Capitolo 1

SCENARIO

Tutti i dispositivi mobili attualmente offrono diverse modalità di accesso ad internet basti pensare a uno smartphone che consente l'accesso a internet sia in modalità Wi-Fi che attraverso la telefonia mobile sfruttando tecnologie come il 3G fino al più recente 4G.
In questo capitolo si vuole descrivere un'architettura che consente a un user app che fornisce un servizio multimediale in esecuzione su di un mobile device *multi-homed*, ovvero che monta più di un'interfaccia di rete, di sfruttare tutte le sue NIC (Network Interface Card) in un contesto di mobilità. È interessante studiare uno scenario che fa uso di un'app multimediale (come può essere ad esempio un'applicazione per chiamate VoIP) in quanto sono app *real-time* e generano una grande mole di traffico. Le app appartenenti alle categorie dei servizi multimedial real-time vengono solitamente realizzate sfruttando il protocollo UDP: l'architettura presentata in questo capitolo fornisce un meccanismo in grado da rendere possibile l'inoltro di ciascun datagram UDP attraverso l'interfaccia di rete più adatta e disponibile al momento della trasmissione. Questa architettura è detta ABPS (Always Best Packet Switching) ma prima di descriverne i suoi principali aspetti verrà descritto lo stato dell'arte per quel che riguarda la gestione della mobilità dei nodi mobili.

1.1 Seamless Host Mobility & State Of the Art

Nel corso degli ultimi anni sono state sviluppate diverse architetture che consentono a un nodo mobile in movimento di avere accesso continuo a servizi di rete in particolare sono stati sviluppati diversi approcci che cercano di far si che device che montano più interfacce di rete possano effettuare un *handover* da un interfaccia di rete all'altra in maniera del tutto trasparente all'app utente in esecuzione, ovvero in maniera *seamless*. Per handover o handoff si intende il processo di cambio di interfaccia di telecomunicazione da parte di un dispositivo multi-homed (*vertical handoff*) oppure il cambio di punto di accesso mantenendo la stessa tecnologia di telecomunicazione (*horizontal handoff*, ad esempio cambio di AP all'interno di una stessa rete WLAN).
In generale una buona architettura per la seamless mobility dovrebbe essere responsabile di identificare univocamente ciascun nodo mobile permettendogli di essere raggiungibile dall'altro nodo coinvolto nella comunicazione (Correspondent Node che potrebbe essere anch'esso un nodo mobile) e dovrebbe, inoltre, monitorare la QoS fornita dalle diverse reti a cui il nodo mobile potrebbe connettersi in modo da prevedere la necessità di un handoff ed eventualmente eseguirlo in maniera *seamless* assicurando la piena continuità della comunicazione.
Vediamo ora una rassegna di tutte le soluzioni sviluppate finora per implementare meccanismi di seamless handoff in un contesto di un nodo mobile che attraversa reti eterogenee.

Implementazioni a livello network Tra le architetture presenti che lavorano a livello network vi è Mobile IP version 6 e le sue ottimizzazioni come ad esempio FMIP (Fast Handover Mobile IPv6), HMIP (Hierarchical Mobile IPv6) e PMIP (Proxy Mobile IPv6). Tutte queste architetture adottano un *Home Agent* ovvero un'entità aggiuntiva che opera all'interno della rete alla quale il nodo mobile appartiene. L'home agent ricopre il ruolo

di *location registry* ovvero un servizio *always on*: quando un nodo mobile cambia interfaccia di rete e quindi indirizzo IP lo comunica al location registry (*registration phase*) che tiene una mappa degli indirizzi. Quando un Correspondent Node vuole comunicare con il nodo mobile invia al location registry una *lookup phase* per ottenere l'indirizzo corrente del mobile node. Tutti i nodi coinvolti devono avere il supporto a IPv6: in particolare l'indirizzo attuale e l'identificativo univoco del nodo mobile sono trasmessi attraverso delle estensioni di IPv6. Il fatto che tutti i nodi debbano necessariamente supportare IPv6 rappresenta un limite di questo approccio architetturale. Un altro limite di questo approccio è che presso un home agent può essere registrato l'indirizzo di una sola interfaccia di rete per ogni nodo impedendo così un supporto al multihoming visto che la latenza introdotta dai numerosi messaggi di autenticazione procurerebbe un overhead insostenibile per la tipologia di comunicazione multimediale che dovrebbe essere veloce e snella.

