.1.0.14
        device=TUNL0, num=0, dst=10.1.0.14
```

9.5 RMI: funzionalità di Accounting

Per implementare la procedura di Accounting è stato sviluppato uno Script Shell Bash richiamabile attraverso il comando *system*.
Inizialmente si sono dovuti risolvere due problemi distinti:

- *Individuazione dell'esatto punto in cui richiamare lo Script*

  E' chiaro che le operazioni di Accounting devono essere avviate solamente in seguito alla registrazione del Mobile Node da parte del Foreign Agent.

  Per risolvere il problema si è fatto ricorso ad una caratteristica del protocollo Mobile IP:

  avvenuta la registrazione del Mobile Node, il protocollo richiede l'instaurazione di un tunnel tra l'Home Agent ed il Foreign Agent.

Da ciò è nata l'esigenza di individuare, con precisione, la parte di codice, del software Dynamic-Hut Mobile IP, interessata all'attivazione dell'interfaccia di tunnel.
In particolare si è dovuto determinare l'interfaccia associata con il Mobile Node in questione.

- *Individuazione del meccanismo necessario per monitorare le risorse*

  Scopo finale delle procedure di Accounting è quello di ottenere un "resoconto" delle attività del Mobile Node.
  E' necessario, quindi, stabilire le modalità attraverso le quali monitorare i parametri di Accounting: pacchetti inviati, pacchetti ricevuti, byte inviati, byte ricevuti.
  Si è così deciso di adottare uno *sniffer* di rete attivabile attraverso il comando ***tcpdump***. Una caratteristica di *tcpdump* è di essere facilmente configurabile:
  è possibile impostare lo *sniffer* in maniera tale da "catturare" solamente i pacchetti che rispecchiano particolari condizioni.
  In particolare, è possibile configurarlo con l'obiettivo di prelevare i pacchetti che transitano su di una specifica interfaccia di rete e che sono caratterizzati da ben definiti Source Address e Destination Address.

Dalle considerazioni sopra esposte deriva che:

- lo Script Shell sarà richiamato in seguito all'attivazione dell'interfaccia di tunnel;
- riceverà in input:
  - home address del Mobile Node
  - indirizzo IP dell'Home Agent
  - interfaccia di tunnel, TUNLi, che il Foreign Agent ha associato con il Mobile Node.

In base a tali informazioni è possibile individuare i messaggi destinati al Mobile Node e quelli da lui inviati. In particolare si prenderanno in considerazione i pacchetti TCP e UDP:

pacchetti inviati

Lo sniffer si deve mettere in ascolto sull'interfaccia ethernet:
tcpdump -p -l -n -q -i eth0 ip proto\\ tcp or ip proto \\ udp and src host *home address*

pacchetti ricevuti

Il protocollo Mobile IP stabilisce che i pacchetti destinati al Mobile IP siano inviati, tramite tunnel, dall'Home Agent e ricevuti dal Foreign Agnet:
tcpdump -l -n -q -i *interfaccia tunnel* ip proto\\ tcp or ip proto \\ udp and src host *indirizzo IP Home Agent*

Le opzioni fornite al comando *tcpdump* consentono di ottenere un output compatto e ben definito dal quale sarà possibile "prelevare" i parametri di Accounting.

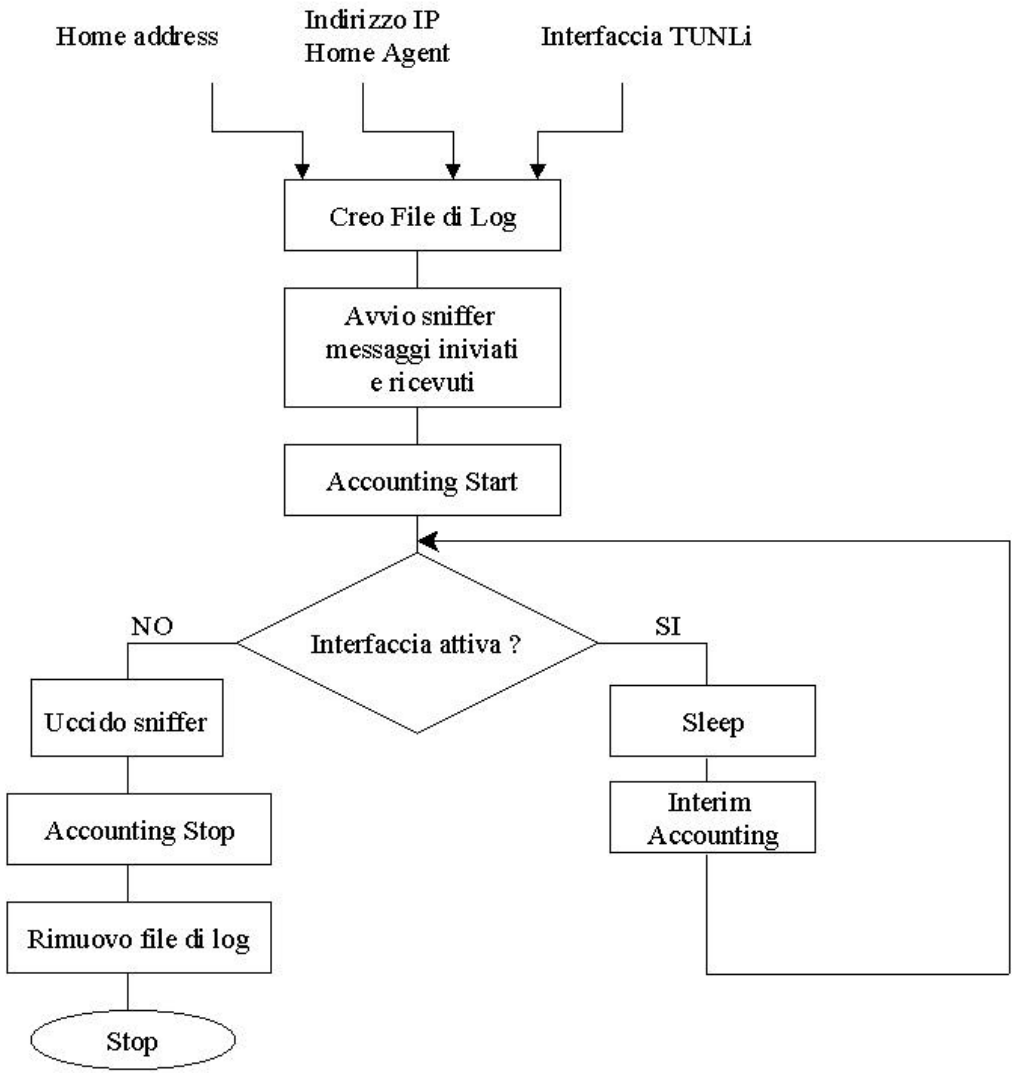
Utilizzare come mezzo di riscontro l'interfaccia di tunnel, consente di risolvere un ulteriore problema:
per evitare di interrompere l'esecuzione del programma principale, lo Script Shell deve essere "lanciato" in modalità *background*. E' quindi importante individuare un meccanismo che permetta di bloccarne il funzionamento in maniera automatica.
Il protocollo Mobile IP prevede che l'interfaccia di tunnel sia eliminata una volta scaduto il *binding* del Mobile Node.
