Capitolo3

48

ninux.org

Contents

1 Progetto della Rete

Prima di acquistare del materiale o di decidersi sulla piattaforma hardware da adottare, occorre farsi una chiara idea sulla natura del problema di comunicazione. Probabilmente, state leggendo questo libro perché intendete collegare tra loro reti di computer, al fine di condividere risorse fino a raggiungere la più estesa Internet. Il progetto di rete che scegliete di realizzare dovrà rispondere alle esigenze di comunicazione che state tentando di soddisfare. Dovete connettere un sito remoto ad una connessione Internet nel centro del vostro campus universitario? La vostra rete potrà presumibilmente crescere, fino ad includere diversi siti remoti? La maggior parte dei vostri componenti di rete sarà installata in postazioni fisse, o la vostra rete si espanderà fino a comprendere centinaia di portatili ed altri dispositivi che migrano da una cella all'altra?

Quando si affronta un problema complesso, si rivela spesso utile tracciare un grafico delle risorse a disposizione e del problema. In questo capitolo, daremo un'occhiata alle modalità che altre persone hanno scelto per costruire reti wireless in grado di soddisfare le proprie esigenze di comunicazione, comprendendo anche i diagrammi essenziali delle strutture di reti. Procederemo quindi con l'affrontare i concetti di networking che definiscono la suite TCP/IP, ovvero il principale linguaggio del networking che si impiega su Internet. Dimostreremo diversi metodi ormai comuni per ottenere che l'informazione fluisca efficacemente attraverso la vostra rete verso il resto del mondo.

1.1 Progettare la rete fisica

Potrebbe sembrare bizzarro parlare della rete "fisica" quando si costruiscono reti wireless. Dopo tutto, dov'è la parte fisica della rete? Nelle reti wireless, il mezzo fisico che impieghiamo per la comunicazione è, ovviamente, l'energia elettromagnetica. Ma nel contesto di questo capitolo, il termine "rete fisica" intende riferirsi al banale concetto di dove mettere le cose. Dove sistemare l'attrezzatura, in modo che sia possibile raggiungere i client wireless? Sia che si intenda coprire l'area di un edificio o che si intenda coprire diversi chilometri, le reti wireless sono suddivise in queste tre configurazioni logiche:

- collegamenti punto-punto (*point-to-point links*)
- collegamento punto-multipunto (*point-to-multipoint links*)
- reti multipunto-multipunto (*multipoint-to-multipoint clouds*)

La struttura di rete fisica da adottare dipenderà dalla natura del problema che si intende risolvere. Mentre parti differenti della rete possono sfruttare ognuna delle citate configurazioni, ogni singolo collegamento ricadrà in una delle tre tipologia sopra riportate. L'applicazione di ciascuna di tali tipologie è meglio spiegata con degli esempi.

1.1.1 Punto-Punto

Collegamenti ***punto-a-punto*** (*Point-to-point links*) garantiscono, tipicamente, una connessione Internet dove l'accesso non sia altrimenti disponibile. Ad un capo di tale collegamento verrà offerta la connessione ad Internet, mentre all'altro estremo Internet viene connessa. Per esempio, una università può disporre di una connessione veloce di tipo frame relay o VSAT al centro del campus, ma non può permettersi lo stesso tipo di connessione per un edificio distaccato. Se l'edificio principale gode di una visuale libera verso il sito distaccato, una connessione punto-a-punto può essere impiegata per connettere assieme i due edifici. Con tale accorgimento, si possono estendere come capacità, od addirittura sostituire, i collegamenti di tipo telefonico già esistenti. Con antenne adatte e visuale libera, sono possibili collegamenti affidabili punto-a-punto anche oltre i trenta chilometri.

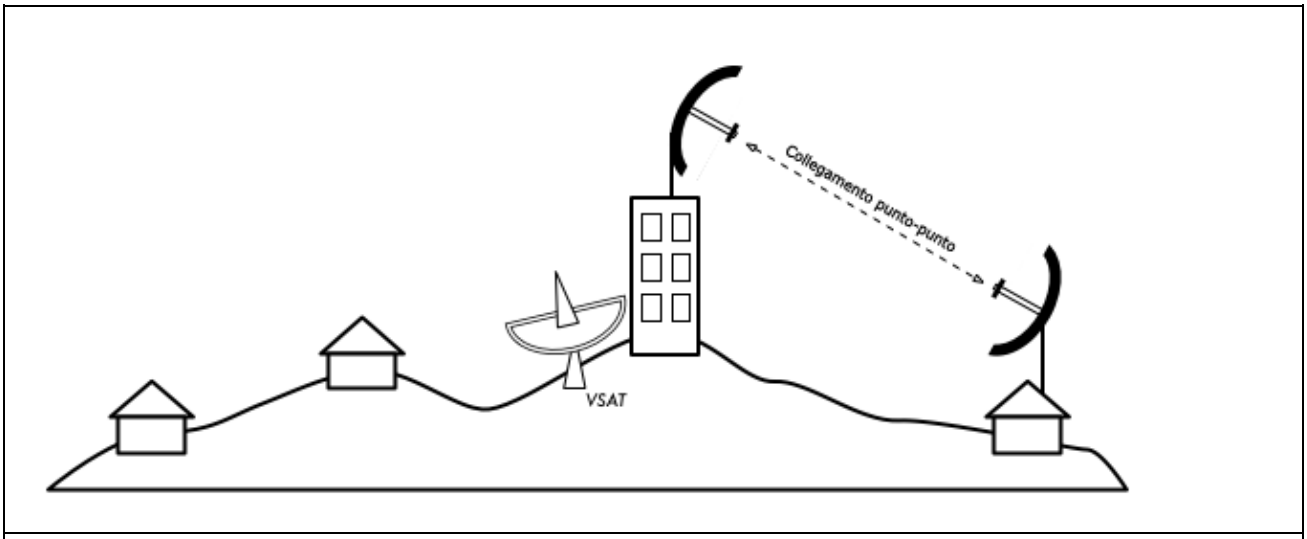


Figura 3.1: Un collegamento punto-a-punto permette ad un sito distaccato di attingere ad una connessione Internet centrale.

Naturalmente, una volta che una connessione punto-punto è stata messa in piedi, altre connessioni possono essere impiegate per estendere la rete ulteriormente. Se l'edificio distaccato del nostro esempio è in cima ad una collina, può essere in visibilità di altre importanti aree che non sarebbero direttamente visibili dal campus centrale. Installando un secondo collegamento punto-punto sul sito remoto, un altro nodo può raggiungere la rete e far così uso della connessione centrale verso Internet.

I collegamenti punto-punto non devono, necessariamente, riguardare l'accesso ad Internet. Supponiamo per esempio di dover condurre una stazione di monitoraggio ambientale, su di una collina, con lo scopo di raccogliere i dati che questa registra nel tempo. Si potrebbe connettere il sito con un collegamento punto-punto, permettendo la raccolta dati ed il monitoraggio in tempo reale, senza la necessità di portarsi fisicamente sul posto. Le reti wireless assicurano sufficiente banda per portare grandi quantità di dati (compresi audio e video) tra due punti che siano tra loro connessi, anche se mancano di allacciamento diretto ad Internet.

1.1.2 Punto-multipunto

La seconda disposizione di rete maggiormente diffusa è la ***punto-multipunto*** (point-to-multipoint). Ove diversi nodi sono in connessione con un punto centrale di accesso, questa è un'applicazione del punto-multipunto. Il classico esempio di una configurazione punto-multipunto è l'impiego di un punto di accesso wireless che garantisce la connessione a diversi laptop. I laptop non comunicano direttamente tra di loro, ma devono rimanere nel raggio di azione dell'access-point per poter usare la rete.

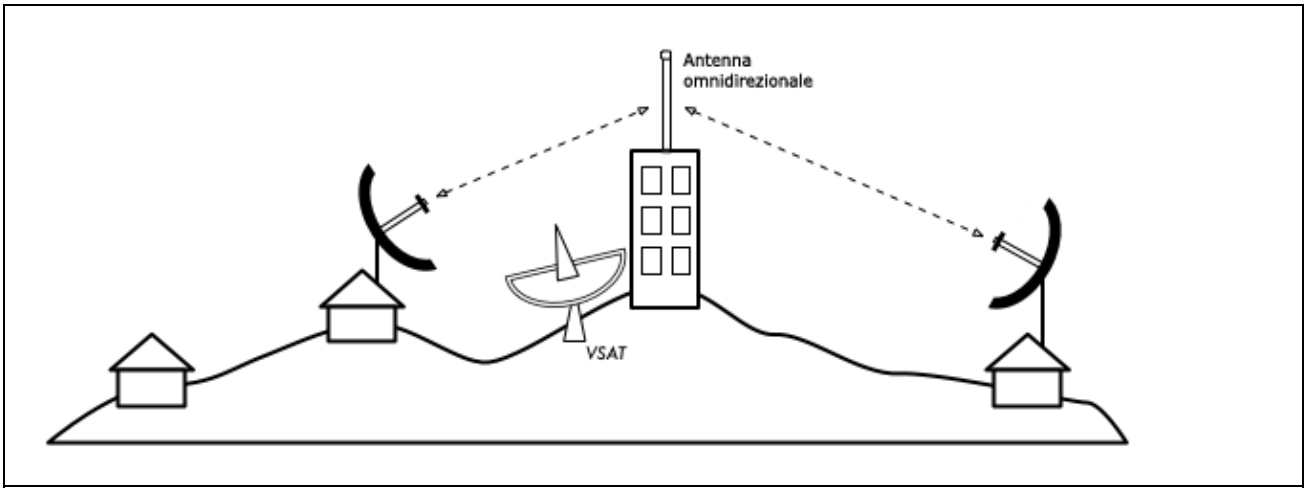


Figura 3.2: Il VSAT centrale è ora condiviso tra diversi siti remoti. I tre siti possono tra loro comunicare anche direttamente, a velocità decisamente superiori a quelle del VSAT.

Il networking punto-multipunto può anche applicarsi al precedente esempio dell'università. Si supponga che l'edificio distaccato sulla cima della collina sia connesso al campus centrale con un collegamento punto-punto. Piuttosto che tirare su diversi collegamenti punto-punto per distribuire l'accesso ad Internet, può venir impiegata un'unica antenna che sia visibile dai diversi edifici lontani. Questo è un classico esempio di una connessione ***punto*** (sito distaccato sulla collina) ***-multipunto*** (molti edifici nella valle sottostante) su area estesa.

Si osservi come sussistano limiti nelle prestazioni di collegamenti punto-multipunto su distanze molto estese, limiti che verranno discussi più avanti nel capitolo. Questi collegamenti sono possibili ed utili in diverse situazioni, ma si eviti di ricadere nel classico errore di installare un singolo traliccio radio ad alta potenza nel bel mezzo della città, con la pretesa di portare il servizio a migliaia di utenti, così come si potrebbe invece fare per una stazione radio FM. Come si vedà più avanti, le reti di dati si comportano in modo decisamente differente dalle trasmissioni della radio.

1.1.3 Multipunto-multipunto

Il terzo tipo di configurazione di rete è quello ***multipunto-multipunto***, definito anche rete ***ad-hoc*** o ***mesh***. In una rete multipunto-multipunto, non c'è un'autorità centrale. Ogni nodo sulla rete si prende carico del traffico di ogni altro nodo, secondo necessità, ed ogni nodo comunica direttamente con ogni altro.

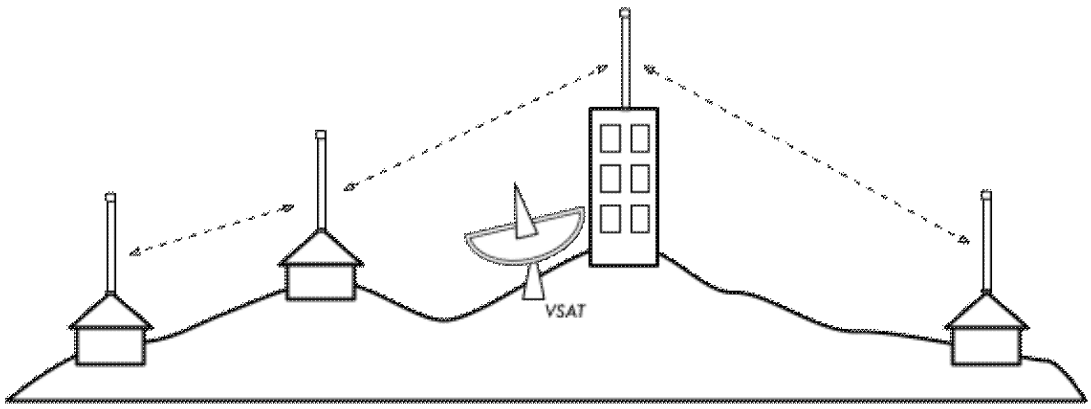


Figura 3.3: una maglia (mesh) multipunto-multipunto. Ogni punto riesce a raggiungere ogni altro a velocità molto alta, così come può raggiungere Internet tramite il VSAT centrale.

I vantaggi di tale configurazione di rete risiedono nel fatto che, anche se nessuno dei nodi fosse in contatto con l'access point centrale, questi potrebbero comunque comunicare tra loro. Le realizzazioni a regola d'arte di reti mesh sono auto-riconfiguranti, nel senso che riescono a riconoscere automaticamente i problemi di routing e riescono a risolverli nel modo opportuno. Estendere una rete mesh è semplice come aggiungere nuovi nodi. Se uno dei nodi nella "nuvola" si trova ad essere un gateway (varco) verso Internet, allora l'accesso può essere condiviso tra tutti i client presenti.

Due gravi svantaggi di tale tipologia sono la complessità crescente e la bassa prestazione. Anche la sicurezza, in una rete simile, rappresenta un serio problema, poiché ogni singolo partecipante può, potenzialmente, prendersi carico del traffico di ogni altro. Reti multipunto-multipunto tendono ad essere complicate nella diagnostica dei problemi, a causa del grande numero di variabili che insorgono quando i nodi cambiano di posizione. Le reti multipunto-multipunto, tipicamente, non dispongono della stessa capacità di reti punto-punto o punto-multipunto, a causa dell'overhead supplementare necessario per il routing della rete e della più serrata competizione per l'impiego dello spettro elettromagnetico.

Tuttavia, le reti a maglia (mesh networks) sono utili in diverse situazioni. Alla fine di questo capitolo, vedremo un esempio di come rendere attiva una rete a maglia multipunto-multipunto impiegando un protocollo di routing chiamato OLSR.

1.1.4 Impiega la tecnologia che risolve il problema

Tutti questi progetti di rete possono essere usati per complementarsi a vicenda in una rete più grande, e possono ovviamente far uso delle tradizionali tecniche di una rete su cavo, ove possibile. Si fa infatti comunemente ricorso ad un collegamento wireless a lunga distanza per assicurare l'accesso Internet ad una postazione remota, impiegando poi un access point su tale postazione per garantire l'accesso a livello locale. Uno dei client di questo access point può poi, a sua volta, comportarsi come nodo di maglia, permettendo alla rete di espandersi tra gli utenti dei laptop che, alla fine, usano tutti il collegamento punto-punto originale per aver accesso ad Internet.

Ora che è stata fornita una chiara idea sul modo con cui vengono tipicamente impostate le reti wireless, si può iniziare a comprendere come sia possibile la comunicazione attraverso tali reti.

1.2 La rete logica

La comunicazione diventa realizzabile solo quando i partecipanti impiegano un linguaggio comune. Quando però la comunicazione diventa più complessa che una semplice radio-diffusione, il ***protocollo*** acquista un'importanza pari a quella del linguaggio. Tutte le persone in un auditorium possono parlare lo stesso Inglese, ma in assenza di regole per stabilire chi abbia diritto di prendere il microfono, la comunicazione delle idee di un singolo individuo all'intera platea diventa praticamente impossibile. Si immagini ora un auditorium che si estenda al mondo intero, ove siano compresi tutti i computer esistenti. Senza un insieme di protocolli di comunicazione comuni per regolare quando e come un computer possa prendere la parola, Internet sarebbe solo una disordinata confusione, dove tutte le macchina provano a parlare nello stesso momento.

TCP/IP si riferisce alla suite di protocolli che permettono la realizzazione delle conversazioni sull'Internet globale. Se si comprende TCP/IP, si possono costruire reti in grado di crescere praticamente a qualsiasi dimensione, per arrivare a diventare parte, alla fine, dell'Internet globale.

1.2.1 Il modello TCP/IP

Le reti di dati sono spesso descritte come costituite su strati diversi. Ogni strato dipende dalle operazioni condotte da tutti gli strati sottostanti, prima che la comunicazione possa aver luogo, ma ogni strato scambia i dati solo con lo strato superiore o con quello inferiore ad esso. Il modello TCP/IP delle reti descrive cinque strati, come evidenziato dal diagramma sotto riportato:

Figura 3.4: Il modello di rete TCP/IP.

La precedente sezione sulla configurazione della rete descriveva il primo strato: lo ***strato fisico***. Si tratta del mezzo fisico sul quale la comunicazione ha luogo. Può essere un cavo di rame di tipo CAT5, un fascio di fibre ottiche, onde radio, od anche un altro mezzo.

Lo strato soprastante è chiamato ***strato data link***. Quando due o più nodi condividono lo stesso mezzo fisico (per esempio, diversi computer attestati ad un hub, od una sala piena di laptop che usano tutti lo stesso canale radio), essi usano lo strato data link per determinare a chi spetti trasmettere sul mezzo. Esempi comuni di protocolli di data link sono Ethernet, il Token Ring, l'ATM, ed i protocolli di rete wireless (802.11a/b/g). Le comunicazioni su questo strato sono definite ***link locali***, poichè tutti i nodi connessi su questo strato possono comunicare direttamente l'uno con l'altro. Sulle reti che assumono Ethernet come modello di riferimento, i nodi vengono distinti sulla base del proprio ***indirizzo MAC***, che è un numero univoco di 48 bit assegnato ad ogni periferica di rete dal suo costruttore.

Appena sopra dallo strato data link c'è lo ***strato Internet***. Per il TCP/IP, questo è detto Internet Protocol (***IP***). Sullo strato Internet, i pacchetti possono lasciare la rete del collegamento locale per essere ritrasmessi su altre reti. I router prendono in carico questa funzione su una rete, disponendo di almento due interfacce di rete, una per ogni rete che devono interconnettere. I nodi su Internet sono raggiungibili grazie al loro ***IP address***, che è globalmente unico.

Diventato possibile il routing su Internet, si rende ora necessario raggiungere un particolare servizio disponibile presso un indirizzo IP dato. La funzione è soddisfatta dallo strato successivo, lo ***strato di trasporto***. TCP ed UDP sono classici esempi di strati di trasporto. Alcuni protocolli dello strato di trasporto (come TCP) assicurano che tutti i dati arrivino a destinazione, siano riassemblati e quindi consegnati allo strato superiore, nell'ordine previsto.

Alla fine, sulla cima della pila si trova lo ***strato applicativo***. È lo strato che si interfaccia con la maggior parte degli utenti della rete, ed è a livello di questo strato che avviene la comunicazione per le persone. HTTP, FTP e SMTP sono tutti protocolli dello strato applicativo. La persona si pone al di sopra di tutti questi strati, e non deve conoscere praticamente nulla di tutti gli strati sottostanti, per impiegare in modo efficace la rete.

Un modo per riconoscere il modello TCP/IP può essere quello che prevede una persona che intenda consegnare una lettera ad un ufficio in un palazzo del centro. Occorre prima interagire con la stessa strada (lo strato fisico), prestare attenzione al traffico che altri conducono sulla strada (lo strato data-link), giungere al posto giusto per immettersi su altre strade ed arrivare all'indirizzo giusto (lo strato Internet), portarsi al piano giusto ed al corretto numero di stanza (lo strato di trasporto), e finalmente trovare il destinatario o un commesso che possa prendere in carico la lettera (lo strato applicativo). I cinque strati possono facilmente essere ricordati usando il trucco mnemonico "**F**orse **D**omani **I**ncontrerò **T**ue **A**miche", che naturalmente ricorda: " **F**isico / **D**ata-link / **I**nternet / **T**rasporto / **A**pplicativo."

1.3 reti wireless 802.11

Prima che i pacchetti possano essere inoltrati ed instradati su Internet, il primo strato (quello fisico) ed il secondo (quello data link) devono essere connessi. Senza connessione sul collegamento locale, i nodi della rete non possono comunicare tra di loro, né possono instradare pacchetti.

