MSA - 24.03.2021

Abbiamo aperto questo nuovo capitolo dopo quello relativo alle comunicazioni wireless. Avevamo aperto questo nuovo capitolo dedicato a trattare i temi legati alla mobilità dei nodi, dove quello che avevo rimarcato è che le problematiche relative create dalla presenza di nodi mobili all'interno di un'infrastruttura di calcolo sono problemi che riguardano due aspetti diversi: quello della raggiungibilità, la posizione precisa occupata da un nodo del sistema in modo da potergli inviare comunicazioni, e l'altro invece è di garantire la continuazione di una sessione di lavoro in corso anche se avvengono cambiamenti di posizione nel mentre. Sono state proposte varie soluzioni, che leggeremo come punti in uno spazio a quattro dimensioni, dove le quattro dimensioni sono quelle viste ieri. Ieri abbiamo discusso la prima delle quattro, quali valori può assumere la coordinata che descrive una coordinata lungo la direzione della dimensione del tracciamento. Oggi esploriamo possibili valori per le altre dimensioni.

Seconda dimensione riguarda l'ampiezza del movimento di un nodo che una certa soluzione è in grado di gestire. Quando parliamo di ampiezza, anche se la cosa potrebbe sembrare istintivamente una dimensione geografica, ma piuttosto ci interessiamo della dimensione di rete di questi spostamenti. Spostamenti commisurati rispetto alla struttura di una rete globale, dove i concetti di distanza possono essere correlati, ma non necessariamente a distanze fisiche piccole possono corrispondere distanze di rete piccole. Immaginate un nodo che possiede due interfacce di rete diverse, a queste due possono essere assegnati due indirizzi IP diversi associati, e questi due indirizzi IP potrebbero fare riferimento a sotto reti che dal punto di vista della topologia della rete internet possono essere distati fra di loro. Network distance numero di hop tra mittente e destinatario. Riguardano soluzioni che hanno una portata limitata, soluzioni di micromobilità, cercano di risolvere il problema della mobilità all'interno di una stessa sotto rete. Poi soluzioni di macro mobilità che si muovo all'interno di un singolo sotto dominio di rete, e poi problemi di mobilità globale su come rendere raggiungibile un nodo su scala globale, che può trovarsi in qualsiasi punto della rete internet.

Terza dimensione, a quale livello della pila protocollare si colloca la soluzione. E qui possibili risposte sono sotto il livello di rete, al livello di rete o ad un livello superiore. Soluzioni sotto il livello di rete sono soluzioni all'interno di una rete di livello 2 omogenea. Sappiamo benissimo che una rete cellulare tipicamente offre un'infrastruttura che è in grado di coprire un'estensione geografica notevole. Dal punto di vista della rete internet globale questa è comunque una singola entità omogenea al suo interno che può offrire una sua soluzione locale dedicata a risolvere il problema della mobilità all'interno di quella specifica rete. Sotto il livello di rete abbiamo soluzioni che fanno da supporto a quelle dei livelli più elevati.

Il livello di rete che sarà uno di quelli su cui ci soffermeremo maggiormente nell'esplorare alcune soluzioni, qui come abbiamo discusso nella parte iniziale del corso attualmente il livello di rete è il punto di unificazione della varietà di componenti che abbiamo sotto e sopra. Il vantaggio è di essere la soluzione unica che va bene per tutti, appunto si sposa con

quello che è il punto di unificazione tra tutte le componenti eterogenee che stanno sopra e sotto. Sul versante negativo, soluzioni a livello di rete non riescono a cogliere alcune specificità dei livelli superiori, anche perché non è ben definita l'interfaccia di comunicazione per i principi di separazione dei livelli, per cui decisioni che possono esser espressi a livello di rete possono essere prese alla cieca rispetto alle esigenze particolari di sessioni in corso gestite da protocolli di livello superiore, portando ad inefficienze che sarebbe preferibile evitare. Altro problema come vedremo soluzioni prese a questo livello possono causare delle inefficienze nell'instradamento complessivo dei pacchetti.

