UNIVERSITÀ DI PISA

Facoltà di Ingegneria

Corso di Laurea in Ingegneria delle Telecomunicazioni

TESI DI LAUREA

Protocollo di routing HWMP per reti wireless mesh: sviluppo di un prototipo ed analisi sperimentale

Relatori

Prof. Stefano Giordano

Ing. Rosario Garroppo

Candidato

Giorgio Barsacchi

Anno Accademico 2006 – 2007

INDICE

Introduzione

1 Wireless Mesh Network 5

1.1 Aspetti generali 5

1.1.1 Architettura di rete 7

1.1.2 Caratteristiche delle WMNs 9

1.2 Routing nelle reti mesh 11

1.2.1 Protocolli di routing on-demand 12

1.2.2 Protocolli di routing proactive 13

1.2.3 Protocolli di routing ibridi 14

1.3 Come trovare path a costo minimo 15

1.3.1 Requisiti per le metriche 17

1.3.2 Approccio Cross-layer 21

1.4 Medium Access Control 22

1.5 Scenari di applicazione 25

1.6 Implementazioni esistenti 29

2 Il protocollo HWMP 35

2.1 Draft 802.11s 35

2.1.1 Struttura di una rete WLAN 36

2.1.2 Formato dei pacchetti 40
2.2 Mesh networking 42
2.2.1 Procedure 43
2.2.2 Scanning 45
2.2.3 Creazione dei link 45
2.2.4 Misure sulla qualità dei link 47
2.2.5 Access Point 49
2.3 Wireless Mesh Network 51
2.3.1 Aspetti generali 53
2.3.2 Routing ad albero nell'HWMP 58
2.4 Il problema dei sei indirizzi 63
2.5 Nuove proposal del draft 66
2.5.1 Modifiche del tree-based routing 66
2.5.2 Routing tra stazioni 68

3 Architettura software 71
3.1 Il problema dell'inoltro delle trame dati 71
3.1.1 Considerazioni e limitazioni delle reti mesh 76
3.2 Soluzione implementata 79
3.2.1 Gestione dei frame data 83
3.2.2 Modifiche al draft 91
3.3 Codice sorgente 93
3.3.1 Struttura del programma 94

3.3.2 Architettura software 97
3.3.3 Inizializzazione dei link 100
3.3.4 Statistiche e metrica implementata 103
3.3.4.1 Il limite dell'airtime metric 106
3.3.5 Selezione dei percorsi 109
3.3.5.1 Routing preventivo 109
3.3.5.2 Routing on-demad implementato 111
3.4.1 Struttura RREQ 111
3.4.2 Generazione RREQ 113
3.4.2.1 Attivazione delle procedure on-demand 117
3.4.3 Ricezione RREQ 119
3.4.4 Struttura RREP 125
3.4.5 Generazione RREP 126
3.4.6 Ricezione RREP 127
3.4.7 RERR 129

4 Sviluppo del prototipo 133

4.1 MadWiFi 134
4.1.1 Gestione delle interface del MadWiFi 136

4.1.2 Limitazioni dei driver MadWiFi su WMN 139
4.1.3 Invio e ricezione dei messaggi 140

4.2 Struttura dei Mesh Point implementati 142
4.3 Bridge Linux ed EbTables 146
4.4 Requisiti software 148
4.5 Sistema operativo 149

5 Analisi sperimentali 151

5.1 Debug e procedure 152
5.2 Creazione dei nodi mesh 153
5.3 Scenario n°1 154
5.3.1 Prove condotte 165
5.3.2 Procedure on-demand 168
5.3.3 Servizi IP 171
5.4 Scenario n°2 171
5.5 Scenario n°3 176
5.5.1 Routing reactive 184

Conclusioni 203
Bibliografia 209
Ringraziamenti 211

Introduzione

Negli ultimi anni il numero di dispositivi wireless è cresciuto rapidamente, nello stesso tempo l'accesso alla rete Internet sta diventando una necessità per un numero sempre maggiore di persone. Combinando questi due fenomeni si può facilmente dedurre che la richiesta di connettività ad Internet da dispositivi mobili sarà destinata a crescere.

La rivoluzione del wireless, innescata dal successo dello standard IEEE 802.11, ha comportato inoltre l'esigenza di analizzare, studiare e sviluppare nuove soluzioni basate proprio sul famoso "Wi-Fi".

Al momento i limiti di questa tipologia di rete, nonostante i numerosi gruppi di ricerca attivi in quest'area, sono ancora molti e uno dei più restrittivi è rappresentato sicuramente dalla copertura. Costruire reti Wi-Fi di grandi dimensioni senza infrastrutture dedicate e costose è

di fatto impossibile. Nasce, quindi, la necessità di creare soluzioni solide e performanti per espandere la capacità e la copertura delle reti Wi-Fi esistenti.

In particolare, le Wireless Mesh Networks (WMN) rappresentano una tecnologia promettente che ha catturato l'interesse di università e produttori grazie alla facilità di implementazione e ai costi ridotti. Questo tipo di rete ha l'obbiettivo di fornire connettività wireless ad un numero elevato di utenti, in modo flessibile ed economico. Le WMN utilizzano più access-point, nel nostro caso con tecnologia Wi-Fi, connessi reciprocamente, garantendo così un incremento della copertura sostanziale, una maggiore scalabilità e affidabilità ed infine una gestione ottimale della banda disponibile.

Garantire una connettività wireless che permetta l'accesso alla rete Internet, sta diventando una sfida sempre più agguerrita e le mesh a tutt'oggi rappresentano un ottimo candidato alla vittoria.

Lo scopo di questa trattazione è presentare l'implementazione del protocollo di routing HWMP (Hybrid Wireless Mesh Protocol) che permette, attraverso complicati algoritmi di routing, una gestione efficiente delle reti mesh. In seguito si descriverà lo sviluppo di un prototipo di WMN realizzato presso il laboratorio di simulazione di reti di telecomunicazione del Dipartimento d'Ingegneria dell'Informazione a Pisa e le analisi sperimentali svolte su di esso.

La tesi è articolata in 5 parti.

Il Capitolo 1 descrive in modo generale la struttura e le problematiche delle Wireless Mesh Networks , focalizzandosi sugli algoritmi di routing sinora utilizzati. Sono inoltre presentate alcune soluzioni esistenti di reti mesh e i possibili scenari di questa tecnologia.

All'interno del Capitolo 2, sono presentate le funzionalità del protocollo HWMP facente parte del draft 802.11s e le procedure che vengono applicate per instradare i frame all'interno della mesh.

Nel Capitolo 3 si descrive il lavoro svolto per la realizzazione del codice sorgente che implementa il protocollo HWMP. In questa parte vengono inoltre descritte le scelte realizzate per rendere il protocollo perfettamente funzionante e la soluzione proposta in collaborazione con Ivan Muccini per il prototipo della WMN.

Il Capitolo 4 descrive l'architettura del prototipo, sviluppato mediante l'utilizzo di schede wireless Atheros pilotate dai driver MAdWiFi, e le sue funzionalità.

Il Capitolo 5, infine, contiene la presentazione delle prove svolte, dirette alla verifica di ottemperanza del progetto alle funzionalità fissate come obiettivo. Tale verifica sarà condotta tramite la rappresentazione dei messaggi scambiati dagli access-point mesh, la visualizzazione delle tabelle di ogni nodo e grafici rappresentanti la topologia della rete.

1 Wireless Mesh Networks

1.1 Aspetti generali

Una rete mesh è per definizione qualsiasi tipo di rete wireless dotata di una certa topologia. Lasciando questa definizione, generica e priva di grande significato, le Wireless Mesh Networks (WMNs) in pratica sono un insieme di router wireless statici connessi reciprocamente per formare un'infrastruttura distribuita alla quale si possono connettere client mobili. Le WMNs nascono dalla necessità di risolvere le limitazioni e migliorare le prestazioni delle reti ad-hoc, WLAN (wireless local area networks), WPANs (wireless personal area networks) e WMANs (wireless metropolitan area networks).

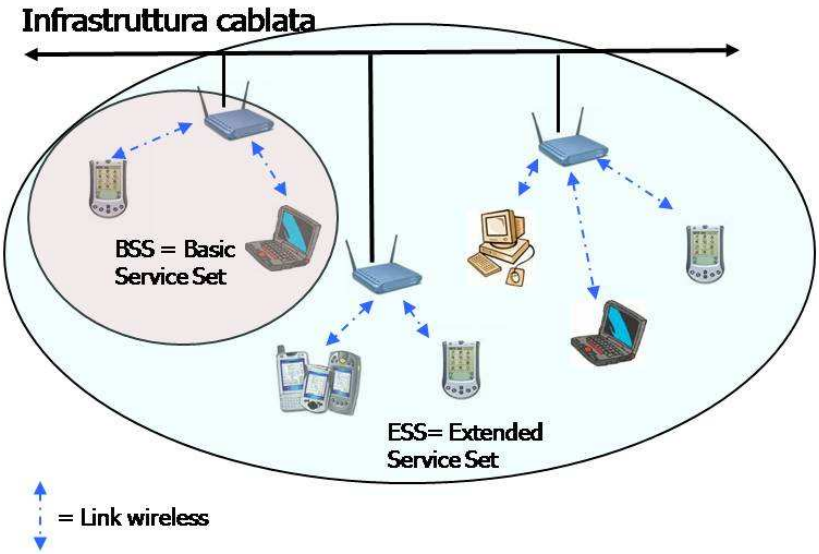

Fig 1.1 Il paradosso del wireless, tipicamente gli Access-point sono connessi alla rete cablata

Una rete WMN è dinamicamente autoconfigurante in modo completamente trasparente per gli utenti che vi sono connessi, i nodi infatti stabiliscono e mantengono automaticamente la connettività al loro interno. Le funzionalità gateway/bridge di ogni router mesh permettono inoltre l'integrazione delle WMN con molte tipologie di reti: Wi-Fi, Wi-Max, reti di sensori e reti cellulari. Le WMN possono essere costruite in modo incrementale, aggiungendo un router per volta, garantendo una flessibilità impensabile per qualsiasi rete cablata. Un altro punto di forza di questa tecnologia è

rappresentato dai costi ridotti degli apparati che sfruttano standard come l' IEEE 802.11 già perfettamente funzionanti.

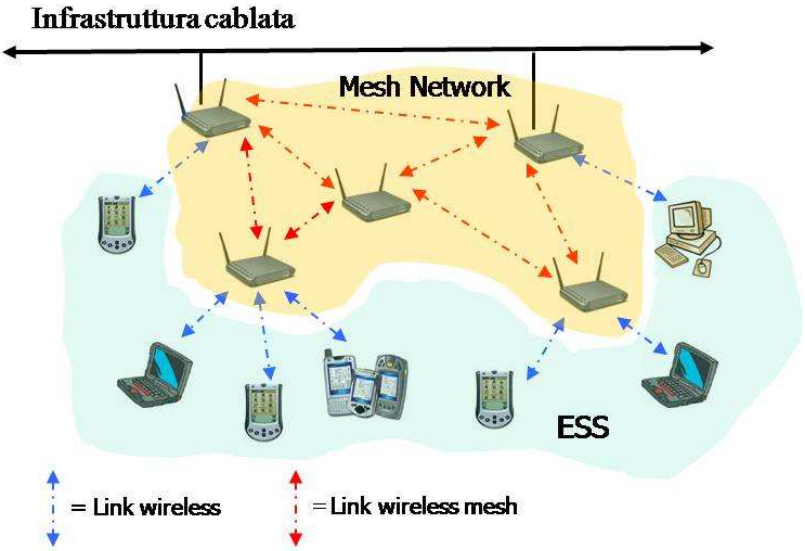

Fig 1.2 Tipica rete wireless mesh

1.1.1 Architettura di rete

L'architettura delle WMNs è costituita da due tipologie di nodi: i mesh router e i mesh client. I primi hanno una mobilità limitata, costituiscono la backbone della rete e forniscono l'accesso ai client che possono essere fissi o mobili. Oltre alle capacità di gateway e ripetitore di segnale, già presenti nelle normali reti wireless, i router

mesh sono dotati di funzionalità di routing aggiuntive per supportare le reti mesh.