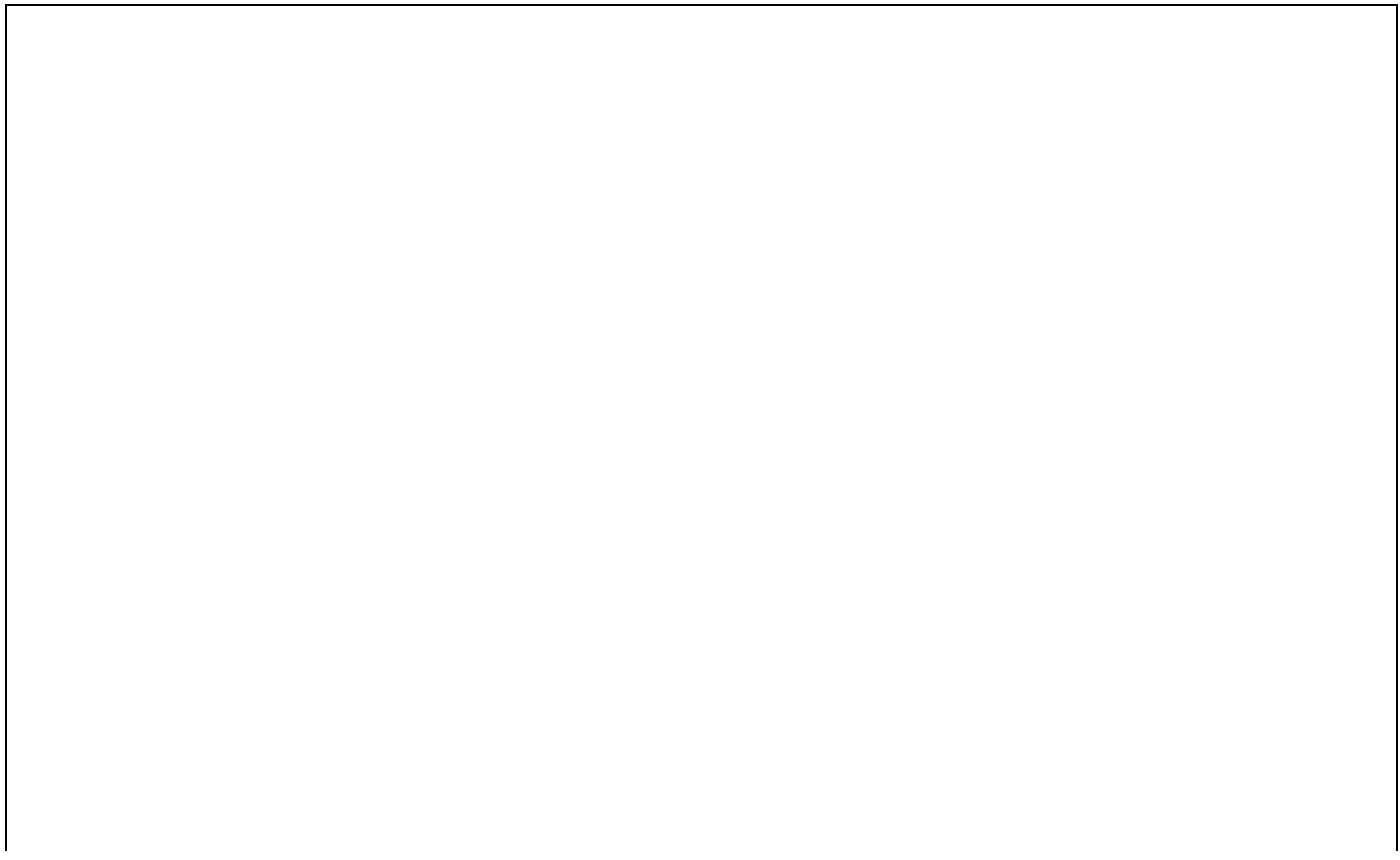
Per garantire connessione fisica, le periferiche wireless devono operare nella stessa finestra dello spettro radio. Come si è visto nel capitolo 2, ciò significa che le radio 802.11a potranno comunicare con altre radio 802.11a sulla banda dei 5GHz, mentre le radio 802.11b/g comunicheranno con altre radio 802.11b/g sulla banda dei 2.4 GHz. Ma una periferica 802.11a non potrà colloquiare con una periferica 802.11b/g, poichè usano segmenti completamente diversi dello spettro elettromagnetico.

In modo più specifico, le schede wireless devono accordarsi su un canale comune. Se una scheda radio 802.11b è impostata sul canale 2 mentre un'altra è impostata sul canale 11, le due radio non comunicheranno tra di loro.

Quando due schede wireless sono configurate per impiegare lo stesso protocollo sullo stesso canale radio, sono allora pronte per negoziare la connettività sullo strato data link. Ogni periferica 802.11a/b/g può lavorare in uno dei quattro possibili modi:

1. ***Master mode*** (altrimenti chiamato ***AP*** or ***modo infrastruttura***) è usato per rendere disponibile un servizio simile ad un access point tradizionale. La scheda wireless crea una rete con un nominativo specifico (chiamato ***SSID***) ed un proprio canale, ed offre servizi di rete su questo. Posta in modo master, la carta wireless governa tutte le comunicazioni relative alla rete (autenticando i client wireless, gestendo le contese sul canale, ripetendo i pacchetti, etc.). Le schede wireless poste in modo master possono comunicare solo con altre schede che le siano associate in modalità *managed* (gestita).
2. ***Managed mode*** viene talvolta chiamato ***client*** mode. Le schede wireless poste in managed mode si aggregheranno a reti create da un master, e provvederanno automaticamente a reimpostare il proprio canale di lavoro per adeguarsi al canale del master. Provvederanno quindi a presentare ogni credenziale necessaria al master, e se queste credenziali saranno accettate, queste schede verranno definite ***associate*** (associated) al master. Le schede in Managed mode non comunicano direttamente tra di loro, ma comunicano solo con il master loro associato.
3. ***Ad-hoc mode*** crea reti multipunto-multipunto dove non è presente un signolo nodo master, od Access Point. Nel modo ad-hoc, ogni scheda wireless comunica direttamente con i propri vicini. I nodi devono essere nel raggio d'azione di ogni altro nodo corrispondente per comunicare, e devono accordarsi sul nome della rete e sul canale da impiegare.
4. ***Monitor mode*** è impiegato da alcuni strumenti (come Kismet, vedasi al capitolo sei) che ascoltano passivamente il traffico presente su un dato canale. Quando sono in Monitor Mode, le schede wireless non trasmettono dati. Tale caratteristica è importante per analizzare problemi su un collegamento wireless o per osservare l'impiego dello spettro elettromagnetico in una zona locale. Il Monitor Mode non è usate per le normali comunicazioni.

Nella realizzazione di un collegamento punto-punto o punto-multipunto, una radio dovrà tipicamente operare in Master Mode, mentre le altre verranno poste in Managed Mode. In una rete multipunto-multipunto, le radio opereranno tutte in modalità ad-hoc, sì che possano comunicare direttamente una con le altre.



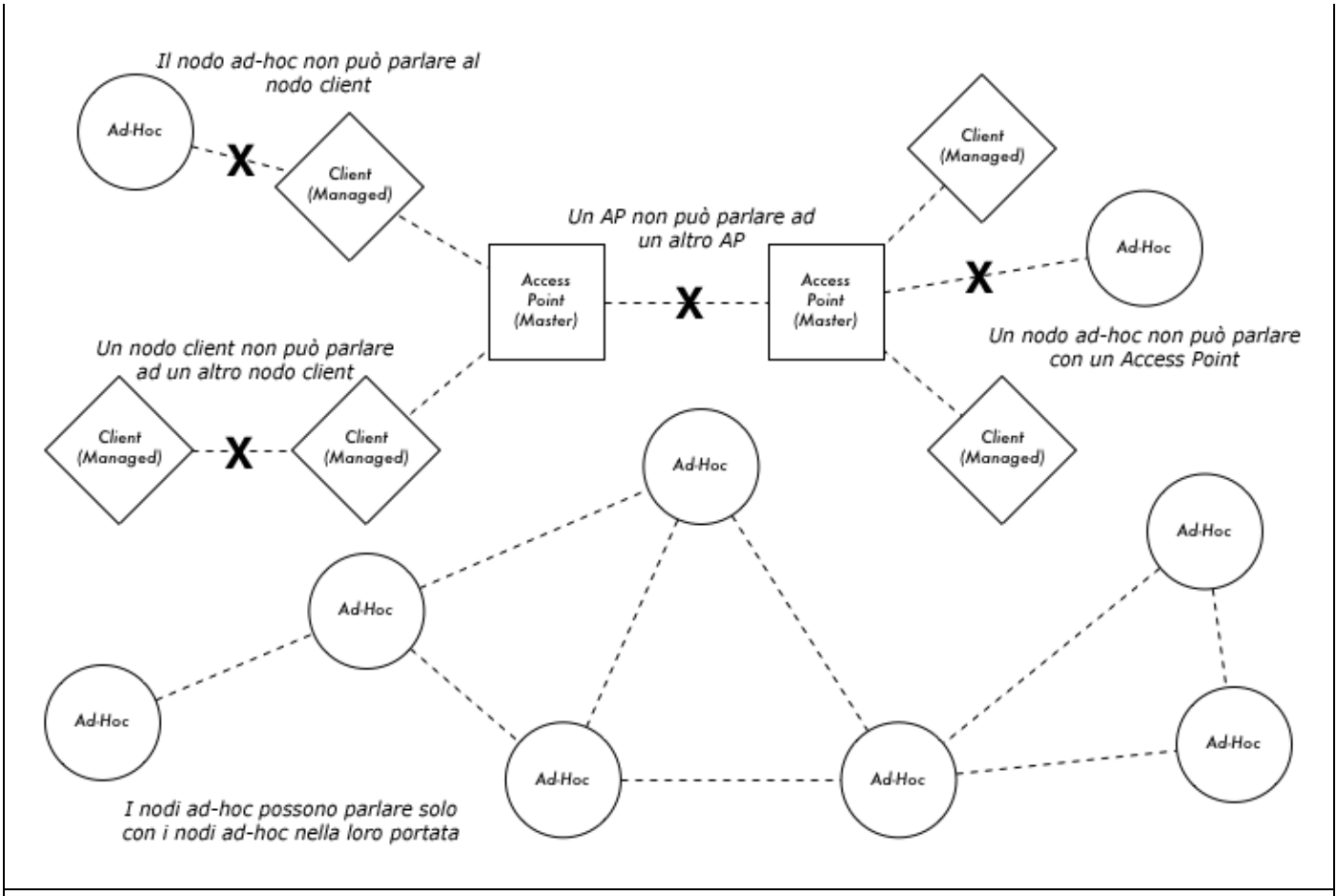


Figura 3.5: Access Point, Client, e nodi Ad-Hoc.

È importante mantenere queste modalità in mente quando si progettano le configurazioni di rete. Si ricordi come i client in Managed Mode non possano comunicare direttamente gli uni con gli altri, sì da rendere probabile l'impiego in un sito ripetitore a maggiore altezza che sia in Master Mode o Ad-Hoc Mode. Come si vedrà più avanti nel capitolo, il modo Ad-Hoc è più flessibile ma presenta maggiori problemi di prestazioni, rispetto al Master Mode ed al Managed Mode.

Ora che le schede wireless garantiscono connettività sia nello strato fisico che in quello data-link, sono in grado di cominciare a trasferire i pacchetti sul terzo strato, lo strato internetworking.

1.4 reti Internet

Indirizzi IP, indirizzamento di rete, routing e forwarding sono tutti concetti importanti e correlati nell'ambito delle reti Internet. Un ***indirizzo IP*** è un identificatore per un nodo di rete quale un PC, un server, un router od un bridge. ***Indirizzamento di Rete*** è il sistema impiegato per assegnare tali identificatori raggruppandoli in gruppi significativi. Il ***Routing*** tiene traccia di dove questi gruppi possano essere trovati nella rete. Il risultato del processo di routing è mantenuto in una lista chiamata ***tabella di routing***. Il ***Forwarding*** è l'azione di impiegare la tabella di routing per spedire un pacchetto dati o verso la sua destinazione finale, o verso "il prossimo salto" che lo avvicina alla destinazione.

1.4.1 Indirizzi IP

In una rete IP, l'indirizzo è un numero di 32 bit, normalmente scritto sotto forma di quattro numeri ad otto bit, separati da punti. Esempi di indirizzi IP sono 10.0.17.1, 192.168.1.1, o 172.16.5.23.

1.4.2 indirizzamento di rete

Reti interconnesse devono concordare un piano di indirizzamento IP. Nella Internet globale, commissioni di persone distribuiscono gruppi di indirizzi IP in modo coerente per assicurare che indirizzi duplicati non vengano usati da reti differenti, provvedendo altresì che ci si possa riferire in modo rapido a gruppi di indirizzi. Questi gruppi di indirizzi sono chiamati sotto-reti o ***subnets*** come abbreviazione. Sottoreti più ampie possono essere ulteriormente suddivise in sottoreti minori. Talvolta, un gruppo di indirizzi collegati è chiamato Spazio di Indirizzi o ***address space***.

Su Internet, nessuna persona e nessuna organizzazione possiede effettivamente questi gruppi di indirizzi perché gli indirizzi hanno significato solo se il resto della comunità di Internet concorda nel loro utilizzo. Per accordo, gli indirizzi sonon distribuiti alle organizzazioni sulla base dei loro bisogni e della loro dimensione. Un'organizzazione che abbia ricevuto un segmento di indirizzi potrebbe quindi assegnarne una porzione ad un'altra organizzazione, sulla base di un accordo di servizio. Indirizzi che vengono assegnati in questa maniera, partendo dalle commissioni internazionalmente riconosciute per poi essere via via spezzati gerarchicamente da comitati nazionali o regionali, sono detti ***indirizzi IP globalmente instradati*** (*globally routed IP addresses*).

A volte non è conveniente, se non impossibile, ottenere per un individuo od un'organizzazione più di un indirizzo IP globalmente instradato. In questo caso può essere impiegata una tecnica conosciuta come *Network Address Translation* (traduzione dell'indirizzo di rete), o ***NAT***. Un dispositivo NAT è un router con due porte di rete. La porta esterna impiega un indirizzo IP globalmente instradato, mentre la porta interna usa un indirizzo IP appartenente ad un segmento particolare, chiamato ***indirizzi privati***. Il router NAT permette al singolo indirizzo globale di essere condiviso da parte di tutti gli utenti interni, che impiegano indirizzi privati. Il router NAT converte i pacchetti da una forma di indirizzamento all'altra, quando i pacchetti lo attraversano. Gli utenti interni credono di essere direttamente connessi ad Internet e non richiedono né software particolare, né driver, per condividere il singolo indirizzo IP globale.

1.4.3 Routing

Internet cresce e cambia costantemente. Nuove reti sono aggiunte in continuazione, mentre i collegamenti tra le reti sono aggiunti, sono rimossi, cadono e vengono ripristinati. È compito del ***routing*** determinare il percorso migliore verso la destinazione, e creare tabelle di routing che elenchino il percorso migliore per ogni possibile destinazione.

Routing Statico è il termine usato per le tabelle di routing compilate a mano. È talvolta conveniente per piccole reti, ma può facilmente diventare impraticabile e soggetto ad errori per reti di maggiore dimensione. Ancora peggio, se il percorso migliore verso una rete diventa inimpiegabile, per un'avaria hardware o per altre ragioni, il routing statico non farà uso del miglior percorso secondario.

Routing Dinamico è una soluzione dove gli elementi di rete, in particolare i router, si scambiano reciprocamente informazioni sul loro stato e sullo stato dei propri vicini nella rete, e quindi usano queste informazioni per rilevare automaticamente il percorso migliore e per compilare la tabella di routing. Se ci sono cambiamenti, come un router che si blocca od un nuovo router che entra in azione, allora i protocolli di routing dinamico apportano aggiustamenti alle tabelle di routing. Il sistema di scambio dei pacchetti e la definizione delle decisioni è denominato ***protocollo di routing***. Ci sono diversi protocolli di routing che sono usati oggi su Internet, tra cui OSPF, BGP, RIP, and EIGRP.

Le reti wireless sono come le reti su cavo, per quanto riguarda la loro necessità di protocolli di routing, ma sono anche tanto differenti, da richiedere protocolli di routing diversi. In particolare, le connessioni su reti su cavo tipicamente o funzionano bene, o non funzionano affatto (in altre parole, un cavo Ethernet o è allacciato, o non lo è). La situazione non è così chiara quando si tratta di reti wireless. Le comunicazioni radio possono essere affette da oggetti che si muovono sul percorso del segnale, o da disturbi che interferiscono. Conseguentemente, i collegamenti possono funzionare bene, o male, o in modo sfumato tra i due estremi.

Poichè i protocolli attuali non tengono in conto la qualità del collegamento nel definire le decisioni, i comitati IEEE 802.11 e l'IETF stanno lavorando sulla standardizzazione dei protocolli per le reti wireless. Al momento, non è ancora chiaro se si imporrà un singolo standard per affrontare la qualità variabile di un collegamento.

Nel frattempo, sono in corso diversi tentativi di affrontare il problema. Alcuni esempi sono ***Hazy Sighted Link State*** (***HSLS***), ***Ad-hoc On-demand Distance Vector*** (***AODV***), e ***Optimized Link State Routing*** (***OLSR***). Un altro è ***SrcRR***, una combinazione del DSR e dell'ETX, realizzato dal progetto Roofnet del M.I.T. Più avanti, in questo capitolo, vedremo un esempio di come realizzare una rete usando OLSR per le decisioni di routing.

1.4.4 Forwarding

Il ***Forwarding*** è diretto, in confronto con l'indirizzamento ed il routing. Ogni volta che riceve un pacchetto di dati, il router consulta la tabella di routing che possiede internamente. Partendo dal bit più significativo (o di maggior ordine), la tabella di routing viene scandita per ricercare il valore che corrisponda per il maggior numero di bit all'indirizzo di destinazione. Tale valore (il primo campo di ogni riga) è denominato il ***prefisso*** dell'indirizzo. Se viene trovato nella tabella di routing un prefisso che corrisponda, allora il ***contatore dei salti*** (*hop counter*) od il campo ***time to live*** (***TTL***) è decrementato. Se il risultato è zero, allora il pacchetto viene lasciato cadere ed un pacchetto di segnalazione di errore viene rinviata al mittente. Altrimenti, il pacchetto viene inviato al nodo od alla interfaccia specificata nella tabella di routing. Come esempio, se la tabella di routing contiene questi valori...

```
Destination···· Gateway········ Genmask········ Flags Metric· Iface¶
10.15.6.0····· 0.0.0.0········ 255.255.255.0·· U···· 0····· eth1¶
10.15.6.108···· 10.15.6.7····· 255.255.255.255 UG··· 1····· eth1¶
216.231.38.0··· 0.0.0.0········ 255.255.255.0·· U···· 0····· eth0¶
0.0.0.0········ 216.231.38.1··· 0.0.0.0········ UG··· 0····· eth0¶
```

...ed un pacchetto arriva con indirizzo di destinazione 10.15.6.23, questi verrà allora spedito al gateway 10.15.6.7 (poichè il primo campo, di ingresso, trova sulla linea di tale gateway una corrispondenza più completa rispetto dalla rotta della rete 10.15.6.0)

Una destinazione 0.0.0.0 è convenzionalmente considerata il ***default gateway***. Se nessun altro prefisso trova corrispondenza con l'indirizzo di destinazione, allora il pacchetto viene spedito al *default gateway*. Per esempio, se l'indirizzo di destinazione fosse 72.1.140.203, allora il router indirizzerebbe il pacchetto al gateway 216.231.38.1 (che sarà, verosimilmente, più prossimo alla destinazione finale, e così via).

Se per il pacchetto in ingresso non è trovata nessuna corrispondenza valida (cioè, se non esiste un default gateway e non c'è corrispondenza con il prefisso di una rotta stabilita), allora il pacchetto viene lasciato cadere ed un pacchetto di errore viene restituito al mittente.

Il campo TTL è impiegato per riconoscere i giri a vuoto dei pacchetti (*routing loops*). Senza tale campo, un pacchetto potrebbe essere continuamente rimbalzato tra un router ed un altro, qualora questi si indicassero a vicenda come prossimo passo verso la destinazione finale. Questo tipo di giro a vuoto può dare origine ad un forte traffico non necessario sulla rete, tale da minacciarne la stabilità. L'impiego del TTL non scongiura i giri a vuoto, ma contribuisce ad evitare che questi distruggano la rete a causa di un semplice errore di configurazione.