Soluzioni a livello superiore, di trasporto ad esempio, sono soluzioni che non si collocano unicamente a questo livello e necessitano un supporto dei livelli sottostanti. Sono soluzioni che riescono più propriamente a tenere conto delle specifiche esigenze che vengono dal livello applicativo, relative ad una specifica modalità di interazione, però soluzioni proposte a questo livello cominciano ad essere ritagliate per uno specifico protocollo di trasporto. Non sono più soluzioni universali che vanno bene per tutti, ma richiedono una moltiplicazione degli sforzi che significa anche un potenziale problema di sicurezza. Aumento quante più cose metto in campo, tanto più maggiore è la superficie di attacco del sistema. Aumento i punti attraverso cui si può intromettere un tentativo di compromissione dell'integrità del sistema.

Soluzioni più vicine al livello applicativo, livello di sessione, protocollo SIP ad esempio. Soluzioni analoghe a quelle proposte al livello di trasporto.

Ultima dimensione è quella che riguarda il livello di coinvolgimento delle entità in gioco del sistema. Da un lato i nodi che si muovono e dall'altra l'infrastruttura eventualmente presente. L'infrastruttura che se presente fa da supporto ai desideri di comunicazione di questi nodi tra di loro o con altri nodi fissi. In questo caso le soluzioni proposte possiamo definirle completamente decentralizzate, in cui gli attori che entrano in gioco sono i nodi mobili, i punti terminali dell'interazione, e dall'altro lato soluzioni che invece gran parte del lavoro necessario al problema della mobilità è affidato all'infrastruttura che supporta questi nodi. Sono soluzioni che rispecchiano due filosofie diverse di un sistema distribuito. Se vogliamo discutere qualche elemento distribuito, nel caso di soluzioni host-based seguono una filosofia end-to-end, cioè che c'è in mezzo deve essere neutrale rispetto a ciò che avviene alle due estremità, e la risoluzione dei problemi è affidata ai due estremi, ad esempio la filosofia del protocollo TCP. Può avere i suoi vantaggi questo tipo di approccio, però chiaramente richiede un coinvolgimento diretto dei nodi, che loro siano consapevoli di questo, e che su ogni nodo mobile sia installata la logica applicativa di controllo per implementare la soluzione scelta. Network intelligence invece la rete è l'attore principale, richiedono all'infrastruttura di entrare in gioco e di non essere neutrale, i vantaggi sono che alleviano i nodi terminali da gran parte delle responsabilità. I nodi terminali possono essere totalmente inconsapevoli delle azioni che vengono intraprese, e non richiedono di modificazione del loro stack protocollare.

In un solo colpo possiamo vedere tutti i possibili valori che possono assumere le quattro dimensioni. Proviamo a fare un piccolo esercizio di applicazione della classificazione sul protocollo 802.11. Come sappiamo è un protocollo che anche se pure in maniera limitata gestisce la mobilità dei nodi all'interno di uno stesso ESS. Dal punto di vista della

dimensione del tracciamento, è una soluzione di tipo pro attivo, in quanto è realizzato dal meccanismo di associazione e riassociazione tramite i segnali di beacon. Un nodo che si è agganciato ad un sistema gestito da un ESS, spostandosi rileva la presenza di un altro AP con la qualità del canale offerto migliore, il nodo mobile si aggancia al nuovo AP e la nuova collocazione del nodo mobile viene registrata all'interno del sistema di distribuzione, a prescindere dal fatto che quel nodo sia impegnato o meno in una comunicazione con altri nodi che fanno parte dello stesso ESS. La posizione del nodo mobile viene tenuta costantemente aggiornata. Siamo in presenza di un tracciamento pro attivo. Dal punto di vista della portata, siamo in una situazione di micromobilità. Questo tipo di protocollo copre problematica di mobilità limitate ad un singolo ESS, a valle di un router che definisce una specifica sotto rete all'interno dell'architettura globale della rete internet. Se si valicano i confini di questo router, la soluzione offerta da questo protocollo non è in grado di gestire la raggiungibilità del nodo. Dal punto di vista del livello siamo sotto il livello di rete, livello 2, e dal punto di vista delle entità coinvolte la gestione della soluzione è data da una cooperazione forte tra l'infrastruttura ed il nodo stesso.