Sfruttando tale caratteristica, ed analizzando in maniera opportuna l'output del comando *ifconfig* (per stabilire se l'interfaccia sia ancora attiva), sarà possibile

interrompere lo Script Shell attraverso "l'uccisione" di *tcpdump* effettuata mediante il comando *kill*.

Prima di mostrare il diagramma di flusso caratterizzante lo Script Shell è necessario rimarcare un ultimo aspetto:
i messaggi inviati al Server Radius, tramite il comando *radpwtst*, devono contenere i parametri di Accounting, è quindi necessario prelevare singolarmente, dall'output di *tcpdump*, il numero di pacchetti inviati, il numero di byte inviati, il numero di pacchetti ricevuti ed il numero di byte ricevuti.
Tale obiettivo è stato raggiunto attraverso l'utilizzo di *file log* di durata pari al periodo di esecuzione dello Script Shell. Più precisamente:

- sfruttando l'operazione di redirezione dell'output di un comando sarà possibile inserire, in file differenti, l'output derivante, rispettivamente, dallo sniffer dei messaggi inviati e ricevuti;
- attraverso il comando *awk* è stato possibile prelevare i singoli parametri di Accounting.

Di seguito sono schematizzate, tramite diagramma di flusso, le operazioni eseguite dallo Script Shell :
l'invio periodico di messaggi di *Interim Accounting* è evidenziato dalla necessità di inserire, all'interno del ciclo, un ritardo di durata pari al periodo di trasmissione di tali messaggi.



Ritengo che sia importante mostrare il resoconto complessivo della procedura di Accounting che sarà memorizzato nel Foreign AAA Server e che potrà essere utilizzato per finalità di Billing.

Nell'esempio, la quantità di informazioni inviate dal Mobile Node 10.1.0.5 sarà molto elevata in quanto si è simulato il trasferimento di un file di dimensioni notevoli dal Mobile Node, presente nella Foreign Network, ad un'altra macchina del laboratorio NetLab:

```
Wed Sep 26 15:47:33 2001
        User-Name = "10.1.0.5"
        Service-Type = Outbound
        NAS-IP-Address = 127.0.0.1
```

```
        NAS-Port = 1
        Acct-Status-Type = Start
        Acct-Interim-Interval = "150"


Wed Sep 26 15:50:10 2001
        User-Name = "10.1.0.5"
        Service-Type = Outbound
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        Acct-Input-Packets = 6
        Acct-Output-Packets = 6
        Acct-Input-Octets = 168
        Acct-Output-Octets = 360


Wed Sep 26 15:52:59 2001
        User-Name = "10.1.0.5"
        Service-Type = Outbound
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        Acct-Input-Packets = 7414
        Acct-Output-Packets = 15506
        Acct-Input-Octets = 3689
        Acct-Output-Octets = 23025665

Wed Sep 26 15:55:47 2001
        User-Name = "10.1.0.5"
        Service-Type = Outbound
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        Acct-Input-Packets = 11341
        Acct-Output-Packets = 22537
        Acct-Input-Octets = 3745
        Acct-Output-Octets = 32273465




Wed Sep 26 15:58:40 2001
        User-Name = "10.1.0.5"
        Service-Type = Outbound
        NAS-IP-Address = 127.0.0.1
        NAS-Port = 1
        Acct-Status-Type = Stop
        Acct-Input-Packets = 11341
        Acct-Output-Packets = 22537
        Acct-Input-Octets = 3745
        Acct-Output-Octets = 3227346
```

Si osservi che, pur avendo specificato un *Interim-Interval* pari a 150 secondi, l'invio dei pacchetti, a causa della velocità di calcolo della macchina, non potrà rispettare in maniera precisa tale valore.