1.4.5 Comporre il tutto in una visione unica

Ciascun nodo della rete può inviare pacchetti di dati all'indirizzo IP di un altro nodo, una volta che tutti

abbiano ricevuto il proprio indirizzo IP. Attraverso l'uso del routing e del forwarding, questi pacchetti possono raggiungere i nodi sulla rete che non sono fisicamente connessi al nodo di origine. Questo processo sintetizza la gran parte di ciò che avviene su Internet. Tutto ciò è illustrato nelle figure seguenti:

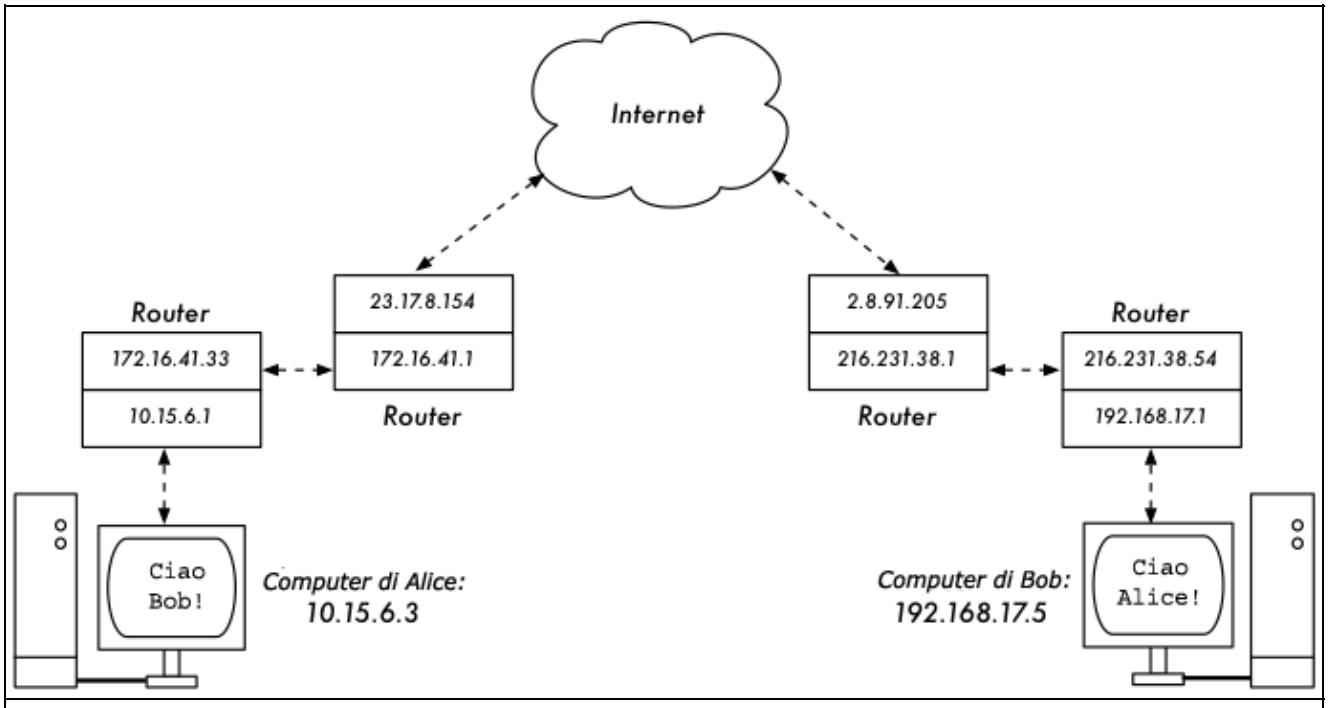


*Figura 3.6: Reti su Internet. Ogni segmento di rete dispone di un router con due indirizzi IP, ponendolo in un "collegamento locale" (*link local*) su due reti differenti. I pacchetti sono passati tra router fintantochè non raggiungano la loro destinazione finale*

In questo esempio, potete vedere il percorso che completano i pacchetti quando Alice scambia messaggi con Bob impiegando un servizio di *istant messaging*. Ogni linea punteggiata rappresenta un cavo Ethernet, un collegamento wireless, od ogni altra possibile rete fisica. Il simbolo *a nuvola* viene comunemente usato per rappresentare "Internet", e corrisponde ad un numero di reti IP che vi partecipano. Né Alice, né Bob devono preoccuparsi di come le proprie reti cooperino tra loro, fintantochè i router inviino il traffico IP fino alla destinazione finale. Se non fosse per i protocolli di Internet e la collaborazione di ciascuno sulla rete, questo tipo di comunicazione non sarebbe possibile.

Ora che abbiamo visto come i pacchetti fluiscano sulle reti IP, vediamo un tipo particolare di rete IP: una maglia OLSR.

1.5 Reti a Maglia con OLSR

Gran parte delle reti wireless lavorano in Infrastructure Mode; sono costituite di un access point posto da qualche parte, con una scheda radio che lavora in Master Mode, ed un collegamento ad una linea DSL od ad un'altra rete di grande dimensione, di tipo su cavo. In questo ***hotspot***, l'access point lavora tipicamente da Master Station che distribuisce l'accesso ad Internet ai propri client, che funzionano invece in Managed Mode. Questa topologia è simile al servizio mobile telefonico GSM. I telefonini si connettono ad una stazione base; senza la presenza di tale stazione base, i telefonini non sarebbero in grado di comunicare tra loro. Se desiderate giocare uno scherzo, chiamate l'amico che siede dall'altro lato del tavolo; il vostro telefono spedice alla stazione base del vostro provider telefonico che può essere lontana un paio di chilometri, ed è la stazione base che reinvia poi il segnale al telefono del vostro amico.

Anche le schede WiFi in Managed Mode non possono comunicare direttamente. I client - ad esempio, due portatili sullo stesso tavolo - devono impiegare un access point come relay. Tutto il traffico tra i client aggregati ad un access point deve quindi essere spedito due volte. Se i client A e C comunicano, il cliente A

spedisce i propri dati all'access point B, quindi l'access point ritrasmette i dati al cliente C. La singola trasmissione può raggiungere, nel nostro esempio, i 600 kByte/sec (all'incirca, la velocità massima raggiungibile con il protocollo 802.11b). Così, poichè i dati devono essere ripetuti dall'access point prima che raggiungano il proprio destinatario, la velocità effettiva tra due client sarà solo di 300 kByte/sec.

Nel modo ad-hoc non c'è un rapporto gerarchico master-client. I nodi possono comunicare direttamente, fintantochè siano nel raggio d'azione delle proprie interfacce wireless. Così, nel nostro esempio entrambi i computer potrebbero raggiungere la massima velocità se lavorassero in modalità ad-hoc, in condizioni ideali.

Lo svantaggio della modalità ad-hoc è che i client non ritrasmettono il traffico destinato ad altri client. Nel caso dell'access point (modalità infrastructure), invece, se due client A e C non possono vedersi direttamente con le loro interfacce wireless, sono comunque in grado di comunicare, fintantochè l'Access Point sia nel raggio wireless di entrambi i client.

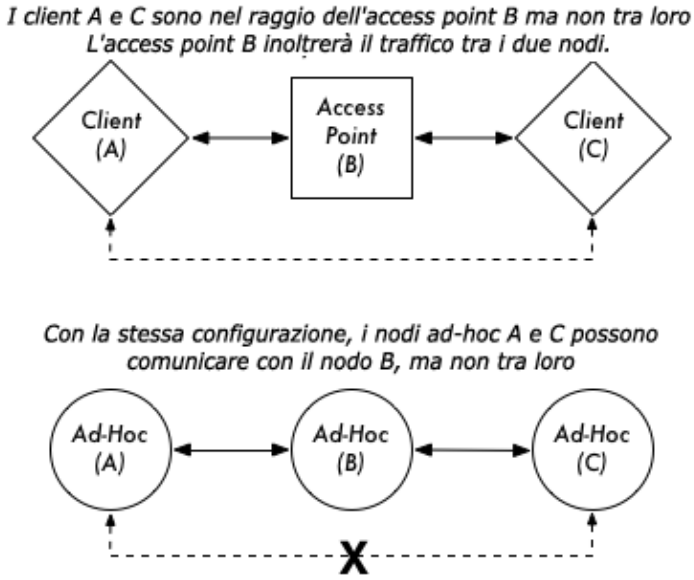


Figura 3.7: L'Access Point B ritrasmetterà il traffico tra i client A and C. Nella modalità Ad-Hoc, il nodo B non ripeterà il traffico tra A e C per default.

I nodi Ad-hoc non ritrasmettono il traffico per default, ma possono comportarsi in modo simile se viene applicato un opportuno ***routing***. Le reti a maglia (*Mesh networks*) sono basate sulla strategia che rende ogni nodo - capace di costituire maglie - relay per estendere la copertura della rete wireless. Maggiore il numero dei nodi, migliore diventa la copertura radio e la portata della nuvola di maglie.

Un importante costo dev'essere menzionato a questo proposito. Se il dispositivo usa solo un'interfaccia radio, la banda disponibile è ridotta in modo significativo ogni volta che il traffico viene ripetuto da nodi intermedi posti sul percorso da A a B. Inoltre, ci sarà interferenza nella trasmissione a causa della condivisione dello stesso canale da parte dei nodi. Cosi, economiche reti a maglia su modalità ad-hoc possono garantire una buona copertura radio sull'ultimo miglio di una rete di una comunità wireless al costo della velocità, specialmente se la densità dei nodi e la potenza di trasmissione sono alte.

Se una rete ad-hoc è costituita solamente di pochi nodi che sono accesi ed attivi in modo continuo, che non si muovono e che dispongono sempre di collegamenti radio stabili - una lunga lista di condizioni - diventa possibile compilare a mano le tabelle di routing per tutti i nodi.

Sfortunatamente, le condizioni citate si incontrano difficilmente nel mondo reale. I nodi possono cadere, dispositivi WiFi sono presenti nelle vicinanze, e le interferenze possono rendere inimpiegabili i collegamenti

radio in qualsiasi momento. Nessuno ha l'intenzione di aggiornare a mano diverse tabelle di routing ogni volta che un nuovo nodo è aggiunto alla rete. Impiegando invece protocolli di routing che mantengono in modo automatico le specifiche tabelle di routing su tutti i nodi coinvolti, diventa possibile evitare questo problema. I protocolli di routing di maggiore impiego nel mondo cablato (protocolli come OSPF) non funzionano al meglio in un ambiente wireless perché non sono progettati per contrastare i collegamenti con attenuazioni o le topologie che cambiano con rapidità.

1.5.1 Mesh Routing con olsrd

Il demone Optimized Link State Routing - olsrd - fornito da olsr.org è un'applicazione di routing sviluppata per il routing nelle reti wireless. Ci si concentrerà su questo software di routing per diverse ragioni. È un progetto open-source che supporta Mac OS X, Windows 98, 2000, XP, Linux, FreeBSD, OpenBSD e NetBSD. Olsrd è disponibile per access point che funzionano sotto Linux, come il Linksys WRT54GL, l'Asus WL-500G, l'AccessCube od i PocketPC che funzionano su Familiar Linux, e viene fornito come standard sui kit Metrix che funzionano su Metrix Pebble. Olsrd può gestire interfacce multiple ed è estensibile con appositi moduli aggiuntivi (plug-in). Supporta IPv6 ed è attivamente sviluppato ed impiegato da reti di comunità in tutto il mondo.

Si noti come esistano diverse versioni dell'Optimized Link State Routing, che è nato come un draft IETF scritto dall'istituto francese INRIA. La realizzazione distribuita da olsr.org ha visto la luce come tesi di master di Andrea Toennesen all'università di Unik. Basato sull'esperienza pratica della comunità delle reti libere, il demone di routing venne modificato. Olsrd attualmente si differenzia significativamente dalla proposta originale, perché include un dispositivo chiamato Link Quality Extension che rileva il tasso di pacchetti perduti tra i nodi e ricalcola le rotte sulla base di queste informazioni. Questa estensione rompe la compatibilità con i demoni di routing che seguono la proposta INRIA. Il demone olsrd disponibile da olsr.org può essere configurato per comportarsi in ossequio alla proposta IETF che manca di questa caratteristica, ma non v'è ragione per disabilitare la Link Quality Extension, a meno che non sia espressamente richiesta la piena aderenza con le altre realizzazioni.

1.5.2 La Teoria

Dopo che il demone olsrd è stato attivato per un tempo adeguato, un nodo apprende dell'esistenza di ogni altro nodo nella nuvola di maglie, e riconosce anche quale nodo possa essere impiegato per indirizzargli il traffico. Ogni nodo mantiene aggiornata una tabella di routing che descrive l'intera nuvola di maglie. Questo approccio al mesh routing viene chiamato ***routing proattivo***. Al contrario, gli algoritmi di ***routing reattivo*** ricercano le rotte solo quando è necessario spedire dei dati verso un nodo specifico.

Ci sono vantaggi e svantaggi nel routing proattivo, e per realizzare il mesh routing ci sono molte altre impostazioni differenti, meritevoli di citazione. Il maggior vantaggio del routing proattivo risiede nel fatto che viene reso noto chi sia presente all'esterno e non si deve quindi aspettare che la rotta venga trovata. Tra gli svantaggi, ci sono il maggior sovraccarico di traffico ed il maggior carico sulla CPU. A Berlino, la comunità Freifunk impiega una nuvola di maglie dove olsrd deve gestire più di 100 interfacce. Il carico medio sulla CPU di un Linksys WRT54G a 200 MHz, causato da olsrd, è circa del 30%, nella rete di Berlino. C'è chiaramente un limite alla scalabilità di un protocollo proattivo, limite che dipende da quante interfacce siano coinvolte e da quanto frequentemente le tabelle di routing vengano aggiornate. Mantenere le rotte in una nuvola di maglie coon nodi statici richiede meno sforzo di quanto sia invece necessario in una maglia dove i nodi siano in costante movimento, poichè le tabelle di routing devono essere aggiornate con frequenza minore.

1.5.3 Il Meccanismo

Un nodo, su cui gira olsrd, diffonde periodicamente messaggi di 'hello' in modo che i propri vicini possano riconoscerne la presenza. Ogni nodo mantiene una statistica di quanti messaggi di 'hello' siano stati ricevuti o persi da parte di ognuno dei suoi vicini, riuscendo così a ricevare informazioni sulla topologia dei nodi vicini

e sulla qualità dei collegamenti. Le informazioni ricavate sulla tipologia sono poi diffuse via radio come messaggi di controllo della topologia (messaggi TC) ed inoltrati dai vicini che olsrd ha preventivamente eletto come relay multipunto.

Nel routing proattivo Il concetto di relay multipunto è un'idea nuova che è sorta con la bozza di OLSR. Se ogni nodo ridiffondesse via radio le informazioni di topologia che ha ricevuto, potrebbe generarsi un sovraccarico eccessivo nella rete. Queste trasmissioni sono ridondanti, se un nodo ha diversi vicini. Un nodo olsrd, allora, decide quali vicini siano relay multipunto favorevoli per inoltrare i propri messaggi di controllo della tipologia. Si noti che i relay multipunto sono scelti con l'unico scopo di inoltrare i messaggi TC. Il contenuto utile (*payload*) viene soggetto a routing che può coinvolgere ogni nodo disponibile.

Altri due tipi di messaggio sono presenti in OLSR per passare informazioni: se un nodo presenta un gateway ad altre reti (messaggi HNA) o se ha più interfacce (messaggi MID). Non c'è molto da dire su quale compito svolgano questi messaggi, a parte il fatto che esistono. I messaggi HNA rendono olsrd molto utile quanto si tratti di connettere Internet con un dispositivo mobile. Quando un nodo di maglia si sposta intorno, potrà riconoscere dei gateway nelle altre reti, e sceglierà sempre il gateway che presenta la rotta migliore. Comunque, olsrd non è assolutamente a prova di errore. Se un nodo dichiara di essere un gateway verso Internet - funzione che non ricopre. in realtà, perché non lo è mai stato o perché si trova disconnesso al momento - gli altri nodi presteranno fede all'affermazione. Il finto-gateway diventa un buco nero. Per superare questo problema, è stato scritto un plugin (modulo aggiuntivo) per il gateway dinamico. Il plugin nel gateway verificherà automaticamente se questi sia connesso e se il collegamento stia ancora in piedi. In caso negativo, l'olsrd terminerà di inviare falsi messaggi HNA. È fortemente raccomandato di inserire ed impiegare questo plugin, piuttosto che dare manualmente l'abilitazione all'invio di messaggi HNA.

1.5.4 In Pratica

Olsrd realizza il routing basato su IP con un'applicazione nello spazio-utente; l'installazione è quindi piuttosto semplice. I pacchetti per l'installazione sono disponibili per OpenWRT, Accesscube, Mac OS X, Debian GNU/Linux e Windows. OLSR è un componente standard di Metrix Pebble. Se si deve compilarlo dai sorgenti, occorre leggere la documentazione che è diffusa all'interno del pacchetto del sorgente. Se ogni cosa è configurata ammodo, tutto ciò che rimane da fare è l'avvio del programma olsr.

Prima di tutto, occorre assicurarsi che ogni nodo abbia un indirizzo IP, assegnato staticamente ed unico, per ogni interfaccia usata per la maglia. Non è raccomandato (né è praticabile) impiegare DHCP in una rete a maglia basata su IP. Una richiesta DHCP non verrà soddisfatta da un server DHCP se il nodo che la inoltra richiede più di un salto per essere raggiunto, ed inserire dei relay DHCP su una maglia è pressochè impraticabile. Questo problema potrebbe essere risolto usando IPv6, poichè in tal modo sarebbe disponibile uno spazio-indirizzi enorme per generare un indirizzo IP a partire dall'indirizzo MAC di ogni scheda coinvolta (come suggerisce in "IPv6 Stateless Address Autoconfiguration in large mobile ad hoc networks" di K. Weniger e M. Zitterbart, 2002).

Potrebbe servire allo scopo anche una pagina wiki, dove ogni persona interessata potrebbe scegliere un indirizzo IPv4 unico per ognuna delle interfacce sulle quali il demone olsr verrebbe fatto girare. In sintesi, non c'è una soluzione facile per rendere automatico tale processo, se si ricorre ad IPv4.

L'indirizzo di broadcast, per convenzione generale, dovrebbe essere 255.255.255.255 su interfacce che si affacciano sulla rete a maglia. Non c'è nessun motivo, per inserire esplicitamente l'indirizzo di broadcast, poichè olsrd può essere configurato per sostituire gli indirizzi di broadcast con tale valore predefinito. Occorre solo essere sicuri che tali impostazioni siano uniformi in ogni parte. Olsrd può raggiungere tale scopo da solo. Quando un file predefinito di configurazione di olsrd è distribuito, questa caratteristica dovrebbe essere abilitata per evitare confusione del tipo "perché gli altri nodi non riescono a vedere la mia macchina?!?"

Ora configuriamo l'interfaccia wireless. Di seguito un comando, come esempio di come configurare una scheda WiFi, con il nome wlan0, usando Linux:

```
iwconfig wlan0 essid olsr.org mode ad-hoc channel 10 rts 250 frag 256
```

Occorre verificare che la parte wireless della scheda WiFi sia stata configurata in modo che abbia una connessione ad-hoc verso gli altri nodi della maglia direttamente raggiungibili (nodi entro il singolo salto). Occorre anche assicurarsi che l'interfaccia si aggreghi allo stesso canale wireless, che usi lo stesso nome di rete wireless ESSID (Extended Service Set IDentifier) e che sia caratterizzato dallo stesso Cell-ID come tutte le altre schede WiFi che compongono la maglia. Molte schede WiFi, od i loro rispettivi driver, non si comportano in maniera conforme a quanto previsto dagli standard 802.11 per il networking ad-ho, e così può fallire miseramente il tentativo di connettersi ad una cella. Le stesse schede possono non essere in grado di connettersi ad altri dispositivi sullo stesso tavolo, anche se questi sono impostati con il corretto canale e nome di rete wireless.Queste schede possono, piuttosto, confondere altre schede che si comportano invece conformemente allo standard, creando il proprio indicativo di cella (Cell-ID) sullo stesso canale con lo stesso nome di rete wireless. Le schede WiFi costruite dall'Intel e che sono distribuite con i notebook Centrino sono famose per comportarsi in tale maniera.

È possibile verificare tutto con il comando **iwconfig**, quando si usa Linux. Di seguito, l'output che si ottiene sulla mia macchina.

```
wlan0 IEEE 802.11b· ESSID:"olsr.org" ¶
····· Mode:Ad-Hoc· Frequency:2.457 GHz· Cell: 02:00:81:1E:48:10 ¶
····· Bit Rate:2 Mb/s·· Sensitivity=1/3 ¶
····· Retry min limit:8·· RTS thr=250 B·· Fragment thr=256 B ¶
····· Encryption key:off ¶
····· Power Management:off ¶
····· Link Quality=1/70· Signal level=-92 dBm· Noise level=-100 dBm ¶
····· Rx invalid nwid:0· Rx invalid crypt:28· Rx invalid frag:0 ¶
····· Tx excessive retries:98024 Invalid misc:117503 Missed beacon:0 ¶
```

È importante impostare la soglia del 'Request To Send' (RTS) per una maglia. Ci saranno delle collisioni sul canale radio tra le trasmissioni dei nodi dello stesso canale radio, e l'RTS mitigherà tali effetti. RTS/CTS introduce un handshake prima di ogni pacchetto di trasmissione per sincerarsi che il canale sia chiaro. Si introduce del sovraccarico, ma si incrementano le prestazioni in caso di nodi nascosti - ed i nodi nascosti sono presenti per default sulla maglia! Questo parametro imposta la dimensione in Byte del più piccolo pacchetto per il quale il nodo spedisce l'RTS. La soglia RTS deve avere un valore minori della dimensione del pacchetto IP e il valore di 'soglia di frammentazione' - qui posto a 256 - altrimenti sarà disabilitato. Il TCP è molto sensibile alle collisioni, così è importante attivare l'RTS.

La frammentazione permette di spezzare un pacchetto IP in una serie di frammenti minori che vengono trasmessi sul medium. Tutto questo aggiunge sovraccarico, ma in un ambiente rumoroso ciò riduce il costo dell'errore e permette ai pacchetti di attraversare le scariche di rumore. Le reti a maglia sono molto rumorose perché i nodi impiegano lo stesso canale e, quindi, è probabile che le trasmissioni inteferiscano a vicenda. Questo parametro imposta la massima dimensione in byte che permetta la pacchetto di non essere spezzettato per poi essere recapitato a pezzi - un valore uguale alla massima dimensione IP disabilita il meccanismo, cos' dev'essere minore della dimensione del pacchetto IP. Impostare la soglia di frammentazione è raccomandato.