Mobility management in internet

Siamo nel capitolo mobilità, ma iniziamo ad esplorare una soluzione specifica, alcuni standard proposti in particolare esploreremo dopo una piccola panoramica generale iniziale esploreremo alcune soluzioni che riguardano la gestione della mobilità all'interno di una rete internet, assumendo la presenza di un'infrastruttura che è quella internet esistente. Dal punto di vista della standardizzazione sono soluzioni standardizzate all'interno dell'organismo che governa internet.

Siamo interessati a soluzioni che si muovono nella sfera della rete internet. Non prenderemo in considerazione ce soluzioni che si muovo a livello 2. Queste sono soluzioni sotto il livello della rete internet. Dal punto di vista delle rete internet le precedenti sono soluzioni a livello sottostante (reti cellulari, 802.11 ecc). Problema della mobilità a livello della rete internet. Abbiamo illustrato ieri il punto. Sapendo come funzione l'instradamento dei messaggi all'interno della rete internet, il cambio di posizione di un nodo a cui è associato un indirizzo IP, lo strumento utilizzato per pilotare l'instradamento dei messaggi verso la loro destinazione, se la posizione occupata dal nodo mobile non è più topologicamente corretta rispetto alla rete, questo rende il nodo stesso irraggiungibile.

Le soluzioni sono di due tipi: una è la soluzione in cui l'indirizzo IP associato ad un nodo è comunque immutabile, su una scala temporale abbastanza amplia. Queste rispetto alla classificazione che abbiamo discusso sono soluzioni a livello network. Oppure con una maggiore varietà un'altra via è quella di non considerare immutabile l'indirizzo IP associato ad un nodo, ma assumere che questo possa variare, in modo da stare dietro allo spostamento del nodo, cercando di mantenere associato al nodo l'indirizzo IP topologicamente corretto rispetto alla posizione che un nodo occupa nel tempo. C'è una maggiore varietà di soluzioni che si collocano a diversi livelli della pila protocollare. Noi ci soffermeremo a soluzioni che si pongono sul livello network. Facciamo una breve

panoramicar su soluzioni che si collocano a livelli diversi prima di focalizzarci sul livello rete.

Guardiamo alla prima famiglia di soluzioni. Quelle basate sull'idea di mantenere fisso, unico, l'indirizzo IP associato ad un nodo. Qui l'idea è quella di raffinare i meccanismi di routing adottati. Raffinare significa aumentare le informazioni presente nelle tabelle di routing associate ai vari router, con informazioni relative ai singoli nodi mobili. Nel caso in questione, se il nodo si è agganciato alla rete il cui prefisso sarebbe diverso, l'informazione sull'interfaccia verso cui il router deve instradare viene registrata nella tabella del router, dove compare l'interfaccia verso cui devono essere instradati i messaggi relativi all'indirizzo. Soluzione semplice che non richiede nessuna modifica rilevante alla modalità di funzionamento dell'architettura internet. I problemi che questo tipo di approccio pone, c'è il rischio che le tabelle di routing che ogni router deve gestire possono aumentare di dimensione. Per aggiornare le tabelle i messaggi possono assumere anche dimensioni rilevamenti in funzione del numero di nodi di cui bisogna tenere traccia, ed anche la frequenza dei messaggi può diventare eccessiva sulla rete, sopratutto se i nodi di cui bisogna tenere traccia sono caratterizzati da un'elevata mobilità. Tutto questo crea problemi di scalabilità, se il numero di nodi mobili cresce entro una certa soglia e/o se la frequenza con cui i nodi si spostano cresce entro una certa soglia. Per questa ragione soluzioni di questo tipo sono praticate però principalmente al livello di micromobilità, quindi rispetto alla dimensione dell'ampiezza spaziale misurata sullo spazio della rete coperte da queste soluzioni siamo ad un livello limitato, all'interno di un singolo dominio di rete.