Implementazioni tra livello rete e trasporto Esistono alcune possibili implementazioni di architetture per la seamless host mobility che introducono un nuovo layer posto tra il livello rete e quello trasporto: questa nuova astrazione dovrà essere aggiunta su tutti i nodi prendenti parte alla comunicazione. Alcuni esempi possono essere HIP (Host Identity Protocol) e LIN6 (Location Independet Addressing for IPv6). Il location registry si comporta in maniera simile a un server DNS mappando l'identificativo di un host e la sua attuale posizione restando però all'esterno della rete di appartenenza del nodo mobile. Un limite di questo approccio è nella necessità di modificare lo stack di rete di tutti i nodi coinvolti.

Implementazioni a livello trasporto Vi sono alcuni protocolli che operano a livello trasporto: ogni nodo coinvolto in una comunicazione si comporta in maniera pro-attiva fungendo da location registry informando direttamente il proprio Correspondent Node ogni qualvolta la configurazione di rete cambia. Il limite di questo approccio sta nel fatto che se entrambi i mobile end-system cambiano contemporaneamente gli indirizzi IP a seguito

di un handoff diventano mutuamente irraggiungibili. Inoltre, come nel precedente approccio, questo tipo di architettura richiederebbe una modifica delle applicazioni sia sul nodo mobile che sul suo correspondent node.

Implementazioni a livello Sessione Sono state progettato alcune soluzioni che operano a livello sessione come ad esempio TMSP (Terminal Mobility Support Protocol) che sfrutta un SIP server ausiliario collocato fuori dalla rete di un nodo mobile che funge da location registry che mappa ciascun identificativo SIP di utente al suo indirizzo IP attuale. Ogni nodo mobile esegue un client SIP che manda un messaggio di tipo REGISTER per aggiornare il suo indirizzo IP. I messaggi INVITE, al solito, sono utilizzati per avviare comunicazioni con altri nodi così come i messaggi di tipo re-INVITE. Gli approcci operanti a livello Session non sembrano essere particolarmente efficienti per i ritardi introdotti dal pattern message/response dei sistemi basati SIP. In letteratura vi sono altre soluzioni alcune parziali come IEEE 802.11e e IEEE 802.11r che però coinvolgono solamente la gestione dell'interfaccia di rete Wi-Fi (handover orizzontali) e soluzioni proprietarie come LISP di CISCO.

1.2 Always Best Packet Switching

Un'architettura progettata all'interno del Dipartimento di Informatica dell'Università di Bologna che supera molti dei limiti delle implementazioni precedentemente descritte è ABPS (Always Best Packet Switching). L'architettura ABPS è composta da due componenti principale:

- **fixed proxy server**, una macchina esterna alla rete in cui si trova il mobile node; munito di IP pubblico statico e fuori da qualsiasi firewall o NAT. Il fixed proxy server gestisce e mantiene tutte le comunicazione da un mobile node verso l'esterno e viceversa: nel caso di un handoff e quindi di una riconfigurazione delle interfacce di rete del nodo mobile il fixed proxy server nasconde questi cambiamenti al correspondent

node facendo si che la comunicazione continui in maniera del tutto trasparente.

- **proxy client**, in esecuzione su ogni mobile node, mantiene per ogni NIC una connessione verso il fixed proxy server. Applicazioni in esecuzione su un nodo mobile possono quindi sfruttare un multi-path virtuale creato tra il proxy client e il fixed proxy server per comunicare con il resto del mondo.

