

MSA - Mobility Management in Internet

Soluzioni a livello di rete

- **Indirizzo IP fisso:** idea è quella di raffinare i meccanismi di routing adottati. Raffinare significa aumentare le informazioni presenti nelle tabelle di routing associate ai vari router, con informazioni relative ai singoli nodi mobili
 - Nella tabella di routing non memorizzo solamente il prefisso della sottorete, ma l'indirizzo completo di ogni singolo nodo mobile
 - Soluzione semplice che non richiede nessuna modifica rilevante
 - Abbiamo però problemi di scalabilità riguardo alla dimensione della tabella di routing, nelle dimensioni eccessive dei pacchetti per l'aggiornamento della tabella e per gli aggiornamenti frequenti della tabella
- **Indirizzo IP dinamico:** idea è che l'indirizzo IP possa cambiare in maniera da mantenere la corrispondenza con la topologia della rete
 - Il nodo che si sposta, si aggancia ad un altro dominio di rete, perde il vecchio indirizzo IP e gliene viene associato uno nuovo adeguato alla nuova posizione
 - I pacchetti che arrivano con il nuovo indirizzo verranno correttamente instradati alla nuova posizione
 - Per risolvere la questione della raggiungibilità l'idea potrebbe essere quella di utilizzare il servizio DNS, anche se i DNS non sono stati pensati per gestire questo tipo di problema, a causa del meccanismo di consistenza debole su cui è basato il servizio
 - Altro problema è che se l'indirizzo IP cambia, protocolli di trasporto come UDP e TCP assumono che l'end point dell'interazione rimanga costante per l'intera sessione

Soluzioni diverse al livello di rete

- **Livello di rete:** protocollo DHCP, nato per gestire problemi di mobilità e per la configurazione automatica dell'aggancio di un nodo ad una rete. In particolare, un'informazione che il server DHCP fornisce ad un nodo che si aggancia ad una rete è l'indirizzo IP
 - Soluzione che risolve parzialmente il problema della raggiungibilità, in quanto il nodo ottiene un indirizzo IP solamente nel caso in cui è lui stesso ad iniziare la comunicazione
 - Non risolve in nessun modo il problema della continuità di una sessione nel momento dell'hand-off con il passaggio ad una rete diversa
- **Livello di trasporto:** idea è che nel momento in cui il nodo mobile cambia sottorete ed ottiene un nuovo indirizzo IP, il nuovo indirizzo viene comunicato al partner utilizzando la comunicazione esistente, e dunque i partner concordano un trasferimento della sessione in corso sulla nuova connessione
 - **mSCTP:** estensione del protocollo SCTP, protocollo di trasporto pensato per situazioni di streaming che, tra le caratteristiche, supporta sessioni che

avvengono tra nodi che hanno interfacce di rete diverse con indirizzi IP differenti

- La variante mSCTP prevede la possibilità che la lista degli indirizzi IP di riserva possa variare dinamicamente
- **TCP + DNS:** visione più completa, per cui garantire la continuità della sessione ma anche la raggiungibilità del nodo
- **Livello applicativo:** protocollo SIP

Mobile IP

- Abbiamo l'esistenza di due indirizzi IP:
 - **Home address:** continua a svolgere il ruolo di identificativo unico del nodo
 - **Care of address:** indirizzo variabile, varie per essere costantemente allineato con la posizione attualmente occupata dal nodo mobile
- Come viene realizzata la raggiungibilità?
 - Chiunque voglia parlare con il nodo mobile ignora che il nodo abbia cambiato posizione e continua a parlare con lui utilizzando il suo home address
 - Il protocollo prevede dei meccanismi di reindirizzamento verso la destinazione attuale del nodo mobile in caso di spostamento
- **Location directory (LD):** tabella mantenuta all'interno della home network che mantiene l'associazione tra indirizzo identificativo del nodo mobile ed il suo indirizzo temporaneo
- Come avviene la comunicazione in modo più preciso?
 - CN costruisce il messaggio in maniera standard, utilizzando come indirizzo di destinazione l'indirizzo IP dello home address di MN
 - Il pacchetto arriva nella home network e viene intercettato dallo HA
 - Se il nodo mobile è presente nella home network, il pacchetto attraversa l'HA ed arriva a destinazione. Altrimenti HA prende il pacchetto e consulta la tabella di localizzazione. Incapsula il pacchetto con un nuovo header IP dove come campo di destinazione è indicato il CoA del nodo mobile, dunque il FA
 - Quando arriva nella rete di destinazione, il pacchetto viene intercettato da FA che rimuove l'header aggiunto da HA e consegna il pacchetto al nodo mobile
 - Il nodo mobile risponde direttamente inviando un pacchetto a CN
- **Posizione HA:** lo HA può essere incastonato nel router o può essere un'entità a se stante all'interno della rete
 - La prima soluzione non richiede l'ingresso nella rete del pacchetto, riduce la latenza per completare la comunicazione, ma non sempre è possibile installare all'interno di un router questa funzionalità
 - Soluzione del secondo tipo svincola il protocollo Mobile IP dalle responsabilità del router e, per poter intercettare i pacchetti, HA è autorizzato ad agire come proxy del protocollo ARP
- Quest'idea molto semplice si realizza e si implementa grazie alla presenza di tre funzionalità: Agent Discovery, Registrazione e Tunneling

