MSA - 30.03.2021

Stiamo parlando di Mobile IP nella sua versione base. Nella realizzazione della versione base le funzionalità sono di advertisement svolta dai due tipi di agenti coinvolti, l'HA ed il FA, e la funzione di registrazione e di tunnelling. La funzione di advertisement l'abbiamo commentata la scorsa volta. La scelta dai progettisti del protocollo di piuttosto che definire un nuovo formato di messaggio, appoggiarsi ad un formato ed una modalità di gestione già preesistente, la funzione e relativi messaggi di router advertisement già presente nel protocollo ICMP. Scelta fatta per ragioni di economia. Come tutte le scelte questo vantaggio si può pagare in termini di non perfetta aderenza di ciò che già esisteva rispetto alle esigenze di quello che si vuole andare a realizzare. Una di queste situazioni, sopratutto in alcune variabili di configurazione di router advertisement, per esempio la definizione data al parametro relativo all'intervallo minimo tra l'emissione di due messaggi di adv consecutivi da parte di una delle entità in gioco, che nello standard definito per i messaggi router advertisement era stabilito avere un valore minimo di 3 secondi, che dal punto di vista della presenza di un router con nodi fissi è sufficiente, non si immagina che il router che controlla l'accesso cambi ogni tre secondi; dal punto di vista di una situazione di nodi mobili, tre secondi possono essere anche troppo lunghi, sopratutto in situazioni in cui un nodo entra in una nuova sotto rete ed ha una sessione di lavoro in corso, ad esempio TCP. In tre secondi di pacchetti in transito ne possono passare anche tanti. Il tempo necessario per prendere atto è maggiore di tre secondi, la cosa non è proprio il massimo. C'è questo possibile effetto negativo.

La funzione precedente con i messaggi di pubblicizzazione fatti circolare da HA e/o FA servono a consentire ad un nodo mobile di acquistare consapevolezza della sua situazione: se si trovato o tornato nella rete di casa, o se si trova in una rete che non è la sua di casa. Se si trova in una rete esterna di conseguenza deve informare il suo HA della sua nuova posizione. Informarlo significa creare o modificare se era stato già creato, un mobility binding, concretamente una riga della tabella location directory in cui è registrata l'associazione tra il suo HA e l'indirizzo temporaneo, CA. Questa associazione ha una durata limitata. Se deve prolungarsi nel tempo ci deve essere un refresh periodico. Come vedremo tra un attimo, questa registrazione può avvenire in due modi diversi. O usando il FA come intermediario, oppure con un colloquio diretto tra il nodo mobile il suo HA.

Lo scopo di questa funzione è quello, in generale tranne il caso particolare in cui il nodo mobile è ritornato a casa ed informa il suo HA che non è necessario svolgere la funzione di reinderizzamento, lo scopo fondamentale di questa registrazione comunicare all'HA l'attuale care of address del nodo mobile. CA può assumere due configurazioni diverse: foreign agent care-of address oppure il colocated care-of address. Nel primo caso l'indirizzo temporaneo è un indirizzo IP che identifica il FA della rete in cui si trova il nodo mobile. In questo caso il valore dell'indirizzo viene acquisito dal nodo mobile tramite il messaggio di advertisement trasmesso dal FA, utilizzando il CA condiviso da più nodi mobili. La seconda tipologia, si tratta di un indirizzo che identifica, se pur in modo temporaneo, esattamente un singolo nodo mobile. E' un indirizzo topologicamente corretto rispetto alla rete, appartiene alla rete in cui si trova il nodo mobile, e viene acquisito dal nodo mobile stesso.

Tipicamente la soluzione più semplice è quella di utilizzare il protocollo DHCP. In questo caso il punto terminale del tunnel è il nodo mobile, non più il FA. Dunque deve essere lui a ricevere il pacchetto transitato sul tunnel e rimuovere l'header aggiuntivo.