Una volta che sono stati assegnati un indirizzo IP valido ed una maschera di rete, una volta che l'interfaccia wireless sia attiva, il file di confifurazione di olsrd dev'essere alterato perché olsrd trovi ed impieghi le interfacce con le quali si intende farlo lavorare.

Per Mac OS-X e Windows è disponibile una simpatica GUI per configurare e controllare il demone disponibile. Sfortunatamente, questi tenta l'utente che manchi di competenze a commettere errori stupidi -

quali annunciare la presenza di un buco nero. Su BSD e Linux il file di configurazione è:

1.5.5 Un semplice file di configurazione olsrd.conf

Non verrà di seguito presentato un file di configurazione completo. Ci saranno invece alcune impostazioni essenziali che devono essere controllate.

```
UseHysteresis·········· no¶
TcRedundancy··········· 2¶
MprCoverage············ 3¶
LinkQualityLevel······· 2 ¶
LinkQualityWinSize····· 20¶
¶
LoadPlugin "olsrd_dyn_gw.so.0.3"¶
{¶
···· PlParam···· "Interval"·· "60"¶
···· PlParam···· "Ping"····· "151.1.1.1"¶
···· PlParam···· "Ping"····· "194.25.2.129"¶
}¶
¶
Interface "ath0" "wlan0" {¶
···· Ip4Broadcast 255.255.255.255¶
}¶
```

Ci sono molte altre opzioni disponibili nel **olsrd.conf**, ma queste opzioni base dovrebbero permettervi di iniziare. Dopo che questi passi sono stati completati, olsrd può essere avviato con un semplice comando all'interno di un terminale:

```
olsrd -d 2
```

Si raccomanda di lanciare il programma con l'opzione di debugging "-d 2", quando lo si usi su una workstation, specialmente se si tratta del primo avvio. Si può così osservare come si comporti olsrd e monitorare quale sia la qualità dei link con i vicini. Sui dispositivi embedded, invece, il livello di debug dovrebbe essere posto a zero (off), perché le operazioni di debugging caricano pesantemente la CPU.

I dati in uscita del debugging dovrebbero essere simili a questo:

```
--- 19:27:45.51 ------------------------------------------- DIJKSTRA¶
¶
192.168.120.1:1.00 (one-hop)¶
192.168.120.3:1.00 (one-hop)¶
¶
--- 19:27:45.51 ------------------------------------------------ LINKS¶
¶
IP address····· hyst·· LQ···· lost·· total· NLQ··· ETX¶
192.168.120.1··· 0.000· 1.000· 0····· 20···· 1.000· 1.00¶
192.168.120.3··· 0.000· 1.000· 0····· 20···· 1.000· 1.00¶
¶
--- 19:27:45.51 ---------------------------------------- NEIGHBORS¶
¶
```

```
IP address····· LQ···· NLQ··· SYM·· MPR·· MPRS· will¶
192.168.120.1··· 1.000· 1.000· YES·· NO··· YES·· 3¶
192.168.120.3··· 1.000· 1.000· YES·· NO··· YES·· 6¶
¶
--- 19:27:45.51 ------------------------------------------ TOPOLOGY¶
¶
Source IP addr·· Dest IP addr···· LQ···· ILQ··· ETX¶
192.168.120.1··· 192.168.120.17·· 1.000· 1.000· 1.00¶
192.168.120.3··· 192.168.120.17·· 1.000· 1.000· 1.00¶
```

1.5.6 Impiego di OLSR su Ethernet e su interfacce multiple

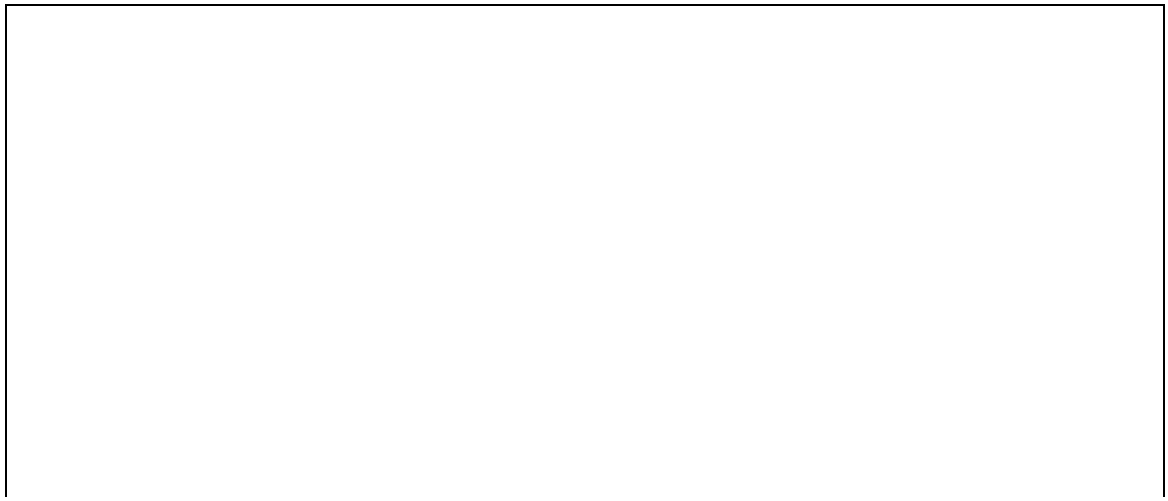
Non è necessario disporre di un'interfaccia wireless per provare od impiegare olsrd - sebbene sia per queste interfacce che olsrd è stato progettato. Olsrd può essere benissimo impiegato su qualsiasi NIC (scheda di rete). Le interfacce WiFi non necessariamente devono operare in modo ad-hoc per formare una maglia quando i nodi dispongano di più di una interfaccia. Per dei collegamenti dedicati potrebbe essere un'interessante opzione mantenerli attivi in Infrastructure Mode. Molte schede WiFi posseggono driver che presentano problemi in Ad-hoc Mode, ma l'Infrastructure Mode funziona bene - perché tutti si aspettano che almeno questa prestazione sia garantita. Il modo ad-hoc non è così popolare, così la realizzazione di un modo ad-hoc è sempre stata trascurata da molti produttori. Con la crescente attenzione alle reti a maglia, la situazione dei driver sta ora migliorando.

Molte persone usano olsrd su interfacce wireless ed altre cablate, non hanno bisgono di tenere conto dell'architettura della rete. Si limitano a collegare antenne alle loro schede WiFi, collegare cavi alle loro schede Ethernet, abilitare olsrd ad essere lanciato su tutti i computer e su tutte le interfacce e quindi danno il via al tutto. Tutto ciò è piuttosto un abusare di un protocollo che era stato concepito per permettere il wireless networking su link con perdite, ma perché impedirlo?

Ci si aspetta che olsrd sia un sovra-protocollo. Chiaramente non è necessario inviare un messaggio di Hello su un'interfaccia ogni due secondi, ma funziona. Questo comportamento non dev'essere assunto come raccomandazione, è solo incredibile cosa facciano le persone di questo protocollo, ed hanno successo. Infatti è entusiasmante l'idea di mettere a disposizione un protocollo che risolva tutto per dei principianti che desiderino reti LAN di dimensioni medio-piccole.

1.5.7 Plugin

Diversi plugin sono disponibili per olsrd. Si veda sul sito olsr.org per una lista completa. Di seguito, una breve HOW-TO per il plugin che visualizza la topologia di una rete.



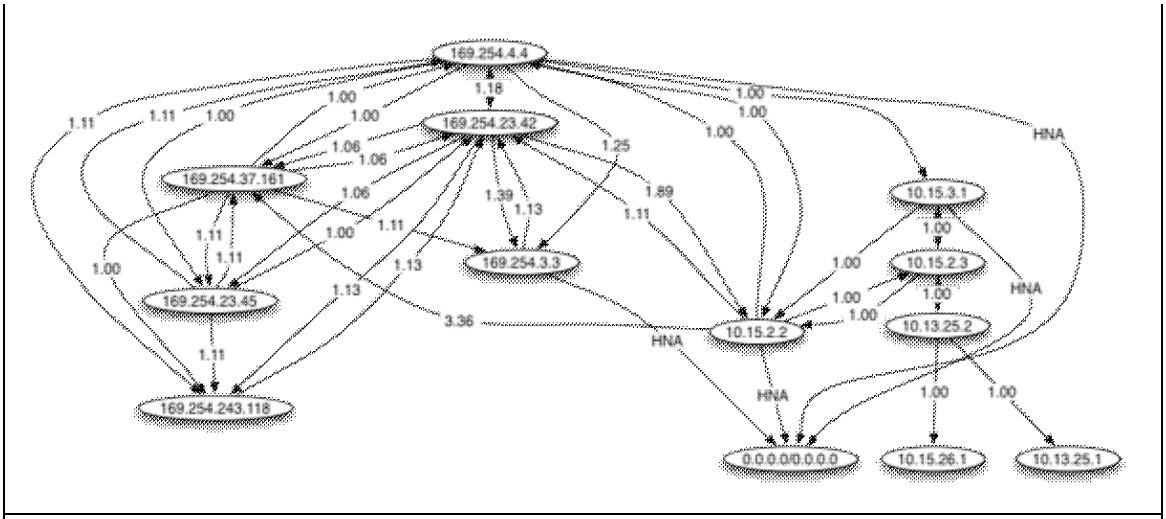


Figura 3.8: Una topologia di rete OLSR generata automaticamente.

Spesso, per la comprensione di una rete a maglia, è molto utile riuscire ad esibirne la topologia di rete in modo grafico. Olsrd_dot_draw presenta come risultato la tipologia nel formato "dot file" sulla porta 2004 in TCP. Gli strumenti graphviz possono quindi essere impiegati per tracciarne i grafici.

1.5.8 Installare il plugin dot_draw

Si compilino i plugin olsr separatamente e li si installi. Per caricare il plugin, aggiungere la seguente riga al file **/etc/olsrd.conf**

```
LoadPlugin "olsrd_dot_draw.so.0.3"¶
{¶
····· PlParam "accept" "192.168.0.5"¶
····· PlParam "port" "2004"¶
}¶
```

Il parametro "accept" specifica quale macchina sia abilitata a visualizzare le informazioni della topologia (al momento, solo una) e, di default, è impostato "localhost".

Far ripartire olsr e verificare se si ottenga output sulla porta TCP 2004

```
telnet localhost 2004
```

Dopo un certo periodo, si dovrebbe ottenere del testo come risultato.

Si può allora salvare l'output delle descrizioni grafiche e lanciare i tool **`dot`** o **`neato`** dal pacchetto graphviz, al fine di ottenere le immagini.

Bruno Randolf ha scritto un breve script perl che richiede periodicamente le informazioni di topologia da olsrd e le visualizza impiegando gli strumenti di graphviz e di ImageMagick.

Per prima cosa, si installino sulla workstation i seguenti pacchetti:

- graphviz, http://www.graphviz.org/
- ImageMagick, http://www.imagemagick.org/

Si scarichi lo script da: http://meshcube.org/nylon/utils/olsr-topology-view.pl

Ora è possibile lanciare lo script con il comando: **`./olsr-topology-view.pl`** , e vedere così gli aggiornamenti della topologia in tempo quasi-reale.

1.5.9 Risoluzione dei malfunzionamenti

Fintantochè le schede WiFi riescono a 'vedersi' una con l'altra tramite collegamenti radio, la richiesta di un ping funzionerà, a prescindere dall'esecuzione di olsrd. Ciò succede perché le ampie netmask rendono effettivamente ogni nodo su un link-local, sì da accantonare qualsiasi problema di routing già con il primo hop. È la prima cosa che si dovrebbe controllare se il comportamento della rete non sia quello aspettato. Gran parte dei malditesta che vengono forniti dalle schede WiFi nella modalità Ad-Hoc sono causati dal fatto che i driver per il modo Ad-Hoc sono realizzati in modo approssimativo. Se non è possibile ottenere il ping diretto con i nodi in visibilità, si tratta probabilmente di un problema di scheda e driver, od, in alternativa, sono errati i parametri di impostazione della rete.

Se le macchine possono ottenere il ping una dall'altra, ma olsrd non riesce a ricavare le rotte, allora dovrebbero essere ricontrollati gli indirizzi IP, la netmask ed il broadcast.

È forse in azione un firewall? Verificare che non intercetti la porta UDP 698.

Buon divertimento!

1.6 Stima della Capacità

I collegamenti wireless possono assicurare agli utenti un ***throughput*** maggiore, rispetto alle tradizionali connessioni ad Internet, quali la VSAT, la linea telefonica o la DSL. Il Throughput è altrimento denominato ***capacità del canale***, o semplicemente ***larghezza di banda*** (sebbene tale termine non abbia attinenza con la larghezza di banda radio). È importante comprendere che la velocità dichiarata di un dispositivo wireless (il ***data rate***) indica la velocità alla quale questi riesce a comunicare simboli via radio, non l'effettivo throughput che potrà essere osservato in pratica. Come accennato in precedenza, un singolo collegamento 802.11g può raggiungere i 54Mbps via radio, ma assicurerà un throighput effettivo fino a 22Mbps; il resto è sovraccarico che le radio impiegano per coordinare il proprio segnale usando il protocollo 802.11g.

Si noti che il throughput è una misura di bit sul tempo. 22Mbps significa che, in un qualsiasi secondo, 22 megabit possono essere inviati da un capo del collegamento all'altro. Se l'utente tenta di spingervi più di 22 megabit, l'operazione richiederà un tempo maggiore di un secondo. Poichè non possono essere inviati immediatamente, i dati vengono inseriti in una ***coda***, per poi essere trasmessi il più presto possibile. Questo accodamento di dati allunga i tempi necessari perché l'ultimo bit inserito in coda possa attraversare il collegamento. Il tempo che si rende necessario per l'attraversamento del collegamento è chiamato ***latenza***, ed una latenza più pesante è chiamata ***ritardo***. Il collegamento potrà anche trasferire tutto il traffico accodato, ma chi lo riceve potrà lamentare un incremento del ritardo.

Quale troughput sarà richiesto per i vostri utenti? Dipende da quanti essi siano, e da come intendano impiegare il collegamento wireless. Applicazioni diverse di Internet richiedono valori diversi di throughput.

Applicazione	**BW / Utente**	**Note**
Messaggi di Testo / IM	< 1 Kbps	Poichè il traffico è rado ed asincrono, IM accetterà alta latenza.
Posta Elettronica	da 1 a 100 Kbps	Come per IM, la posta elettronica è asincrona ed intermittente, quindi ammetterà latenza. Allegati pesanti, virus e spam incrementano sensibilmente l'impiego di banda. Si noti come i servizi di posta elettronica via web (come Yahoo ed Hotmail) debbano essere

		considerati navigazione sul web, piuttosto che posta elettronica.
Navigazione web	50 - 100+ Kbps	I Web browser impiegano la rete solo quando richiedono dati. La comunicazione è asincrona, quindi un sensibile ritardo può essere accettato. Quando i browser richiedono più dati (immagini di grandi dimensioni, download pesanti, etc.), l'impiego di banda s'innalzerà in maniera significativa..
Streaming audio	96 - 160 Kbps	Ogni utente di un servizio di streaming audio service impiegherà una relativamente ampia larghezza di banda in modo costante, fintantochè trasferisce audio. Il servizio può accettare una latenza occasionale, impiegando dei buffer ampi presso i partecipanti. Periodi più lunghi di ritardo causeranno invece degli "slittamenti" dell'audio, se non addirittura la caduta della sessione.
Voice over IP (VoIP)	24 - 100+ Kbps	Come nello streaming audio, il VoIP richiede una quantità costante di banda per ciascuno degli utente per la dirata della chiamata, ma tale quantità di banda è pressochè equivalente nelle due direzioni del collegamento. La latenza su una connessione VoIP è avvertita immediatamente e disturba l'impiego. Ritardi superiori a pochi millisecondi sono inaccettabili per il VoIP..
Streaming video	64 - 200+ Kbps	Come per lo streming audio, l'occasionale latenza è evitata ricorrendo all'uso di buffer sugli utenti. Per funzionare con buona qualità, lo streaming video richiede alto throughput e bassa latenza.
Applicazioni peer-to-peer per il filesharing (BitTorrent, KaZaA, Gnutella, eDonkey, etc.)	0 - infiniti Mbps	Se pure accettano valori arbitrari di latenza, le applicazioni peer-to-peer tendono a saturare tutto il throughput disponibile trasmettendo dati a quanti più utenti possibile, quanto più in fretta possibile. L'impiego di queste applicazioni sarà causa di ritardo e problemi di throughput per tutti gli altri utenti della rete, a meno che non si adottino attente allocazioni di banda.

Per valutare il throughput necessario per la rete, si moltiplichi il numero di utenti previsti per l'applicazione che verrà presumibilmente richiesta. Per esempio, 50 utenti interessati prevalentemente alla navigazione web consumeranno presumibilmente 2.5 Mbps di throughput, o qualcosa di più nei momenti di punta, ed accetteranno una discreta latenza. Al contrario, 50 utenti VoIP che lavorino nello stesso momento richiederanno almeno 5Mbps di throughput **in entrambe le direzioni** con assolutamente nessuna latenza. Dal momento che gli apparati wireless 802.11g sono ***half-duplex*** (possono, cioè, alternativamente trasmettere o ricevere, ma non possono compiere le due azioni nello stesso momento), occorrerà di conseguenza raddoppiare il throughput richiesto, per un totale di **10Mbps**. I collegamenti wireless dovranno garantire tale capacità ogni secondo, o la conversazione soffrirà di ritardi.

Poichè sarà improbabile che tutti gli utilizzatori richiedano la connessione precisamente nello stesso momento, si ricorre comunemente alla pratica detta della ***sovriscrizione*** (permettendo, cioè, più utenti di quanto la banda massima possa sostenere). Una sovriscrizione di un fattore da 2 a 5 è piuttosto comune. Con tutta probabilità, la sovriscrizione verrà impiegata nella fase di costruzione dell'infrastruttura di rete. Attraverso l'attenta osservazione del throughput sulla rete, sarà poi possibile pianificare quando incrementare vari segmenti della rete, e quante risorse supplementari siano necessarie.

Per quanta capacità verrà fornita, gli utenti troveranno alla fine delle applicazioni che la satureranno. Come si vedrà alla fine di questo capitolo, impiegare tecniche di *bandwith shaping* (allocazione di banda) può contribuire a ridurre i problemi di latenza. Ricorrendo al bandwith shaping, al web caching ed ad altre tecniche, si possono ridurre significatamente i valori di latenza, migliorando il throughput complessivo della rete.

Per avere un'idea del ritardo avvertito su connessioni molto lente, l'ICTP ha realizzato un simulatore di larghezza di banda. Questo simulatore provvederà a scaricare una pagina web, impiegando la massima

velocità e la velocità ridotta secondo le impostazioni che si sceglieranno. Questa dimostrazione offre un'immediata comprensione di come l'utilità di Internet, come strumento di comunicazione, venga ridotta da basso throughput e da alta latenza. Il simulatore è disponibile sotto http://wireless.ictp.trieste.it/simulator/

1.7 Pianificazione del Collegamento

Un sistema di comunicazione base consiste di due radio, ciascuna con la propria antenna, che sono separate dal percorso che dev'essere coperto. Per poter instaurare una comunicazione, le due radio richiedono un segnale minimo che raggiunga le antenne e che venga quindi presentato ai loro ingressi. La determinazione della fattibilità del collegamento è un processo chiamato calcolo del ***link budget***. Se i segnali possano o meno essere scambiati tra le radio dipende dalla qualità dell'attrezzatura usata e dal degrado del segnale dovuto dalla distanza, degrado chimato ***path loss*** (perdita di percorso).

1.7.1 Calcolare il link budget

La potenza disponibile in un sistema 802.11 può essere caratterizzata dai due seguenti fattori:

- ***Potenza di Trasmissione***. È espressa in milliwatt o in dBm. La potenza di trasmissione varia dai 30mW ai 200mW o più. La potenza di trasmissione è spesso dipendente dalla velocità della trasmissione stessa. La potenza di trasmissione di un particolare dispositivo dovrebbe essere esplicitata dalla documentazione fornita dal produttore, ma può essere difficile da trovare. Può allora essere d'aiuto la consultazione di database disponibili online, quali quello offerto da Seattle Wireless (http://www.seattlewireless.net/HardwareComparison).
- ***Guadagno d'Antenna***. Le antenne sono dispositivi passivi che amplificano il segnale ricevuto grazie alla loro forma fisica. Le antenne presentano la stessa caratteristica in trasmissione ed in ricezione. Un'antenna da 12 dB è tale senza dover specificare se sia in modalità di ricezione o di trasmissione. Le antenne paraboliche presentano un guadagno di 19-24 dB, le antenne omnidirezionali di 5-12 dB, quelle settoriali di 12-15 dB.
- ***Livello minimo di Segnale ricevuto*** o, semplicemente, la sensibilità del ricevitore. Il minimo RSL (*Received Signal Level*, livello di segnale ricevuto) è sempre espresso in debibel negativi (- dBm) ed è la minima potenza di segnale che la radio riesce a distinguere. Il minimo RSL dipende dalla velocità, e come regola generale la velocità trasmissiva più bassa (1 Mbps) garantisce la sensibilità massima. Tale minimo è, tipicamente, compreso tra i -75 e -95 dBm. Come per la potenza di trasmissione, il dettaglio del RSL dovrebbe essere specificato dal produttore dell'apparato.
- ***Perdite di Cavo***. Parte dell'energia del segnale è persa nei cavi, nei connettori ed in altri dispositivi, presenti nel tratto tra l'antenna e la radio. La perdita dipende dal tipo di cavo usato e dalla sua lunghezza. La perdita di segnale per cavi coassiali corti, che includano i connettori, è relativamente bassa, compresa tra i valori di 2-3 dB. È opportuna mantenere i cavi tra antenna e radio i più corti possibili.