Agent Discovery

- Consente ad HA e FA di rendere nota la loro presenza, permettendo al nodo mobile di capire se si trova nella sua home network, se ascolta il messaggio del suo HA, o in una rete differente in caso contrario, dovendo avvisare l'HA della sua nuova posizione temporanea
- Consiste nell'invio periodico di messaggi all'interno della rete (**advertisement message**) coperta da una delle entità. Messaggi di questo tipo ne circolano di varia natura, e proprio per questa natura la scelta che è stata fatta dal comitato è stata quella di appoggiarsi ad un meccanismo già definito nello standard internet, in particolare i messaggi definiti dal protocollo ICMP
- L'idea è di aggiungere ai campi del messaggio ICMP un'estensione per trasportare informazioni necessarie per la realizzazione di alcune funzioni di gestione della mobilità
- **Campi dell'estensione:**
 - **COA:** il campo viene trasmesso se il messaggio viene emesso dall'entità che svolge il ruolo di FA. Il 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 quel messaggio. COA è un indirizzo che identifica la 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 verranno destinati al FA che, dopo aver rimosso l'header aggiuntivo, li inoltrerà al MN
 - **Registration lifetime:** il campo indica la durata della registrazione, cioè per quanto tempo l'associazione tra un FA ed un COA deve essere considerata valida. Se l'associazione non viene rinnovata, scaduto il termine non viene più ritenuta valida
 - **Altri campi:**
 - Specificare che il FA impone ai nodi mobili di registrarsi presso di lui
 - Segnalare che il FA non accetta più l'arrivo di registrazioni di nodi mobili presso di lui
 - Ruolo dell'entità che emette il messaggio, FA o HA
 - Capacità o meno dell'agent di supportare alcune varianti del protocollo
 - Supporto della funzione di reverse tunneling
- La scelta di utilizzare il protocollo ICMP come base si può pagare in termini di non perfetta aderenza alle esigenze di ciò che si vuole andare a realizzare
 - **Intervallo minimo tra l'emissione di due messaggi:** ICMP indica un valore minimo di 3 secondi tra l'emissione di due messaggi, sufficiente dal punto di vista di un router con nodi fissi, ma non nel caso di un nodo mobile che entra nella sottorete ed ha una sessione TCP in corso

Registrazione

- Lo scopo di questa funzione in generale è di comunicare all'HA l'attuale care of address, cioè l'indirizzo temporaneo, del nodo mobile
- L'ottenimento del CoA può avvenire in due modi differenti:

- **Foreign Agent Care-of address:** l'indirizzo temporaneo è n indirizzo IP che identifica il FA della rete in cui si trova il nodo mobile. 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 richiesta di registrazione, e la relativa risposta, viene inviata al FA che provvederà all'inoltro verso lo HA
- **Colocated care-of address:** l'indirizzo, topologicamente corretto rispetto alla rete in cui si trova il nodo mobile, viene acquisito dal nodo mobile sesso utilizzando il protocollo DHCP, tipicamente. In questo caso il punto finale del tunnel è il nodo mobile, non più il FA, dunque deve esser elui a ricevere il pacchetto transitato sul tunnel e rimuovere l'header aggiuntivo
 - La richiesta di registrazione viene inviata dal MN direttamente allo HA
- I messaggi di registrazione sulla rete viaggiano come pacchetti UDP. La trasmissione non è affidabile, il protocollo Mobile IP ha un suo meccanismo di eventuale ritrasmissione della registrazione
- **Campi del messaggio di richiesta registrazione:**
 - **COA:** nel caso in cui il nodo mobile sia rientrato nella sua rete di casa, sarà il suo HA
 - **Identification:** campo presente a scopi di sicurezza, serve a proteggere contro gli attacchi di tipo replay. Questo campo serve ad associare una richiesta di registrazione con la relativa risposta, non permettendo di riutilizzarla in futuro come una richiesta emessa nel passato
 - **Altri campi:**
 - Informare l'HA su eventuali esigenze o capacità del nodo mobile che sta chiedendo di fare la registrazione
- **Campi del messaggio di risposta registrazione:**
 - Comunica se la registrazione ha avuto successo o no, e nel caso di insuccesso per quale motivo
 - **Lifetime:** tornando ai messaggi di advertisement, il campo lifetime era il limite superiore che può essere dato alla variabile durante la registrazione. Dunque un nodo mobile può richiedere che la sua registrazione valga per un tempo non superiore. Quando il tempo di vista si approssima alla scadenza ed il nodo non ha cambiato posizione, deve reinviare un messaggio di registrazione per tenerla in vita