La registrazione può avvenire in due forme. Una indiretta, che rimbalza la richiesta di registrazione verso l'HA ed anche la replica avviene in due passi, oppure direttamente in un colloquio diretto tra il nodo mobile e l'HA. Le due tipologie corrispondono alle due tipologie di ottenimento del CA. Quella indiretta si applica in situazioni in cui il CA è quello che viene acquisito da un FA, la registrazione diretta nel caso in cui il CA viene acquisito autonomamente dal nodo mobile.

I messaggi di registrazione viaggiano sulla rete come pacchetti UDP, quindi con un certo carico utile che serve a veicolare tutte le informazioni necessarie. Si utilizza UDP e non TCP per questioni di leggerezza del protocollo, per evitare l'overhead per stabilire la sessione. Non è necessaria essendo uno scambio singolo. Questo significa che la trasmissione non è affidabile, il protocollo Mobile IP ha un suo meccanismo di eventuale ritrasmissione della registrazione.

Giusto per avere un'idea minimale, un messaggio di registrazione trasporta varie informazioni tra cui l'informazione fondamentale ed alcuni bit di controllo che servono ad informare l'HA su eventuali esigenze o capacità del nodo mobile che sta chiedendo di fare la registrazione. Il campo COA, nel caso in cui il nodo mobile sia rientrato nella sua rete di casa, sarà il suo HA. Campo importante, presenti a scopi di sicurezza perché serve sopratutto in modo semplice ed efficace a proteggere contro un tipo di possibile attacco, quelli di tipo replay, che in assenza di questo campo potrebbero essere facilmente messi in atto, anche in caso di pacchetti di registrazione completamente crittografati. Basterebbe semplicemente catturare i messaggi di registrazione emessi da un nodo mobile, senza la necessità di conoscere il contenuto, basterebbe rimandarli in un tempo futuro per rendere irraggiungibilità il nodo mobile. Questo nodo serve ad accoppiare richieste di registrazione con la relativa replica, non permettendo di riutilizzare in futuro una richiesta emessa nel passato.

La replica ha un formato analogo e comunica se la registrazione ha avuto successo o no, nel caso di insuccesso per quale motivo. Altra informazione importante per quanto tempo la registrazione sarà valida. Se ricordate, tornando ai messaggi di advertisement che vengono emessi dagli agenti, uno dei campi era quello del lifetime. Il valore riportato in quel campo è il limite superiore che può essere dato a questa variabile durante la registrazione. Un nodo mobile può chiedere che la sua registrazione valga per un tempo non superiore, ma eventualmente inferiore, all'estremo superiore pubblicizzato nei messaggi di advertisement. Quando il tempo di vita si approssima alla scadenza ed il nodo non ha cambiato posizione, deve re inviare un messaggio di registrazione per tenerla in vita, altrimenti verrà rimossa dallo home agent.

Veniamo alla funzione di tunneling. Il tunneling non è nulla di nuovo, una tecnica che conoscete ampliamene, si utilizza in tutte le situazioni in cui una connessione logica tra sorgente e destinazione, in cui il canale logico è poggiato su un canale di livello più basso, il modo per realizzarlo concretamente piuttosto che seguire il percorso è dal mittente logico

il messaggio viene passato ad un'altra entità che sta sullo stesso nodo ad un livello più basso, che utilizza un altro tipo di protocollo di livello inferiore, questo messaggio viene quindi arricchito di un nuovo header, viaggia lungo il percorso fisico o virtuale che sia a seconda del livello della stratificazione, arriva al pari dell'incapsulatore che c'era da questa parte, arriva al pari dall'altra parte, il pacchetto viene spogliato della sua intestazione, riemerge il pacchetto originario e questo viene poi portato a destinazione. Logicamente il destinatario si vede arrivare un pacchetto che è come se avesse viaggiato lungo questo percorso.

E' esattamente quello che avviene nella stratificazione dei protocolli internet. Quello che c'è di diverso in questa situazione è che i due header che si sovrappongono appartengono allo stesso livello protocollare. In particolare questo può avvenire in due forme: standard, più due opzionali, di cui ne commenteremo una sola. L'idea di fondo è che se questo è il pacchetto originale arrivato allo HA, il pacchetto verrà arricchito di un nuovo header IP, quello che c'era prima diventa carico utile da trasportare. In questo carico utile la parte header trasportata non è detto che sia esattamente uguale allo header originario. Lo vedremo in particolare nel caso dell'opzione minimal encapsulation.