Altra famiglia di soluzioni sono quelle che assumono che l'indirizzo IP può cambiare. E possa cambiare in maniera da mantenere la corrispondenza con la topologia della rete. L'idea è che il nodo che si sposta, si aggancia ad un altro dominio di rete, perde il vecchio indirizzo IP e ne viene associato uno nuovo adeguato alla nuova posizione. A questo punto pacchetti che arrivano con il nuovo indirizzo verranno correttamente istradati alla nuova posizione.

A quale livello si colloca la gestione di questo cambiamento di indirizzo? E poi, a parte questo, c'è il problema di come gestire la questione della raggiungibilità, e l'idea potrebbe essere quella di dire di utilizzare il servizio DNS. Il problema per questo tipo di soluzione banale è che i DNS non sono stati pensati per gestire questo tipo di problema, DNS è un sistema distribuito e decentralizzato, basato sul meccanismo di consistenza debole, per cui gli aggiornamenti si propagano lentamente tra i ari server DNS, con una lentezza che probabilmente non è compatibile con la tempestività richiesta in certi scenari nel tenere aggiornate le informazioni sulla posizione di un nodo. DNS non è una buona soluzione per risolvere il problema della raggiungibilità in presenza di cambi di indirizzo IP. L'altro aspetta è se l'indirizzo IP cambia, dome evitare che il cambio di IP provochi l'interruzione di una sessione di lavoro in corso mentre il nodo si sposta e cambia indirizzo IP. Come sappiamo molti protocolli di trasporto come TCP o UDP assumono che l'end point dell'interazione (numero porta, indirizzo IP), rimanga costante per l'intera sessione. Se uno degli elementi che caratterizzano il punto terminal e cambia, la sessione di lavoro crolla ,e quindi va risolto anche questo aspetto.

Soluzioni possibili che si collocano a livelli diversi dal livello rete che poi saranno soluzioni su cui si soffermeremo maggiormente. Una prima soluzione che si colloca sotto il livello di rete è il protocollo DHCP. E' un protocollo che non è nato per gestire problemi di mobilità, è un protocollo che serve per gestire in maniera automatica la configurazione dell'aggancio del nodo ad una rete di vari paramenti necessari per la vita del nodo fintanto che rimane agganciato alla stessa rete, informazioni sul server DNS di riferimento, nome dominio ecc. In particolare un'informazione che il server DHCP fornisce ad un nodo che si aggancia ad una rete coperta da questo server è l'indirizzo IP che sia topologicamente corretto per quella specifica sotto rete. Nel momento in cui un nodo entra dentro una sotto rete, contattando il server DHCP può ottenere un indirizzo IP che sia corretto per quella sotto rete. Questa è una soluzione che risolve parzialmente posti dalla mobilità dei nodi. In particolare l'aspetto di raggiungibilità. Il nodo ottenuto in questo modo l'indirizzo IP è raggiungibile a patto che sia lui ad iniziare una sessione di lavoro con un altro partner, perché nel momento in cui avvia questa sessione comunica il suo attuale indirizzo IP al suo partner, ed a questo punto il nodo mobile diventa raggiungibile. Non risolve il problema del mantenimento della continuità di una sessione nel momento dell'handoff con il passaggio ad una rete diversa. La sessione crolla.

A livello di trasporto sono state proposte soluzioni che prevedono un cambio di indirizzo. Varie soluzioni sono state proposte, come dicevamo poco fa sono vari i protocolli di trasporto che potrebbero esser presi in considerazione. L'idea generale è che nel momento in cui il nodo mobile cambia sotto rete, con un prefisso differente, il nodo mobile in qualche modo ottiene un nuovo indirizzo IP per esempio facendo riferimento ad un protocollo come DHCP. Questo nuovo indirizzo viene comunicato al partner utilizzando al comunicazione esistente ed a questo punto i due nodi concordano un trasferimento della sessione in corso sulla nuova connessione.