Tunneling

- Quando il pacchetto originale arriva allo HA, questo viene arricchito di un nuovo header IP, trasformando quello che c'era prima in carico utile
- **Esempio della situazione:**
 - CN invia pacchetto ad HA, l'home address del nodo mobile
 - Il pacchetto viene catturato dall'HA. Se il nodo non si trova nella rete mobile, allora il vecchio pacchetto viene incapsulato in uno nuovo, nel cui header sarà indicato il CoA del nodo mobile come destinazione

- Tutti gli altri campi rimarranno uguali, con l'unica eccezione del campo TTL che verrà decrementato di 1 rispetto al pacchetto originario. Questo per fare in modo che ovunque sia il nodo mobile, distante quanto vogliamo in termini di numero di hop da percorrere per passare dalla home network alla foreign network, comunque questa distanza non deve essere visibile né al nodo mobile e né a chi interagisce con lui
- **Header minimale:** c'è una duplicazione completa del vecchio header nel nuovo, a meno di informazioni modificate. L'overhead causato dalla duplicazione può essere più o meno importante a seconda della grandezza del carico utile, ma sono comunque byte in più
 - Dovendo l'header esterno essere un header IP completo, viene ridotto l'header interno, che non è l'originale ma una sua versione ridotta, dove quello che viene conservato è tutto ciò che non può essere ricostruito usando le informazioni presenti nell'header esterno

Route Optimization

- 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 sui ritardi tra i nodi
- Il meccanismo di ottimizzazione dei percorsi prevede che la prima volta che qualcuno vuole comunicare con il nodo mobile, contatta l'HA essendo l'unica informazione a disposizione e da lì verranno rimbalzati verso il FA relativo alla posizione attuale del nodo mobile
- A questo punto il nodo CN può chiedere di essere informato lui su qual'è la posizione attuale nel nodo mobile, in modo da indirizzare i pacchetti direttamente verso il suo FA. Tutto questo avviene arricchendo il nodo corrispondente che si fa carico gestendo la binding cache. Si tratta di una replica in piccolo limitata agli interessi del nodo CN, che innesca meccanismi di gestione della cache e problemi sull'obsolescenza delle informazioni, che si risolvono usando tecniche analoghe a quelle che si usano in tutte le situazioni di questo tipo
- **Flusso dei messaggi:**
 - CN vuole parlare con il nodo MN, connesso ad un primo FA
 - CN manda i dati alla home network, dove vengono catturati dall'HA
 - CN manda anche un messaggio di binding request, chiedendo di essere informato sulla posizione occupata dal nodo mobile
 - HA costruisce il tunnel verso il FA usando le tecniche di incapsulamento viste
 - 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
 - Mentre lo scambio è in corso MN cambia posizione, che invia tramite il suo nuovo FA la richiesta di registrazione al suo HA
 - CN di tutto ciò non è informato, continua ad inviare pacchetti al vecchio FA che lo avviserà del cambio di posizione di MN