Immaginate che questo sia un pacchetto IP che seguendo le normali regole di instradamento di internet è stato emesso da un nodo CN, l'indirizzo mittente, e destinato al nodo MN, l'indirizzo HA del nodo mobile, quello che identifica univocamente il nodo mobile. Grazie alla presenza del campo destinazione, il pacchetto è arrivato nella home network di MN. Se il nodo mobile non si trova nella sua home network, il pacchetto viene catturato dall'HA. Concretamente significa che al vecchio pacchetto viene sovrapposto un altro header, che è esattamente uno header IP, con tutti i campi identici, alcune informazioni vengono ricopiate dal vecchio al nuovo. L'indirizzo sorgente risulta essere lo HA, il destinatario risulta essere il CA che l'HA ricava dalla sua tabella. E' l'indirizzo che in quella tabella risulta associato a questo indirizzo. Una cosa da notare è il valore che assume il campo TTL. Presente nello header esterno, è uguale a quello dell'header interno arrivato nella home network di MN. Il valore di TTL presente nell'header interno, quello che riemergerà quando questo pacchetto arriverà nella rete che ospita MN, il valore preesistente viene decrementato di 1, e tale rimarrà per tutto il viaggio del pacchetto attraverso il tunnel, mentre il valore esterno verrà decrementato ad ogni passaggio di un router. La scelta dei progettisti è di fare in modo che ovunque sia il nodo mobile, distante quanto vogliamo in termini di distanze misurate in numero di hop da percorrere per passare dalla home network di MN alla rete che lo ospita, comunque questa distanza non deve essere visibile ne al nodo mobile e ne a chi interagisce con lui. Il tunnel è come se fosse una specie di via segreta che consente in un solo passo di arrivare dalla rete di casa del nodo mobile alla sua posizione attuale.

Quello che si può notare è che c'è una duplicazione completa del vecchio header nel nuovo, a meno di alcune informazioni modificate. L'overhead creato dalla duplicazione può essere più o meno importante a seconda della grandezza del carico utile trasportato, ma sono comunque byte in più. Per ridurre l'impatto dell'overhead una possibilità opzionale è di fare uso di una tecnica di incapsulamento minimale. L'header esterno deve essere un header IP completo altrimenti non potrebbe viaggiare sulla rete. Quello che viene ridotto è l'header interno, che non è quello originale ma una sua versione ridotta, dove quello che

viene conservato è tutto ciò che non può essere ricostruito usando le informazioni presente nell'header esterno. Si lasciano le informazioni non replicate, le altre verranno riaggiunte arrivati alla fine del tunnel.

Il percorso che seguono i pacchetti in una sequenza di interazioni tra un nodo corrispondente ed un nodo mobile segue un percorso triangolare. Questo triangolo può causare inefficienze più o meno gravi dal punto di vista dell'impatto che hanno sull'infrastruttura di comunicazione e cui ritardi tra CN ed MN, che dipendono dalla posizione relativa occupata da queste tre identità. La cosa potrebbe diventare eclatante in situazioni in cui la distanza tra CN ed MN è molto piccola, fisicamente connessi alla stessa sotto rete di internet, però due nodi con HA differenti devono percorrere tutto il percorso. E' un caso limite ma da l'idea dell'inefficienza di questo modo per rendere raggiungibile un nodo mobile. L'idea originaria molto semplice viene aggiustata per ridurre per quanto possibile l'impatto di queste inefficienze.

