Hardware di rete

41

ninux.org

Contents

1 Hardware di rete

Negli ultimi anni,un interesse senza precedenti per l'hardware wireless ha portato ad un enorme varietà di prodotti economici sul mercato,tale che è impossibile catalogare tutti i componenti disponibili.In questo capitolo vedremo una serie di caratteristiche e attributi che sono desiderabili in un componente wireless, e vedremo parecchi esempi di prodotti commerciali e fai-da-te che hanno lavorato bene nel passato.

1.1 Wired wireless

Con un nome come wireless (senza fili), si potrebbe essere sorpresi da quanti cavi sono coinvolti nel realizzare un semplice collegamento punto-punto. Un nodo wireless consiste di molti componenti, i quali devono essere connessi tra loro con un cablatura adeguata. Ovviamente occorre un computer connesso ad un rete ethernet e un router wireless, o un "ponte" (⚠ bridge?? /!\) alla stessa rete. I componenti radio devono essere connessi alle antenne, ma a lungo possono avere bisogno di interfacciarsi con un amplificatore,con un limitatore di tensione,o con un altro dispositivo. Molti componenti richiedono energia, tramite una linea AC,o usando un trasformatore DC. Tutti questi componenti usano varie specie di connettori, per non menzionare un'ampia varietà di cavi e relativi spessori.

Ora moltiplicando questi cavi e connettori per il numero di nodi che si vogliono portare online, probabilmente ci si chiederà perchè viene chiamato "senza fili". Il diagramma nella prossima pagina fornisce un'idea dei cavi richiesti per un classico collegamento punto-punto. Da notare che il diagramma non è in scala, né rappresenta necessariamente la scelta migliore per la struttura di una rete, però ci introduce ai molti componenti e connettori comuni che probabilmente si incontreranno nell'ambiente.

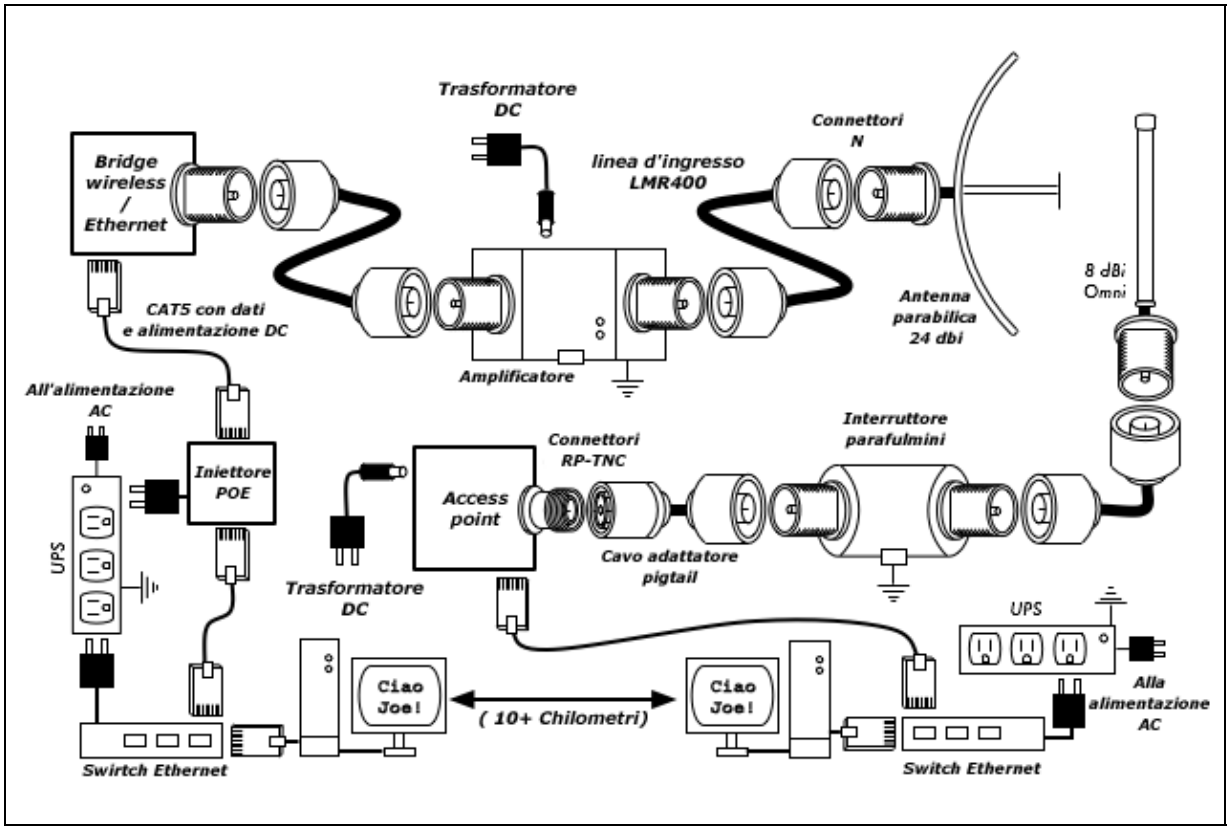

Figura 5.1: Interconnessione di componenti.