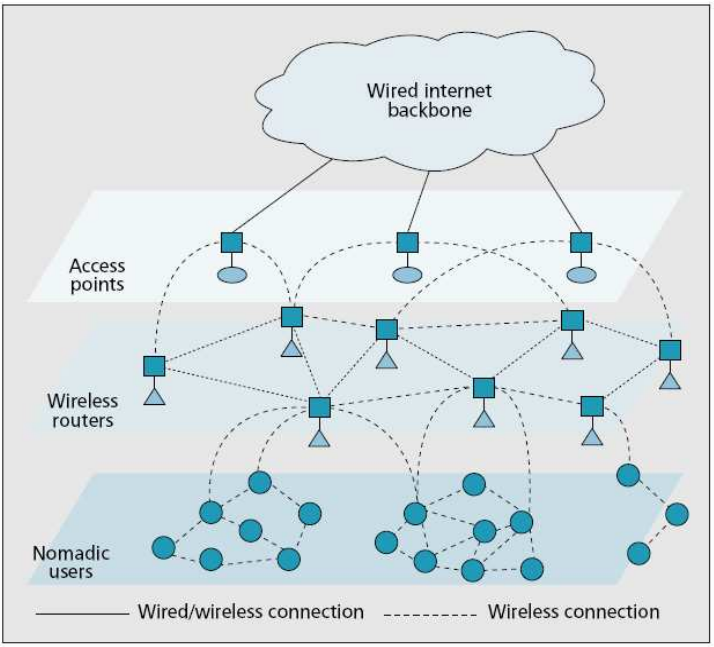

Fig 1.3 Architettura di rete mesh

Per garantire la flessibilità della rete i router sono spesso dotati di molteplici interfacce wireless equipaggiate con tecnologie di accesso diverse tra loro, questo per ottenere un incremento della banda disponibile. I client in genere sono forniti con una sola modalità di accesso, questo per rendere le piattaforme hardware e software da distribuire agli utenti più semplici ed economiche. L'architettura

delle WMN può essere classificata in tre gruppi principali [1], distinti dalle funzionalità delegate ai nodi :

- **Hierarchical Wireless Mesh Networks**:

  La rete è formata da diversi livelli ,dove tipicamente i client accedono alla rete di backbone formata dai router mesh ad un livello superiore.

- **Flat Wireless Mesh Networks**:

  I nodi client hanno funzionalità di router , la topologia è simile alle reti ad-hoc.

- **Hybrid Wireless Mesh Networks**:

  Infrastruttura composta da router wireless che si interfacciano attraverso molteplici tipologie di reti .

1.1.2 Caratteristiche delle WMN

In questo paragrafo si elencano le funzionalità della rete mesh , si cerca quindi di fornire una panoramica sui principali aspetti che contraddisinguono questo tipo di rete[1].

- **Rete wireless multi-hop**

  L'obbiettivo principale delle WMNs è di espandere la copertura delle reti wireless esistenti. Il Multi-hop consente di condividere le risorse di rete tra tutti i nodi della mesh senza sacrificare le capacità del canale.

- **Infrastruttura wireless**

La backbone wireless fornisce un'ampia copertura e una connettività robusta grazie alla capacità autoconfigurante . Se un mesh router cade o semplicemente viene spostato le conseguenze per gli utenti sono minime.

- **Integrazione**

Le WMN sono in grado di integrare diverse tipologie di rete attraverso le funzionalità aggiuntive introdotte nei router mesh.

- **Routing dedicato**

I nodi sono equipaggiati con protocolli dotati di algoritmi sofisticati per una gestione delle risorse ottimale e bilanciata.

- **Interfacce radio multiple**

La possibilità di utilizzare più risorse radio moltiplica la banda disponibile e le capacità a disposizione dei singoli utenti. Sono attualmente in corso numerosi studi sull'interferenza dei canali Wi-Fi e molti centri di ricerca si stanno dedicando all'implementazione di WMNs operanti su molteplici canali e su molteplici tecnologie. Un esempio è rappresentato da una rete che fornisce aeccesso con 802.11g agli utenti e inoltra i pacchetti sulla backbone wireless con modalità 802.11a, lavorando quindi su frequenze ben distinte.

- **Mobilità**

  Una rete mesh può cambiare topologia in base allo spostamento degli utenti, riesce quindi a fornire una connettività flessibile e nello stesso tempo robusta.

1.2 Routing nelle reti mesh

Il routing e il forwarding, in un contesto dinamico e complesso come quello delle WMNs risentono di numerosi problemi che non sono stati ancora risolti [2]. Diversamente dalle reti cablate, le reti wireless hanno diverse proprietà e limitazioni come:

- Banda
- Topologia dinamica
- Interferenza
- Copertura

Questi fattori comportano l'uso di protocolli di routing dinamici che basano il loro funzionamento sulle analisi dello stato di congestione della rete. Stimare la qualità dei link è diventato quindi un fattore chiave per creare protocolli di routing con buone prestazioni.

I protocolli di routing per WMNs in letteratura , basandosi su come i pacchetti vengono inoltrati da parte dei nodi della rete, possono essere divisi in due categorie: on-demand e proactive. Esistono inoltre alcuni protocolli ibridi che integrano le due tecniche al loro

interno con varie modalità. Questi protocolli hanno costi differenti in termini di overhead e complessità di gestione che cercheremo di analizzare nei prossimi paragrafi.

1.2.1 Protocolli di routing on-demand

Proposti originariamente per le reti ad-hoc, i protocolli on-demand o reactive creano solamente route su richiesta ossia solamente quando la sorgente ha bisogno di inviare pacchetti verso la destinazione. Il flooding è utilizzato come mezzo per scoprire la route a costo minimo verso il destinatario. Questo tipo di protocollo utilizza in modo minimo le risorse di rete.

Il routing on-demand garantisce quindi notevole connettività con un basso overhead , risultando ideale per reti con frequenti cambiamenti di topologia. Generalmente questi protocolli sono poco indicati per le reti mesh che per natura sono piuttosto statiche. La scalabilità di questi algoritmi di routing è limitata , l'uso del flooding satura, per brevi intervalli temporali, le risorse di una rete estesa come tipicamente è una WMN e impone forti ritardi nello stabilire un collegamento tra sorgente e destinazione. Alcuni esempi importanti di protocoli on-demand sono DSR[4] , AODV[5].

1.2.2 Protocolli di routing Proactive

Nella modalità proactive ogni nodo, dove per nodo si intende un router mesh, mantiene una o più tabelle contenenti le informazioni di routing per raggiungere gli altri nodi presenti nella rete. Tutti i router sono inoltre tenuti ad aggiornare le tabelle periodicamente per mantenere una visione della rete consistente. Quando la topologia della rete cambia i nodi devono inoltrare messaggi di update che attraversando la rete forniscono informazioni aggiornate ad ogni router per un corretto instradamento dei pacchetti. Le route verso ogni destinazione sono quindi calcolate prima che siano necessarie.

Il routing proactive può essere diviso in ulteriori due categorie: source routing e hop-by-hop routing. Nel source routing il nodo sorgente dopo aver calcolato la route inserisce l'intero path (sequenza di router da attraversare) nell'header per inoltrare i pacchetti. I nodi intermedi sono quindi tenuti a instradare il pacchetto basandosi sulle indicazioni contenute nell'header. A causa della dimensione ridotta dei pacchetti che circolano nelle reti mesh il source routing impone un overhead pesante per ogni pacchetto ed è quindi sconsigliato il suo utilizzo.

L'hop-by-hop routing è basato sul mantenere in ogni nodo tabelle aggiornate che per ogni destinazione indicano il router next-hop che lega sorgente e destinazione con il path a minore costo. Ogni

pacchetto quindi ha bisogno solamente dell'indirizzo di destinazione. Il forwarding dei pacchetti molto semplice e il basso overhead rendono l'hop-by-hop routing dominante nelle reti cablate. Per ragioni molto simili questa tipologia di routing è preferibile anche per le reti mesh, dotate di nodi statici. Si deve però considerare che i nodi delle reti mesh sono in genere ridondanti per garantire robustezza, flessibilità e collegamenti con qualità elevata. Questo comporta una notevole mole di pacchetti di controllo "on the air" che può comportare la saturazione prematura delle risorse di rete. L'hop-by-hop routing necessità inoltre di molti accorgimenti, una rete wireless impone dei vincoli molto più restrittivi rispetto ad una rete fissa. Il protocollo più rappresentativo del proactive routing è sicuramente l'OLSR [6], largamente utilizzato da molti produttori nella realizzazione di WMN.

1.2.3 Protocolli di routing ibridi

I protocolli di routing ibridi sfruttano le principali caratteristiche di entrambe le tipologie di routing precedentemente descritte. Uniscono quindi alla forte scalabilità del routing proactive la possibilità di stabilire path su richiesta. Il protocollo di riferimento che sfrutta questa modalità di routing è l'HWMP che verrà descritto nel

dettaglio nei paragrafi successivi in quanto protocollo di riferimento del draft IEEE 802.11s [7] relativo alle reti mesh.
Per assicurare che le risorse di rete siano utilizzate in modo efficiente i protocolli di routing devono avere buone prestazioni in termini di throughput e tempi di ritado contenuti. Le metriche devono quindi avere la capacità di catturare le caratteristiche della rete wireless per ottenere dei path ottimi .

1.3 Come trovare il path a costo minimo

Fare del routing su reti wireless multi-hop utilizzando come metrica la tradizionale hop-count non è una condizione sufficiente per costruire buoni path [8], dove per buoni path si intendono quei percorsi che consentono un trasferimento di dati con ritadi contenuti e throughput consistente. La causa principale di tutto questo è da imputare ai link wireless che hanno caratteristiche fortemente variabili nel tempo impossibili da catturare per una metrica come l'hop-count.
Questo problema è enfatizzato inoltre dalla maggioranza di meccanismi per la "route discovery", che non sono capaci di scoprire le capacità dei link wireless. L'approccio usuale consiste nello scambio di pacchetti di Hello o Probe mandati in modalità broadcast per stimare la capacità del link che lega tra loro due nodi. Una volta

ottenuti i dati i router stimeranno poi la metrica da applicare su quel determinato link. Si deve notare però che la modalità di invio broadcast è critica per le reti Wi-Fi perché i pacchetti vengono inoltrati al rate minimo, questo per raggiungere il maggior numero di vicini.

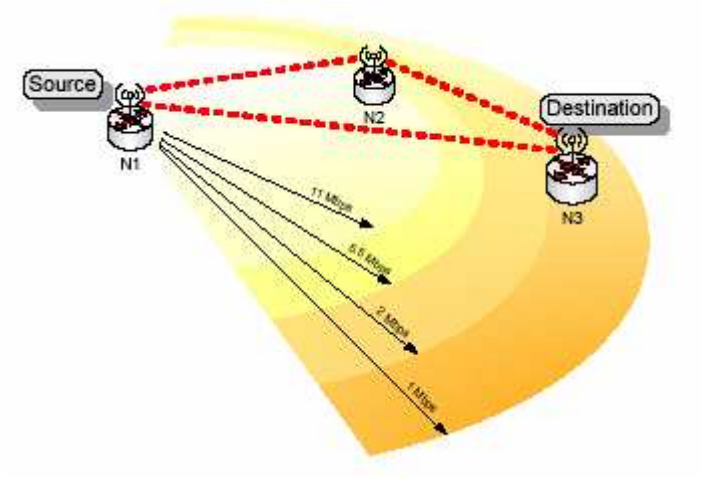

Fig. 1.4 relazione tra rate e copertura del seganle Wi-Fi.

Inoltre, maggiore è il rate con cui si mandano i pacchetti minore sarà il range che potrà essere raggiunto (figura 1.4), per questo l'invio di pacchetti broadcast per saggiare le capacità della rete non rappresenta un metodo ottimale di valutazione delle risorse disponibili [8] infatti:

- I Probe o Hello in genere hanno dimensioni ridotte che non rispecchiano quelle dei normali pacchetti inviate sulle reti Wi-Fi.
- I pacchetti sulle reti Wi-Fi sono inviati ad un rate superiore a quello utilizzato per le trame broadcast.

Per esempio, facendo riferimento alla figura 1.4, il nodo destinatario N3 collocato nella zona arancio potrà ricevere i pacchetti di Hello, ma difficilmente potrà smistare traffico dati proveniente dalla sorgente N1 con un rate consistente. Se invece di un collegamento diretto si utilizzasse il multi-hop attraverso N2 i dati potrebbero essere trasmessi con 2 collegamenti a 11 Mbps invece che uno ad 1Mbps. Questo esempio non deve sembrare banale , sono infatti in corso numerosi studi sulla capacità dei link multi-hop su cui di fatto è basata l'architettura delle mesh networks. I protocolli di routing, che selezionano i path utilizzando l'hop-count, hanno la naturale attitudine a scegliere i collegamenti più lunghi, sono quindi un approccio fallimentare per le mesh network che incrementano, all'aumentare del numero dei nodi, flessibilità e robustezza .