Per concludere si riportano alcune fasi significative dell'intero processo di Accounting:

invio accounting start

```
INDIRIZZO IP DEL TERMINALE A CUI FARE ACCOUNTING= 10.1.0.5
IL NUMERO DEL TUNNEL RISULTA =TUNL0
AVVIO LA PROCEDURA DI ACCOUNTING
Kernel filter, protocol ALL, TURBO mode (575 frames), datagram packet
socket
tcpdump: listening on TUNL0
Kernel filter, protocol ALL, TURBO mode (575 frames), datagram packet
tcpdump: listening on eth0
Merit AAA server Version 3.6B , licensed software
COPYRIGHT 1992, 1993, 1994, 1995, 1996, 1997, 1998
THE REGENTS OF THE UNIVERSITY OF MICHIGAN
ALL RIGHTS RESERVED

'10.1.0.5' authentication OK
```

invio interim accounting

```
INVIO INTERIM ACCOUNTING
Merit AAA server Version 3.6B , licensed software
COPYRIGHT 1992, 1993, 1994, 1995, 1996, 1997, 1998
THE REGENTS OF THE UNIVERSITY OF MICHIGAN
ALL RIGHTS RESERVED

'10.1.0.5' authentication OK
```

invio accounting stop

```
TUNL0: error fetching interface information: Device not found

23 packets received by filter
20 packets received by filter
Merit AAA server Version 3.6B , licensed software
COPYRIGHT 1992, 1993, 1994, 1995, 1996, 1997, 1998
THE REGENTS OF THE UNIVERSITY OF MICHIGAN
ALL RIGHTS RESERVED

'10.1.0.5' authentication OK
```

10 Test di laboratorio

Lo scopo del presente capitolo è di verificare le prestazioni dell'architettura sviluppata. Più precisamente si vuole accertare che il sistema soddisfi i requisiti specificati in sede di progetto.
Tutti i test sono stati effettuati nei locali dello IASI-CNR, in particolare, con riferimento alla struttura del laboratorio NetLab riportata nel precedente capitolo, si è fatto uso, complessivamente, delle seguenti risorse:

- sotto-reti utilizzate:
  - rete rossa;
  - rete gialla;
- macchine utilizzate:
  - pc-linux.rossa.netlab.it (Home Agent, Home Radius Server, Home Radius Mobility Interface);
  - pc-server.rossa.netlab.it (Mobile Node);
  - pc-linux1.rossa.netlab.it (Mobile Node);
  - pc-linux2.gialla.netlab.it (Foreign Agent, Foreign Radius Server, Foreign Radius Mobility Interface).

10.1 Premessa ai test

I risultati dei test sono presentati in forma tabellare e raccolti in un successivo paragrafo.
Le notazioni utilizzate per redigere le schede dei test sono:

- **Nome test**

  Consente di identificare univocamente ciascun test. Di seguito si riporta la convenzione utilizzata per la classificazione dei test:
  Nome Test:[(tipo_test)/(numerazione)]
  tipo_test: **S**oftware|**AUT**hentication|**ACC**ounting
  numerazione: numerazione crescente del test nell'ambito dello stesso tipo

- **Ambiente di test**

  E' fornita una schematizzazione delle risorse utilizzate per effettuare il particolare test.

- **Obiettivo**

  Rappresenta lo scopo del test.

- **Azioni**

  Elenco delle azioni svolte per eseguire i test.

- **Risultato**

  Esito del test e breve descrizione.

10.2 Classificazione dei test

Per realizzare il piano dei test, si è effettuata una classificazione degli stessi in tre gruppi distinti che rispecchiano i requisiti di progetto.

I primi test effettuati, appartenenti alla categoria Software, consentono di verificare l'efficienza dei prodotti utilizzati per la realizzazione del sistema: Dynamic-Hut Mobile IP e Merit Radius Server.
In particolare, lo scopo dei test è di accertare la corrispondenza dei software suddetti con le caratteristiche basilari dei rispettivi protocolli.

Per quanto concerne la verifica delle prestazioni del sistema sviluppato, si è deciso di suddividere i test nelle categorie Autenticazione ed Accountig.

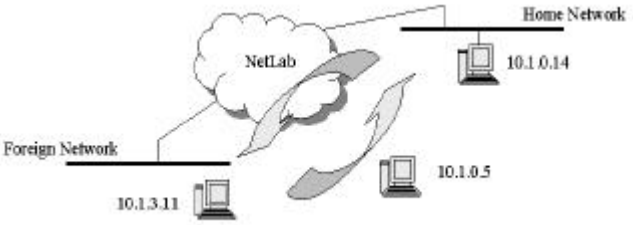
In tal modo è stato possibile analizzare, con maggior dettaglio, le funzionalità della Radius Mobility Interface. Lo scopo dei test è stato, principalmente, quello di verificare il corretto scambio di messaggi tra le entità coinvolte e quindi di accertare l'effettivo "colloquio" tra il protocollo Mobile IP ed il protocollo RADIUS.