Giusto per dare dei riferimenti ma non andremo in profondità, alcune soluzioni prospettate a questo livello riguardano solamente il tema del mantenimento della sessione in corso, protocollo di hand off. Il primo mSCTP è un'estensione del protocollo SCTP, protocollo trasporto pensato per situazione idi streaming. Tra le caratteristiche supporta una sessione di streaming che avviene tra nodi che hanno interfacce di rete diverse. Il protocollo permette di gestire situazioni in cui alle interfacce sono assegnate indirizzi IP diversi, primari e secondari, ed il protocollo STCP è in grado di gestire le transizioni da un indirizzo IP all'altro mantenendo la sessione di streaming in corso. La variante mSCTP prevede la possibilità che la lista degli indirizzi IP di riserva possa variare dinamicamente. Ci sono anche soluzioni che invece hanno una visione più completa per cui cercano non solo di garantire la continuità della sessione ma anche garantire la raggiungibilità del nodo. Abbiamo una soluzione proposta che estende TCP ed usa meccanismi offerti dal server DNS.

E poi anche soluzioni a livello superiore con il protocollo SIP.

Le soluzioni su cui ci soffermeremo sono soluzioni che si collocano a livello rete. Tra queste soluzioni possiamo riconoscere soluzioni che non richiedono cambio di indirizzo IP, quelle appunto che prevedono semplicemente un annotazione nelle tabelle di routing della posizione attuale occupata da un nodo, e soluzioni che prevedono un cambio di indirizzo,

quelle su cui sui soffermeremo maggiormente. Dal punto di vista dell'ampiezza degli spostamenti coperti si collocano a vari livelli. Delle soluzioni sulla slide discuteremo le prime due, mobilità globale e macro mobilità.

Iniziamo con Mobile IP, che è uno standard dell'IETF. Essendo uno standard, la filosofia seguita da questa soluzione è di offrire una soluzione interna al modello internet, che sfrutti pienamente i meccanismi di instradamento offerti dalla rete internet come la conosciamo. Rilasciando, rispetto alla concezione iniziale di internet di un mondo statico, il vincolo che l'indirizzo IP sia unico e costante. In questa soluzione si basa sull'esistenza di due distinti indirizzi, entrambi associati allo stesso nodo. Due indirizzi che con una separazione di ruoli. Uno dei due continua a svolgere il ruolo di identificativo unico del nodo, quindi mantiene il ruolo, ma in parte perde il ruolo di essere anche indicativo della posizione occupata dal nodo stesso e quindi del percorso da eseguire per raggiungerlo. L'altro indirizzo invece che è associato al nodo è un indirizzo variabile, e varia per essere costantemente allineato con la posizione attualmente occupata dal nodo mobile. Questi due indirizzi vengono chiamati home address, dove la casa di un nodo mobile è la sotto rete presso cui il nodo si è registrato la prima volta, ed un indirizzo temporaneo che è quello che varia nel tempo ed usato per localizzare il nodo mobile.

Come viene realizzata la raggiungibilità? Se il nodo coinvolto nella gestione del protocollo non è un nodo mobile non succede nulla. L'indirizzamento di pacchetti ad un nodo che non si sposta avviene in modo tradizionale. Chi vuole interagire con il nodo utilizza l'home address del nodo mobile ed indirizza verso questo indirizzo. Se invece il nodo è un nodo che si muove, l'idea di base di questa soluzione è che chiunque vuole parlare con il nodo mobile ignora che il nodo abbia cambiato posizione, continua a parlare con il nodo utilizzando il suo home address, essendo l'unico indirizzo noto per i partner. Il protocollo prevede dei meccanismi di reindirizzamento verso la destinazione attuale del nodo mobile in caso di spostamento.

Da qualche parte bisogna mantenere l'associazione tra l'indirizzo identificativo ed il suo indirizzo temporaneo che rappresenta la posizione. L'associazione viene mantenuta all'interno di una tabella a due campi. La tabella viene mantenuta all'interno della home network di un nodo mobile. Nella sua rete di casa esiste un'entità che mantiene questa tabella, la tiene aggiornata ,e la utilizza poi per consentire ai pacchetti indirizzati al nodo mobile di arrivare alla destinazione corretta.

Se vogliamo guardare l'organizzazione risultante, l'idea è che ci vuole inviare messaggi al nodo mobile li invia verso la rete di casa usando lo home address. Nella home network esiste una funzione di re indirizzamento che usando come chiave di accesso l'home address accede alla tabella, ricava l'indirizzo attuale del nodo mobile, provvede a re instradare verso la rete che corrisponde a quell'indirizzo il messaggio arrivato. A destinazione è necessaria una funzione inversa g, che riceve questo pacchetto e lo fa arrivare alla destinazione.