1.3.1 Requisiti per le metriche

Per assicurare buone prestazioni le metriche devono soddisfare quattro requisiti principali [9]:

- **Scalabilità**

Il costo dei path non deve essere soggetto a cambiamenti frequenti, questo infatti provoca un grande volume di messaggi di controllo che inonda e satura le risorse di rete. Le metriche che garantiscono scalabilità possono essere divise in load-sensitive e topology dependent. Le prime sono sensibili al carico della rete e il costo dei link è determinato dal traffico presente sui link stessi. Sono particolarmente indicate per protocolli on-demand in quanto la rete, utilizzando tali protocolli non risente di modifiche topologiche consistenti anche se le metriche sono in continuo cambiamento.

Le metriche topology dependent si basano sulla topologia delle reti ed assegnano un costo in base alla capacità del link. Per esempio stimano il rapporto seganle rumore o il rate dei collegamenti instaurati con gli access point vicini. Queste ultime metriche sono preferibili per le reti mesh che risentono dell'alta variabilità dei link wireless. Anticipando alcune considerazioni che verranno fatte nei capitoli successivi, per il nostro test è stato necessario utilizzare delle metriche topology-dependent che sono risultate essere più stabili garantendo ottimi collegamenti e velocità di convergenza.

- **Buone prestazioni**

Per ottenere metriche performanti si devono considerare i seguenti aspetti :

- **Lunghezza del path**, le metriche devono assumere un costo maggiore all'aumentare della lunghezza delle route. In questo modo si scoraggiano collegamenti a basso rate.
- **Capacità del link,** questo parametro è in controtendenza con quello precedente. All'aumentare della distanza la qualità del link decresce è necessario un bilanciamento di questi due aspetti.
- **PER,** la percentuale di perdita dei pacchetti è sempre un paramentro da considerare. Per link wireless comunque la PER dipende anche da quanto il mezzo è occupato dagli altri access-point, non si può quindi basare una metrica solo su questo aspetto come invece è sufficiente per le reti cablate .
- **Interferenza,** questo parametro è fondamentale per le reti wireless e nello

stesso tempo risulta un vincolo molto difficile da considerare. In particolare non solo si deve cercare di ridurre l'interferenza che deriva da comunicazioni non facenti parte della stessa mesh, ma si deve tenere presente anche le interferenze che si generano nelle comunicazioni interne.

- **Algoritmi efficienti**, anche se le metriche riescono a catturare in modo ottimale le caratteristiche dei link è necessario avere algoritmi che riescano a gestire velocemente e correttamente queste informazioni.
- **Routing senza Loop,** come nelle reti cablate anche nelle wireless ottenere delle topologie senza loop è un requisito indispensabile.

Sfortunatamente a causa della mancanza di un controllo centralizzato e della natura inaffidabile dei link wireless la qualità delle route cambia in modo veloce ed imprevedibile. Implementare un protocollo che universalmente riesca a gestire questi aspetti e nello stesso tempo sia stabile rimarrà ancora a lungo una sfida per molti gruppi di ricerca in tutto il mondo.

1.3.2 Approccio Cross-Layer

Un architettura stratificata, come la pila ISO OSI, ha lo scopo di dividere il compito del networking in più livelli e definire una gerarchia di servizi che devono essere forniti individualmente dai diversi piani. I protocolli in genere sono progettati per rispettare le regole di tale architettura, in questo modo possono essere costruiti in modo indipendente dai livelli direttamente connessi. I motivi per implementare protocolli cross-layer, ossia protocolli che amalgamo al loro interno vari livelli, sono comunque molti, primo tra tutti è l'efficienza [10]. Purtroppo l'implementazione di reti wireless di grandi dimensioni risulta molto complicata e l'utilizzo di un approccio senza livelli è quasi obbligatorio. La mobilità degli utenti e la qualità dei link wireless generano problemi che devono essere trattati e risolti in tutti i livelli dell'architettura.

L'implemetazione di soluzioni mesh basate proprio su un approccio cross-layer sembra aver catturato l'attenzione di molti gruppi di ricerca. Infatti la necessità di affidabilità, sicurezza, robustezza è primaria rispetto alla semplicità si realizzazione di una soluzione. Non bisogna però essere troppo pessimisti , se da un lato le reti mesh rendono i collegamenti e lo smistamento dei pacchetti molto complicato offrono anche possibilità che le reti cablate non possono sfruttare. Per esempio, il piano fisico può essere capace di ricevere

pacchetti multipli simultaneamente e la natura “broadcast” del canale può essere sfruttata il molti modi.

1.4 Medium Access Control (MAC)

Nelle reti mesh il protocollo di medium access control riveste un ruolo fondamentale nel coordinare l’accesso ai canali da parte di tutta la rete mesh. L’assenza di infrastruttura che caratterizza le tradizionali reti wireless obbligano, per le reti mesh, una gestione ed un controllo distribuiti tra tutti i nodi. Un’altra caratteristica delle WMNs, che rende complicato il meccanismo di accesso al mezzo, è rappresentata dall’utilizzo del multi-hop per l’inoltro dei pacchetti. Il sorgente ed il destinatario che non sono collegati direttamente infatti possono scambiarsi pacchetti attraverso i nodi intermedi della rete. In questo contesto, trasmissioni simultanee possono provocare collisioni anche se i sorgenti registrano uno stato del canale libero. Questo a causa dell’inefficienza del “carrier sensing” (monitoraggio della rete da parte degli host interessati ad inoltrarvi pacchetti) in reti multi-hop. Le situazioni che si devono evitare sono due : nodo nascosto e nodo esposto.

Il caso del nodo nascosto si presenta quando un nodo (nodo B) risiede al di fuori della copertura di un nodo trasmittente (nodo A) , ma entro il range del un nodo ricevente (nodo C) .

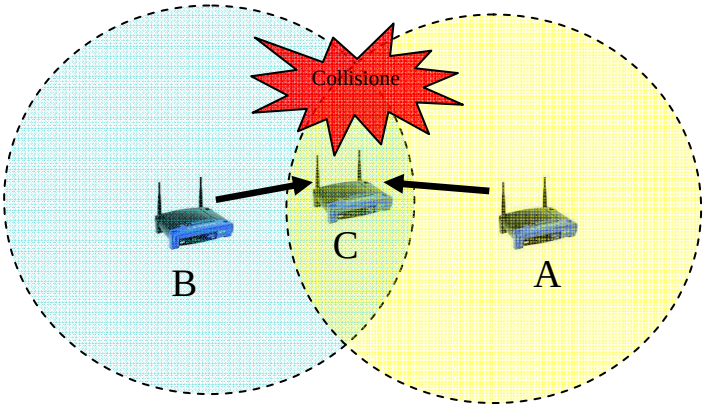

Fig 1.5 Caso del nodo nascosto in reti basate sullo standard IEEE 802.11

Poiché il nodo A e il nodo B sono fuori il loro rispettivo raggio di azione questi potrebbero teoricamente trasmettere simultaneamente. Se il nodo B inizia una comunicazione con il nodo C , sondando la rete e trovandola libera, si genererà una sicura collisione.

Il problema del nodo esposto invece si presenta quando un access-point è costretto a non inviare dati , registrando uno stato della rete occupato , anche quando potrebbe inviarli senza generare alcuna collisione.

Nell'esempio un nodo esposto (nella figura nodo C) è all'esterno della copertura del trasmettitore (nodo A) ma all'interno del raggio di trasmissione del ricevitore (nodo B) . Quando il nodo B invia pacchetti il nodo esposto è inibito nella sua comunicazione con D , anche se questa trasmissione non interferirebbe nel processo di ricezione del nodo trasmittente A .

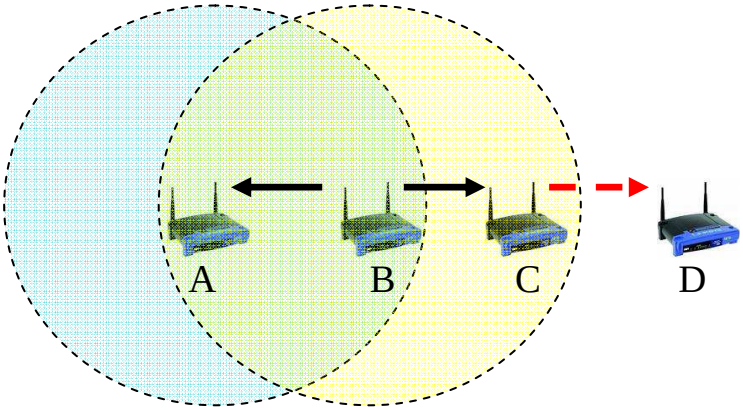

Fig 1.6 Caso del nodo esposto in reti basate sullo standard IEEE 802.11

Questi problemi oltre all'impiego di smart-antennas e all'utilizzo del multi-channel rendono il meccanismo di accesso al mezzo progettato dallo standard IEEE 802.11 non idoneo all'implementazione sulle reti mesh. Molti gruppi di ricerca infatti stanno cercando alternative al CSMA/CA, MAC default dello standard Wi-Fi. L'approccio da seguire anche in questo caso è Cross-Layer , come precedentemente descritto nella sezione 1.3.3. Le reti wireless aggiungono numerose variabili al problema del routing rispetto a quelle cablate e necessitano di una trattazione dei problemi aggregata, volta non a migliorare uno aspetto specifico, ma ad amalgamare tutte le soluzioni di tutti i livelli della pila ISO/OSI. Non è possibile quindi disegnare un nuovo MAC senza tener conto delle problematiche del routing,

della mobilità, dell' interferenza e anche se qui non trattata, della sicurezza.

1.5 Scenari di applicazione

La ricerca e lo sviluppo nel campo delle mesh networks è motivata dalle numerose applicazioni che può avere questa tecnologia e che, invece, tipologie di reti come le cellulari ed ad-hoc non possono realizzare. In questa sezione verranno presentati alcuni possibili scenari in cui potrebbero operare le WMNs [1] :

- **Accesso a banda-larga.**

  La banda larga è già diffusa in molte abitazioni attraverso le IEEE 802.11 WLANs. La collocazione dell'access point è comunque obbligata, deve infatti essere installato nei pressi di una presa telefonica. Questo porta ad avere molte zone "morte" in casa, ossia zone dove il segnale non è sufficiente per una connessione alla rete Internet. Installare più access-point è una soluzione costosa e non conveniente a causa del cablaggio ethernet necessario. Un rimedio molto semplice potrebbe essere quello di utilizzare un ripetitore Wi-Fi, ma l'efficienza di questo sistema resterà sempre molto bassa per ovvi motivi. Le WMNs, come mostrato nella figura sottostante possono risolvere questo problema .

Fig 1.7 Rete mesh in ambiente casalingo

L'access point deve essere sostituito da una serie di wireless-mesh-router connessi reciprocamente. La loro installazione è molto semplice, è sufficiente che solo uno di loro sia connesso alla rete Internet per distribuire in tutta la casa un accesso a banda-larga veloce, robusto e sicuro. Le zone con scarso segnale sono così eliminate e inoltre la collocazione dei router mesh è facilmente modificabile ed estendibile.

- **Reti in comune con il vicinato**

In una comunità, l'usuale architettura dell'accesso alla rete è basta sul cavo DSL connesso direttamente alla rete internet . Inoltre molte abitazioni sfruttano un wireless router collegato alla

DSL come ultimo passo per la connessione. Questo scenario presenta i seguenti svantaggi:

- L'utilizzazione di ogni rete e cavo DSL rimane sempre molto bassa.
- Una larga percentuale di zone all'esterno delle abitazioni rimane senza accesso alla rete.
- I servizi wireless devono essere attivati individualmente.
- Ogni casa ha un solo path avviabile per raggiungere l'accesso Internet o comunicare con i vicini.

Installare una WMN in questo contesto mitigherebbe questi aspetti negativi e potrebbe dar vita ad alcuni servizi che altrimenti non potrebbero essere utilizzati. Basti pensare ad uno storage dei file distribuito, al video streaming o ad un servizio di videosorveglianza di tutto il vicinato.

- **Enterprise networking**

Con questo termine si caratterizzano le reti di medie dimensioni che possono connettere interi edifici o quelle di larghe dimensioni che possono connettere anche più strutture.

Molti uffici sono dotati di connessioni Wi-Fi, ma queste sono solo isole separate. Al momento la loro connessione può avvenire solo tramite connessioni Ethernet che incrementano di

molto il costo di questa tipologia di reti. In più realizzare una backhaul più estesa non garantisce un incremento di affidabilità o banda della rete ma solo un aumento della capacità locale.