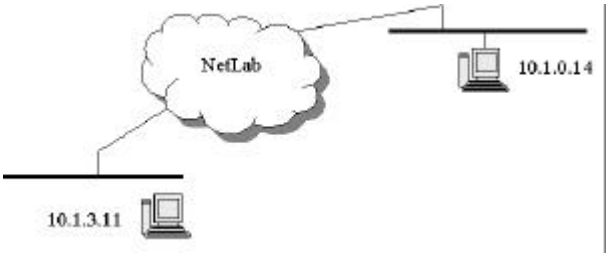
10.3 Risultati dei test

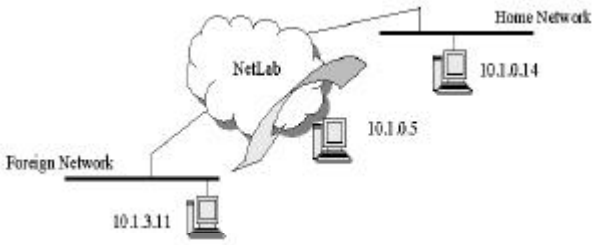
In questa sezione sono riportati i risultati ottenuti nella fase di sperimentazione. I risultati dei singoli test vengono mostrati in forma schematica, evidenziandone il successo o l'insuccesso e dandone una breve descrizione.
La verifica dell'effettivo raggiungimento degli obiettivi è stata effettuata attraverso l'analisi dei messaggi di debug forniti dal sistema sotto esame.
Tutte le prove effettuate sono state condotte con successo.

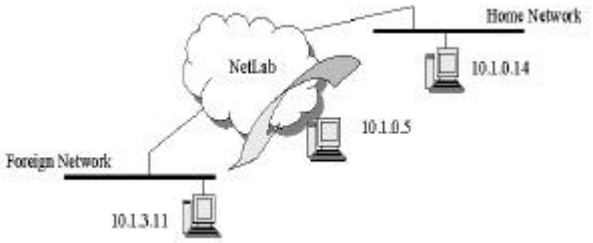
TIPO TEST	RISULTATO	DESCRIZIONE
CATEGORIA SOFTWARE		
S/1	OK	Verificare il rispetto dei requisiti del protocollo Mobile IP
S/2	OK	Verificare il rispetto dei requisiti del protocollo RADIUS
CATEGORIA AUTENTICAZIONE		
AUT/1	OK	Autenticazione di un MN che richiede i servizi di un Foreign Agent
AUT/2	OK	Gestione di un esito negativo della richiesta di autenticazione
AUT/3	OK	Autenticazioni del Mobile Node nell'ambito di una stessa sessione
AUT/4	OK	Eliminazione della entry necessaria per le autenticazioni locali
AUT/5	OK	Verificare la scalabilità della Radius Mobility Interface
AUT/6	OK	Autenticazione di un MN che fa ritorno nella Home Newtork
CATEGORIA ACCOUNTING		
ACC/1	OK	Invio di un Accounting Start Message
ACC/2	OK	Invio di un Accounting Stop Message
ACC/3	OK	Invio degli Interim Accounting Message
ACC/4	OK	Verifica dell'effettiva memorizzazione dei parametri di accounting

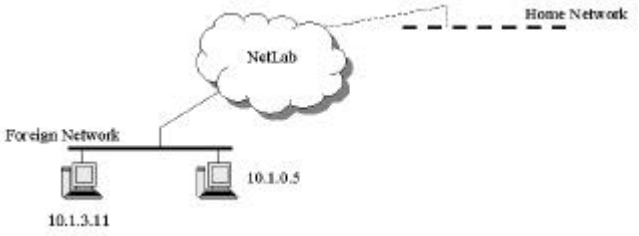
10.4 Test effettuati

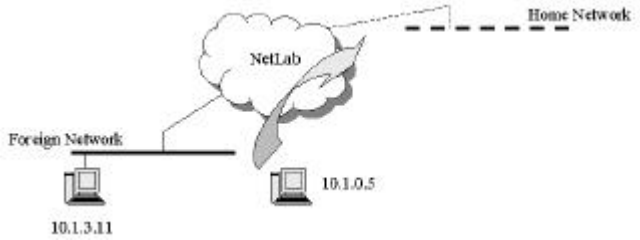
TEST	S/1
AMBIENTE	10.1.0.5 Mobile Node 10.1.0.14 Home Agent 10.1.3.11 Foreign Agent 
OBIETTIVO	Verificare il rispetto dei requisiti del protocollo Mobile IP
AZIONI	?? registrazione del MN nella Foreign Network ?? instaurazione tunnel tra HA e FA ?? invio e ricezione datagrammi da parte del MN ?? deregistrazione del MN nella Home Network
RISULTATO	OK Il software è conforme alla rfc 2002

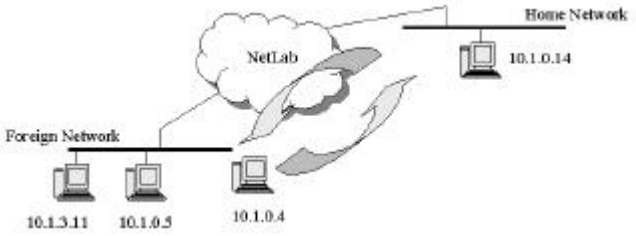
TEST	S/2
AMBIENTE	10.1.3.11 Radius Server 10.1.0.14 Radius Server 
OBIETTIVO	Verificare il rispetto dei requisiti del protocollo RADIUS
AZIONI	?? autenticazione locale di un utente ?? autenticazione di un utente tramite Proxy Server ?? invio dei messaggi Accounting Start e Accounting Stop ?? invio dei messaggi di Interim Accounting
RISULTATO	OK Il software è conforme alle specifiche delle rfc

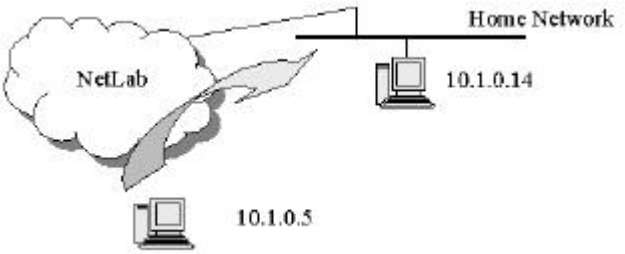
TEST	AUT/1
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 10.1.0.14 Home Radius Server / Home Agent 