Quando si calcola la perdita di percorso, diversi fattori devono essere considerati. Occorre mettere in conto la ***perdita nello spazio libero***, la ***attenuazione*** e lo ***scattering***. La potenza del segnale si riduce a causa della diffusione geometrica del fronte d'onda, comunemente conosciuta come perdita nello spazio libero. Trascurando il resto, più lontano sono le due radio, minore sarà il segnale ricevuto, a causa delle perdite in spazio libero. Tutto ciò è indipendente dall'ambiente circostante, ma è legato alla sola distanza. Questa perdita si genera perché l'energia del segnale irradiato si espande secondo una funzione della distanza dal trasmettitore.

Impiegando i decibel per esprimere la perdita, ed adottando i 2.45 GHz come frequenza di ricetrasmissione, l'equazione per la perdita in spazio libero diventa:

```
Lfsl = 40 + 20*log(r)
```

dove Lfsl (attenuazione in spazio libero) è espressa in dB ed r è la distanza tra il trasmettitore ed il ricevitore, espressa in metri.

Il secondo contributo alla perdita sul percorso è dato dall'attenuazione, ovvero dall'assorbimento di parte di potenza del segnale nell'attraversamento di ostacoli quali alberi, mura, finestre e pavimenti di edifici. L'attenuazione può variare in modo pesante, dipendendo dalla struttura degli oggetti che il segnale attraversa, ed è di difficile quantificarla. Il modo più semplice per esprimere questo contributo alla perdita totale è quello di aggiungere una "perdita ammissibile" alla perdita in spazio libero. Per esempio, l'esperienza indica che gli alberi aggiungono un 10-20 dB di perdita per albero presente sul percorso, mentre i muri contribuiscono per 10-15 dB, in funzione della costruzione.

Sul percorso del collegamento, l'energia RF (Radio-Frequenza) lascia l'antenna trasmittente e si espande. Parte di questa energia raggiunge direttamente l'antenna ricevente, mentre altra vi arriva dopo essere rimbalzata sul terreno. Questo segnale riflesso, avendo percorso un tragitto più lungo di quello diretto, arriva all'antenna ricevente in ritardo, interferendo con il segnale principale. Questo effetto è chiamato ***multipath***, fading o dispersione di segnale. In alcuni casi i segnali riflessi si sommano assieme e non causano problemi. Quando si sommano fuori fase, il segnale ricevuto è trascurabile. Ciò viene denominato ***nulling***. Esiste una semplice tecnica per trattare il multipath, chiamata ***diversità d'antenna*** (*antenna diversity*): consiste nel dotare la radio di una seconda antenna. Il multipath è infatti un fenomeno fortemente legato al percorso. Se due segnali si annullano in fase in un punto, non si sommeranno distruttivamente in un secondo punto, vicino al primo. Se sono presenti due antenne, almeno una di quete dovrebbe essere in grado di ricevere un segnale utile, anche se l'altra sta ricevendo un segnale distorto. Nei dispositivi commerciali, viene impiegato la diversità d'antenna che ne attiva l'una o l'altra. Il segnale è così ricevuto solo da un'antenna per volta. Quanto trasmette, la radio usa l'antenna che è stata impiegata per ultima nella ricezione. La distorsione causata dal multipath riduce la capacità del ricevitore di ricostruire il segnale in una modo simile alla perdita di segnale. Un modo semplice per inserire gli effetti dello scattering nel calcolo delle perdite di percorso è di cambiare l'esponente del fattore distanza nella formula della perdita in spazio libero. L'esponente tende ad incrementare con il percorso in un ambiente con pesante scattering. Un 3 come esponente può essere usato in un ambiente esterno con alberi, mentre un 4 come esponente è impiegabile per un ambiente interno.

Quando si considerano assieme le perdite di spazio libero, l'attenuazione e lo scattering, la perdita di percorso è:

```
L(dB) = 40 + 10*n*log(r) + L(allowed)
```

Per una valutazione speditiva della fattibilità del collegamento, ci si può limitare a stimare la sola perdita in spazio libero. L'ambiente può apportare ulteriori perdite di segnale, e dovrebbe essere considerato per una valutazione esatta del collegamento. L'ambiente è in effetti un elemento importante, che che non dovrebbe mai essere trascurato.

Per valutare se un collegamento sia possibile, si dovrebbero conoscere le caratteristiche del materiale che viene usato e si dovrebbe stimare la perdita di percorso. Si noti che, nel condurre tale calcolo, si debba solo aggiungere la potenza di trasmissione da un capo del collegamento. Se si impiegano radio differenti nei due estremi del collegamento, occorre calcolare due vole la perdita sul percorso, una per ogni direzione, impiegando la corretta potenza di trasmissione per ognuno dei due calcoli. Aggiungendo tutti i guadagni e sottraendo tutte le perdite porta a:

```
·· Potenza di Trasmissione della Radio 1¶
+ Guadagno d'Antenna della Radio 1¶
- Perdite di Cavo della Radio 1¶
+ Guadagno d'Antenna della Radio 2¶
- Perdite di Cavo della Radio 2¶
```

```
------------------------¶
···· = Guadagno Totale¶
```

Sottraendo le perdite di percorso al guadagno totale:

```
·············· Guadagno Totale¶
············· – Perdite di Percorso¶
··········· ––––––––––––––¶
= Livello di segnale ad un capo del collegamento (al ricevitore della
Radio 2)¶
```

Se il livello di segnale che si ottiene è maggiore del minimo livello di segnale ricevuto, allora il collegamento è fattibile! Il segnale ricevuto è sufficientemente potente per le radio da poter essere usato. Si ricordi che il minimo RSL è sempre espresso in decibel negativi, quindi -56dBm è migliore di -70dBm. Su un dato percorso, la variazione nelle perdite di percorso nel tempo può essere rimarchevole, quindi un certo margine di sicurezza (divverenza tra il livello di segnale ed il minimo livello di segnale ricevuto) dovrebbe essere considerato. Questo margine è la quantità di segnale che, superando la sensibilità della radio, dev'essere ricevuta per garantire un collegamento stabile e di buona qualità anche sotto cattive condizioni meteorologiche o durante altri disturbi atmosferici. Un margine d'errore di 10-15 dB può andar bene. Per garantire spazio all'attenuazione ed al multipath nel segnale ricevuto, un margine di 20dB dovrebbe essere sufficiente.

Una volta che si sia calcolato il link budget verso una direzione, occorre ripetere il calcolo nella direzione opporta. Si sostituisca la potenza di trasmissione della seconda radio, e si verifichino i risultati verso il minimo livello di segnale ricevuto della prima radio.

1.7.2 Esempio di Calcolo di link budget

Come esempio, si intenda stimare la fattibilità di un collegamento di 5km, con un access point ed una radio come client. L'access point è connesso ad un'antenna omnidirezionale che ha un guadagno di 10 dBi, mentre il client è connesso ad un'antenna settoriale con guadagno 14dBi. La potenza di trasmissione dell'access point è di 100mW (ovvero, 20dBm), mentre la sua sensibilità è di -89dBm. Per il client, la potenza di trasmissione è di 30mW (o 15dBm) e la sua sensibilità è di -82 dBm. I cavi di connessione tra antenne e radio sono brevi, con una perdita di 2dB a ciascun lato del collegamento radio.

Sommando tra loro tutti i guadagni e sottraendo tutte le perdite nel collegamento tra AP e client, si ottiene:

```
+ 10 dBi (Guadagno d'Antenna della Radio 1)¶
–· 2 dB· (Perdita nel Cavo d'Antenna della Radio 1)¶
+ 14 dBi (Guadagno d'Antenna della Radio 2)¶
–· 2 dB· (Perdita nel Cavo d'Antenna della Radio 2)¶
––––––––––––––––––––––––––––––¶
20 dB = Guadagno Totale¶
```

Trasmettendo quindi una potenza di 20dBm sull'AP, sul client radio - a distanza nulla dall'AP - si riceverebbero un segnale di potenza:

```
+ 20dBm¶
+ 20dB ¶
```

```
---------------------------------- ¶
40dBm = Potenza Segnale Ricevuto a Distanza Nulla (Prx0)¶
```

Considerando come il client radio non sia a distanza nulla dall'AP, occorrerà inserire la Perdita di Percorso che, su un collegamento di 5km dove si considera il solo spazio libero, sarà:

```
Perdita di Percorso(dB) = 40 + 20log(5000) = 113 dB
```

Sottraendo la Perdita di Percorso dalla Potenza del Segnale Ricevuto a Distanza Nulla si ottiene:

```
40 dBm - 113 dB = -73 dBm
```

Poichè -73dBm è una potenza magggiore della sensibilità della radio client (-82dBm), il livello di segnale è sufficiente alla radio client per raccogliere la trasmissione dell'access point. Rimangono 9dB di margine (-73dBm - -82dBm) che consentiranno un funzionamento dignitoso quando sia bel tempo, ma che potrebbero rivelarsi insufficienti in caso di avverse condi-meteo.

Si calcoli ora il collegamento nella direzione che parte dal client e prosegue verso l'access point:

```
·· 15 dBm (Potenza di Trasmissione della Radio 2)¶
+ 14 dB· (Guadagno d'Antenna della Radio 2)¶
-· 2 dB· (Perdita nel Cavo d'Antenna della Radio 2)¶
+ 10 dB· (Guadagno d'Antenna della Radio 1)¶
-· 2 dB· (Perdita nel Cavo della Radio 1)¶
---------------------------------¶
····· 35 dBm = Potenza del Segnale Ricevuto a Distanza Nulla (Prx0)¶
```

Naturalmente, la Perdita di Percorso è la stessa sul viaggio di ritorno. Il segnale ricevuto sull'access point diventa quindi: Obviously, the path loss is the same on the return trip. So our received signal level on the access point side is:

```
35 dBm - 113 dB = -78 dBm Potenza del Segnale Ricevuto presso l'AP
```

Poichè la sensibilità dell'AP è -89dBm, 11dB sono garantiti come margine (-78dBm - -89dBm). Nel complesso, questo collegamento dovrebbe funzionare, ma si potrebbe puntare ad aumentare il margine di sicurezza del guadagno. Usando un'antenna a parabola (*dish antenna*) a 24dB sul lato client, piuttosto che l'antenna settoriale a 14dB, si otterrebbe un incremento del guadagno di 10dB in entrambe le direzioni del collegamento (si ricordi, infatti, come il guadagno d'antenna sia lo stesso sia in ricezione, che in trasmissione). Un'opzione più costosa potrebbe essere quella di impiegare radio con maggiore potenza ad entrambi i lati del collegamento, ma si osservi come l'aggiunta di un amplificatore, o l'impiego di una scheda radio di maggior potenza, ad un solo lato del collegmamento non ne migliori la qualità complessiva.

Strumenti disponibili online possono essere impiegati per calcolare il link budget. Per esempio, il *Green Bay Professional Packet Radio's Wireless Network Link Analysis* (http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi) è uno strumento eccellente. La *Super Edition* genera un file PDF che contiene la zona di Fresnel ed i grafici dei percorsi radio. Gli script di calcolo possono

essere scaricati dal sito web ed essere installati sul proprio computer. Si approfondirà l'argomento di un eccellente strumento online nella prossima sezione, *Software per la Pianificazione del Collegamento*).

Anche il sito web Terabeam dispone di un eccellente calcolatore, disponibile online (http://www.terabeam.com/support/calculations/index.php).

1.7.3 Tavole per il Calcolo del Link Budget

Per calcolare il link budget, si approssimi semplicemente la distanza, quindi si ricorra alla tavola seguente:

1.7.3.1 Perdita in Spazio Libero a 2.4GHz

Distanza (m)	100	500	1,000	3,000	5,000	10,000
Perdita (dB)	80	94	100	110	113	120

1.7.3.2 Guadagno d'Antenna Totale:

Guadagno d'Antenna Radio 1 (dB)	+ Guadagno d'Antenna Radio 2 (dB)	= Guadagno Totale d'Antenna
_	_	_

1.7.3.3 Perdite:

Perdita del Cavo d'Antenna sulla Radio 1 (dB)	Perdita del Cavo d'Antenna sulla Radio 2 (dB)	Perdita in Spazio Libero (dB)	= Perdita Totale (dB)
_	_	_	_

1.7.3.4 Link Budget per collegamento Radio 1 -> Radio 2:

Potenza TX Radio 1 (dBm)	+ Guadagno Totale d'Antenna Antenna (dB)	- Perdita Totale (dB)	= Potenza del Segnale Ricevuto (dBm)	> Sensibilità della Radio 2(dBm)
_	_	_	_	_

1.7.3.5 Link Budget per collegamento Radio 2 -> Radio 1:

Potenza TX Radio 2 (dBm)	+ Guadagno Totale d'Antenna Antenna (dB)	- Perdita Totale (dB)	= Potenza del Segnale Ricevuto (dBm)	> Sensibilità della Radio 1(dBm)
_	_	_	_	_

Se il segnale ricevuto è maggiore della sensibilità in entrambe le direzioni del collegamento, il collegamento è fattibile.

1.7.4 Software per la Pianificazione del Collegamento

Se il calcolo a mano del link budget è impegnativo, ci sono diversi strumenti a disposizione che possono contribuire ad automatizzare il processo. Oltre a calcolare la Perdita in Spazio Libero, questi strumenti tengono anche conto di diversi altri rilevanti fattori (come assorbimento per gli alberi, effetti del terreno, clima, ed addirittura stime di perdita di percorso in tratte urbane). In questa sezione, si discuterà di due strumenti liberi che sono utili per pianificare collegamenti wireless: le utility per la progettazione interattiva della rete online Green Bay Professional Packet Radio e Radop,pboòe-

1.7.4.1 CGI per il Progetto interattivo

Il *Green Bay Professional Packet Radio group* (GBPRR) ha realizzato diversi strumenti decisamente utili per pianificare i collegamenti, ponendoli poi gratuitamente a disposizione online. Si possono ricercare sotto http://www.qsl.net/n9zia/wireless/page09.html . Poichè sono su Internet, questi strumenti richiederanno per funzionare il semplice impiego di un navigatore che disponga di accesso ad Internet.

Si esaminerà ora il primo strumento di lavoro, il **Wireless Network Link Analysis**. È reperibile online presso: http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi .

Per iniziare, si inserisca il canale che dev'essere impiegato nel collegamento. Il canale può essere descritto in MHz o GHz. Se la frequenza non è nota, si consulti la tabella in Appendice B. Si osservi come la tabella riporti la frequenza centrale di ogni canale, mentre lo strumento richiede la massima frequenza trasmessa. Per ricavare la massima frequenza trasmessa per un canale, basta addizionare 11MHz alla frequenza centrale.

Quindi, si proceda con i dettagli del lato trasmettitore del collegamento, comprendendo il tipo di linea trasmissiva, il guadagno d'antenna, ed altri particolari. Si cerchi di inserire quanti più dati sia possibile, provvedendo eventualmente a stimarli. Si possono inserire anche l'altezza dell'antenna e l'elevazione del sito: questi dati verranno usati per determinare l'angolo di elevazione dell'antenna. Per ricavare la zona libera di Fresnel, sarà necessario usare il calcolatore della zona di Fresnel del GBPRR.

La sezione successiva è molto simile, e si riferisce all'altro capo del collegamento. Si inseriscano tutti i dati nei campi relativi.

Per finire, l'ultima sezione descrive il clima, il terreno e la distanza del collegamento. Si inseriscano più dati possibili, provvedendo eventualmente a stimarli. La distanza di collegamento può essere calcolata specificando la latitudine e la longitudine di entrami i siti, oppure può essere inserita direttamente a mano.

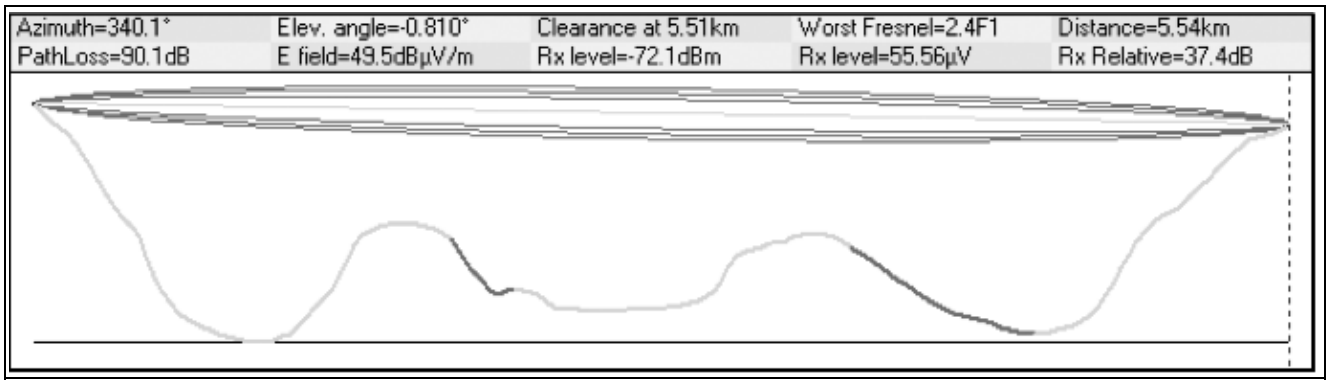
Ora, si clicchi sul bottone *Submit* per ottenere un resoconto dettagliato sul link proposto. Questo resoconto include tutti i dati inseriti, così come la perdita di percorso previsto, l'incidenza di errori (*error rate*) ed il periodo di operatività (*uptime*). Questi numeri sono tutti completamente teorici, ma possono offrire un'idea della fattibilità del link. Giocando con i valori inseriti in ingresso, si può provare un "cosa-succede-se", per vedere come la variazione dei parametri influirà sulla connessione.

Oltre allo strumento base per l'analisi del collegamento, GBPRR fornisce "un'edizione speciale" che fornirà anche un resoconto in PDF, come pure un numero di altri strumenti molto utili (compreso il calcolatore della zona di Fresnel, il calcolatore delle Distanze & Angoli di Brandeggio, il calcolatore per la conversione in Decibel, giusto per citarne qualcuno). Viene anche fornito il codice sorgente di gran parte di questi strumenti.

1.7.4.2 RadioMobile

Radio Mobile è uno strumento di progetto e simulazione di sistemi wireless. Stima le prestazioni di un collegamento radio impiegando le informazioni disponibili sul materiale e su una mappa digitale dell'area. È un programma sotto licenza "public domain" che gira sotto Windows, o sotto Linux con l'impiego delle API di Wine.

Radio Mobile usa un ***modello digitale del rilievo del terreno*** per il calcolo della copertura, indicando la potenza del segnale ricevuto su vari punti lungo il percorso. Costruisce automaticamente un profilo tra due punti sulla mappa digitale, mostrando l'area di copertura e la prima zona di Fresnel. Nella simulazione, controlla la linea di vista e calcola la Perdita di Percorso, includendo le perdite dovute ad ostacoli. È possibile creare reti di tipologie differenti, comprese le reti master/slave, le punto-punto e le punto-multipunto.



Il software calcola l'area di copertura dalla stazione base in un sistema punto-multipunto. Funziona per sistemi che siano caratterizzati da una frequenza di lavoro dai 20 kHz ai 200 GHz. Le ***Mappe digitali di Rilievo*** (DEM, *Digital Elevation Map*) sono liberamente disponibili da differenti fonti, e sono disponibili per gran parte del mondo. Le DEM non mostrano la linea di costa od altri punti cospicui, rapidamente riconoscibili, ma possono facilmente essere combinate con altri tipi di informazione (quali foto aere, o carte topografiche) su strati differenti, per ottenere una rappresentazione più utile ed immediatamente riconoscibile. Si possono digitalizzare le proprie mappe e combinarle con le DEM. Le mappe digitali di rilievo possono essere combinate con le mappe ottenute dallo scanner, dalle foto satellitari e con i servizi cartografici su Internet (come Mapquest) per costruire dei diagrammi di predizione.