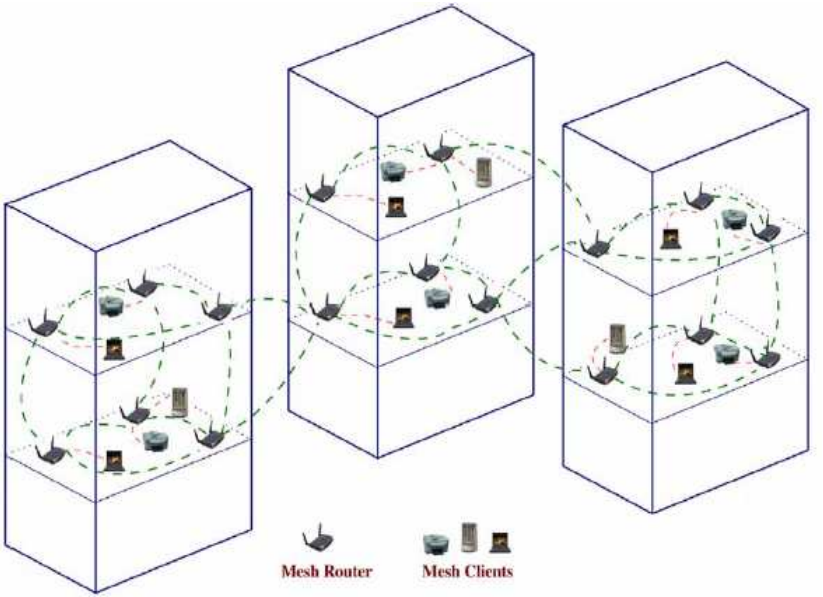

Fig 1.8 Rete mesh di medie dimensioni denominata anche rnterprise networking

Attraverso le WMNs le connessioni Ethernet potrebbero essere eliminate garantendo , attraverso più mesh router collegati a più accesi backhaul alla rete Internet, una grande flessibilità, affidabilità ed una copertura più efficiente. Le risorse sarebbero sfruttate in modo più oculato e i costi si ridurrebbero drasticamente. Questo tipo di WMNs è comunque difficile da

gestire ed implica una complessità della topologia non indifferente. La struttura delle enterprise networks può essere utilizzata per molti altri usi sia pubblici che commerciali: aeroporti, hotel,centri sportivi, centri di convegni, ecc.

- **Reti metropolitane**

Le reti mesh negli ambienti metropolitani hanno numerosi vantaggi, il rate di trasmissione a 54Mbps è molto elevato ed inoltre le WMN non necessitano di infrastrutture cablate. Questa tipologia di rete rappresenta quindi un buon mezzo per risolvere il problema del digital-divide, basti pensare che attualmente antenne Wi-Fi per outdoor raggiungono coperture di vari chilometri. Purtroppo in questo scenario la scalabilità è un fattore limitante, un numero elevato di utenti porterebbe al crash della rete.

Altri scenari possibili possono essere il monitoraggio dei sistemi di trasporto, la building automation (monitoraggio di tutti gli apparecchi in dotazione a un edificio) e servizi di sorveglianza distribuiti.

1.6 Implementazioni esistenti

Attualmente la maggior parte dei grandi produttori ha realizzato soluzioni proprietarie mesh. In varie città in tutto il mondo sono in

corso test e progetti che hanno lo scopo di creare vaste backhaul wireless attraverso le WMNs.

L'esempio più importante forse è rappresentato dalla città di San Francisco in California in cui il sindaco ha dato la massima disponibilità alla dislocazione di router con tecnologia mesh [12]. Google, Earthlink e Meraki sono a tutt'oggi in concorrenza per fornire una vasta rete mesh wireless completamente gratuita.

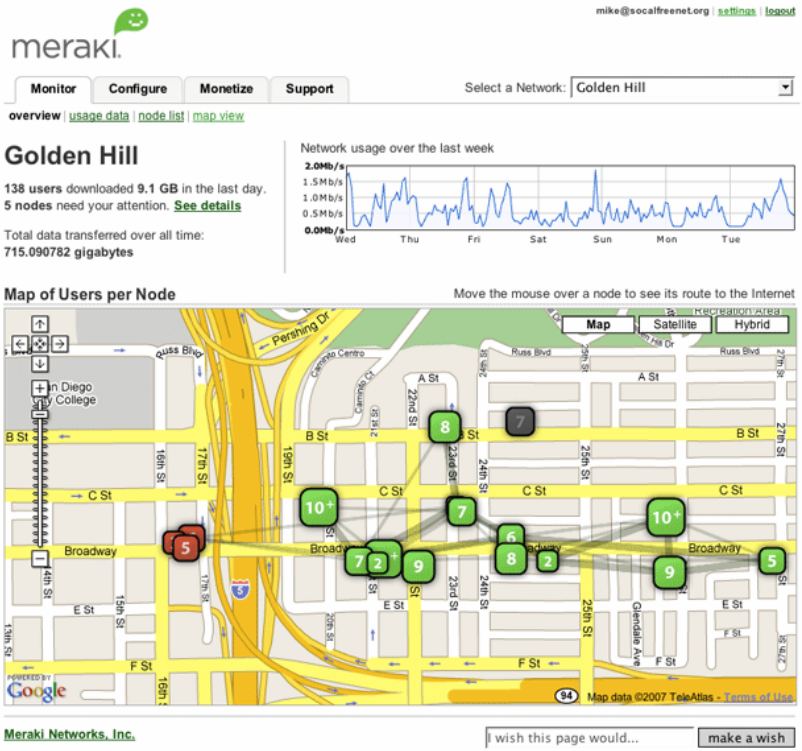

Fig 1.9 Screenshot del software messo a disposizione da Meraki.

I router utilizzati hanno un costo di circa 70 euro e sono forniti i un software che permette una gestione quasi totale della rete mesh. Basti pensare che ogni utente può:

- Monitorare la propria rete casalinga o in comune con il vicinato.
- Settare la banda di cui ha bisogno in quel particolare istante.
- Stabilire gli accessi alla propria rete e opzionalmente fornire banda a utenti esterni.

Un'altra realtà è rappresentata da Wili-box [13] una società che commercializza prodotti mesh wireless basati sullo standard IEEE 802.11 . I nodi implementati sono due Mesh Node e Mesh Gateway. Dove il primo serve per espandere il raggio di azione della mesh stessa, mentre il secondo fornisce funzioni di gateway,firewall e switch. Il software realizzato da questa compagnia prevede due tipi di servizi:

- Mesh Set, che ha lo scopo di collegare i mesh node con un cammino a costo minimo verso il mesh gateway.
- Service Set, che invece si occupa di fornire l'accesso ai clienti della rete mesh.

La rete è realizzata interamente a livello due e in modo trasparente rispetto ai livelli superiori e il sistema operativo utilizzato è Linux.

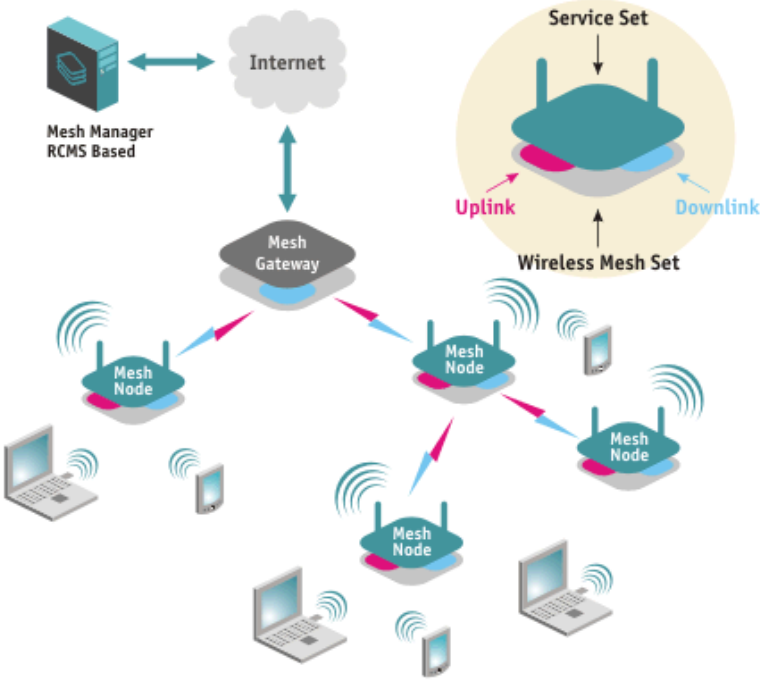

Fig 1.10 Esempio di rete Mesh creata da Wili-box

Roofnet è invece un progetto dell'università MIT negli USA nato nel 2003 con l'obbiettivo di connettere atraverso lo standard Wi-Fi un grande numero di nodi. Attualmente sono venti i nodi che si scambiano informazioni utilizzando tecnologia 802.11g . Questa rete mesh è forse la più importante a livello universitario, molti articoli infatti, sono stati scritti basandosi su rilevazioni e calcoli condotti proprio su Roofnet. Il progetto inoltre, proprio come avviene per

questa tesi, sfrutta driver open-source. E' quindi realizzato in ambiente Linux e sfruttando i driver per dispositivi wireless MadWiFi.

2 Il protocollo HWMP

2.1 Draft 802.11s

Nel giugno 2004 si ebbe il primo incontro del task group 802.11s, dove furono presentate numerose proposte per la standardizzazione di reti WLAN mesh. L'obiettivo era di creare un draft per reti multi-hop in grado di fornire una backbone wireless a un numero di utenti elevato, circa cinquanta, in uno scenario urbano. La discussione si focalizzò sulle varie modalità di routing possibili per questa tipologia di reti.

Oggi la standardizzazione delle reti WLAN è ancora in corso. Nelle sezioni successive sarà presentata la versione dell'ultimo draft "ufficiale" la 1.0.6 rilasciata nel Febbraio 2006 [7] e alcune proposal

datate Marzo 2007 [14]. In generale i principi basilari del routing su WLAN mesh sono stati affrontati e una trattazione non deve sembrare affrettata. Purtroppo l'interesse che hanno suscitato le wireless mesh per i grandi produttori ha reso la standardizzazione un processo lungo e travagliato. Si pensi che il rilascio del prossimo draft ufficiale 1.1.0, previsto per Febbraio 2007, sia stato rimandato a Ottobre nonostante alcune aziende stiano già implementando i propri prodotti mesh, sinonimo che il tempo è ormai maturo per realizzare WMNs.

Questo capitolo ha lo scopo di descrivere le funzionalità del HWMP, protocollo di routing default per lo standard 802.11s e la sua implementazione. In seguito saranno presentate modifiche e aggiunte al draft originale che era incompleto in alcune parti e non performante. Questo lavoro non è una sterile implementazione di un protocollo di routing ma ha la pretesa di fornire una soluzione originale basata su idee e studi effettuati dal "Pisa Mesh Team" rispettando i principi dettati dallo standard 802.11s.

2.1.1 Struttura di una rete WLAN

Una WLAN mesh è una rete dotata di due o più Mesh Point (access-point con funzionalità mesh) interconnessi attraverso link basti su standard IEEE 802.11. Una rete WLAN supporta zero o più punti

d'ingresso (Mesh Portal), l'autoconfigurazione della topologia della rete e una selezione dei path dinamica attraverso il multi-hop. Gli elementi fondamentali che la caratterizzano sono i Mesh Point, i MAPs (Mesh Access Points che oltre a fornire servizi mesh offrono l'accesso alla rete) e gli STA ossia i dispositivi con i quali gli utenti si connettono alla Mesh. La tipica struttura di una rete mesh è raffigurata nell'immagine sottostante:

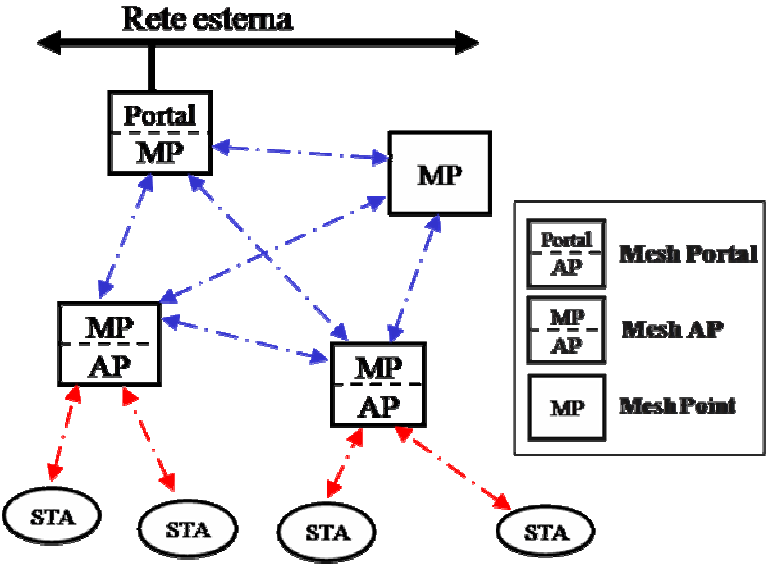

Fig 2.1 Rappresentazione Wireless Mesh Network 802.11s.