I requisiti posti a suo tempo dall'IETF. Piccola carrellata sulla terminologia. Ogni protocollo ha la sua terminologia. I nodi mobili in 802.11 si chiamavano STA, nelle reti cellulari MH, qua MN.

HA sta per home agent, l'entità che realizza la funzione F di cui parlavamo. E' l'entità che gestisce la tabella in cui viene conservata l'informazione dell'accoppiamento tra home address ed indirizzo attuale occupato dal nodo mobile. La rete viene chiamata home network. La rete che attualmente ospita il nodo mobile MN è indicata con Foreign network. All'interno è presente la funzionalità g che può essere svolta da un'entità specifica identificata con FA. CN è il nodo mittente che vuole raggiungere il nodo mobile MN. Care of Address si intende l'indirizzo temporaneo, l'indirizzo che associato allo home address nella tabella gestita dall'HA ed è l'indirizzo che consente ai messaggi di arrivare a destinazione. Come avviene in maniera più precisa? CN costruisce il suo messaggio in maniera standard, quindi a livello IP nell'header del pacchetto registra mittente CN e come indirizzo destinazione lo home address di MN. Il pacchetto viaggia per internet e seguendo le normali regole di instradamento arriverà nella home network. Qui il pacchetto viene intercettato dall'HA. Possono succedere due cose. Se il nodo mobile è presente nella home network il pacchetto attraversa l'HA ed arriva a destinazione. Se il nodo non si trova nella home network deve essere re instradato. Intercettamento del pacchetto destinato al MN avviene in due modi: HA incastonato nel router che controlla l'accesso all'home network, funzionalità aggiuntiva del router. Non è detto che la funzione di HA però sia incastonata nel router della rete. Può essere che la funzione sia svolta da un'entità fisicamente distinta che sta a valle del router. In questo caso l'HA è autorizzato ad agire come proxy del protocollo ARP. Agendo in qualità di proxy ARP è autorizzato di impossessarsi di un pacchetto che a livello IP non è indirizzato a lui. Prende il pacchetto e consulta la tabella. Incapsula il pacchetto in un nuovo header IP, aggiungendo una nuova intestazione dove l'indirizzo destinazione è l'indirizzo registrato nella tabella gestita dallo home agent. Un pacchetto costruito in questo modo viene re instradato verso il router, e da qui essendo l'header esterno pilota l'avanzamento del pacchetto lungo la rete, questo pacchetto arriverà alla FA seguendo le normali regole di instradamento. Quando arriva nella foreign network il pacchetto viene catturato dal FA, che si preoccupa di rimuovere l'header che era stato aggiunto dall'HA tramite il tunnel, quindi fa riemergere il campo destinazione originario che utilizzando il protocollo ARP verrà reindirizzato verso il nodo mobile.

Collocazione dell'HA spiegato graficamente. Sono soluzioni che hanno i loro pro e contro. La seconda non richiede l'ingresso nella rete del pacchetto, riduce la latenza per completare la comunicazione, c'è però da dire che non sempre è possibile installare all'interno di un router questa funzionalità aggiuntiva. Soluzione del primo tipo svincola il protocollo Mobile IP dalle responsabilità del router, chiunque può installare Mobile IP all'interno di una rete, a prescindere dalle decisioni prese da chi gestisce il router.

Tornando al nostro scenario, il percorso inverso è più semplice. Il protocollo non entra in gioco in nessun modo, a patto che il nodo mittente sia un nodo fisso. Giuso per dare una visione di insieme, grafico riassuntivo sulle slide.