Radio Mobile può essere scaricato da qui: http://www.cplus.org/rmw/download.html

La pagina principale del sito Radio Mobile, con esempi e tutorial, è disponibile sotto: http://www.cplus.org/rmw/english1.html

1.7.4.3 RadioMobile e Linux

Radio Mobile gira anche impiegando Wine con Ubuntu Linux. Mentre l'applicazione funziona, alcuni bottoni possono apparire fuori della propria posizione e possono quindi essere difficili da leggere.

A noi è riuscito far funzionare Radio Mobile con Linux impiegando il seguente ambiente:

- IBM Thinkpad x31
- Ubuntu Breezy (v5.10), http://www.ubuntu.com/
- Wine version 20050725, dall**Ubuntu Universe repository**

Informazioni dettagliate su come installare Radio Mobile su Wine sono disponibili sotto http://www.cplus.org/rmw/download.html. Sono da seguire tutti i passaggi, ad eccezione del passo 1 (poichè risulta difficile estrarre una libreria DLL dal file VBRUN60SP6.EXE sotto Linux). Si potrà ricorrere od alla copia del file MSVBVM60.DLL da una macchina Windows, che già abbia installato l'ambiente run-time di Visual Basic 6, od allo scarico del file da Internet, dopo aver cercato MSVBVM60.DLL con Google.

Si riprenda quindi dal passo 2 dell'URL sopra riportata, assicurandosi di scompattare il file scaricato nella stessa directory nella quale è stato posto il file DLL scaricato. Si osservi come non occorra poi preoccuparsi delle prescrizioni che seguono il passo 4; sono fasi successive che sono necessarie solo per utenti Windows.

Alla fine, si può lanciare Wine da un terminale con il comando:

```
# wine RMWDLX.exe
```

A questo punto, si dovrebbe vedere Radio Mobile che funziona nella sessione X Windows.

1.7.5 Eliminare il Rumore

Le bande U-NII e ISM - non soggette a licenza - rappresentano un segmento molto limitato dello spettro elettromagnetico conosciuto. Dato che tale regione può essere impiegata senza corrispondere pagamenti di licenza, molti dispositivi di consumo la impiegano per una vasta serie di applicazioni. Telefoni cordless, ripetitori video, bluetooth, baby monitor ed anche forni a microonde conmpetono con le reti wireless per l'impiego della limitatissima banda su 2.4 GHz. Questi segnali, così come quelli di altre reti wireless, possono comportare problemi significativi per i collegamenti wireless a lunga distanza. Di seguito sono descritti alcune misure che si possono intraprendere per ridurre la ricezione di segnali indesiderati.

- **Aumentare il guadagno d'antenna su entrambi gli estremi del collegamento punto-a-punto**'. Le antenne non solo aumentano il guadagno in un collegamento, ma aumentando la loro direttività si tende ad abbattere il rumore che proviene dalle aree prossime al collegamento. Due antenne a parabola ad alto guadagno, puntate una verso l'altra, ridurranno fortemente il rumore dalle direzioni che sono fuori dal percorso del collegamento. Usando invece antenne omnidirezionali, si raccoglierà il rumore da tutte le direzioni.
- **Non usare un amplificatore** Come si vedrà nel capitolo quattro, gli amplificatori possono peggiorare i problemi di interferenza, amplificando indiscriminatamente tutti i segnali ricevuti, compreso le sorgenti di rumore. Gli amplificatori causano inoltre problemi di interferenza per altri utenti della stessa banda che siano nelle vicinanze.
- **Usare antenne settoriali anzichè un'antenna omnidirezionale** Con l'impiego di più antenne settoriali, si può ridurre il rumore complessivo ricevuto ad un punto di distribuzione. Impiegando canali scalati su ciascuna antenna settoriale, si può inoltre aumentare la banda disponibile per i vostri utenti.

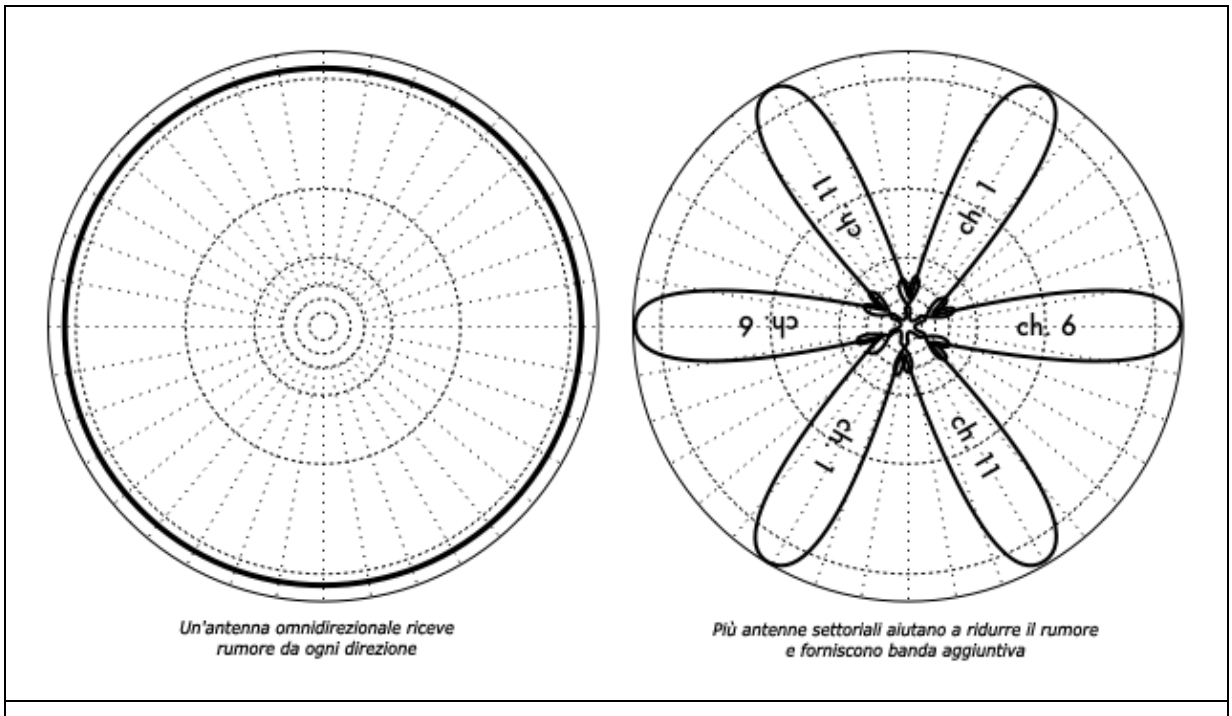


Figure 3.10: Confronto tra una singola antenna omnidirezionale e più antenne settoriali

- **Usare il miglior canale disponibile** Si ricordi che i canali dell'802.11b/g sono ampi 22MHz, ma sono scalati tra loro di appena 5 MHz. Si conduca una *site survey* (verifica d'ambiente), come spiegato nel capitolo otto, e si selezioni un canale che sia il più lontano possibile dalle sorgenti di rumore presenti. Si ricordi che il panorama wireless può cambiare in ogni momento, quando le persone inseriscono nuovi dispositivi (telefoni cordless, altre reti, etc.). Se il vostro collegamento registra difficoltà nell'inviare i pacchetti, potrebbe esser necessario condurre un'altra *site survey* e scegliere un canale differente.

- **Impiegare salti più ridotti e dei ripetitori, piuttosto che un unico balzo a lunga distanza**. Si mantengano i collegamenti punto-a-punto i più brevi possibile. Se può essere possibile creare un collegamento di 12km che tagli da parte a parte la città, si creeranno comunque ogni genere di interferenze. Se è possibile spezzare il collegamento unico in due o tre salti più ridotti, il collegamento complessivo risulterà probabilmente più stabile. Naturalmente, ciò non sarà possibile sui collegamenti rurali a lunga distanza, dove l'alimentazione e le infrastrutture non sono disponibili, ma d'altro canto anche i problemi di interferenza in tali condizioni diventano meno probabili.
- **Se possibile, si usino le bande di 5.8GHz, 900MHz od altre bande non soggette a licenza**. Anche se questa è solo una soluzione a breve termine, ci sono attualmente molti più dispositivi di consumo che impiegano la banda dei 2.4GHz. Impiegando l'802.11a od un dispositivo che porti la banda da 2.4GHz a 5.8GHz si potranno evitare i problemi di congestione. Se si riesce a trovarli, alcuni vecchi apparati wireless (802.11) impiegano la banda libera a 900MHz (sfortunatamente, a bit rate decisamente minori). Altre tecnologie, come Ronja (http://ronja.twibright.com/), impiegano tecnologia ottica per collegamenti a corta distanza, senza interferenze.
- **Se tutto il resto fallisce, adottare lo spettro soggetto a licenza**. Ci sono posti dove tutto lo spettro libero è impiegato completamente. In questi casi, può essere ragionevole affrontare la spesa addizionale per apparati proprietari che impieghino una banda meno congestionata. Per collegamenti punto-a-punto a lunga portata, che richiedano larga banda e la massima disponibilità, questa è senz'altro un'ozione da valutare. Naturalmente, queste caratteristiche sono ottenibili a prezzi decisamente superiori rispetto all'impiego di apparati per lo spettro libero.

Per riconoscere le sorgenti di rumore, sono necessari degli strumenti che esibiscano cosa stia succedendo nell'etere a 2.4GHz. Vedremo di seguito alcuni esempi di tali strumenti nel capitolo sei.

1.7.6 Ripetitori

L'elemento più critico nell'impostare collegamenti di rete sulle lunghe distanze è la ***linea di vista*** (spesso abbreviata in ***LOS***, *Line Of Sight*). I sistemi a microonde terrestri non possono tollerare grandi colline, alberi, od altri ostacoli sul percorso di un collegamento a lunga distanza. Occorre disporre di una chiara percezione della disposizione del terreno tra i due punti per poter determinare se il collegamento sia possibile.

Ma anche se ci fosse una montagna tra due punti, si ricordi come gli ostacoli possano a volte essere trasformati in vantaggi. Le montagne possono bloccare il segnale, ma nell'ipotesi che l'alimentazione possa essere fornita, possono anche rappresentare ottimi luoghi per i ***ripetitori***.

I ripetitori sono nodi che vengono configurati per ritrasmettere un traffico che non è destinato a loro stessi. In una rete a maglia, ogni nodo è un ripetitore. In una rete con infrastruttura tradizionale, i nodi devono essere configurati per inoltrare il traffico verso altri nodi.

Un ripetitore può impiegare uno o più dispositivi wireless. Quando si impieghi un solo elemento radio (è il caso detto ***ripetitore a braccio unico***, *one-arm repeater*), l'efficienza totale è sotto la metà della banda disponibile, poichè la radio inviare o ricevere dati in modo alternativo, ma non in contemporanea. Tali dispositivi sono più economici, semplici, ed hanno minori pretese per l'alimentazione. Un ripetitore con due (o più) elementi radio può impiegarli al massimo delle loro capacità, posto che siano configurati su canali che non si sovrappongano. Naturalmente, i ripetitori possono disporre di una connessione Ethernet per garantire connettività locare su cavo.

I ripetitori possono essere acquistati come soluzione hardware completa, od essere altrimenti facilmente assemblati aggregando due o più nodi wireless con un cavo Ethernet. Quando si valuti di impiegare un ripetitore basato su tecnologia 802.11, si tenga presente che i nodi devono essere configurati in modalità master, managed od ad-hoc. Tipicamente, entrambi gli elementi radio in un ripetitore sono configurati in modalità master, per consentire a più utenti di connettersi ad entrambi i lati del ripetitore. Ma a seconda della configurazione della rete, uno o più dispositivi possono ricorrere alla modalità ad-hoc od anche a quella client.

Tipicamente, i ripetitori sono usati per superare ostacoli sul percorso di un collegamento a lunga distanza. Per esempio, ci possono essere edifici sul percorso, ma questi edifici sono abitati. ACcordi possono spesso essere composti con i proprietari dell'edificio per fornire loro banda come contropartita dei diritti di impiego del tetto e dell'alimentazione elettrica. Se i proprietari dell'edificio non sono interessati, gli inquilini dei piani più alti possono venir persuasi ad installare gli apparati su una finestra.

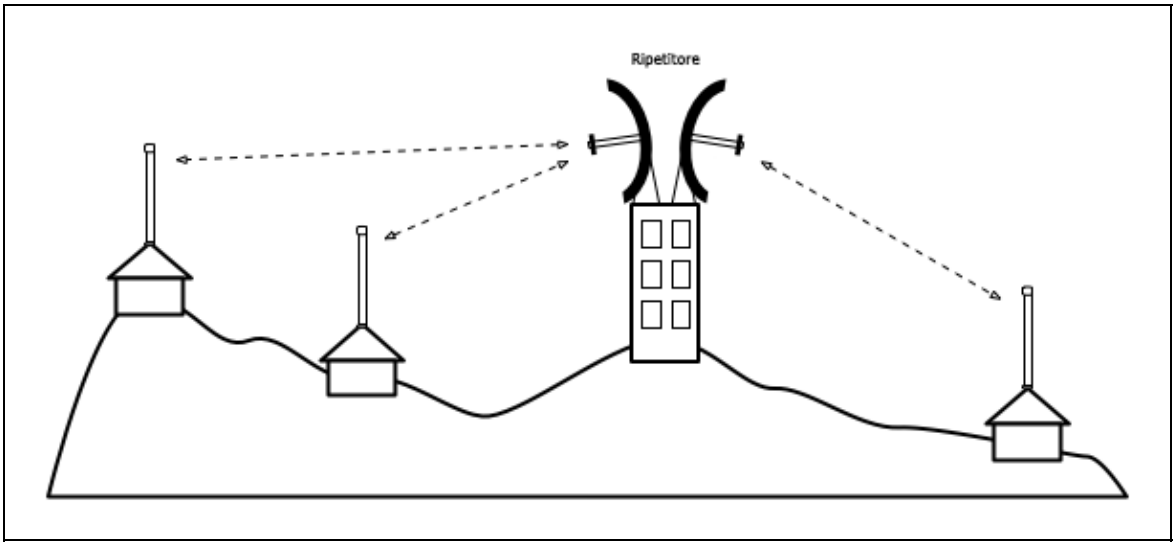


Figura 3.11: Il ripetitore inoltra i pacchetti in aria tra i nodi che non hanno diretta visibilità.

Se non si riesce a scavalcare un ostacolo, si può però spesso aggirarlo. Piuttosto che usare un link diretto, si provi l'approccio a salto multiplo per evitare l'ostacolo.

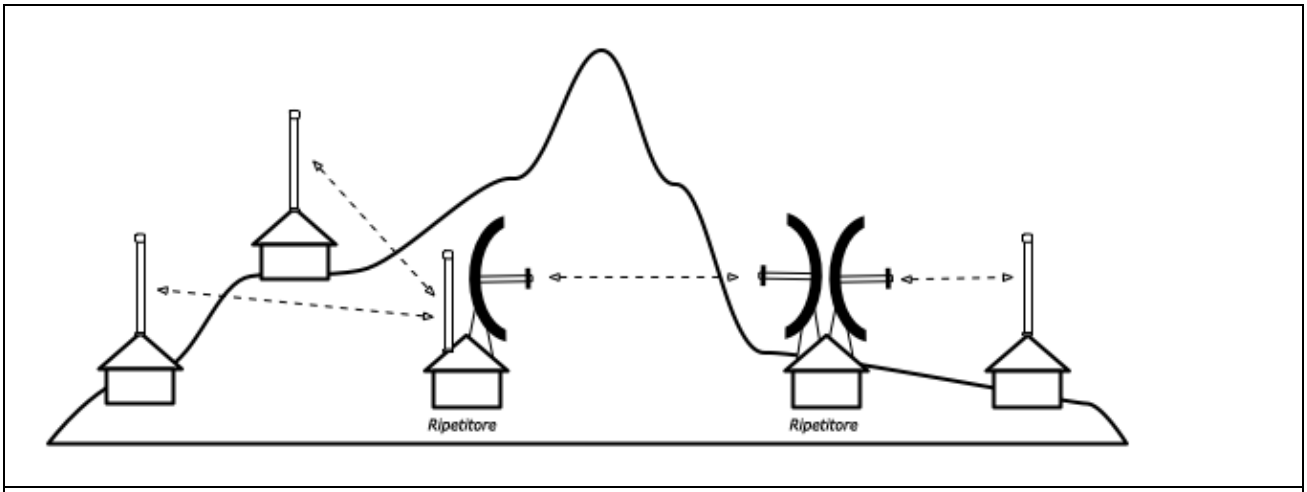


Figura 3.12: L'alimentazione non era disponibile in cima alla collina, ma si risolse il problema impiegando ripetitori multipli attorno alla base.

Infine, si può valutare di compiere un passo indietro per procedere in avanti. Se è disponibile un alto sito in una direzione diversa, e se tale sito ha visibilità oltre l'ostacolo, un collegamento stabile può essere realizzato tramite un percorso indiretto.

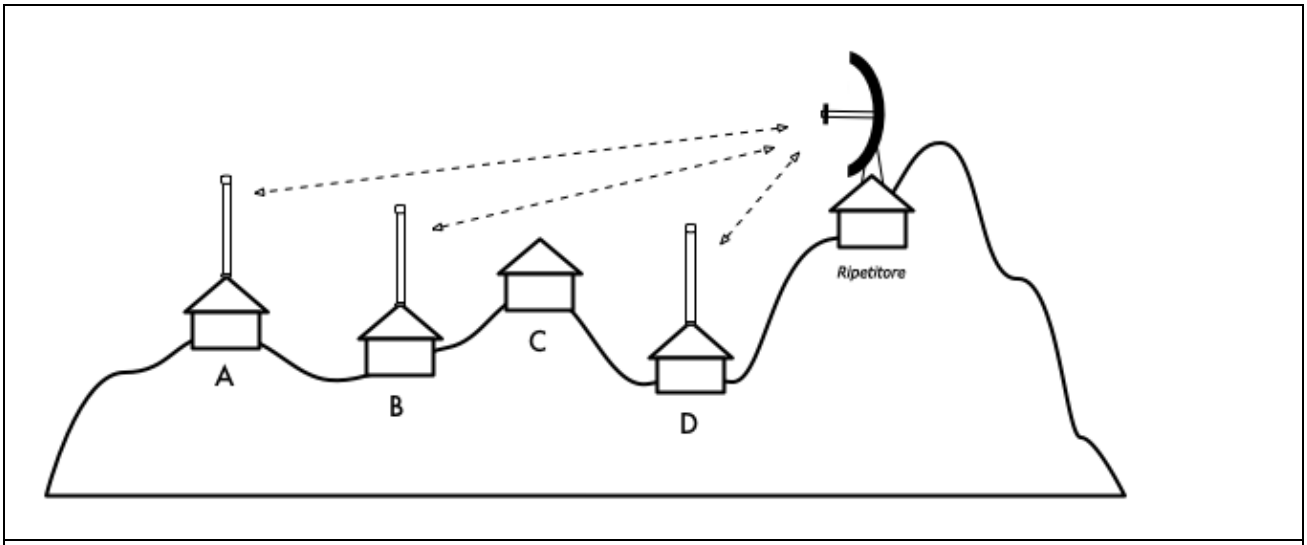


Figura 3.13: Il sito D non garantiva un collegamento pulito tra i siti A o B, poichè il sito C è sul percorso e non è interessato ad accogliere un nodo. Con l'installazione di un ripetitore più alto, i nodi A, B e D possono connettersi. Si noti come il traffico dal nodo D in effetti si allontani dal resto della rete, prima di essere rilanciato.

I ripetitori in una rete ricordano il principio de "i sei gradi di separazione". Il concetto spiega come, a prescindere dalla persona ricercata, siano necessari al massimo cinque intermediari per arrivare a contattarla. I ripetitori su alti siti possono "vedere" un gran numero di intermediari e, se il nodo è in vista del ripetitore, diventa possibile connettersi ad ogni altro nodo raggiungibile dal ripetitore.

1.8 Ottimizzazione del Traffico

La larghezza di banda viene misurata come quantità di bit su un intervallo di tempo. Sfortunatamente, la banda garantita da qualsiasi connessione di rete non è infinita. Si può sempre scaricare (o caricare) tutto il traffico che si richieda, basta attendere per tempi sufficientemente lunghi. Naturalmente, gli esseri umani non sono utenti pazienti come i computer, e non accettano di aspettare tempi infiniti perché le proprie informazioni attraversino la rete. Per tale ragione, la larghezza di banda dev'essere gestita e soggetta a priorità, così come ogni altra risorsa limitata.

È possibile migliorare significativamente il tempo di risposta, e massimizzare la velocità di trasferimento, eliminando dalla rete il traffico ridondante o non desiderato. Questa sezione descrive diverse tecniche di uso comune per sincerarsi che la rete trasporti solo il traffico che deve effettivaemente aattraversarla.

1.8.1 Web caching

Un Proxy Server web è un server sulla rete locale che mantiene copie delle pagine che siano state recentemente richieste o che siano più spesso richiamate. Quando un nuovo utente richiede queste pagine, queste vengono fornite dal proxy server locale, anzichè essere ricevute via Internet. Ciò si traduce in un accesso web decisamente più veloce, in molti casi, riducendo inoltre l'impiego della banda su Internet. Quando viene realizzato un proxy server, l'amministratore deve tener conto che alcune pagine non sono mantenibili in cache; per esempio, pagine che siano il risultato di script lato server, od altro contenuto generato dinamicamente.