OBIETTIVO	Autenticazione di un MN che richiede i servizi di un Foreign Agent
AZIONI	?? il MN invia un Registration Request Message al FA ?? il FA comunica la necessità di autenticare il MN alla RMI ?? la RMI invia un Access Request Message al Foreign Radius Server ?? il Foreign Radius Server rilancia la richiesta all'Home Radius Server ?? la RMI riceve l'esito dell'autenticazione e lo comunica al FA ?? il FA elabora il messaggio di registrazione
RISULTATO	OK Il Foreign Agent elabora il messaggio di registrazione solo in seguito all'autenticazione del MN effettuata dall'Home Radius Server

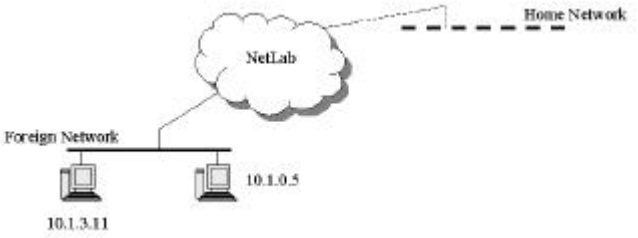
TEST	AUT/2
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 10.1.0.14 Home Radius Server / Home Agent 
OBIETTIVO	Gestione di un esito negativo della richiesta di autenticazione
AZIONI	?? il MN invia un Registration Request Message al FA ?? il FA comunica la necessità di autenticare il MN alla RMI ?? la RMI invia un Access Request Message al Foreign Radius Server ?? il Foreign Radius Server rilancia la richiesta all'Home Radius Server ?? la RMI riceve un Access Reject dal Raius Server ?? la RMI comunica l'esito negativo dell'autenticazione al FA ?? il FA non rilancia la richiesta di registrazione
RISULTATO	OK Il Foreign Agent rifiuta la richiesta di registrazione a causa della non autenticazione del MN

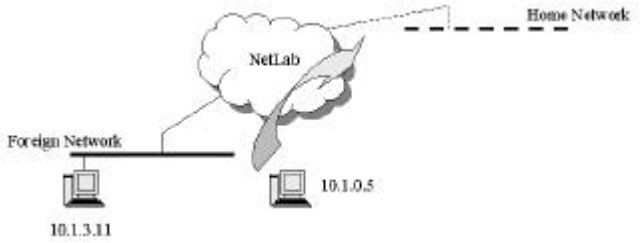
TEST	AUT/3
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Autenticazioni del Mobile Node nell'ambito di una stessa sessione
AZIONI	?? il MN invia un Registration Request Message al FA ?? il FA comunica la necessità di autenticare il MN alla RMI ?? la RMI autentica localmente il MN e comunica l'esito al FA ?? il FA elabora il messaggio di registrazione
RISULTATO	OK Un Mobile Node, inizialmente autenticato dall'Home Radius Server, subirà le successive autenticazioni all'interno della stessa Foreign Network

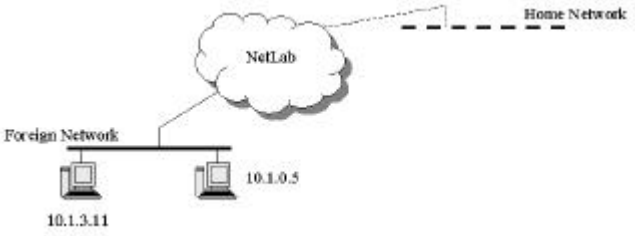
TEST	AUT/4
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Eliminazione della entry necessaria per le autenticazioni locali
AZIONI	?? il MN abbandona la Foreign Network ?? il FA, allo scadere di un timeout, elimina il binding relativo al MN ?? Contemporaneamente anche la RMI effettua l'eliminazione della entry necessaria per effettuare le autenticazioni locali del MN
RISULTATO	OK La RMI elimina in maniera corretta l'entry utilizzata per le autenticazioni locali. In questo modo, nel caso in cui il MN torni nella stessa Foreign Network, l'autenticazione avverrà, nuovamente, tramite l'Home AAA Server.