- A questo punto CN contatta nuovamente l'HA per richiedere la posizione attuale del nodo MN, a cui il HA risponderà e CN aggiornerà il valore della sua cache
- **In alternativa:** quando HA riceve il nuovo messaggio di registrazione da parte del nodo mobile, invia subito il messaggio di warning a CN, che in precedenza aveva richiesto informazioni sulla posizione del nodo mobile
- Questo meccanismo introduce un elemento di reattività, che però non serve a compensare la perdita di precisione causata da un tracciamento meno preciso, ma serve soltanto a ridurre l'impatto negativo dell'instradamento triangolare
- **Smooth hand-off:**
 - Nella soluzione vista in precedenza, quando CN invia dati al vecchio FA, questo risponde con un messaggio di warning, dunque la comunicazione con MN viene interrotta
 - In questo caso il cambio di posizione di un nodo viene prorogato al vecchio FA, che viene informato sulla nuova posizione occupata dal nuovo nodo mobile
 - CN continua ad inviare pacchetti al vecchio FA che, oltre a rispondere con il messaggio di Warning, li inoltra verso il nuovo FA, in modo che i pacchetti dati non vengono persi
 - Il guadagno va molto al di là dell'evitare di perdere pacchetti e doverli ritrasmettere, già di per sé un guadagno. Ma se si pensa al protocollo TCP, l'effetto causato dalla perdita di pacchetti può indurre ad un abbassamento anche drammatico del throughput

Firewall e Reverse Tunneling

- Nodo mobile si trova in un FN protetto da firewall e vuole parlare con un suo partner che può stare ovunque nella rete. Il pacchetto emesso dal nodo mobile avrà come indirizzo mittente l'indirizzo di HA, indirizzo però non appartenente alla rete, e dunque potrebbe essere bloccato dal firewall
- Altro caso, se il nodo mobile vuole comunicare con un partner che appartiene alla sua HM. Se HM dotata di firewall, quest'ultimo vedrà arrivare dall'esterno un pacchetto con sorgente un indirizzo della sottorete, e non farà passare il pacchetto
- Rimedio è noto come lo standard **reverse tunneling**:
 - MN invia pacchetto al FA che lo incapsula e lo invia all'HA
 - HA cattura il pacchetto e lo instrada verso il nodo di destinazione
 - Pacchetto riuscirà a passare per il firewall in quanto avrà indirizzo mittente topologicamente corretto
- Questa soluzione però introduce nuovamente la *triangolazione dei pacchetti*, risolvibile solamente in un unico modo:
 - Il punto terminale del tunnel è CN e non HA
 - Il lavoro di decapsulamento deve essere svolto da CN, che è tenuto ad avere implementato questo standard nel suo stack protocollare

IPv6

- Versione 6 introdotta per ovviare al problema dell'esaurimento dello spazio di indirizzamento della versione precedente, causata dall'utilizzo di indirizzi a 32 bit
- Versione originale di Mobile IP è stata aggiornata, portando ad una semplificazione ed ad una migliore realizzazione rispetto alla versione precedente
- Vengono rimossi i FA, le cui funzioni passano completamente in carico al nodo mobile, grazie alle funzioni di autoconfigurazione dei nodi introdotte dalla versione 6 del protocollo, e dunque di dotarsi in modo autonomo di un COA topologicamente corretto. Avendo a disposizione 128 bit per costruire un indirizzo, un modo semplice per farlo è, dopo aver acquisito un prefisso di rete valido, aggiungere al prefisso il proprio indirizzo MAC, di livello 2
- Integra protocolli di sicurezza e realizza nativamente il meccanismo di ottimizzazione dei percorsi e di smooth hand-off, in quanto è il nodo mobile che comunica ai suoi corrispondenti la sua posizione se questi fanno richiesta di essere aggiornati
- **Flusso dei messaggi:**
 - MN entra in una rete, ascolta messaggi di advertisement o invia un sollecito, per avere le informazioni sulla presenza di un router e quindi sul prefisso di rete da usare
 - Viene fatto un controllo sul COA auto-configurato dal nodo mobile, in modo che non porti alla creazione di duplicati
 - MN invia messaggio di registrazione al suo HA
 - Nodo corrispondente invia i pacchetti usando l'indirizzo identificativo di MN, dunque quello relativo all'HA, che intercetterà i pacchetti e li inoltrerà al nodo mobile
 - MN contatta direttamente il nodo corrispondente, lo informa della sua posizione attuale con un preambolo iniziale che fa da meccanismo di sicurezza ed invia il messaggio di BU che verrà usato dal nodo corrispondente per aggiornare la sua cache
 - Il nodo corrispondente costruisce il tunnel, il cui punto terminale sarà il nodo mobile
- Si risolvono i problemi di routing triangolare e di attraversamento dei firewall