E' il meccanismo è quello di ottimizzazione dei percorsi. L'idea è molto semplice: se c'è qualcuno che vuole comunicare con il nodo mobile, la prima volta che vuole comunicare con lui l'unica informazione che ha è l'indirizzo che identifica il nodo mobile stesso, quindi la prima volta chiaramente i pacchetti andranno verso l'HA e da li verranno rimbalzati verso l'attuale posizione del nodo mobile. A questo punto il nodo CN può chiedere di essere informato lui di qual'è l'informazione del nodo mobile. Se lo scambio deve durare nel tempo, li indirizzerà direttamente verso il nodo mobile. Tutto questo avviene arricchendo il nodo corrispondente e se ne fa carico gestendo quella che nella terminologia del protocollo viene chiamata binding cache. E' una replica in piccolo, limitata agli interessi del nodo CN, delle informazioni contenute nella tabella che viene mantenuta nella sua interezza dallo home agent. Questo innesca meccanismi di gestione della cache, problema dell'obsolescenza delle informazioni ecc. A parte queste problematiche generali, le se risolve usando tecniche analoghe a quelle che si usano in tutte situazioni di questo tipo. Questa tecnica ha anche un effetto collaterale positivo, quello di ottimizzare le prestazioni del protocollo nelle sue azioni di hand-off da una sotto rete all'altra.

La realizzazione della funzione di ottimizzazione dei percorsi si basa sulla trasmissione di messaggi che possono appartenere alle quattro tipologie, utilizzati nel modo che vediamo. Immaginiamo di avere l'entità in gioco, il nodo CN, che vuole parlare con il nodo mobile MN è inizialmente connesso ad un primo FA, e successivamente si collega ad una nuova sotto rete con un nuovo FA. All'inizio dei giochi il nodo corrispondente conosce solo l'HA del nodo mobile, quindi manda i dati da alla home network, catturati dall'HA. Assieme a questi dati CN manda anche un messaggio di binding request, chiedendo di essere informato sulla posizione occupata dal nodo mobile. HA costruisce il tunnel usando le tecniche di incapsulamento già viste. Oltre questo l'HA manda a CN il messaggio di update, che consente a CN di registrare nella sua cache quello che è il CA del nodo mobile. In questo scenario sarà un CA collocato con il FA. Da questo punto in poi non c'è bisogno di seguire il triangolo, CN costruisce pacchetti dove il tunnel è realizzato in proprio, e l'indirizzo destinazione sarà direttamente quello del FA associato al nodo mobile. Questo FA farà riemergere il pacchetto originario ed arriverà ad MN, che risponderà in maniera diretta. Mentre lo scambio è in corso, MN cambia posizione. Per effetto di questo cambio, MN manda la sua richiesta al FA che la inoltra allo HA che ne prende atto, registra

l'informazione nella tabella. CN di tutto ciò non è informato. Si crea il problema di inconsistenza. CN non è informato, l'informazione che ha nella cache è obsoleta, e CN continua a mandare pacchetti con il vecchio CA. Catturati dal vecchio FA, realizza che il nodo mobile non è più presente nella sua rete ed emette un messaggio di warning per avvisarlo della situazione cambiata. Il nodo corrispondente ricontatta l'HA per avere le informazioni aggiornate. Possibile variante è che il messaggio di Warning venga inviato direttamente allo HA, ed a questo punto l'HA invia direttamente il contenuto aggiornato della sua tabella al nodo corrispondente. In questo caso si riduce la latenza di aggiornamento, non bisogna aspettare il warning.