In che modo quest'idea abbastanza semplice si realizza e si implementa propriamente. E' implementata grazie alla presenza di tre funzionalità distinte che sono: la funzione di scoperta, agent discovery, utilizzata da HA e FA se presente, consente alle entità di rendere nota la propria presenza. Permette anche al nodo di capire se si trova nella sua home network, se ascolta il messaggio del suo HA o altrimenti se sete il messaggio di un FA deve avvisare l'HA della sua posizione temporanea. Altra funzione è quella di registrazione, il cui

ruolo è quella di tenere aggiornata la tabella gestita dallo HA sulla posizione attuale occupata dai nodi mobili, utilizzata dal nodo mobile quando acquisisce un nuovo COA address, indirizzo temporaneo. Poi abbiamo al funzione di tunneling vero e proprio che è quella che realizza quel tunnel tra HA e FA di cui abbiamo parlato.

Funzione di pubblicizzazione. Consiste nell'invi periodico di messaggi all'interno della rete coperta da una delle entità che abbiamo nominato, è un'attività analoga per scopi a quella dell'emissione disegnali di beacon di cui abbiamo già parlato. Messaggi di questo tipo ne circolano di varia natura, e proprio per questa natura la scelta che è stata fatta dal comitato dell'IETF che ha definito lo standard è quello di, piuttosto che definire un nuovo meccanismo di advertisement, di fusione dei messaggi, quello di appoggiarsi ad un meccanismo già definito nello standard di internet. In particolare facendo riferimento a messaggi definiti dal protocollo ICMP, la scelta fatta è stata quella di agganciarsi ai messaggi di router discovery già definiti advertisement già definiti all'interno del protocollo. Sono messaggi emessi periodicamente dai router presenti in una sotto rete ed il loro scopo quello di pubblicizzare la presenza del router a tutti i nodi agganciati a quella specifica rete. Questo è il formato tipico di questi messaggi. L'idea dell'IETF, in modo analogo a quello visto con i segnali di beacon dove il segnale porta con se tutta una serie di informazioni necessarie a supportare varie tipi di funzioni, 'l'idea è di aggiungere ai campi del messaggio di advertisement un'estensione che trasporta informazioni necessaria per la realizzazione di alcune funzioni di gestione della mobilità.

I campi che riguardano la parte di mobilità sono quelli che vediamo. Informazione importante sono i campi indirizzo, COA, campi che vengono trasmessi se il messaggio viene emesso dell'entità che svolge il ruolo di FA. In questo caso, questo messaggio elenca uno o più indirizzi che possono essere utilizzati da un nodo mobile come indirizzo temporaneo finché si trova nella rete governata dal FA che sta emettendo questo messaggio. In questa situazione questo COA è un indirizzo che identifica l'entità FA stessa. Questo vuol dire che il nodo mobile si dota come indirizzo che lo identifica all'interno della FN di un indirizzo che identifica il FA. I messaggi che viaggeranno nel tunnel le che arriveranno al nodo mobile, verranno catturati dal FA e sarà lui che una volta ricevuto il messaggio indirizzato al nodo mobile provvederà a liberarlo dell'header aggiuntivo del tunnel e farlo arrivare pulito al nodo mobile. Conseguenza di questo schema è che tipicamente più nodi mobili che sono ospitati da un FA condivideranno uno stesso COA. Oltre questa informazione c'è spazio per supportare altre informazioni come la durata di una registrazione, per quanto tempo l'associazione tra uno HA ed un COA deve essere considerata valida, l'associazione ha un tempo limitato che scade. Se l'associazione non iene rinnovata, scaduto il termine l'associazione non viene considerata valida. Se è ancora valida c'è bisogno di un rinnovo attivo da parte delle entità coinvolte. Questo serve ad informare sul tempo di validità dell'associazione. E dopo una serie di bit che forniscono informazioni su HA e FA. Un bit serve a specificare che il FA impone ai nodi mobili di registrarsi presso di lui. Il FA può anche segnalare che non accetta più l'ingresso di nodi mobili presso la propria rete. Gli altri bit servono a segnalare il ruolo dell'entità che emette il messaggio, se è FA o HA. Altre informazioni riguardano la capacità o meno dell'agente di supportare alcune varianti del protocollo che discuteremo più avanti, un altro meccanismo di incapsulamento. Ultimo è se supporta la funzione di reverse tunneling che serve ad ovviare ad uno dei problemi che

evidenzieremo la prossima volta, e quindi la capacità di gestire una possibile soluzione a questo problema.