In questa tipologia di WMN, che possiamo classificare come infrastucture, le stazioni (STA) non contribuiscono al forwarding dei pacchetti della mesh, non è quindi necessario, da parte degli utenti finali, avere dispositivi che supportino la modalità mesh. Questo ovviamente si traduce in costi ridotti per gli apparati utilizzati dagli utenti, si possono, infatti, sfruttare dispositivi basati sullo standard Wi-Fi già in commercio.

Altra particolarità delle WLAN aderenti allo standard 802.11s è di avere un livello MAC totalmente trasparente ai protocolli di livello superiore.

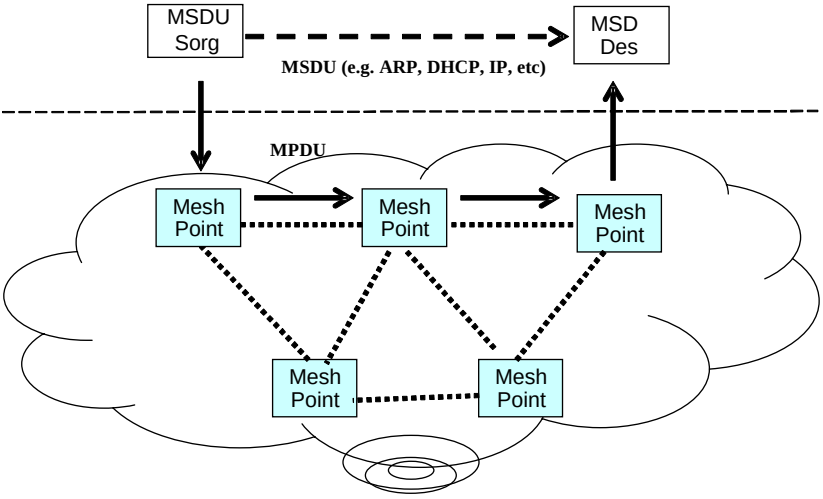

Fig 2.2 Livello di trasporto MAC di una WLAN 802.11s

Tutti i mesh point sono dotati di un bridge il quale lavora con un livello MAC con funzionalità mesh che risponde allo standard 802.11s e opzionalmente anche con un livello MAC Wi-Fi base, delegato all'accesso degli utenti. Al bridge saranno quindi connessi due tipi di reti: una mesh e una tradizionale Wi-Fi.

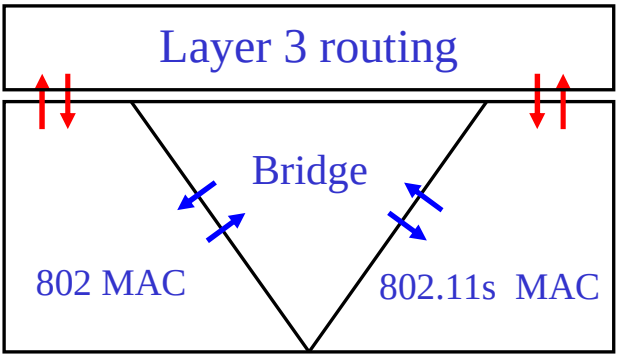

Fig 2.3 Architettura logica di un MP all'interno di una rete mesh

I frame sono instradati attraverso i bridge in dotazione ai Mesh Point (MP), di fatti all'interno della mesh non si può parlare propriamente né di routing né di pacchetti, il livello tre è completamente assente. Ogni STA è come se fosse connessa direttamente con il Portal, solo agli estremi della rete si scambiano messaggi analizzando l'header IP. Questa modalità, ai fini delle prestazioni, è molto efficiente e rende le mesh perfettamente integrabili con le reti oggi esistenti.

Lo standard non dedica molta attenzione a questo punto, che invece rappresenta il fulcro su cui basare la formazione della rete 802.11s, forse per lasciare il massimo grado di libertà agli sviluppatori.

2.1.2 Formato dei pacchetti

Il draft 802.11s, pur essendo solo un'estensione del Wi-Fi, utilizza un formato dei pacchetti diverso apportando numerose modifiche. Questo comporta modifiche che devono essere implementate al livello data-link in ogni dispositivo facente parte alla rete mesh. Nella figura 2.4 riportata a pagina successiva, sono elencati tutti i frame utilizzati dal nuovo draft e la loro relazione con lo standard IEEE 802.11. I messaggi che già comparivano nel Wi-Fi hanno subito lievi modifiche, sono stati solamente aggiunti alcuni campi con varie funzionalità. Com'è possibile notare sono introdotti numerosi messaggi di management che hanno lo scopo di coordinare il funzionamento dei MP per svolgere il routing o più correttamente l'instradamento dei frame all'interno della rete mesh. Le loro funzioni servono quindi per stabilire i percorsi, scambiare informazioni sulle metriche e sulle stazioni associate ad esempio.

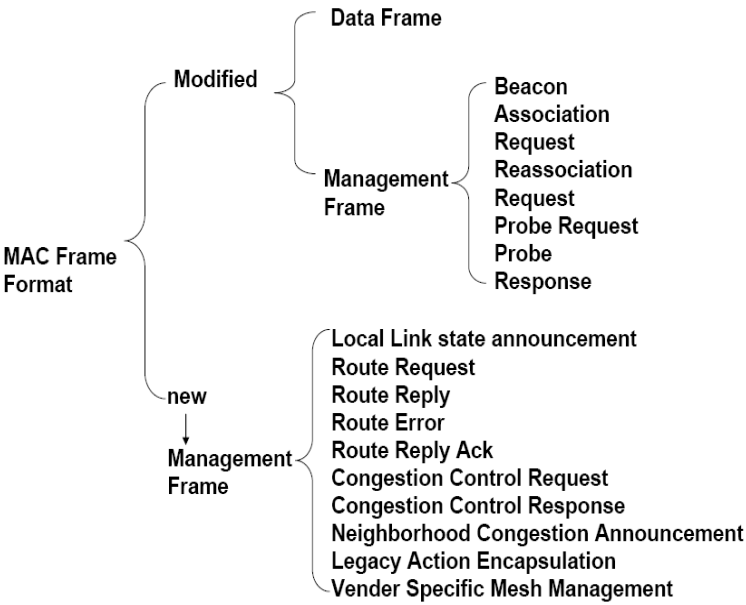

Fig. 2.4 Elenco pacchetti introdotti nel draft 802.11s

I pacchetti dati presentano un campo aggiuntivo delle dimensioni di 24 bit chiamato Mesh Forwarding Control. La sua funzione è di evitare il loop dei frame all'interno della mesh.

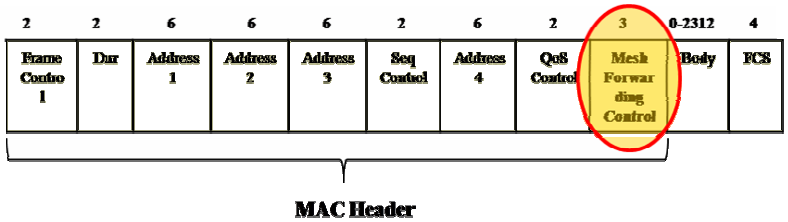

Fig 2.5 Frame 802.11s, in evidenza il nuovo campo Mesh Forwarding Control.

I frame di management devono supportare la modalità di collegamento tra MP per questo sono dotati di nuovi Information Element (IE). Questi ultimi sono collocati nel campo Frame Body e gestiscono le nuove funzionalità apportate dal draft 802.11s per lo smistamento dei pacchetti nella rete. Alcuni esempi sono illustrati nei paragrafi successivi.

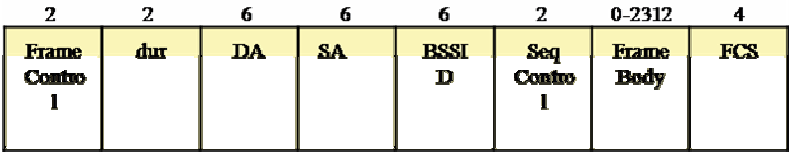

Fig 2.6 Frame management, le modifiche fatte dallo standard riguardano il corpo del messaggio, il Frame body al cui interno sono inseriti gli IE.

Ovviamente i frame di controllo non sono stati cambiati, l'obiettivo del draft mesh non è certo quello di ridisegnare completamente il MAC dello standard Wi-Fi.

2.2 Mesh Networking

Elencare dettagliatamente lo scambio di pacchetti che implementa il draft 802.11s, richiederebbe un intero capitolo e sarebbe di scarsa utilità. In questa sezione ci si limita quindi a descrivere i

procedimenti con cui sono mantenuti i link wireless tra mesh point, questi, infatti, sono la base della creazione di reti mesh.
Lo scopo ultimo è fornire un'analisi della creazione e della gestione della topologia in una WLAN mesh.
Un ottimo approccio è di descrivere la sequenza di operazioni che un MP deve portare a termine, dallo start-up fino a una fase di regime in cui la rete può considerarsi stabile. In questo modo si riesce a dare una logica e una motivazione alle procedure che altrimenti potrebbero essere piatte e prive d'immediato senso .

2.2.1 Procedure

All'avvio un MP esegue la seguente sequenza di operazioni:

1) Scanning attivo o passivo per scoprire altri MP.
2) Selezione del canale.
3) Inizio invio beacon (messaggi con i quali un router annuncia la sua presenza nella rete, utilizzato anche nel Wi-Fi).
4) Creazione di link con i vicini
    a. Autenticazione
    b. Associazione
    c. Autenticazione 802.11i e scambio di password
5) Misura della qualità dei link
6) Inizializzazione dei path

7) Inizializzazione degli AP, se il router ha funzionalità MAP.

Questa sequenza e i relativi messaggi che la caratterizzano sono illustrati nella figura sottostante.

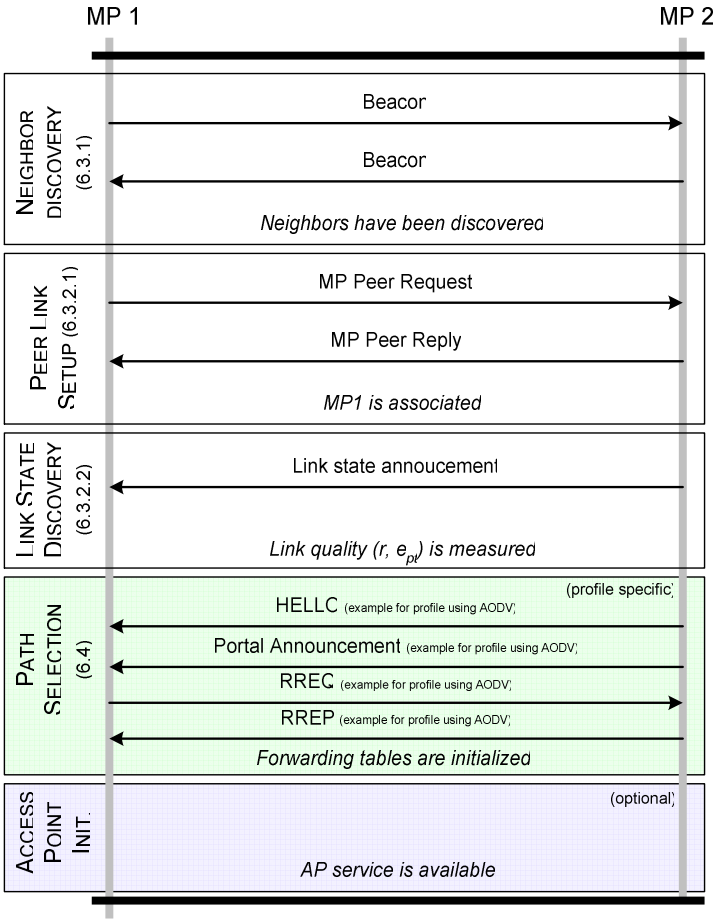

Fig 2.7 Tipica sequenza di messaggi scambiati dai Mesh Point.

In questa tesi non ci soffermeremo su tutti gli aspetti che riguardano il draft, ma cercheremo di concentrarci esclusivamente su quelli effettivamente realizzati, ossia quelli riguardanti il routing.