Mentre i componenti usati varieranno di nodo in nodo, ogni installazione comprenderà queste parti:

1. Un computer o una rete collegata a uno switch Ethernet
2. Un diposistivo che connetta la rete ai dispositivi wireless (router, ponte, ripetitore)

3. Un'antenna collegata alla linea di alimentazione, o integrata nel dispositivo stesso
4. Componenti elettrici che consistono in gruppi di alimentazione, condizionatori e limitatori di tensione

La reale selezione dell'hardware dovrebbe essere determinata stabilendo i requisiti del progetto, determinando il budget disponibile e verificando che il progetto sia fattibile usando le risorse disponibili (includendo pezzi di ricambio e costi di manutenzione continui). Come discusso nel primo capitolo, stabilire lo scopo del progetto è critico prima di decidere per l'acquisto.

1.2 Scegliere i componenti wireless

Sfortunatamente, in un mondo di produttori di hardware competitivi e budget limitati, il prezzo è il fattore a cui si presta maggiore attenzione. Il vecchio detto "ottieni quello che paghi" spesso si conferma nell'acquisto di prodotti hi-tech ma non per questo va considerato una verità assoluta. Mentre il prezzo è un importante fattore per decidere sull'acquisto, è vitale capire precisamente cosa si ottiene per i propri soldi in modo da fare una scelta corretta che rispecchi le proprie necessità.

Quando si sceglie del materiale wireless da usare nella propria rete, bisogna essere sicuri di considerare questi fattori:

- **Interoperabilità.** L'apparecchiatura che si vuole considerare lavora con quella di altri produttori? Se non fosse così,sarebbe un problema per questo segmento della vostra rete? Se il materiale in questione utilizza un protocollo aperto (quale 802.11b/g), allora è molto probabile che lavorerà con altre apparecchiature.
- **Portata.** Come detto nel quarto capitolo, la portata non è qualcosa riguardante un pezzo particolare dell'attrezzatura. Il raggio d'azione di un dispositivo dipende dall'antenna a cui è collegato, il terreno circostante e le caratteristiche dell'apparecchio all'altro capo del collegamento, insieme ad altri fattori. Piuttosto che contare sulla valutazione approssimata del fornitore è più utile conoscere la ***potenza di trasmissione*** della radio così come il ***guadagno dell'antenna*** (se inclusa). Con queste informazioni è possibile calcolare la portata teorica come descritto nel capitolo tre.
- **Sensibilità radio.** Quanto è sensibile il dispositivo radio ad un dato bit rate? Il produttore dovrebbe fornire queste informazioni, almeno riguardo alle velocità più basse e più alte. Ciò può essere usato per misurare la qualità dell'hardware, permettendo di completare il calcolo del budget per il collegamento. Come visto nel capitolo tre, un numero minore è migliore per la sensibilità radio.
- **Throughput.** I costruttori indicano sempre il bit rate più alto raggiungibile come la velocità standard del proprio prodotto.Tenere presente che il tasso indicato (es 54Mbps) non è mai il throughput reale del dispositivo (es circa 22Mbps per 802.11g). Se le informazioni sul tasso di rendimento non sono disponibili per il dispositivo che state valutando, una buona regola pratica è quella di dividere per due la "velocità" e sottrargli il 20% circa. Quando si hanno dubbi meglio testare il throughput su un'unita di prova prima di comprare una grande quantità di apparecchiature che non hanno una valutazione ufficiale di throughput.
- **Accessori Richiesti.** Per mantenere basso il prezzo iniziale i produttori spesso non includono componenti richiesti per un uso normale. Il prezzo include tutti gli adattatori di alimentazione? (Gli alimentatori sono tipicamente inclusi; i connettori power over Ethernet tipicamente no. Controllare bene i voltaggi di input, visto che spesso i dispositivi hanno un'alimentazione Stati Uniti-centrica). Sono inclusi pigtails, adattatori, cavi, antenne e schede radio? Se abbiamo intenzione di utilizzarlo all'aria aperta, il dispositivo include una scatola a prova di intemperie?
- **Disponibilità.** Si è in grado di sostituire facilmente componenti guasti? Si può ordinare il pezzo in grande quantità, se il progetto lo richiede? Quanto è previsto duri questo particolare prodotto, sia in tempi di lavoro sul campo che disponibilità da parte del produttore?
- **Altri fattori.** Assicurarsi che altre caratteristiche necessarie siano presenti per soddisfare le proprie particolari necessita'. Per esempio, il dispositivo è provvisto di un connettore per antenna esterna? Se sì, di che tipo? Ci sono limitazioni per l'utente o per il throughput imposti dal software, e in tal caso, qual è il costo per superare queste limitazioni? Qual è il ⚠ physical form factor ⚠ del dispositivo? Quanta corrente consuma? Supporta l'alimentazione tramite POE? Il dispositivo è provvisto di