Commento da fare sull'effetto collaterale di cui parlavamo. Pensando alla classificazione delle modalità di risoluzione del problema della mobilità che abbiamo dato, lungo le quattro dimensioni possibili, una riguardava il modo usato per aggiornare le informazioni sulla posizione del nodo mobile. La versione originale di Mobile IP adotta una politica puramente pro attiva, perché la funzione di advertisement serve a fare rendere conto ad un nodo mobile della sua posizione attuale, il nodo mobile capisce la sua posizione ed informa il suo HA dalla sua posizione occupata, a prescindere dall'esigenza o meno di comunicazione verso il nodo mobile. Questo nella versione base che però soffriva della triangolazione e dall'inefficienza causata. Questo meccanismo di ottimizzazione introduce un elemento di reattività, perché è un meccanismo che viene attivato esclusivamente se c'è qualcuno che vuole parlare con il nodo mobile. Questa variante rende il protocollo che rispetto alla dimensione del modo di tenere aggiornata l'informazione diventa una politica di tipo parzialmente reattivo e parzialmente pro attivo. Però c'è da notare che quando abbiamo discusso in generale la possibilità di adottare soluzioni ibride, la motivazione discussa all'epoca per questa opzione, quella di adottare soluzioni che sono parzialmente reattive e parzialmente proattive era di ridurre i costi non necessari della modalità pro attiva, dove questi costi vengono ridotti riducendo il modello di precisione con cui si tiene traccia della posizione del nodo mobile, e questa perdita si compensa dall'uso di un approccio reattivo dal momento in cui qualcuno vuole parlare con un nodo mobile. Qua la situazione è un po diversa, in quanto questa soluzione ibrida non serve a ridurre il costo della parte pro attiva, che rimane immutata. Lo sforzo fatto per tenere aggiornata la posizione del nodo mobile rimane identica, continua a mandare i suoi messaggi di registrazione ogni volta che cambia posizione, o più volte per rinfrescare l'associazione esistente. La parte reattiva non serve a compensare la perdita di precisione causata da un tracciamento meno preciso, ma serve soltanto in questo particolare protocollo a ridurre l'impatto negativo di quel fenomeno dell'instradamento triangolare. Ha un ruolo diverso. Quando parleremo di gestione della mobilità all'interno delle reti cellulari, troveremo questa ibridazione tra parte pro attiva e parte reattiva.

L'effetto collaterale è noto con il termine di smooth hand-off. In cosa consiste? Il cambio di registrazione di un nodo viene propagato al vecchio FA, che viene informato di qual'è la nuova posizione occupata dal nodo mobile. L'idea è che nel momento in cui il nodo CN che non è stato ancora informato del cambio di posizione di MB invia i messaggi alla vecchia posizione occupata da MN, l'idea è quella che il vecchio FA quando gli arrivano i vecchi messaggi, oltre ad inviare al nodo corrispondente un warning per dirgli che deve aggiornare la sua cache, piuttosto che far perdere questi pacchetti, grazie all'informazione

ricevuta e registrata dal vecchio FA, vengono inoltrati alla nuova posizione, evitando che vadano persi. Questo ha un impatto positivo che va molto spesso al di là dell'evitare di perdere pacchetti e doverlo ritrasmettere, già di per se un guadagno. Generalmente il guadagno è molto maggiore, basta pensare, caso tipico, all'interazione con il livello superiore, di trasporto, sopratutto se li si colloca un protocollo come TCP. Sappiamo come funziona, è un protocollo che in presenza di perdita di pacchetti interpreta questa perdita come una congestione in punti del percorso, e reagisce abbassando drasticamente la finestra di trasmissione, il numero di pacchetti inviati in trasmissione senza aspettare l'ACK di ritorno. L'effetto causato dalla perdita di pacchetti può causare a livello superiore una chiusura notevole della finestra ed un abbassamento anche drammatico del throughput. Da notare che in questo modo che sto mostrando della realizzazione dello smooth hand-off, la cosa avviene con un colloquio tra vecchio e nuovo FA. In evoluzioni successive del protocollo di questo meccanismo se ne fa carico direttamente il nodo mobile.