2.2.2 Scanning

Lo scanning è una procedura comune a tutti i tipi di rete, prima di connettersi ogni router ha bisogno d'informazioni riguardanti i vicini. Questa procedura può essere svolta, nel protocollo 802.11s, in modo passivo o attivo. Nel primo caso ogni router mesh banalmente resta in ascolto sulla rete per intercettare beacon di stazioni vicine. Nel secondo caso invece il MP è abilitato a inviare messaggi di probe che sondano la rete in cerca di possibili vicini. Quest'ultima soluzione è sicuramente più performante ma anche più "costosa", in termini di utilizzo delle capacità di rete. Generare un gran numero di pacchetti probe potrebbe togliere risorse al traffico dati per esempio.

2.2.3 Procedura per la creazione dei link

Una volta che un MP conosce la dislocazione dei vicini, inizia la procedura attraverso la quale la rete mesh prende forma. Un Mesh Point, infatti, non si collegherà con ogni router mesh omologo nel

suo raggio di azione ma sceglierà con accuratezza i vicini per gestire in modo ottimale le risorse di rete. I criteri attraverso i quali un MP sceglie i vicini sono lasciati liberi dal draft. Tipicamente si preferisce analizzare l'SNR che s'interpone tra i MP se lo scanning è avvenuto in modo passivo, ma se, al contrario, si sia avuto uno scanning attivo, la scelta si può basare su informazioni riguardanti le capacità dei link che sono state raccolte attraverso lo scambio dei messaggi probe.

Value	**Description**
Neighbor MAC address	MAC address of the neighbor MP radio interface
Primary MAC address	Primary MAC address of the MP, if it has more than one radio interface
State	State of the association with the neighbor
Directionality	Directionality value in previous association request
c_o	Operating channel number
p_l	Channel precedence value
R	Reference bit rate (modulation mode)
e_{pt}	PER for the reference frame size at the reference bit rate
Q	Received signal strength or quality (internal units)

Fig 2.8 Dettaglio Neighbor Table

Un MP che vuole creare un link con un altro MP deve inviare un frame *peer request*. Se il frame è stato trasmesso in modo corretto, il vicino, dopo aver valutato le informazioni contenute, deve rispondere

con un messaggio *peer reply* per confermare l'avvenuta creazione di un link bidirezionale o per invalidare la richiesta.
I vicini, una volta stabiliti, sono inseriti in una tabella chiamata Neighbor Table, che ha lo scopo di tener traccia di tutti i router mesh con cui un MP si può relazionare, il relativo next hop, la metrica e molti altri parametri.
I link devono essere mantenuti attivi, i MP sono tenuti a restare sempre in ascolto di messaggi beacon o probe originati dai vicini. Se dopo un certo intervallo temporale, un MP è non attivo (ossia non riceve più beacon) si inizia la procedura di eliminazione del link.

2.2.4 Misura della qualità dei link

La qualità del link e la rispettiva metrica associata richiedono una procedura che consiste nello scambio periodico di frame LLSA.

Octets: 1	1	2	2
ID	Length	r	e_{pt}

Fig 2.9 Information Element LLSA.

Il messaggio è molto semplice e comprende solo la bit-rate e la PER riscontrata dal nodo sorgente che saranno descritte nel dettaglio

successivamente. Lo scopo è effettuare una valutazione delle prestazioni del link in modo simmetrico e popolare la *neighbor table* con tali valori.

Come osservato nel capitolo precedente, la scelta della metrica non è banale, lo standard adotta l'airtime metric. Questa metrica calcola il costo da assegnare a ogni link nel seguente modo:

$$c_a = \left[O_{ca} + O_p + \frac{B_t}{r} \right] \frac{1}{1 - e_{pt}}$$

Parameter	Value (802.11a)	Value (802.11b)	Description
O_{ca}	75µs	335µs	Channel access overhead
O_p	110µs	364µs	Protocol overhead
B_t	8224	8224	Number of bits in test frame

Fig 2.10 Formula airtime metric e relative specifiche.

Dove $O_{ca,}$ O_p e $B_{t,}$ sono parametri costanti da utilizzare secondo la modalità Wi-Fi in uso nei mesh router. Le uniche variabili sono la bit-rate r e la PER e_{pt}.

La bit-rate è espressa in Mbps e rappresenta il rate con cui il MP invia un frame di dimensione standard pari a B_t .
La frame error rate e_{pt} corrisponde invece alla percentuale di pacchetti, di dimensioni B_t e inviati a un rate pari a e_{pt}, corrotti, ossia non inviati nel modo corretto. La stima di questa variabile è lasciata libera. L'obiettivo di questa metrica è stimare il tempo che un MP impiega per trasmettere un singolo frame ed è molto simile alla ETT [8] presentata da DeCouto in un importante articolo riguardante il routing sulle mesh. Questa metrica risulta poco scalabile. Essendo basata sulla PER, soprattutto nelle prime fasi della creazione della mesh, ha la tendenza ad associare ai link costi fortemente variabili generando frequenti cambiamenti nella scelta dei path migliori. Inoltre le dimensioni dei pacchetti sono troppo ridotte per catturare in modo convincente le capacità della rete.

2.2.5 Avvio dell'access point

Prima di interessarci alla parte relativa agli algoritmi di selezione dei path è utile dedicare alcune righe agli AP delle reti mesh. Questi sono tenuti a mantenere una proxy table dove registrano tutte le STA a loro collegate e che, di fatto, non fanno parte della mesh. La procedura di registrazione è illustrata in figura 2.11.

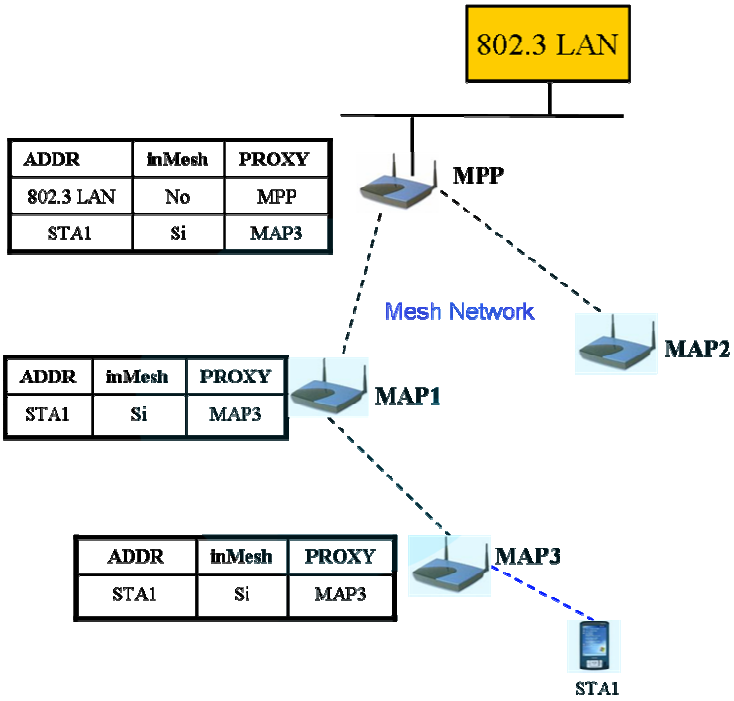

Fig 2.11 Gestione proxy nel draft 802.11s

Durante la fase iniziale una STA si associa con un MP della rete, in questo caso MAP3, utilizzando le procedure standard del protocollo IEEE 802.11. Una volta associata la STA inizia la registrazione verso il MPP (Mesh Point Portal), il portale, infatti, deve conoscere tutte le stazioni associate per riuscire a smistare i pacchetti in entrata e uscita dalla mesh. La stazione manda un frame proxy di registrazione in cui specifica il suo MAC address e il MP cui è associata. La proxy

request inviata segue ovviamente il percorso minimo per arrivare al Portal. MAP1 dopo aver ricevuto il messaggio di proxy registra le informazioni necessarie nella proxy table e trasmette il pacchetto verso il MPP. Lo stesso farà pute il MPP che aggiornerà la sua lista di MAC raggiungibili all'interno della mesh. Il Portal inoltre potrà generare una risposta tramite un proxy reply per confermare l'avvenuta ricezione della proxy request. In questo tutti i MP conoscono le STA associate a loro e ai nodi che attraverso di loro arrivano al MPP.

2.3 Il protocollo HWMP

Il draft dell'802.11s propone due tipi di protocolli per la selezione dei path l'HWMP e il Radio Aware OLSR. L'HWMP è il protocollo di default delle reti aderenti allo standard e deve essere implementato su ogni macchina per garantire l'interoperabilità di tutti i prodotti mesh. L'altro invece è solo un esempio di protocollo da implementare su piattaforme 802.11s.

L'Hybrid Wireless Mesh Proctocol (HWMP) è un algoritmo di selezione dei path che combina la flessibilità del routing on-demand con estensioni per abilitare un efficiente routing proactive verso i Portal. La natura ibrida permette al protocollo di adattarsi sia alle architetture mesh di tipo "infrastucture" o gerarchiche sia a quelle di

tipo flat o ad-hoc. Questa combinazione di capacità rende i MP capaci di implementare una scelta dei percorsi d'inoltro dei frame indipendente, oppure lasciare a una topologia ad albero, supportata dal più dinamico routing on-demand, lo smistamento dei pacchetti. L'HWMP utilizza regole e procedure derivanti dal protocollo AODV con opportune modifiche e ampliamenti; AODV resta comunque un protocollo di routing interamente a livello tre.

Se una mesh non ha una root, ossia nessun nodo MPP, i percorsi saranno stabiliti attraverso una procedura on-demand. Al contrario se la mesh è dotata di root, ci possono essere due possibilità di routing:

- **On-demand**, dove ogni nodo è tenuto a stabilire un path con la root e gestire dinamicamente i percorsi ottimi attraverso RREQ e RREP (messaggi che contraddistinguono il routing on-demand).
- **Ibrido**, dove ogni nodo è parte di un albero che ha per vertice la root. Le route verso i Portal devono essere stabilite e mantenute con messaggi di management, ma ogni nodo può comunque stabilire path in modalità on-demand.

L'approccio utilizzato dal HWMP porta innumerevoli benefici:

- Flessibilità di adattamento ai requisiti che deve avere ogni rete mesh in ogni tipo di scenario.
- La scelta dei percorsi ottimi è affrontata in modo semplice ed efficiente.

- Inoltre quando un nodo è eletto come root nella rete:
    - Il flooding è ridotto alla ricerca delle destinazioni all'esterno della mesh.
    - Il traffico broadcast è tradotto in un più efficiente inoltro unicast dall'albero.
    - Le route on-demand possono utilizzare la topologia dell'albero per istituire percorsi di back-up.

2.3.1 Routing on-demand nel HWMP

L'obiettivo del routing è determinare le route verso le destinazioni e popolare la tabella di routing. I MP, oltre ad essere dotati di Proxy Table e Neighbor Table, hanno una terza tabella che svolge il ruolo di routing table, all'interno della quale sono collocati tutti i MAC raggiungibili dalla sorgente anche se fuori dalla sua copertura.
Il routing on-demand nel HWMP utilizza un meccanismo basato su Route Request (RREQ) e Route Reply (RREP) per stabilire i percorsi tra i MP presenti nella rete. Ogni nodo, dopo aver determinato le metriche associate a ogni link che lo collega ad altri vicini, può iniziare la procedura di routing on-demand.
Quando un nodo S vuole trovare una route per raggiungere la destinazione D, invia un messaggio RREQ in broadcast annunciando

la destinazione D nel campo destination list e inizializzando il metric field a zero.

Octets: 1	1	1	1	1	1	4	6	4
ID	Length	Mode Flags	TTL	Dest Count	Hop Count	RREQ ID	Source Address	Source Seq. Num.

4	1			6	4		1			6	4
Metric	Per Destinaion Flags			Destination Address #1	Destination Seq. Num.# 1	…	Per Destinaion Flags			Destination Address #N	Destination Seq. Num.#N
	DO	RF	Reserved				DO	RF	Reserved		

Fig 2.12 Formato frame RREQ, da inserire nel campo dati di pacchetti management come IE.

Nella figura 2.12 è illustrato il formato del pacchetto RREQ. Tralasciando l'elenco delle funzionalità dei campi presenti, la prima cosa che si nota è che la sua lunghezza non è fissa. Questo è derivato dal fatto che si possono generare RREQ che annunciano più destinazioni diverse tra loro, questo meccanismo risulta però di difficile implementazione. Si può inoltre notare che per ogni destinazione è specificato il MAC address, il numero di sequenza, necessario per processare pacchetti non obsoleti e due flag DO e RF

che gestiscono le politiche d'trasmissione dei RREP da parte dei nodi intermedi.