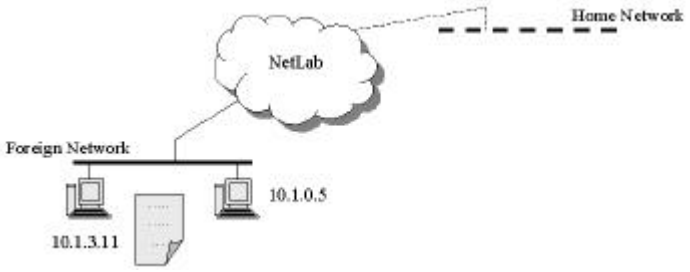
TEST	AUT/5
AMBIENTE	10.1.0.5 Mobile Node 10.1.0.4 Mobile Node 10.1.0.14 Home Radius Server / Home Agent 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Verificare la scalabilità della Radius Mobility Interface
AZIONI	?? il MN 10.1.0.4 invia una richiesta di registrazione ?? ripetizione del test AUT/1 nei confronti del MN 10.1.0.4 ?? ripetizione del test AUT/2 nei confronti di entrambi i MN ?? il MN 10.1.0.4 abbandona la Foreign Network ?? ripetizione del test AUT3 nei confronti del MN 10.1.0.4
RISULTATO	OK La RMI è in grado di gestire adeguatamente sia l'autenticazione iniziale, sia le autenticazioni successive, sia l'eliminazione della entry.

TEST	AUT/6
AMBIENTE	10.1.0.5 Mobile Node 10.1.0.14 Home Radius Server / Home Agent / Radius Mobility Interface 
OBIETTIVO	Autenticazione di un MN che fa ritorno nella Home Newtork
AZIONI	?? il MN invia una richiesta di de-registrazione ?? l'HA, tramite la RMI, invia una richiesta di autenticazione all'Home AAA Server ?? se l'autenticazione va a buon fine, l'HA elabora il messaggio di de-registrazione
RISULTATO	OK L'Home Agent elabora il messaggio di registrazione solo in seguito all'autenticazione del MN effettuata dall'Home Radius Server

TEST	ACC/1
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Invio di un Accounting Start Message
AZIONI	?? il FA elabora il Registration Reply Message ?? il FA comunica la necessità di avviare le procedure di accounting alla RMI ?? la RMI invia un Accounting Start Message al Foreign Radius Server ?? ricevuto un Acknowledgement dal Server la RMI attiva i meccanismi necessari per monitorare l'utilizzo delle risorse
RISULTATO	OK La Radius Mobility Interface gestisce adeguatamente lo scambio di messaggi con il Foreign Radius Server ed avvia correttamente gli "sniffer" di rete.

TEST	ACC/2
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Invio di un Accounting Stop Message
AZIONI	?? il MN abbandona la Foreign Network ?? il FA, allo scadere di un timeout, elimina il binding relativo al MN ?? la RMI elimina l'entry relativa al MN ed interrompe il processo di misurazione dell'utilizzo delle risorse ?? la RMI invia un Accounting Stop Message al Foreign Radius Server ?? Il Foreign Radius Server invia un Acknowledgement alla RMI
RISULTATO	OK La Radius Mobility Interface gestisce adeguatamente lo scambio di messaggi con il Foreign Radius Server ed interrompe correttamente gli "sniffer" di rete.

TEST	ACC/3
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Invio degli Interim Accounting Message
AZIONI	?? la RMI, ad intervalli regolari, preleva i parametri di accounting ?? svolta tale operazione, invia un Interim Accounting Message al Foreign Radius Server ?? Il Foreign Radius Server invia un Acknowledgement alla RMI
RISULTATO	OK La Radius Mobility Interface gestisce adeguatamente lo scambio di messaggi con il Foreign Radius Server e comunica correttamente con gli “sniffer” di rete.

TEST	ACC/4
AMBIENTE	10.1.0.5 Mobile Node 10.1.3.11 Foreign Radius Server / Foreign Agent / Radius Mobility Interface 
OBIETTIVO	Verifica dell'effettiva memorizzazione dei parametri di accounting
AZIONI	?? la RMI invia un Accounting Start Message al Foreign Radius Server ?? parallallelamente è stato avviato uno sniffer di rete indipendente ?? la RMI invia periodicamente Interim Accounting ?? la RMI invia un Accounting Stop Message al Foreign Radius Server ?? viene bloccato lo sniffer di rete
RISULTATO	OK Il resoconto dei dati di accounting memorizzato nel Foreign Radius Server è compatibile con quello fornito dallo sniffer

Conclusioni

Nel presente lavoro è stata proposta un'architettura in grado di affiancare al protocollo Mobile IP le procedure di Authentication, Authorizationand Accounting.

Un'attenta ricerca di mercato ha consentito di stabilire che il protocollo AAA attualmente più diffuso risulta RADIUS.