Anche il caricamento delle pagine web viene apprezzato in modo diverso. Con un collegamento Internet lento, una pagina web tipica viene caricata lentamente, mostrando prima parte del testo e presentando quindi le figure una dietro l'altra. In una rete con un proxy server, ci possono essere dei ritardi durante i quali sembra non succedere niente, quando finalmente la pagina viene caricata in modo pressochè istantaneo. Ciò succede poichè l'informazione viene inviata dal computer così velocemente che si rende necessario un percettibile

intervallo di tempo per costruire la pagina. Il tempo totale che si rende necessario per caricare un'intera pagina può arrivare ai dieci secondi, là ove in mancanza di un proxy server, sarebbero stati necessari 30 secondi per caricare la pagina in modo graduale. Ma se tale fenomeno non viene spiegato ad alcuni utenti impazienti, questi potrebbero lamentarsi della lentezza introdotta dal proxy server. È normalmente compito dell'amministratore di rete gestire con gli utenti problemi di percezione di questo tipo.

1.8.1.1 Proxy server disponibili

Sono diversi i proxy server web disponibili. Di seguito sono elencati i pacchetti software più spesso utilizzati:

- **Squid**. Il software open source Squid è lo standard de facto presso le università. È libero, affidabile, facile da impiegare e da estendere (ad esempio, con l'inserimento di filtraggi sui contenuti e con il blocco delle pubblicità). Squid genera file di log che possono essere analizzati con applicativi come Awstats, o Webalizer, entrambi open source ed in grado di generare buoni report grafici. In generale, è più semplice installarlo come parte di una distribuzione specifica, piuttosto che scaricarlo da http://www.squid-cache.org/ (gran parte delle distribuzioni come Debian, così come versioni derivate da Unix come NetBSD e FreeBSD, vengono distribuite già fornite di Squid). Una buona guida per la configurazione di Squid può essere trovata presso http://squid-docs.sourceforge.net/latest/book-full.html.
- **Microsoft Proxy server 2.0.** Non è disponibile per nuove installazioni, perché è stato superato da Microsoft ISA server e non è più supportato. È tuttavia impiegato presso alcuni enti, sebbene non debba forse esser preso in considerazione per nuove installazioni.
- **Microsoft ISA server.** ISA server è un proxy server decisamente buono, che probabilmente è troppo costoso per ciò che fornisce. Comunque, con gli sconti educational può essere alla portata di alcuni enti. Presenta i propri report grafici, ma i file di log possono essere analizzati anche con i comuni software di analisi come Sawmill (http://www.sawmill.net/). Gli amministratori di un sito che impieghi MS ISA Server dovrebbero dedicare sufficiente impegno per ottenere una configurazione adeguata; in caso contrario, MS ISA Server può tradursi in un consumatore di banda di tutto rispetto. Per esempio, una installazione di default può facilmente consumare più banda di quanta il sito impiegasse precedentemente, perché le pagine più richieste, con date di scadenza serrate (come quelle dei siti di informazione) vengono continuamente aggiornate. Per questo motivo diventa importante impostare correttamente i modi di caricamento, e configurarli perché vengano impiegati prevalentemente in orari notturni. ISA Server può anche essere collegato a prodotti per il filtraggio dei contenuti, come WebSense. Per ulteriori informazioni, si veda: http://www.microsoft.com/isaserver/ e http://www.isaserver.org/ .

1.8.1.2 Impedire agli Utenti di aggirare il Proxy Server

Se, in generale, evadere la censura su Internet ed eludere le politiche di accesso riservato alle informazioni può essere un impegno politico encomiabile, proxy e firewall rimangono però strumenti necessari nelle aree che dispongano di banda molto limitata. Senza di loro, la stabilità e la disponibilità della rete sarebbero minacciate dagli stessi utenti legittimi. Tecniche per aggirare un proxy server possono essere reperito sotto: http://www.antiproxy.com/ . Questo sito risulta utile agli amministratori per valutare come la propria rete risponda a queste tecniche.

Per rendere efficace l'uso di un cache proxy, si potrebbe considerare la semplice impostazione di una politica d'accesso, fidandosi degli utenti. Nella raffigurazione sottostante, l'amministratore deve fidarsi del fatto che i propri utenti non scavalchino il proxy server.

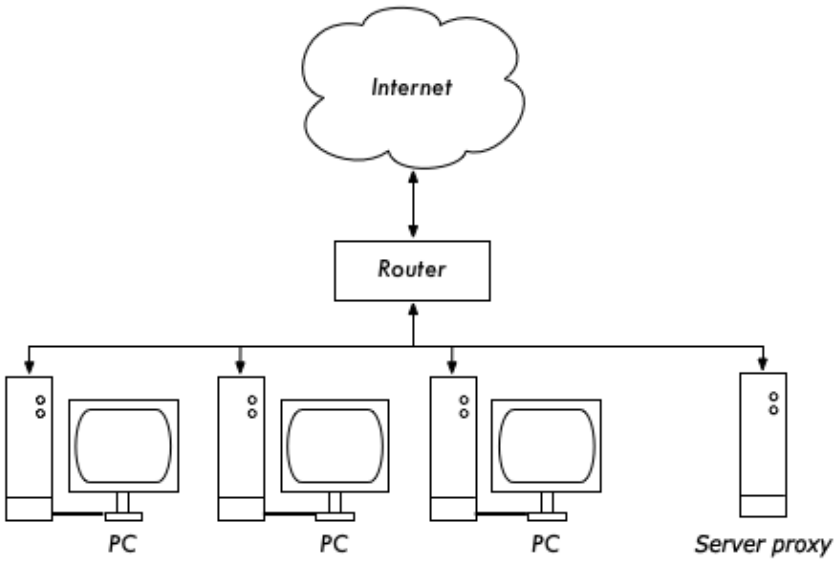


Figura 3.14: In questa rete si confida che gli utenti configurino propriamente i propri PC per l'impiego del proxy server.

In questo caso l'amministratore usa, tipicamente, una delle seguenti tecniche:

- **Non presentare l'indirizzo del default gateway attraverso il servizio di DHCP.** Sulle prime ciò può funzionare, ma qualche utente di rete più smaliziato che intenda scavalcare il proxy server potrebbe trovare - od indovinare - l'indirizzo del default gateway. Una volta che ciò si sia realizzato, la soluzione di come aggirare il proxy tenderà a passare di bocca in bocca.
- **Usare politiche di dominio o di gruppo.** Ciò è molto utile per impostare correttamente il proxy server per Internet Explorer su tutti i computer del dominio, ma non è molto utile per prevenire l'aggiramento del proxy, perché dipende dall'utente che si registra nel dominio NT. Un utente, con un computer su Windows 95/98/ME, può cancellare la propria registrazione e quindi scavalcare il proxy, e qualcuno che conosca la password di un utente locale sul suo computer Windows NT/2000/XP può registrarsi localmente e comportarsi in modo analogo.
- **Supplicare ed altercare con gli utenti.** Non è mai la situazione ideale per l'amministratore di rete.

L'unico modo per assicurarsi che i proxy non vengano scavalcati, è adottare la corretta configurazione di rete, impiegando una delle tre tecniche sotto descritte.

1.8.1.3 Firewall

Un modo più affidabile per assicurarsi che dai PC non si possa aggirare il proxy può essere realizzato impiegando un firewall. Il firewall può essere configurato per permettere al solo proxy server di attraversarlo, cioè a presentare richieste HTTP su Internet. Ogni altro PC è bloccato, come mostrato nella figura sottostante.

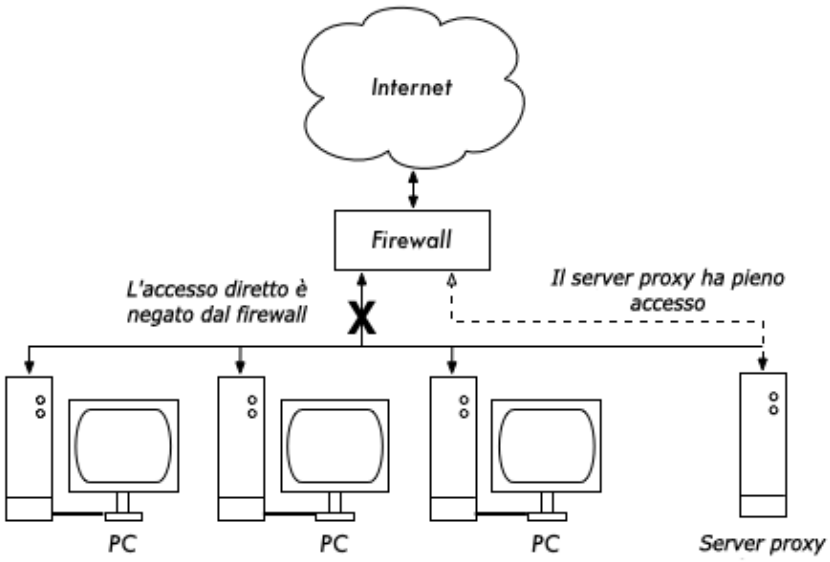


Figura 3.15: Il firewall interdice ai PC l'accesso diretto ad Internet, ma lo consente tramite il proxy server.

Basarsi su un firewall, come nella rappresentazione sopra citata, può essere sufficiente o meno, in funzione da come sia configurato il firewall. Se questi si limita a bloccare l'accesso dalla LAN di campus verso la porta 80 dei server web, gli utenti smaliziati avranno modo di escogitare delle scappatoie. Inoltre, gli utenti saranno comunque in grado di impiegare protocolli avidi di banda, come Kazaa.

1.8.1.4 Doppia scheda di rete

Probabilmente il metodo più sicuro si ottiene installando due schede di rete nel proxy server, connettendo la rete di campus ad Internet come mostrato di seguito. In questo modo, la struttura di rete rende fisicamente impossibile raggiungere Internet senza passare attraverso il proxy server.

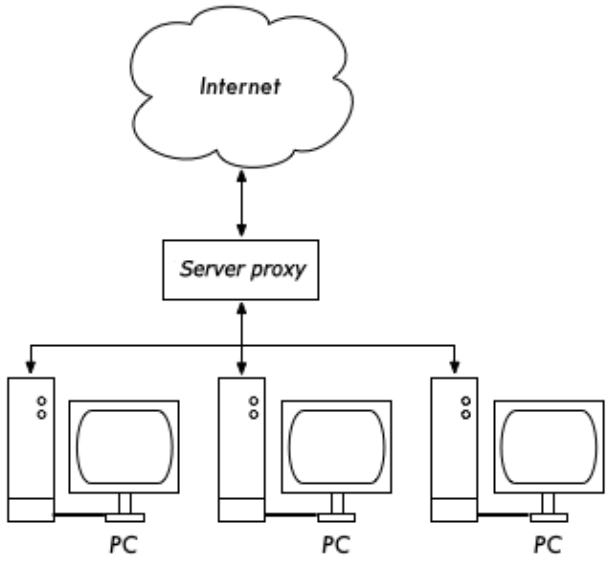


Figura 3.16: L'unica percorso verso Internet attraversa il proxy.

Il proxy server nella figura non dovrebbe avere impostato l'IP forwarding, a meno che gli amministratore non sappiano esattamente cosa intendano lasciar passare.

Un grande vantaggio di questa impostazione è che la tecnica conosciuta come ***transparent proxying*** può venire impiegata. Usare un transparent proxy significa deviare automaticamente le richieste web degli utenti al proxy server, senza alcun bisogno di configurare manualmente i singoli web browser affinchè usino il proxy server stesso. Tutto ciò forza l'intero traffico web ad essere messo in cache, elimina diverse possibilità di errore per gli utenti, e funziona pure con ogni dispositivo che non sia in grado di impiegare un proxy impostatovi manualmente. Per maggiori dettagli sulla configurazione di un transparent proxy con Squid, vedere sotto:

- http://www.squid-cache.org/Doc/FAQ/FAQ-17.html
- http://en.tldp.org/HOWTO/mini/TransparentProxy-2.html

1.8.1.5 Routing impostato su Politiche di Gestione

Un modo per evitare l'aggiramento del proxy, ove si impieghino apparati Cisco, è l'adozione di politiche di routing (**policy routing**). Il router Cisco dirige le richieste web in modo trasparente verso il proxy server. Questa tecnica è impiegata presso la Makerere University. Il vantaggio di questo metodo è che, se il proxy è fuori servizio, le rotte fissate dal policy routing possono essere temporaneamente sospese, consentendo agli utenti di connettersi direttamente ad Internet.

1.8.1.6 Mirroring di un Sito web

Con il permesso del suo proprietario o del suo web master, l'intero contenuto di un sito web può essere posto in mirroring ("ricopiato") in un server locale, nelle ore notturne, se non è troppo corposo. Tale azione potrebbe essere valutata per i siti web di rilievo che possano essere di interesse per l'organizzazione o che possano risultare molto popolari tra gli utenti web. Può essere utile, ma ci possono essere anche potenziali svantaggi. Ad esempio, se il sito che viene ricostruito in locale contiene script CGI od altro contenuto dinamico che richieda un'interazione da parte dell'utente, ciò potrebbe causare problemi. Un esempio è quello di un sito web che richieda ai visitatori di registrarsi on link per una conferenza. Se qualcuno si registra on line su un server ricopiato (e se gli script ricopiati funzionano), chi organizza il sito originale non avrà le informazioni della persona che si è registrata.

Dato che il mirroring di un sito potrebbe ledere i diritti di autore, questa tecnica dovrebbe essere usata solo dietro l'autorizzazione del sito interessato. Se il sito ha in funzione il comando ***rsync***, lo stesso sito può essere ricopiato impiegando lo stesso comando rsync. È questo, probabilmente, il modo più veloce e più efficiente per mantenere sincronizzato il contenuto tra i due siti. Se il web server remoto non impiega rsync, il software che si raccomanda di usare è un programma chiamato ***wget***. È presente in gran parte delle distribuzioni di Unix/Linux. Una versione per Windows può essere reperita sotto http://xoomer.virgilio.it/hherold/, o nel pacchetto di tool liberi di Cygwin Unix (http://www.cygwin.com/).

Uno script può essere impostato perché si attivi ogni notte su un web server locale, e conduca le seguenti azioni:

- Cambi la directory portandosi nella radice dei documenti del server web: per esempio,
- Effettui il mirroring del sito web impiegando il comando:

```
wget --cache=off -m http://www.python.org
```

La copia del sito web si troverà nella directory **www.python.org**. Il web server dovrebbe quindi essere configurato per fornire i contenuti di questa directory su un host virtuale basato sui nomi. Si imposti un server DNS locale che presenti una registrazione fittizia per questo sito. Affinchè tutto ciò funzioni, i PC client dovrebbero essere configurati per impiegare il server DNS locale come DNS primario (Ciò è comunque consigliabile in ogni caso, perché un DNS locale velocizza i tempi di risposta per le richieste web).

1.8.1.7 Arricchire preventivamente la cache impiegando wget

Invece di impostare una copia locale di un sito web, come descritto nella precedente sezione, un approccio migliore è arricchire la cache del proxy adottando un processo automatico. Questo metodo è stato descritto da J. J. Eksteen e J. P. L. Cloete del CSIR di Pretoria, South Africa, in un documento intitolato **Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies**. In questo documento (disponibile presso http://www.isoc.org/inet97/ans97/cloet.htm) i due autori descrivono il funzionamento del procedimento:

- *"Un processo automatico recupera l'home page del sito ed un numero specificato di pagine ulteriori (seguendo in modo ricorsivo i link HTML delle pagine già raccolte) per mezzo di un proxy. Invece di scrivere le pagine recuperate sull'hard disk locale, il processo di copia elimina le pagine scaricate. Tutto ciò viene fatto per conservare le risorse di sistema e per evitare possibili conflitti sul diritto d'autore. Usando il proxy come intermediario, si garantisce che le pagine scaricate siano nella cache del proxy, come se un utente avesse avuto accesso a quelle pagine.*

Quando un utente richiede le pagine già richiamate, gli vengono presentate quelle disponibili nella cache, senza congestionare il collegamento internazionale. Questo processo può essere condotto al di fuori delle ore di punta, con il fine di massimizzare l'impiego della banda e di non interferire con altre attività."

Il comando seguente (impostato per essere eseguito di notte, ogni giorno o settimana) è tutto ciò che si rende necessario (ripetendolo per ogni sito per cui si richieda l'arricchimento preventivo della cache).

```
wget --proxy-on --cache=off --delete after -m http://www.python.org
```

Spiegazione:

- **-m**: ricopia (mirror) l'intero sito. Wget parte da www.python.org e segue tutti i link ipertestuali, sì da scaricare tutte le pagine sottostanti.
- **--proxy-on**: assicurati che wget faccia uso del proxy server. Può non essere necessario nelle impostazioni dove sia impiegato un trasparent proxy
- **--cache=off**: assicurati che i contenuti aggiornati siano scaricati da Internet, e non dal proxy server locale.
- **--delete after**: cancella la copia costruita. Il contenuto in copia rimane nella cache del proxy fintantochè ci sia sufficiente spazio nel disco e posto che i parametri di cache del proxy siano impostati correttamente.

Wget dispone di molte altre opzioni in aggiunta a queste; per esempio, per passare la password per un sito web che la richieda. Quando si impiega questo strumento, Squid dovrebbe essere configurato con sufficiente spazio sul disco per contenere tutti i siti precaricati ed altro (intendendo per altro il normale impiego di Squid rivolto a pagine esterne a quelle dei siti precaricati). Fortunatamente, lo spazio sui dischi rigidi diventa sempre più economico e le dimensioni dei dischi sono sempre più ampie. Comunque, questa tecnica può essere usata solo con pochi siti selezionati. Questi siti non dovrebbere essere troppo grossi, affinchè si completi il processo prima che ricominci l'orario di lavoro, ed inoltre occorre sempre monitorare lo spazio libero disponibile sul disco.

1.8.1.8 Gerarchie di Cache

Se un organizzazione dispone di più proxy server, questi possono condividere informazioni di cache tra di loro. Per esempio, se una pagina web esiste nella cache del server A, ma non nella cache del server B, un utente collegato sul server B potrebbe ottenere l'oggetto dalla cache di A tramite B. ***Inter-Cache Protocol*** (***ICP***) and ***Cache Array Routing Protocol*** (***CARP***) possono permettere la condivisione di informazioni di cache. CARP è considerato migliore. Squid supporta entrambi i protocolli, mentre Microsoft ISA Server

supporta il solo CARP. Per maggiori informazioni, vedere sotto:
http://squid-docs.sourceforge.net/latest/html/c2075.html . Tale condivisione delle informazioni di cache riduce l'impiego di banda esterna nelle organizzazioni dove siano disponibili più proxy server.

1.8.1.9 Specifiche per Proxy

Su una rete di campus universitaria dovrebbero insistere più proxy server, sia per migliorare le prestazioni che per ragioni di ridondanza. Con i dischi rigidi odierni, più economici e capienti, si possono costruire potenti proxy server, con spazio disco di 50 GB e più dedicato alla cache. La prestazione del disco è essenziale, quindi i dischi SCSI, più veloci, sono in grado di offrire prestazioni migliori (sebbene una cache basata su dischi IDE sia comunque meglio di niente). RAID e mirroring non sono raccomandati.

È inoltre consigliabile che un disco rigido separato sia dedicato alla cache. Per esempio, un disco rigido può essere impiegato per la cache, mentre un secondo per il sistema operativo e per la registrazione degli eventi (logging) della cache. Squid è progettato per impiegare quanta più RAM possibile, perché quando i dati sono estratti dalla RAM si raggiungono velocità decisamente superiori a quelle ottenibili sugli hard disk. Per una rete di campus, la memoria RAM dovrebbe essere di 1 GB o più:

- Oltre alla memoria richiesta dal sistema operativo e dalle altre applicazioni, Squid richiede 10 MB di RAM per ogni GB di cache di disco. Quindi, se 50 GB di disco vengono assegnati alla cache, Squid richiederà 500 MB di memoria in più.
- La macchina richiederebbe inoltre 128 MB per Linux e 128 MB per X-Windows.
- Altri 256 MB dovrebbero essere aggiunti per altre applicazioni; sotto queste condizioni di lavoro, dovrebbe filare tutto liscio. Niente migliora le prestazioni di una macchina quanto installare un'ampia memoria, perché ciò riduce la necessità di ricorrere agli hard disk. La memoria è migliaia di volte più veloce di un hard disk. I moderni sistemi operativi mantengono in memoria i dati frequentemente richiesti, se si rende impiegabile sufficiente RAM. Ma ricorrono a memoria virtuale (swap) quando non dispongono di abbastanza RAM.