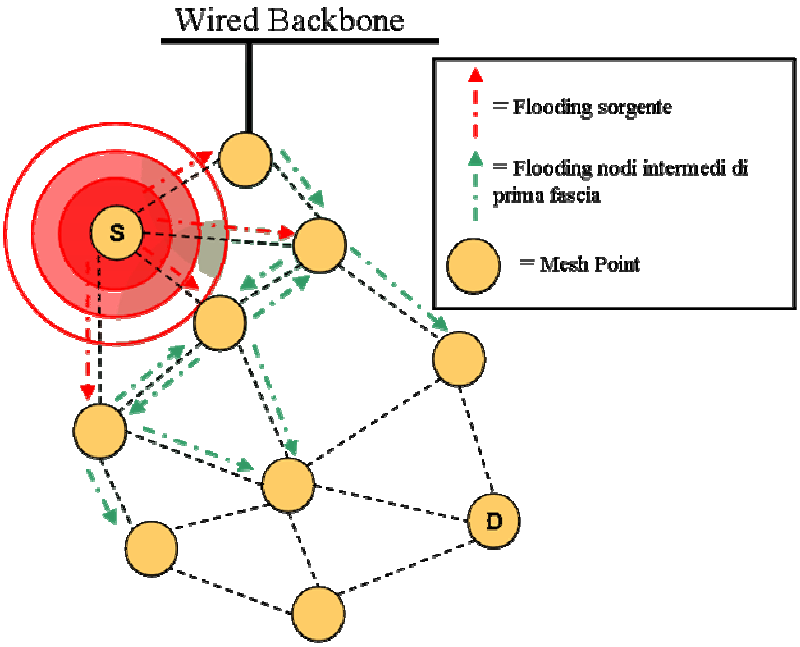

Fig 2.13 Esempio di flooding originato dal nodo S.

Ogni nodo può ricevere copie multiple dello stesso RREQ che è stato originato da S, tutti i RREQ attraversano, infatti, un path diverso per arrivare al nodo D (figura 2.13). Quando un nodo riceve un RREQ, crea una route verso S o aggiorna le informazioni della route stessa se questa è già presente e se il frame ricevuto non è obsoleto e la metrica che annuncia per raggiungere S è migliore di quella presente.

In tutti i casi comunque il pacchetto RREQ deve essere ritrasmesso in broadcast.

Nel momento in cui un nodo esegue il forwarding di un messaggio di management, ossia lo processa e lo inoltra, deve aggiornare il campo metric in modo da riflettere la metrica cumulativa dal nodo sorgente S fino ad arrivare al nodo stesso.

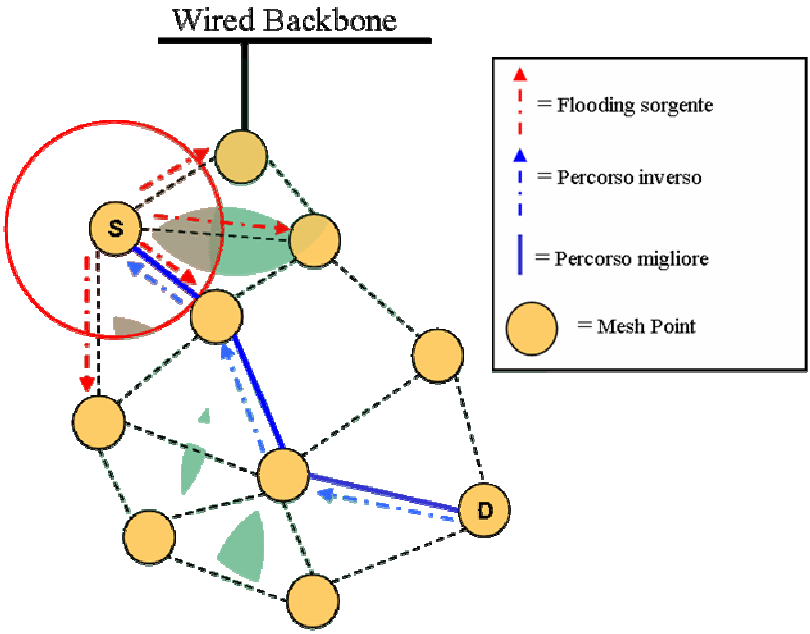

Fig 2.14 *Esempio di generazione RREP da parte della destinazione*

Una volta raggiunta la destinazione D, quest'ultimo dopo aver aggiornato o creato la route verso S dovrà inviare un frame RREP di risposta, in modalità unicast, verso la sorgente (figura 2.14).
I nodi intermedi non sono tenuti a generare RREP se non esplicitato nel messaggio RREQ attraverso i flag DO e RF. Questo meccanismo potrebbe però risultare utile, infatti se un nodo intermedio ha informazioni che riguardano la destinazione D potrebbe fornirle istantaneamente alla sorgente S. L'intervallo temporale necessario per stabilire il collegamento, parametro critico per il routing on-demand, sarebbe così ridotto di molto.
A causa della natura variabile dei link wireless, è possibile che le route stabilite possano diventare obsolete e non risultare più ottime. Per mantenere attivi solo i percorsi migliori, i nodi MP possono opzionalmente inviare dei pacchetti RREQ di mantenimento in modo periodico. Questi permettono a tutti i mesh router di adattare le metriche alle condizioni della rete in modo dinamico e aiutano a mantenere sempre i percorsi ottimi verso ogni destinazione. I RREQ di mantenimento sono del tutto identici agli altri e sono processati con le usuali modalità dai router intermedi e dalla destinazione.
Un altro meccanismo che si può applicare opzionalmente è il "Best Candidate Route Caching". L'obiettivo è di dividere il tempo in intervalli temporali chiamati round all'interno dei quali ogni MP elegge il percorso migliore per raggiungere i nodi della mesh. Una

volta scaduto il round si provvede ad aggiornare la tabella di routing. Questo permette ai MP di cambiare le route in modo efficiente senza portare continui cambiamenti ai percorsi già definiti aumentando, di fatto, la stabilità della rete.

2.3.2 Routing ad albero nel HWMP

Quando un nodo mesh, tipicamente un Portal, è configurato come root tutti gli altri mesh point sono tenuti a stabilire una route di collegamento attraverso RREQ ed RREP. Questo perché ogni nodo deve avere l'accesso alla rete esterna, accesso che può fornire solo la root. Stabilire e mantenere un path ottimo verso di essa rappresenta una necessità al fine dell'efficienza del routing.

4	4	4	1	6*n
Root Seq. Num	Lifetime	Root Metric	Topology Maintenance Policy	Connected Mesh Portal IDs

Octets: 1	1	1	6	1	1	6
Element ID	Length	Flags	Mesh Portal Bridge ID	Priority	Number of Mesh Portals	Mesh Portal Address

Fig 2.15 Formato root annoucement, da inserire come IE nei pacchetti di management.

Il nodo mesh root, una volta configurato, dissemina nella rete messaggi root announcement per annunciare se stesso a tutti i MP della rete (figura 2.16).

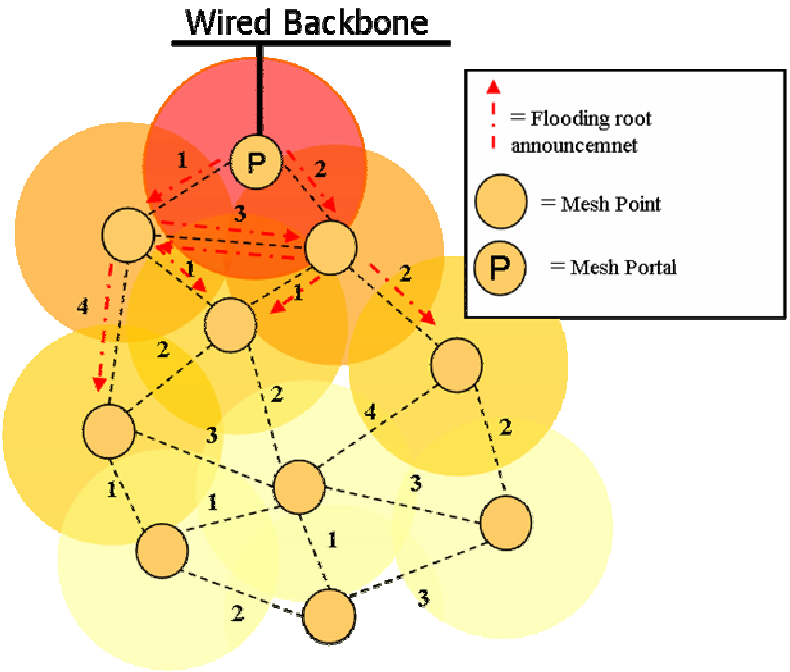

Fig 2.16 Inizializzazione procedura per la creazione di un albero tramite root announcement.

Ogni nodo che riceve tale messaggio deve associarsi alla root attraverso la procedura descritta nel paragrafo precedente. Se la procedura va a buon fine, il MP individua se stesso connesso

direttamente alla root, diventa quindi un figlio dell'albero (figura 2.17). Il nodo dopo aver ricevuto un root announcement deve re-inoltrarlo in broadcast, non prima di aver aggiornato metrica e numero di sequenza ovviamente.

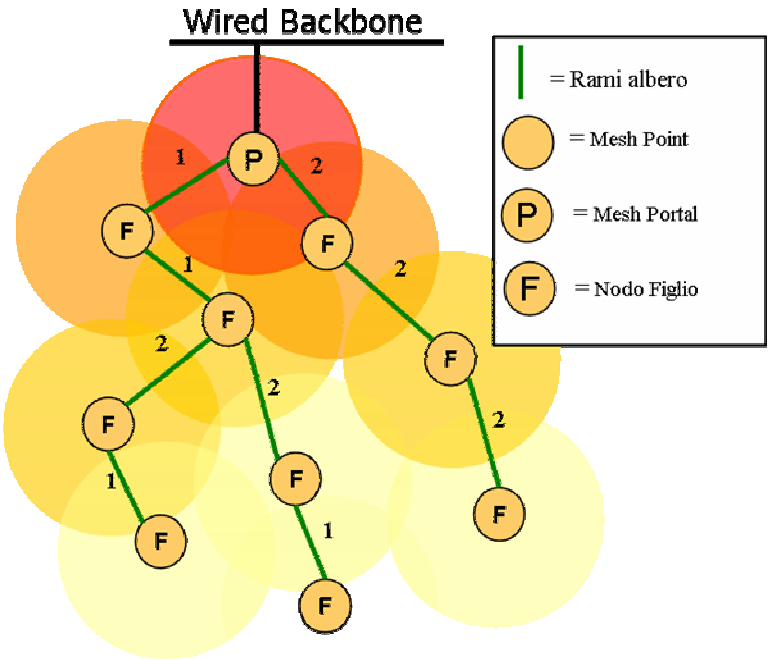

Fig 2.17 Albero proactive, per ogni nodo il percorso verso il Portal è a costo minimo.

I *root announcement* sono inviati periodicamente dalla root con numero di sequenza incrementato. In modo opzionale è possibile

introdurre un periodo di tempo all'interno del quale il MP riceverà i *root announcement*, che possono provenire da più root. Scaduto tale intervallo, il nodo inizierà la procedura di associazione alla root raggiungibile con metrica inferiore. Se un nodo non riceve frame *root announcement* per un certo periodo, deve scollegarsi dall'albero fino alla ricezione di un nuovo frame valido.

Una volta che un nodo ha selezionato un *parent*, un omologo mesh point, per raggiungere la root deve mantenere la route mandando messaggi RREQ periodicamente. Questo per avere la sicurezza di ottenere percorsi che sfruttano la metrica migliore disponibile.

Nel caso in cui un MP collegato all'albero individui un percorso per arrivare alla root con metrica migliore, non è abilitato a cambiare istantaneamente la route. Si devono, infatti, valutare numerosi parametri prima di modificare un albero, il draft comunque lascia a discrezione dello sviluppatore le procedure di riconfigurazione dell'albero. Quando scompare un *parent, infatti,* i figli collegati a lui per raggiungere la root dovranno ristabilire un collegamento con la root e diffondere messaggi di RERR (route error). Questo porta a un grande dispendio di risorse di rete, maggiore nel caso in cui la mesh è composta di un numero elevato nodi.

Per riassumere e dare un quadro generale dell'instradamento dei frame viene riportato un esempio:

Quando un nodo deve mandare un pacchetto e non ha informazioni sulla destinazione, lo inoltra alla root, verso la quale ha sempre un path valido. La root analizza il pacchetto e controlla se il destinatario è esterno o interno alla rete mesh. Nel primo caso, ossia quando nemmeno la root ha nella tabella di forwarding il MAC destinatario, il frame è passato al livello superiore. Nel caso in cui il MP destinatario sia interno, la root modifica il sorgente del pacchetto e lo invia verso il mesh designato.