Questo significa che gli odierni Internet Service Provider saranno favorevoli all'introduzione di un nuovo servizio, quale ad esempio Mobile IP, se questo non richiede, almeno nel breve periodo, una completa revisione delle infrastrutture di rete.
L'utilizzo di RADIUS, come "ossatura" del sistema proposto nella tesi, potrebbe sembrare in contrasto con la tendenza, all'interno delle comunità scientifiche, di proporre come protocollo AAA il recente DIAMETER.
In realtà occorre tener presente che DIAMETER è attualmente in fase di sviluppo, sicuramente porterà delle innovazioni, ma non è detto che gli ISP siano così propensi ad abbandonare un protocollo altamente affidabile ed efficiente come RADIUS.
Proprio per questo motivo, si è voluto progettare ed implementare un sistema AAA per Mobile IP tenendo bene in mente le attuali tecnologie di cui si dispone.
Inoltre si è osservato più volte che l'architettura proposta non ha richiesto nessuna modifica nei confronti dell'implementazione scelta del protocollo RADIUS.
Questo significa che è facilmente trasportabile ed in tal senso nulla vieta di sfruttare la Radius Mobility Interface come interfaccia tra il protocollo Mobile IP e lo stesso DIAMETER.

Nella realizzazione del sistema si sono incontrate difficoltà a causa della completa mancanza di compatibilità tra l'implementazione del protocollo Mobile IP e le procedure di AAA.
Tale caratteristica non è peculiare del solo software scelto, in quanto tutte le implementazioni disponibili propongono delle innovazioni solamente dal punto di vista delle specifiche funzionali proprie di Mobile IP.

Per interpretare correttamente alcune caratteristiche del software Dynamic-Hut Mobile IP ho ritenuto opportuno istaurare una corrispondenza, tramite e-mail, con il gruppo di ricerca, presente all'interno dell'Università di Helsinki, che si occupa del progetto Mobile IP, suscitando così un certo interesse per il lavoro svolto nell'ambito della tesi.
Il risultato è stato il rilascio di nuove versioni di Dynamic-Hut le quali possiedono innovazioni sia dal punto di vista prestazionale, sia nei confronti delle problematiche inerenti all'interfacciamento con il protocollo AAA.
Ovviamente, a causa dell'avanzato stato di preparazione della tesi, non ho potuto usufruire di tali caratteristiche.

Le innovazioni introdotte saranno usufruibili per gli sviluppi del sistema proposto.
Sarà possibile interagire in maniera più profonda con il protocollo Mobile IP, ad esempio, si potrà "ampliare" la Radius Mobility Interface per consentire al Mobile Node di acquisire dinamicamente informazioni quali l'indirizzo IP dell'Home Agent, il proprio Home Address ed infine il Security Association da condividire con l'Home Agent ed eventualmente con il Foreign Agent.

Ulteriori sviluppi possono essere ricercati nell'effettiva implementazione del modello di *Business System* proposto in fase di progettazione.
Si riuscirà in questo modo a completare l'intero processo di Accounting, dalla fase di monitorizzazione delle risorse di rete a quella di fatturazione dell'utente.

Indice delle Figure

Indice delle Tabelle

Bibliografia

[1] C.Perkins, *"IP Mobility Support for Ipv4"* draft-ietf-mobileip-rfc2002-bis-03, September 2000

[2] E.Comer, *Internet Working with TCP/IP principles, protocols, and architectures*, Prentice Hall, 2000

[3] C.Perkins, *"Mobile IP"* IEEE CommunicationS magazine, May 1997

[4] S.Deering, *"ICMP Router Discovery Messages"* rfc1256, September 1991

[5] J.Postel, J.Reynolds, *"Assigned Number"* rfc1700, October 1994

[6] A.Roveri, M.Listanti, N.B.Melazzi, *"Retematica, parte seconda"*, Università degli studi "La Sapienza", Dipartimento INFOCOM, Novembre 2000

[7] C.Perkins, *"Minimal Encapsulation within IP"* rfc 2004, October 1996

[8] S.Hanks, T.Li, D.Farinacci, P.Traina, *"Generic Routing Encapsulation"* rfc 1701, October 1994

[9] C.Perkins, *"IP Encapsulation within IP"* rfc 2003, October 1996

[10] G.Montenegro, *"Reverse Tunneling for Mobile IP"* rfc 2344, January 2001

[11] C.Perkins, *"Mobility Networking through Mobile IP"* IEEE Internet Computing, 1998

[12] R.Rivest, *"The MD5 Message-Digest Algorithm"* rfc1321, April 1992

[13] P.Calhoum, C.Perkins, *"Mobile IP Network Access Identifier Extension for IPv4"* rfc 2794, March 2000

[14] L.Veltri, *"Mobilità su Internet"* Dispense corso di Sistemi di Commutazione, a.a 1999/2000