Altra problematica, attraversamento dei firewall. Questo è un problema semplice ma grave. Una delle origini di questo problema può essere imputata al fatto che il protocollo Mobile IP nella sua concezione originaria è un protocollo nato in un'epoca in cui internet era ancora un mondo di amici, di persone che si fidavano una con l'altra. L'esigenza di avere meccanismi di protezione diffusi massivi non era ancora fortemente sentita. Uno di questi strumenti di protezione sono i firewall, entità che messe a protezione di specifiche porzioni della rete, ognuna protegge una parte di rete, e la protegge implementando delle regole che servono a fare da filtro, a dare o negare a pacchetti che transitano attraverso il firewall il diritto di attraversarlo o di essere rifiutati. Le regole utilizzate possono essere più o meno sofistica, ma c'è tipicamente un certo numero di regole basilari che sono comuni a qualunque firewall degno di questo nome. Il problema è che proprio il nucleo di regole fondamentali da luogo ad una coibentazione problematica con il modo di operare di Mobile IP appena descritto. Primo scenario è che il nodo mobile si trovi in una rete straniera protetta da un firewall. Il nodo mobile vuole parlare con un suo partner che può stare ovunque nella rete. Lui parlerà usando la normale pila protocollare, userà dei pacchetti IP che avranno come indirizzo mittente l'indirizzo di HA, l'indirizzo fisso. Il pacchetto emesso dal nodo mobile può trovarsi ad attraversare il firewall con un indirizzo mittente che non appartiene a quella rete. Una regola basilare che tipicamente tutti i firewall implementano è che se un pacchetto non è corretto allora è sospetto, quindi ha buone probabilità di essere filtrato. Chiaramente un pacchetto in uscita non è un pacchetto che danneggia la rete, però filtrare un pacchetto di questo tipo potrebbe essere una regola di buon vicinato. Se ne potrebbe fare anche a meno. Però la situazione diventa più grave nello scenario del firewall che protegge la rete di casa del nodo mobile. Immaginiamo che il nodo mobile voglia parlare con un partner che appartiene alla rete di casa. Il firewall se lo vede arrivare dall'esterno, che per la topologia di rete non va bene. Un pacchetto di questo tipo che arriva dall'esterno e vuole entrare, qualunque firewall lo interpreta come qualcuno che vuole fingersi ciò che non è, ed il pacchetto viene filtrato. Un nodo mobile non riuscirà mai, uscito dalla sua rete di casa, a parlare con qualcuno rimasto nella rete di casa.

Il rimedio, uno standard, è noto come reverse tunneling. L'idea è che quando il nodo mobile vuole inviare un pacchetto, questo pacchetto in uno scenario in cui c'è un FA attraverso cui il pacchetto passa, lui fa da tramite, lo incapsula mettendo un header che farà viaggiare il

pacchetto dal FA all'HA. L'HA cattura il pacchetto e lo re instrada verso il nodo corrispondente. Questo schema risolve tutti i problemi visti prima. Li risolve perché, immaginando che il firewall stia dal punto di vista della rete in cui si trova il nodo mobile a vallo del FA. Il firewall posizionato sul FA si vedrà entrare un pacchetto che ha come indirizzo mittente a livello IP quello del FA, vuol dire un indirizzo corretto dal punto di vista della topologia, mittente interno e destinatario interno. Il pacchetto che entra nel firewall dell'HA sarà corretto, in quanto avrà mittente esterno e destinatario interno. Il pacchetto deve riattraversare il tunnel, corretto in quanto avrà come indirizzo mittente quello originario del nodo mobile, e come indirizzo destinatario avrà quello di CN. Anche questo firewall verrà attraversato senza problemi.

Il punto è che abbiamo finito di parlare di una tecnica per eliminare il problema della triangolazione, e lo vediamo rientrare dalla finestra. Come si rimedia? Facendo si che il punto terminale del tunnel non sia lo HA ma il nodo corrispondente, nel caso in cui il nodo corrispondente non sia nella home network. Se il punto di terminazione del tunnel è direttamente il nodo corrispondente la triangolazione non c'è, e l'unico overhead è quello dei byte in più. Il lavoro di decapsulamento del pacchetto originario si deve fare carico il nodo CN corrispondente, che è tenuto ad avere implementato nello stack protocollare questo standard. Altrimenti, se il nodo CN è un nodo che per qualche motivo non vuole avere questa variante installata nel suo stack protocollare, la cosa non funziona.