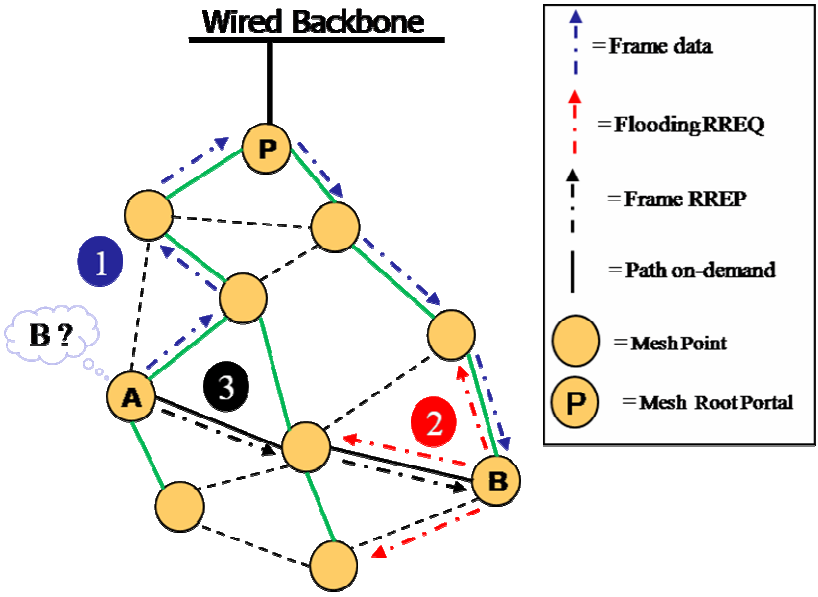

Fig 2.18 Procedure di instaurazione path on-demand intra-mesh.

Una volta che il destinatario riceve il pacchetto e si rende conto del particolare MAC sorgente, riconosce che il sorgente è interno alla rete mesh e provvede a iniziare una procedura di ricerca on-demand per stabilire il path a costo minimo. Questo routing ibrido, permette nelle prime fasi un inoltro dei pacchetti che segue il percorso dell'albero per poi passare verso un più agevole collegamento on-demand, sicuramente più efficiente dal punto di vista del costo totale del path. La procedura descritta permette una trasmissione dei pacchetti veloce senza che la rete sia inutilmente inondata di messaggi broadcast RREQ.
Quando sono presenti più router mesh Portal, la situazione si complica. Infatti, al massimo si può eleggere una sola root, questo limita le capacità della rete con il rischio di far diventare l'unico Portal un collo di bottiglia per l'intera rete. Meglio se ogni Portal esegue il ruolo di root creando più alberi, la gestione risulterà più complicata, ma il guadagno sarà netto.

2.4 Il problema dei sei indirizzi

Il problema dei sei indirizzi si manifesta quando si deve effettuare un collegamento intra-mesh, ossia tra due STA entrambe facenti parti della mesh. In questo caso i pacchetti data per essere indirizzati in modo corretto hanno bisogno di sei indirizzi. Lo standard 802.11 ne

prevedeva fino a quattro, in caso di collegamento di due STA collegate a due MP distinti. Utilizzando invece il protocollo HWMP ed eleggendo una root nella mesh per un forwarding corretto dei pacchetti si ha la necessità dell'aggiunta di ulteriori due indirizzi.

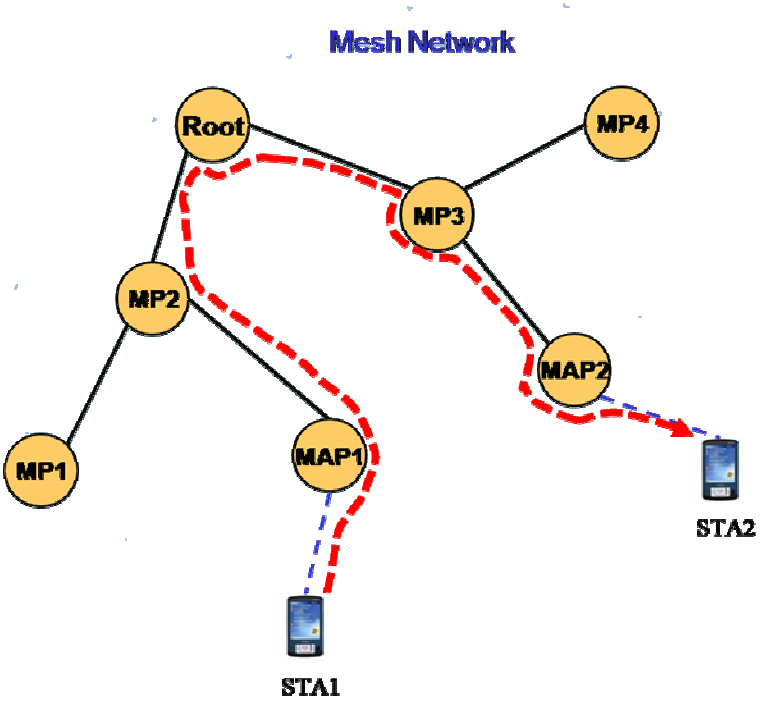

Fig 2.18 Esempio di collegamento intra-mesh tra due stazioni.

Nel dettaglio i due indirizzi sono utilizzati per le comunicazioni punto punto tra tutti gli elementi della mesh. Altri due indirizzi sono necessari per il sorgente MP e il destinatario MP. Gli ultimi due

vengono invece sfruttati per tenere memoria dei due estremi della comunicazione rappresentati dalle STA. Questo problema complica non poco l'implementazione del protocollo di routing HWMP rendendo necessario un cambiamento sostanziale nel formato dei frame e nella loro elaborazione in ricezione. Nella figure 2.19 si può osservare la sequenza dei MAC address da immettere nelle trame durante il collegamento intra-mesh tra STA1 e STA2 raffigurate in figura 2.18.

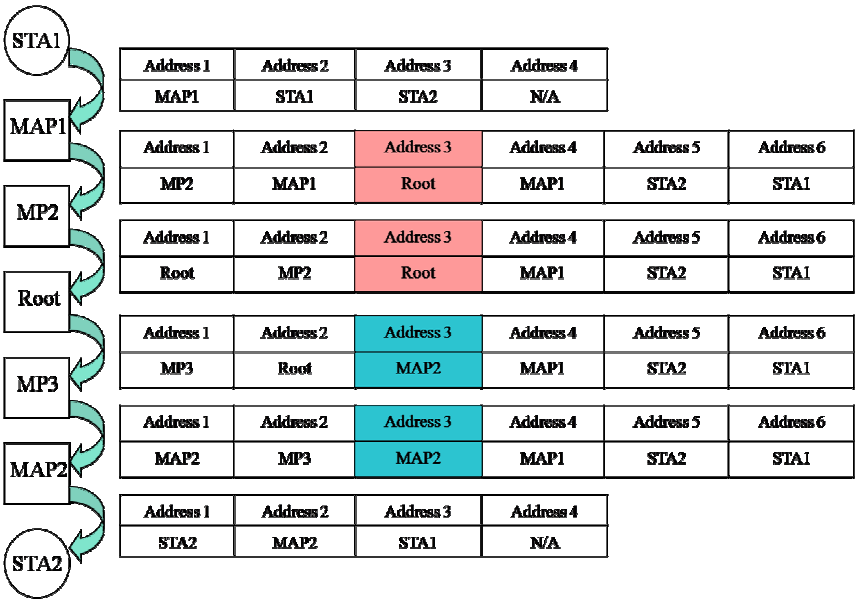

Fig 2.19 Dettaglio degli indirizzi MAC necessari per un collegamento inta-mesh tra STA1 e STA2.

L'utilizzo dei sei indirizzi non era stato preso in considerazione nel primo draft perché ancora il problema non era stato reso evidente. Il'uso di due indirizzi aggiuntivi quindi rappresenta una sorta di "bug" nella struttura di routing proposta nel protocollo HWMP.

2.5 Nuove proposal del draft

In Marzo, mese in cui doveva essere ufficializzato il nuovo draft, sono state invece presentate da ricercatori di varie aziende numerose proposal. Quest'ultime proponevano modifiche all'attuale draft di riferimento e, anche se bocciate, vale la pena riportare alcuni miglioramenti all'802.11s proposti all'interno di quella più significativa l'802.11-07 [10]. Oltre a modificare leggermente alcuni formati di frame questa proposal è incentrata sul routing e le problematiche a esso associate.

2.5.1 Modifiche del tree-based routing

Le modalità di costruzione dell'albero presentate sono due. La prima chiamata Proactive, è basata sull'invio di particolari *proactive RREQ* ed ha l'obiettivo di instaurare i percorsi intra e fuori mesh in modo proattivo. La seconda è quella che già è stata descritta nella sezione

2.3.2 ed evitiamo quindi di riaffrontarla visto che non presenta sostanziali modifiche nelle procedure.

La creazione dell'albero proactive si basa sull'invio, da parte della root designata, di un *proactive RREQ* con destinazione broadcast. Il frame RREQ, come in precedenza avveniva per il *root announcement*, dovrà essere inviato periodicamente, avere metrica zero e numeri di sequenza incrementali. Ogni nodo che riceverà tale pacchetto dovrà creare o aggiornare il path verso la root, calcolare le metriche (hop-count e airtime metric) e rinviare il *proactive RREQ* aggiornato. Per instaurare un collegamento all'albero sarà necessario solo un frame RREP di risposta verso la root, questo snellisce la procedura e la rende più flessibile rispetto a quella presentata nella sezione 2.3.2 .

I MP in genere ricevono più copie dello stesso proactive RREQ proveniente da path diversi. I router mesh devono aggiornare le proprie informazioni solo se il seq. number è maggiore di quello attuale salvato in tabella o nel caso sia identico, il percorso verso la root abbia un costo minore di quello salvato nella tabella di routing.

La nuova proposal inserisce anche i dependent nella gestione dell'albero. Ogni nodo deve dare alla root la lista di tutti i MP che attraverso di loro la raggiungono. In questo modo il MP root può conoscere non solo i nodi collegati ma anche la loro topologia, inserendo altre funzionalità nel routing.

2.5.2 Routing tra stazioni

Un altro aspetto preso in considerazione nella proposal è lo smistamento dei pacchetti aventi come sorgente e destinatari stazioni e non i nodi mesh. L'idea del primo draft era di sviluppare una rete totalmente trasparente, questo era possibile solo tra router mesh ma non tra gli utenti finali della mesh stessa. Infatti, nel draft di Febbraio 2006 non sono considerati i veri estremi dei collegamenti ossia le stazioni. Tutto il traffico di frame data nasce e finisce negli utenti collegati alla WLAN, si è resa così necessaria una ridefinizione di alcune procedure e una sostanziale revisione del routing.

Field	**Value**
ID	TBD
Length	27 + N*11
Flags	Bit 0: 0 (no portal role) Bit 1: 0 (broadcast) Bit 2: 0 (no proactive RREP applicable) Bit 6: Address Extension (AE) (1= if (destination count ==1 && proxied address present), 0 = otherwise) Bit 3 – 5, 7: Reserved

Hop Count	0
Time to Live	Maximum number of hops allowed for this information element, e.g., HWMP_NET_DIAMETER.
RREQ ID	Previous RREQ ID + 1
Originator Address	Own MAC address
Originator's Destination Sequence Number	Previous Originator DSN + 1. See Note 2
Proxied Address	Present only if Bit 6 in Flags = 1. This value is set to the proxied address which is the source of the frame.
Lifetime	The time for which MPs receiving the RREQ consider the forwarding information to be valid, e.g. HWMP_ACTIVE_ROOT_TIMEOUT.
Metric	0
Destination Count	(N)
Per Destination Flags	DO flag, RF flag, as required
Destination Address	MAC address of requested destination
Destination Sequence Number	The latest sequence number received in the past by the originator for any route towards the destination.

Fig 2.20 Esempio di messaggio RREQ presentato nella proposal 802.11-07.

Nel dettaglio sono stati aggiunti nei principali frame di management, oltre agli indirizzi sorgente e destinatario, anche il MAC address della stazione che ha eseguito la richiesta.
Il nuovo indirizzo è chiamato Proxied Address e si riferisce al fatto che i nodi mesh sono dei proxy per gli utenti che vi si collegano. Le funzionalità di questo campo cambiano a seconda del frame e dei flag attivati, ad esempio se il messaggio di management è tra MP, il terzo indirizzo non viene utilizzato.
In questo modo il routing di livello due attraverso l'HWMP è completamente trasparente e gestito interamente dai bridge all'interno dei nodi mesh. Questo rende lo smistamento dei pacchetti ancora più veloce poiché relegato a un livello più basso del consueto *layer tree.*