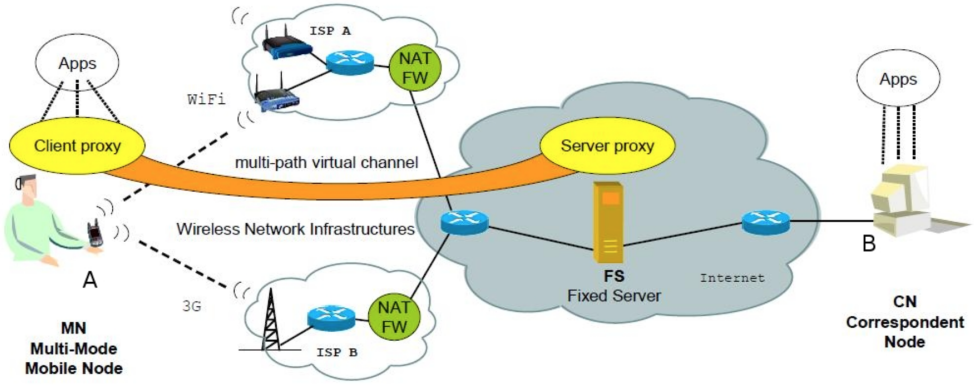

Figura 1.1: Architettura ABPS

Si immagini uno scenario in cui un nodo mobile A munito di più interfacce wireless (ad esempio NIC Wi-Fi e UMTS) stia intrattenendo una comunicazione VoIP con un altro nodo mobile B. Il nodo A implementa il meccanismo ABPS appena descritto quindi sul dispositivo è in esecuzione un ABPS proxy client che mantiene un canale di comunicazione con un ABPS fixed proxy. Supponiamo che il nodo A sta utilizzando l'interfaccia di rete Wi-Fi e quindi risulta essere connesso a una rete WLAN. Se avviene un handoff verso un'altra interfaccia di rete, ad esempio UMTS, per un calo delle prestazioni o per una perdita improvvisa del segnale dell'access point a cui è connesso il nodo mobile il cambio di configurazione di rete avviene in maniera del tutto trasparente al nodo B e alle applicazioni in esecuzione sul

nodo A. Il meccanismo descritto può inoltre decidere su quale interfaccia di rete inoltrare il singolo datagram UDP a seconda delle condizioni della rete a cui ciascuna NIC è connessa. In particolare vi è un monitoraggio del QoS per ciascuna interfaccia di rete wireless e se vi è il sospetto di una perdita di informazioni o di un ritardo di trasmissione un dato pacchetto può essere ritrasmesso su un'altra NIC. Ciascuna interfaccia di rete rimane configurata e attiva e pronta a essere utilizzata nel caso in cui l'interfaccia attualmente in uso abbia dei ritardi o delle perdite.

Qui di seguito viene illustrato un esempio di una possibile implementazione dell'architettura ABPS per il mantenimento di un servizio VoIP basato sui protocolli SIP e RTP/RTCP.
Come si può vedere dalla figura 1.2 il nodo mobile oltre alla user app VoIP mantiene attivo un client proxy: i pacchetti trasmessi dall'app vengono intercettati dal proxy client mantenendo attiva un'interfaccia di rete virtuale settata come default gateway. Per ogni interfaccia di rete reale il proxy client inizializza e mantiene attivo un socket per ogni protocollo di comunicazione e segnalazione.