Classificazione MobileIP v4/v6

- **Tracciamento:** versione base ha un approccio proattivo, mentre la versione con route optimization (opzionale in v4, obbligatoria in v6) è ibrida
- **Livello di rete:** soluzione a livello 3
- **Portata:** livello globale
- **Entità coinvolte:** host-based, soprattutto nella versione 6

Proxy Mobile IPv6

- Mobile IP, essendo una versione host-based, per essere implementata richiede una modifica dello stack protocollare di ogni singolo nodo. Come conseguenza del fatto che i singoli nodi mobili sono coinvolti direttamente nella realizzazione delle funzioni del protocollo, c'è un possibile aumento del tempo di hand-off

- Soluzione alternativa è standard che prende il nome di **Proxy Mobile IPv6**
- Consente di essere installata senza richiedere modifiche a nodi mobili preesistente, ha un uso più efficiente delle risorse wireless ed una maggiore velocità nelle procedure di hand-off. Viene inoltre ridotta la quantità di messaggi che circolano nella rete essendo una soluzione network based, escludendo la necessità di creare tunnel che si estendono anche sulla parte wireless
- **Terminologia:**
 - **LMA:** il punto di aggancia dei nodi mobili rispetto al resto della rete internet. E' un router il cui prefisso di rete identifica la posizione occupata dai nodi mobili all'interno della rete internet. Ogni nodo mobile riceve un indirizzo IP che appartiene topologicamente al dominio gestito dall'LMA
 - **MAG:** entità a cui fisicamente si aggancia un nodo mobile, ognuna di queste avrà un indirizzo IP specifico, utilizzato dall'LMA per inoltrare all'interno del suo dominio i messaggi indirizzati verso il nodo mobile
- Ogni nodo mobile possiede un indirizzo IP, fisso fin quando si trova all'interno del dominio di rete gestito dall'LMA. L'indirizzo rimane costante anche nel cambio di MAG
- Ogni MAG agisce da proxy per ogni nodo mobile dal punto di vista della raggiungibilità. I tunnel vanno da LMA ai singoli MAG
- **Flusso dei messaggi:**
 - Nodo mobile entra all'interno di un dominio di rete
 - Nodo mobile entra in contatto con il MAG che gestisce il pezzo di rete a cui si è connesso fisicamente per la registrazione
 - Superata la registrazione, nodo mobile chiede che venga associato un indirizzo IP che lo renda raggiungibile all'interno del dominio di rete
 - MAG inoltra la richiesta all'LMA, che assegnerà al nodo mobile un prefisso di rete che sia topologicamente corretto
 - LMA aggiunge alla sua tabella di gestione l'informazione sul prefisso e sul MAG a cui il nodo mobile è associato
 - L'informazione viene associata al nodo mobile che si autoconfigura, dotandosi di un indirizzo IP unico
 - I pacchetti che arriveranno ad LMA verranno incapsulati in un tunnel destinato al MAG di riferimento del nodo mobile, quest'ultima informazione contenuta nella tabella dell'LMA
- Se il nodo mobile cambia punto di aggancio avviene l'operazione di distacco, con il vecchio MAG che manda un messaggio di de-registrazione all'LMA che fa partire un timer, il tempo concesso al nodo mobile per avviare una nuova procedura di aggancio ad un nuovo MAG. Scaduto il timer, LMA rimuove dalla sua tabella la riga relativa al nodo mobile in questione. Se il nodo mobile si aggancia successivamente ad un nuovo MAG, la procedura vista si ripete
- **Riassumendo:**
 - Dal punto di vista del nodo mobile, tutto questo dominio di rete appare come un singola rete di livello 2. Una volta ricevuto un indirizzp IP che lo rende

raggiungibile all'interno della rete, questo non cambia fin quando il nodo continua ad essere connesso allo stesso dominio di rete

- Un nodo corrispondente che vuole parlare con il nodo mobile invia i pacchetti all'LMA, che li inolterà al MAG corrispondente per il successivo inoltro al nodo mobile
- Si ripresenta il problema della *triangolazione dei pacchetti*, non risolvibile in quanto il nodo mobile rimane fuori dalla gestione della sua raggiungibilità

- **Classificazione:**

- **Tracciamento:** soluzione puramente proattiva
- **Livello:** livello 3
- **Portata:** mobile IP ha un'ambizione globale, all'interno dell'architettura complessiva di internet. Questa soluzione riesce a gestire soltanto spostamenti che si svolgono all'interno del dominio gestito da un LMA
- **Entità coinvolte:** soluzione puramente network-based