1.8.2 DNS caching ed ottimizzazione

I server DNS caching-only non sono autorevoli per nessun dominio, forniscono piuttosto risultati dalla cache a fronte di interrogazioni presentate dai client loro attestati. Come un proxy server arricchisce di pagine web popolari la propria cache durante un periodo prefissato, gli indirizzi DNS sono posti in cache fintantochè il proprio ***time to live*** (***TTL***) non si estingua. Ciò ridurrà il traffico DNS sulla vostra connessione Internet, poichè la cache DNS sarà in grado di rispondere localmente e molte interrogazioni. Naturalmente, i computer client devono essere configurati per impiegare i server DNS caching-only, come server DNS di riferimento. Quando tutti i client impiegano questo server come proprio server DNS primario, questi si arricchirà presto la cache di indirizzi, sì da poter rapidamente risolvere gli indirizzi che siano stati già richiesti. I server DNS che sono autorevoli per un dominio agiscono anche come riferimento nomi-indirizzi per i computer di cui curano la diffusione dell'indirizzo IP.

1.8.2.1 Bind (named)

Bind è il programma standard di fatto per il *name service* in Internet. Installato e avviato, Bind funziona come caching server (nessuna ulteriore configurazione è necessaria). Bind può essere installato da un pacchetto tipo pacchetto Debian o tipo RPM. L'installazione da un pacchetto è normalmente il metodo più semplice. Su Debian, digitare:

```
apt-get install bind9
```

Oltre a mandare in esecuzione una cache, Bind può anche gestire zone autorevoli, può prestare servizi sotto altre zone autorevoli, può realizzare segmenti di spazi indirizzi, e pressochè ogni altra funzione che è possibile

svolgere con il DNS.

1.8.2.2 dnsmasq

Un caching server DNS alternativo può essere ***dnsmasq***. È disponibile per BSD e per la più parte delle distribuzioni Linux, o dal sito http://freshmeat.net/projects/dnsmasq/ . Il maggior vantaggio di dnsmasq è la flessibilità; può funzionare facilmente sia come caching DNS proxy e come riferimento autorevole per macchine e domini, senza complicate configurazione dei file di zona. Gli aggiornamenti possono essere inseriti nei dati di zona senza nemmeno dover far riavviare il servizio. Può anche funzionare come DHCP server, e integrerà il servizio di DNS con le richieste DHCP delle macchine in rete. È decisamente snello, stabile, ed estremamente flessibile. Bind è probabilmente una scelta indovinata per reti estese (oltre qualche centinaio di nodi), ma la semplicità e la flessibilità di dnsmasq lo rendono interessante per reti di dimensioni medio-piccole.

1.8.2.3 Windows NT

Per installare il servizio DNS su Windows NT4: selezionale il Pannello di Controllo -> Rete -> Servizi -> Aggiungi -> Microsoft DNS server. Inserire il CD NT4 di Windows quando richiesto. La configurazione di un server caching-only in NT è descritta nell'articolo 167234 della Knowledge Base. Dall'articolo:

- *"Installare semplicemente DNS e lanciare il Domain Name System Manager. Cliccare su DNS nel menù, selezionare Nuovo Server, ed inserire l'indirizzo IP del vostro computer dove è stato installato il DNS. Avete ora un server DNS caching-only."*

1.8.2.4 Windows 2000

Per installare il servizio DNS: Menù d'avvio -> Impostazioni -> Pannello di controllo -> Aggiungi / Rimuovi Software. Tra i componenti di "Aggiungi / Rimuovi Software", selezionare Componenti -> Servizi di Rete -> Dettagli -> Domain Name System (DNS). Quindi avviare l'MMC di DNS (Menù di Avvio -> Programmi -> Strumenti di Gestione -> DNS). Dal Menù delle azioni selezionare "Collegare al computer...". Nella finestra "Seleziona il computer target", attivare "Il seguente computer:" ed inserire il nome di un server DNS che si intenda portare nella propria cache. Se è presente un "." [punto] nel manager DNS (appare di default), significa che il server DNS ritiene di essere il server DNS di root di Internet. Senz'altro si sbaglia. Cancellare il "." [punto] per rendere funzionante il tutto.

1.8.2.5 DNS separato e server ricopiato

Lo scopo di un DNS separato (*split DNS*, conosciuto anche come ***orizzonte separato***, *split horizon*) è presentare una visione del dominio dall'interno differente da quella del mondo esterno. Esistono diversi accorgimenti per realizzare un DNS separato; per motivi di sicurezza, è consigliabile disporre di due differenti server DNS (ciascuno con un proprio database), uno interno ed uno esterno al dominio.

Il DNS separato può rendere possibile per dei client di una rete di campus risolvere gli indirizzi IP del dominio del campus in indirizzi locali IP secondo lo standard RFC1918, mentre il resto di Internet traduce gli stessi nomi in indirizzi IP differenti. Tutto ciò si realizza mantenendo due zone su due differenti server DNS relativi allo stesso dominio.

Una delle zone viene impiegata dai client di rete interni, mentre l'altra viene usata dagli utenti esterni di Internet. Per esempio, nella rete sottostante l'utente nel campus Makerere ottiene la risoluzione di http://www.makerere.ac.ug in 172.16.16.21, mentre un utente in qualsiasi altra parte di Internet ottiene invece la risoluzione in 195.171.16.13.

Il server DNS nel campus del disegno sopra riportato mantiene una file di zona per makerere.ac.ug ed è configurato come autorevole per tale dominio. Inoltre, funge come server DNS di cache per il campus

Makerere, e tutti i computer nel campus sono configurati per impiegarlo come proprio server DNS.

I record DNS per il server DNS di campus apparirebbero simili a quanto segue:

```
makerere.ac.ug ¶
www···· CNAME·· webserver.makerere.ac.ug····· ¶
ftp···· CNAME·· ftpserver.makerere.ac.ug····· ¶
mail··· CNAME·· exchange.makerere.ac.ug ¶
mailserver····· A····· 172.16.16.21··· ¶
webserver····· A····· 172.16.16.21··· ¶
ftpserver····· A····· 172.16.16.21¶
```

Ma c'è un secondo server DNS presente in Internet che è in effetti autorevole per il dominio *makerere.ac.ug*. I record DNS per questa zona esterna risulterebbero come segue:

```
makerere.ac.ug· ¶
www···· A 195.171.16.13 ¶
ftp···· A 195.171.16.13 ¶
mail··· A 16.132.33.21· ¶
····· MX mail.makerere.ac.ug· ¶
```

Il DNS separato non è vincolato all'impiego di indirizzi secondo lo standard RFC1918. Un ISP africano potrebbe, per esempio, mantenere siti web per conto di una università, ma anche mantenere copia degli stessi siti web in Europa. Ogni volta che i client di tale ISP provassero ad accedere al sito web, otterrebbero l'indirizzo IP presso l'ISP africano, mantenendo così il traffico all'interno dello stesso Paese. Quanto i visitatori di altri Paesi dovessero accedere al sito web, questi otterrebbero gli indirizzi IP dei siti web ricopiati in Europa. In questo modo, i visitatori internazionali non congestionerebbero i collegamenti satellitari (VSAT) impiegati dall'ISP per visitare il sito web dell'Università. Tale soluzione sta divendanto un'opzione allettante, poichè l'hosting web in prossimità della dorsale Internet è divendato decisamente economico..

1.9 Ottimizzazione del Collegamento Internet

Come accennato precedentemente, flussi di rete fino a 22Mbps possono essere raggiunti impiegando apparati wireless nella banda 802.11g, non soggetta a licenze. Tale quantità di banda sarà probabilmente superiore, per almeno un ordine di grandezza, a quella garantita dal collegamento con Internet, e dovrebbe essere sufficiente per mantenere, senza problemi, differenti utenti Internet contemporaneamente.

Se però la connessione principale con Internet è assicurata da un collegamento VSAT, si incontreranno alcuni problemi di prestazioni, se ci si affida sui parametri di default di TCP/IP. Ottimizzando il collegamento VSAT, è possibile migliorare sensibilmente i tempi di risposta nell'accesso a macchine su Internet.

1.9.1 Fattori TCP/IP su una connessione satellitare

Spesso ci si riferisce ad un collegamento VSAT come ad una rete con ***tubo lungo e grosso***. Questa caratterizzazione si riferisce ai fattori che influenzano le prestazioni TCP/IP su ogni rete che disponga di banda relativamente ampia, ma con alti tempi di latenza. Gran parte delle connessioni Internet in Africa ed in altre parti dei Paesi in via di Sviluppo sono via VSAT. Quindi, se un'università si connette ad Internet attraverso un ISP, questa sezione potrebbe essere considerata se la connessione dell'ISP è via VSAT. L'alta latenza nelle reti satellitari è dovuta alla lunga distanza del satellite ed alla velocità costante della luce. Questa distanza carica di circa 520 ms il percorso di andata e ritorno (RTT, *round-trip time*), rispetto ad un RTT tipico di 140 ms tra l'Europa e gli Stati Uniti.

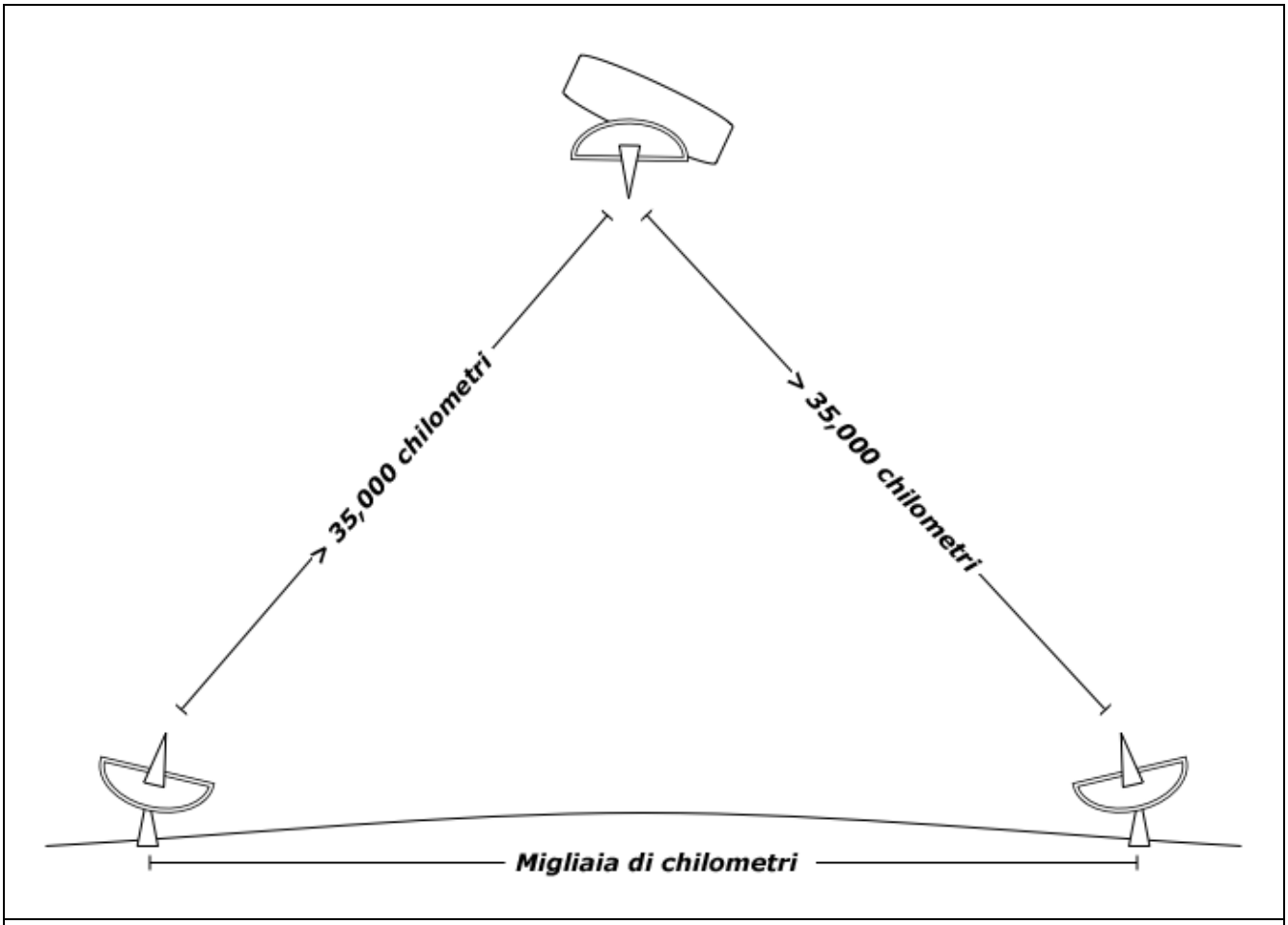


Figura 3.17: A causa della velocità della luce ed alle lunghe distanze coinvolte, un singolo pacchetto di ping può impiegare oltre 520 ms per ottenere un echo su un collegamento VSAT.

I fattori che hanno maggiore influenza sulle prestazioni TCP/IP sono i **lunghi RTT**, i **grandi prodotti larghezza di banda per ritardo**, e gli **errori di trasmissione**.

In generale, i sistemi operativi che acccettano le moderne realizzazioni TCP/IP dovrebbero essere usati su una rete satellitare. Queste realizzazioni accettano le estensioni RFC 1323:

- L'opzione ***scalatura di finestra*** per supportare larghe finestre TCP (maggiori di 64KB).
- ***Riconoscimento di ricezione Selettivo*** (***SACK***, *Selective acknowledgement*) per assicurare un più veloce recupero in caso di errori di trasmissione.
- Marche temporali per valutare opportuni valori di RTT e di timeout in ricetrasmissione per il collegamento in uso.

1.9.2 Lunghi Tempi di Andata e Ritorno (RTT)

I collegamenti satellitari hanno un RTT medio di circa 520ms su singolo salto (primo host - satellite - secondo host). Il TCP impiega il meccanismo della partenza lenta all'inizio di una connessione per determinare i parametri TCP/IP corretti per la connessione stessa. Il tempo dedicato alla fase di partenza lenta è proporzionale, all'RTT, e per un collegamento satellitare ciò significa che il TCP permane in modalità partenza lenta per un tempo maggiore di quanto non sarebbe altrimenti necessario. Tale comportamento riduce drasticamente il flusso nelle connessioni TCP di breve durata. Ciò può essere osservato dal fatto che un piccolo sito web potrebbe impiegare un tempo sorprendentemente lungo per effettuare il caricamento, ma quando un file di grandi dimensioni viene trasferito, velocità di trasferimento adeguate sono raggiunte dopo pochi secondi.

Inoltre, quando i pacchetti vengono perduti, il TCP entra nella fase di controllo di congestione ed, a causa dell'alto RTT, vi rimane per un tempo più lungo, così riducendo il flusso di connessioni TCP sia di breve, che di lunga durata.

1.9.3 Prodotto tra ritardo e larghezza di banda

La quantità di dati in transito su un collegamento in un momento qualsiasi è il prodotto della larghezza di banda e dell'RTT. A motivo dell'alta latenza su un link satellitare, il prodotto larghezza di banda per ritardo è considerevole. Il TCP/IP permette alla macchina remota di trasmettere una certa quantità di dati in anticipo, prima che ne venga riconosciuta la corretta ricezione. La ricevuta è normalmente richiesta per ogni dato inviato su una connessione TCP/IP. In effetti, alla macchina remota viene sempre permesso di inviare una certa quantità di dati senza che le sia ancora arrivata la ricevuta di corretta ricezione, fatto che è importante per raggiungere una buona velocità di trasferimento su connessioni con elevato prodotto ritardo per larghezza di banda. Questa quantità di dati è denominata ***larghezza della finestra TCP***. Tale larghezza è di norma sui 64KB, nelle moderne realizzazioni di TCP/IP.

Sulle reti satellitari, il valore del prodotto ritardo-larghezza di banda è importante. Per impiegare con efficienza il collegamento, la larghezza della finestra della connessione dovrebbe essere uguale a quella del prodotto ritardo-larghezza di banda. Se la massima larghezza della finestra è 64KB, il massimo flusso teorico raggiungibile via satellite è (larghezza della finestra / RTT, ovvero 64KB / 520ms. Tutto ciò offre un massimo trasferimento dat di 123 KB/s, ovvero 984 Kbps, a prescindere dal fatto che la capacità del collegamento possa essere ben più grande.

Ogni header (testata) di un segmento TCP contiene un campo denominato ***advertised window*** (*finestra annunciata*), che specifica quanti byte di dati addizionali il ricevente sia pronto ad accettare. La advertised window rappresenta la dimensione di buffer al momento disponibile presso il ricevente. Per massimizzare le prestazioni, il mittente dovrebbe impostare la dimensione del proprio buffer in trasmissione ed il ricevente quella del proprio buffer in ricezione su valori non inferiori al prodotto ritardo-larghezza di banda. Tale dimensione del buffer arriva ad un valore massimo di 64 KB nella gran parte delle moderne realizzazioni TCP/IP.

Per risolrvere il problema degli stack TCP/IP in sistemi operativi che non estendono la finestra oltre i 64 KB, può essere usata una tecnica nota come ***TCP acknowledgment spoofing*** (si veda Migliorare le Prestazioni del Proxy, poco oltre).

1.9.4 Errori di Trasmissione

Nelle più datate realizzazioni TCP/IP, la perdita di pacchetti viene sempre assunta come dovuta dalla congestione (anzichè ad errori sulla propagazione). Quando questo caso si verifica, il TCP attiva l'eliminazione della congestione, richiedendo tre segnali duplicati di ACK od una partenza lenta, nel caso di un time-out. A causa del forte valore di RTT, una volta che il controllo di congestione sia partito, i collegamenti TCP/IP su satellite impiegheranno un tempo maggiore per ritornare al normale livello di flusso. Errori su un link satellitare avranno quindi effetti molto più pesanti sulle prestazioni del TCP, rispetto a collegamenti a bassa latenza. Per risolvere questa limitazione, sono stati sviluppati accorgimenti come la ***Ricevuta Selettiva*** (***SACK***, *Selective Acknowledgment*). Il SACK definisce esattamente i pacchetti che sono stati ricevuti, permettendo al mittente di ritrasmettere solo i segmenti TCP andati persi a causa di errori in trasmissione.

Il documento *Microsoft Windows 2000 TCP/IP Implementation Details White Paper* spiega come:

- *"Windows 2000 introduce il supporto per un'importante caratteristica prestazionale, conosciuta come Selective Acknowledgment (SACK). SACK è particolarmente importante per connessioni che impieghino larghe finestre TCP."*

SACK è da molto tempo una caratteristica standard per kernel Linux BSD. Occorre assicurarsi che il proprio router Internet e l'estremo opporto del collegamento presso il proprio ISP supportino entrambi il SACK.

1.9.5 Conseguenze per le università

Se un sito dispone di una connessione di 512 Kbps verso Internet, le impostazioni di default di TCP/IP sono probabilmente adeguate, perché la dimensione della finestra di 64 KB può accomodare fino a 984 Kbps. Ma se all'università sono accordati più di 984 Kbps, sul collegamento si potrebbe in alcuni casi non raggiungere la piena larghezza di banda a causa dei fattori "rete a tubo lungo e largo" sopra discusso. L'effetto pratico di tali fattori è che si impedisce ad una singola macchina di sfruttare l'intera larghezza di banda. Ciò non è grave durante la giornata lavorativa, perché molti utenti impiegano l'intera larghezza di banda. Ma se, per esempio, dei download pesanti sono predisposti per il periodo notturno, l'amministratore potrebbe voler far loro sfruttare l'intera larghezza di banda, ed i fattori della "rete a tubo lungo e largo" potrebbero essere d'ostacolo. Ciò potrebbe risultare critico anche se una parte considerevole del traffico di rete dovesse essere convogliata su un singolo tunnel o su una connessione VPN diretta all'altro capo del collegamento satellitare.

Gli amministratori potrebbero valutare l'opportunità di adottare provvedimenti per assicurare che l'intera larghezza di banda venga raggiunta, per mezzo di affinamenti nell'impostazione TCP/IP. Se una università ha messo in piedi una rete dove tutto il traffico transita attraverso un proxy (imposto dalla geometria di rete), allora le uniche macchine che si connettono ad Internet saranno il proxy ed i server di posta.

Per ulteriori informazioni, si veda sotto: http://www.psc.edu/networking/perf_tune.html .

1.9.6 Migliorare le Prestazioni del Proxy (PEP)

Il concetto del miglioramento delle prestazioni di un proxy (PEP, *Performance-enhancing proxy*) è descritto nell'RFC 3135 (si veda http://www.ietf.org/rfc/rfc3135), e consisterebbe in un proxy server con una larga cache di disco che disponga delle estensioni dell'RFC 1323, tra le altre caratteristiche. Un portatile è in sessione TCP con un PEP presso l'ISP. Questo PEP, e quello presso il provider satellitare, comunicano usando una sessione TCP differente, od addirittura un proprio protocollo proprietario. Il PEP presso il provider satellitare ottiene i file dal server web. In questo modo, la sessione TCP viene scissa, ed in tal modo le caratteristiche del collegamento che influiscono sulle prestazioni del protocollo (fattori del tubo lungo e largo) sono risolte (con il TCP acknowledgment spoofing, per esempio). Inoltre, il PEP fa uso di proxy e di pre-faricamento per migliorare ulteriormente l'accesso web.

Un tale sistema può essere costruito da zero impiegando Squid, per esempio, o comprato chiavi in mano da diversi venditori.