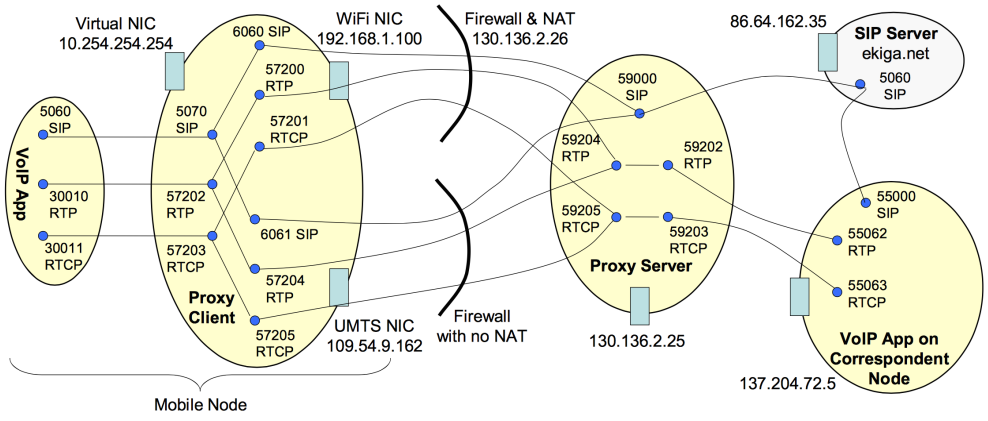

Figura 1.2: Architettura ABPS per una comunicazione VoIP via protocollo SIP e RTP/RTCP

Il fixed proxy server regola il traffico VoIP in invio o ricezione dal mobile node esponendo verso un SIP server (ad esempio ekiga.net) e il correspondent node un indirizzo IP pubblico e statico e delle porte associate a ciascun protocollo VoIP. La comunicazione tra il client proxy e il fixed server proxy può fare uso di un'estensione del protocollo SIP per lo scambio di ulteriori parametri di configurazione (ad esempio identificativo per individuare ciascun proxy client che comunica con ABPS proxy server).

1.2.1 Architettura

Vediamo ora brevemente le caratteristiche principali delle componenti dell'architettura Always Best Packet Switching.

Fixed proxy server Sul fixed proxy server è presente un modulo software chiamato *Policies Module*. Il compito del Policies Module, molto semplicemente, è quello di valutare su quale interfaccia di rete inoltrare un messaggio diretto verso un mobile node: verrà utilizzato l'indirizzo IP mittente dell'ultimo pacchetto ricevuto dal proxy client.

Mobile node L'architettura per supportare ABPS su un nodo mobile risulta essere piuttosto complessa. È composta da:

- **Monitor**, il suo compito principale è quello di monitorare e configurare le diverse interfacce di rete wireless presenti sul nodo mobile. Ogniqualvolta una NIC viene configurata o disabilitata il Monitor invia una notifica al proxy client di tipo *Reconfiguration Notification*.

- **TED (Transmission Error Detector)**, è il componente più importante del sistema; si occupa di monitorare l'invio dei datagram UDP trasmessi dall'app VoIP e di notificare al client proxy se il pacchetto è stato consegnato o meno all'access point. Una volta inviato un certo pacchetto, attraverso la scheda di rete Wi-Fi, TED valuterà il relativo

ACK proveniente dall'access point e tramite la notifica *First-hop Transmission Notification* notificherà al proxy client lo status di consegna di quel pacchetto. TED è implementato in maniera cross-layer nello stack di rete del kernel Linux. TED e la sua implementazione saranno largamente descritti nel capitolo successivo.

- **Wvdial** si tratta di un modulo che implementa Transmission Error Detector per UMTS.

- **Proxy client**, il cui ruolo principale è quello di inoltrare il traffico di una user app verso il ABPS fixed proxy server.
  Il proxy client al suo interno implementa il modulo *ABPS Policies* che implementa una serie di politiche e meccanismi in base alle notifiche provenienti dall'altre componenti in esecuzione sul nodo mobile e dirette verso il proxy client. Le tipologie di notifiche che possono essere ricevute sono quelle precedentemente accennate. Quando il proxy client riceve una notifica di tipo Reconfiguration Notification per ogni nuova interfaccia di rete segnalata come attiva viene creato un nuovo socket e associato a tale interfaccia; viceversa quando un'interfaccia viene segnalata come disabilitata (a seguito ad esempio di un errore di trasmissione) il relativo socket associato viene chiuso.
  Un'altro tipo di notifica che un proxy client può ricevere è proveniente dal TED: in questo l'ULB (UDP Load Balancer), un altro modulo implementato all'interno del proxy client, valuterà in base alla notifica se ritrasmettere un dato datagram e attraverso quale interfaccia di rete.
  L'ultimo tipo di notifica che un proxy client può ricevere è quella proveniente dal protocollo ICMP: semplicemente questa notifica segnala al proxy client che il fixed proxy server (o la porta sul proxy server con la quale si vuole comunicare) è *unreachable* attraverso l'interfaccia di rete attualmente in uso.
  Queste tre tipologie di notifiche permettono al proxy client di stabilire se un determinato pacchetto debba essere ritrasmesso (eventualmen-