Una cosa che forse ho il sospetto di aver omesso è che tutto ciò di cui abbiamo parlato riguarda il protocollo IP nella versione 4, in dismissione sostituita dalla versione 6. La ragione fondamentale per cui la versione 6 è stata introdotta per rimpiazzare la versione precedente è per ovviare al problema dell'esaurimento dello spazio di indirizzamento di cui soffriva la versione precedente. IPv4 utilizza indirizzi a 32 bit. Come coabita un protocollo pensato per la versione 4 con l'avvento della versione 6? Ne beneficia, in quanto la versione 6 possiede nativamente alcune caratteristiche che tornano molto comode per la gestione della mobilità. Per certi versi la versione originaria di Mobile IP ha dovuta essere aggiornata, però per certi versi può essere vista come una semplificazione ed una migliore realizzazione della versione precedente. Gran parte di quello che abbiamo detto rimane invariato, incluse le entità e le funzioni implementate rimangono immutate. Una delle novità rilevanti è che sparisce una delle entità in gioco, i FA. Sostanzialmente le funzioni svolte dai FA passano completamente in carico al nodo mobile, grazie alle funzioni offerte dalla versione 6 di IP. La versione 6 del protocollo IP presuppone che ogni nodo sia dotato della capacità di autoconofigurarsi, e questo significa che ogni nodo mobile è nativamente dotato, se implementa la versione 6 di IP, della capacità di dotarsi di un COA, indirizzo topologicamente corretto per la rete attualmente occupata. Avendo a disposizione 128 bit per costruire un indirizzo, una maniera semplice per costruirselo in proprio, una volta acquisito un prefisso di rete valido, basta aggiungere a questo prefisso il proprio indirizzo del livello 2, univoco su scala globale, ed in questo modo ci si può autocofigurare un indirizzo a livello IP unico globalmente.

Altra cosa interessante è che IPv6 è stata pensata in un momento in cui non ci si fidava più di ciò che circolava sulla rete, con protocolli di sicurezza integrati all'interno del protocollo. Come vedete riportato sulle slide, si realizza nativamente il meccanismo di ottimizzazione e

di soft smooth hand-off perché è il nodo mobile che comunica ai suoi corrispondenti la sua posizione, se questi fanno richiesta di essere aggiornati in proposito.

Giusto per avere un'idea, nel caso del protocollo Mobile IP questo è il modo in cui il protocollo tiene aggiornate le informazioni sulla posizione di un nodo mobile. Quando il nodo mobile entra in una rete, può o ascoltare i messaggi di advertisement che segnalano la presenza di un router e quindi del prefisso di rete da usare, o se non ascolta questi messaggi il nodo mobile può mandare un sollecito per avere le informazioni in proposito. Viene fatto un controllo sul COA auto configurato dal nodo mobile non porti alla creazione di duplicati. Il nodo mobile una volta superato il controllo manda il messaggio di registrazione al suo HA che informa, ed a questo punto il nodo corrispondente inizialmente invia i pacchetti usando l'indirizzo identificativo di MN, ed arriveranno all'HA che li invia al nodo mobile. A questo punto MN contatta direttamente il nodo corrispondente, lo informa della sua posizione attuale con un preambolo iniziale che fa da meccanismo di sicurezza, e superato il preambolo il nodo mobile manda il messaggio di BU che verrà usato dal nodo corrispondente per aggiornare la sua cache ed il nodo corrispondente costruisce il tunnel il cui punto terminale sarà il nodo mobile. Si risolvono i problemi di routing triangolare, di attraversamento dei firewall, non avendo ne problemi di filtraggi anomalo ne problemi nell'instradamento.

Giusto per chiudere questo capitolo, dal punto di vista del tracciamento la versione base ha un approccio pro attivo, mentre la versione con route optimization è ibrida, opzionale nella versione 4 e nativa nella versione 6. Dal punto di vista del livello di rete in cui si colloca ovviamente è una soluzione a livello 3. Dal punto di vista della portata, quanto amplia può essere la mobilità coperta dal meccanismo, siamo a livello globale. Ovunque un nodo si agganci alla rete, usando questo protocollo il nodo mobile sarà raggiungibile. Dal punto di vista delle entità coinvolte, sopratutto nella versione 6, è una modalità host-based.