[15] C.Perkins, David B. Johnson, *"Route Optimization in Mobile IP"* draft-ietf-mobileip-optim-10, November 2000

[16] David B. Johnson, *"Scalable Support for Trasparent Mobile IP Host Internet"*

[17] 3G TR 23.923, *"Combined GSM and Mobile IP Mobility Handling in UMTS IP CN"*, May 2000

[18] C.Perkins, David B.Johnson, *"Special Tunnels for Mobile IP"* draft-ietf-mobileip-spectun-00, November 1997

[19] C.Perkins, David B.Johnson, *"Registration keys for Route Optimization"* draft-ietf-mobileip-regkey-03, July 2000

[20] E. Gustafsson, A.Johnson, C.Perkins, *"Mobile IP Regional Registration"* draft-ietf-mobileip-reg-tunnel-0.4, March 2001

[21] Nicola Blefari-Melazzi, *"Internet: Architettura, Principali Protocolli e Linee Evolutive"*, Dipartimento di Ingegneria Elettronica e dell'Informazione, Università di Perugia, Luglio 2000

[22] M.Listanti, *" La rete Internet ed il protocollo IP"*, dispense del corso di Sistemi di Commutazione, a.a 1999/2000

[23] Sami Kivisaari, *"A Comparison between Mobile IPv4 and Mobile IPv6"*, Departement of Computer Science and Engineering, Helsinki University of Technology, May 2000

[24] W.Fritsche, F.Heissenhuber, *"White paper on Mobile IPv6"*, IPv6 Forum, August 2000

[25] Andràs G. Valkò, *"Cellular IP: a new Approch to Intenet Host Mobility"*, January 1999

[26] Andràs G. Valkò, *"On the Analysis of Cellular IP Access Network"*

[27] A.Katouzian, *"Cellular IP Report"*, 3G Mobile Communication Technologies, Conference Publication No.471, 2000

[28] A.Campbell, J.Gomez, Z.Turanyi, A.Valkò, *"Cellular IP"*, draft-valko-cellularip-01, October 1999

[29] Javier Gozàlvez Sempere, *"An overview of the GSM system"*, Communication Division of University of Strathclyde , Glasgow

[30] C.Bettstetter, Hans-Jorg Vogel, J.Eberspacher *"GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols, and Air Interface"*, IEEE Communications Surveys, 1999

[31] "*GPRS White Paper*", Cisco Systems, 2000

[32] Jani Kokkonen, *"General Packet Radio Service*", Helsinki University of Technology, January 2000

[33] "*Universal Mobile Telecommunications System (UMTS), Combined GSM and Mobile IP mobility handling in UMTS CN"*, ETSI TR 123 923 v3.0.0, May 2000

[34] Seppo Keikkinen, Si Hang, *"Interworkin of GPRS/UMTS with Mobile IP"*, Tampere University of Technology, 2000

[35] B.Adoba, J.Arkko, D.Harrington, *"Introduction to Accounting Management"*, rfc 2975, October 2000

[36] N.Brownlee, C.Milles, G.Ruth, *"Traffic Flow Measurement: Architecture*", rfc 2063, January 1997

[37] M.Canosa, M.De Marco, A.Maiocchi, "*Traffic accounting mechanism for Internet Integrated Services*", Politecnico di Milano

[38] B.J. van Beijnum, R. Pàrhony, M.Goorden, S.Boros, A.Pras, L.Lagendijk, R.Poortinga *"Metering experiment"*, The Internet Next Generation Project, June 2000

[39] B.J. van Beijnum, M.Goorden, E.Wierstra, R.Sprenkels, R.Parhoni, Zsabi, A.Pras, L.Lagendijk, R.Poortinga, *"Internet Accounting Architecture*", The Internet Next Generation Project, July 2000

[40] "*Network Data Management – Usage (NDM-U) for IP- Based Services version 2.0"*, ipdr.org, October 2000

[41] A.Pras, B.Beijnum, R.Sprenkels, R.Parhonyi, "*Internet Accounting*", IEEE Communications Magazine, May 2001

[42] R.A.M.Sprenkels, R.Parhoni, A.Pras, B.J. van Beijnum, B.L. de Goede, *"An Architecture for Reverse Charging in the Internet"*, The Internet Next Generation Project

[43] M. Van Le, *"Possible Scenarios for Content related and Add-Value Accounting Architecture Supporting User Mobility*", The Internet Next Generation Project, May 2001

[44] C.Rigney, S.Willens, A.Rubens, W.Simpson, *"Remote Authentication Dial In User (RADIUS)"*, rfc 2865, June 2000

[45] C.Rigney, "*RADIUS Accounting*" rfc2866 , June 2000

[46] R.Ekstein, B.Sales, O.Paridaens, *"AAA Protocols: Comparison between Radius, Diameter and Cops*", draft-ekstein-aaa-protcomp-00, April 2000

[47] C.Perkins, "*Mobile IP and Security Issue: an overview*"

[48] B.Adoba, M.Beadles, *"The Network Access Identifier"* rfc 2486, January 1999

[49] S.Glass, T.Hiller, S.Jacobs, C.Perkins, "*Mobile IP Authentication, Authorization And Accounting Requirements*" rfc 2977, October 2000

[50] C.Perkins, P.Calhoun, "*Mobile Ipv4 Challenge/Response Extensions*" rfc3012, November 2000

[51] C.Perkins, Pat. R. Calhoun, *"AAA Registration Keys for Mobile IP"*, draft-ietf-mobileip-aaa-key-0.4, March 2001