te attraverso un?altra interfaccia wireless) o definitivamente scartato. Permettono inoltre di realizzare un opportuno algoritmo per la selezione dinamica dell?interfaccia di rete che offre maggiori garanzie di trasmissione.

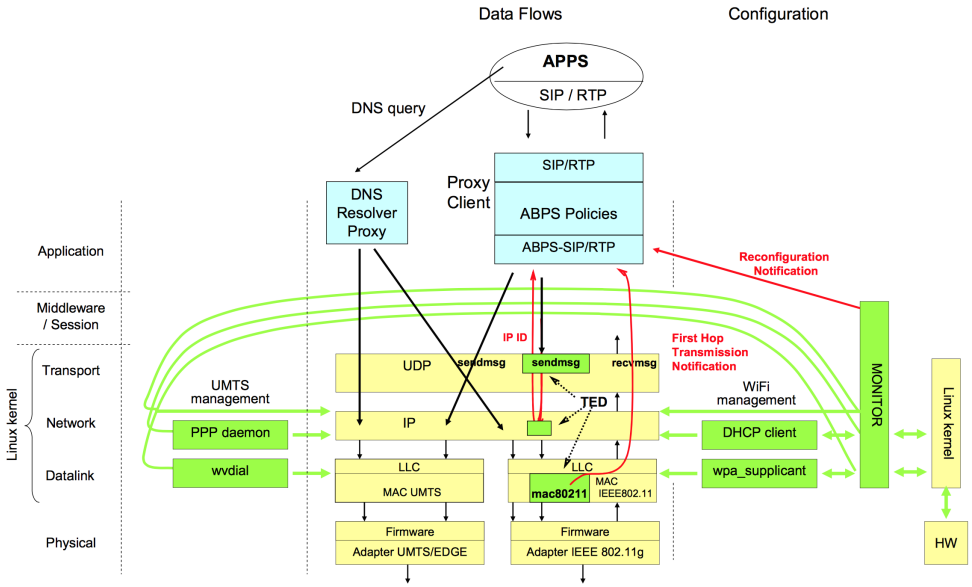

Figura 1.3: Infrastruttura Mobile Node in ABPS

1.3 Considerazioni finali

In questo capitolo abbiamo visto una breve panoramica di Always Best Packet Switching e delle sue funzionalità di base. Abbiamo visto come senza modificare l'infrastruttura di rete è possibile inoltrare il flusso di dati proveniente da un certa applicazione utente su una piuttosto che su un'altra interfaccia di rete di un nodo mobile a seconda dello stato in cui si trova la rete.

Nel caso di una riconfigurazione di rete ABPS abbatte eventuali overhead introdotti da approcci come quello basato su SIP e può far fronte a handoff verticali senza alcun ritardo in quanto, come visto, ciascuna interfaccia di

rete viene mantenuta attiva e pronta all'utilizzo. L'utilizzo di ciascuna NIC è ottimizzato valutando pacchetto per pacchetto su quale interfaccia di rete questo dovrebbe essere inoltrato valutando le condizioni della rete e le QoS desiderate. Inoltre ABPS consente a un nodo mobile di comunicare verso l'esterno anche in presenza di NAT o firewall.

ABPS può essere utilizzato in qualsiasi contesto VoIP.