crittazione, NAT, strumenti di monitoraggio della larghezza di banda o altre caratteristiche critiche per il progetto della rete che si vuole realizzare?

Rispondendo a queste domande prima, si faranno decisioni di acquisto intelligenti quando arriverà l'ora di scegliere l'hardware di rete. E' difficile che ogni singola domanda trovi risposta prima di (comprare) buying gear , ma dando (la giusta) priorità alle domande e pressando il venditore a rispondere prima di impegnarsi in un acquisto, si farà il miglior utilizzo possibile del budget costruendo una rete di componenti adatti alle necessità.

1.3 Soluzioni commerciali vs. fai-da-te

Il progetto della rete quasi sicuramente sarà composto da componenti acquistati da venditori, ma anche da parte che sono di origine o di fabbricazione locale. Questa è una verità economica basilare nella maggior parte del mondo. A questo punto della storia tecnologica umana, la distribuzione globale di informazioni è piuttosto banale, se comparata con la distribuzione globale di beni. In molte regioni del mondo, importare tutti i componenti necessari per costruire una rete comporta una spesa proibitiva per tutti i budget, eccetto i più alti. Si può risparmiare molto denaro nel breve tempo trovando sorgenti locali di parti e lavoro, e importando solo i componenti che devono essere acquistati.

Naturalmente c'è un limite a quanto lavoro può essere svolto da un individuo o da un gruppo in un dato intervallo di tempo. In altri termini, importando tecnologia si può scambiare denaro per attrezzatura che può risolvere un particolare problema in un tempo relativamente breve. L'arte di costruire infrastrutture di telecomunicazione locale si basa sul trovare il giusto equilibrio tra il denaro e lo sforzo che devono essere utilizzati per risolvere il problema.

Alcune componenti, come schede radio e antenna feed line , sono eccessivamente complesse per considerare di fabbricarle localmente. Altre componenti, come antenne e torri, sono relativamente semplici e possono essere fatte localmente per una frazione del costo di importazione. Tra questi estremi si collocano gli stessi dispositivi di comunicazione.

Utilizzando schede radio, schede madri e altre componenti off-the-shelf, si possono costruire dispositivi con caratteristiche comparabili (o anche superiori) alla maggior parte delle implementazioni commerciali. Combinando piattaforme open hardware con software open source può portare ad un significativo "bang for the buck" fornendo soluzioni personalizzate e robuste ad un costo molto basso.

Questo non vuol dire che le apparecchiature commerciali siano inferiore alle soluzioni fai-da-te. Fornendo le cosidette "turn-key solutions" (soluzioni "gira la chiave"), i costruttori non solo risparmiano tempo di sviluppo, ma possono anche permettere a gente relativamente poco preparata di installare e mantenere le apparecchiature. I principali vantaggi delle soluzioni commerciali sono che forniscono ***supporto*** e una (solitamente limitata) ***garanzia sull'attrezzatura***. Forniscono anche una ***piattaforma consistente*** che tende a portare ad un'installazione di rete molto stabile e spesso intercambiabile.

Se una parte dell'apparecchiatura semplicemente non funziona o è difficile da configurare o da aggiustare (troubleshoot), un buon costruttore fornirà assitenza. Se l'apparecchiatura dovesse guastarsi nel suo normale utilizzo (eccetto danni estremi, come un fulmine) allora il costruttore tipicamente la rimpiazzerà. La maggior parte fornirà questi servizi per un tempo limitato come parte del prezzo d'acquisto, e molti offrono supporto e garanzia per un periodo esteso per un contributo mensile. Fornendo una piattaforma consistente, è semplice tenere apparecchiatura di scorta a portata di mano e semplicemente sostituire l'apparecchiatura che si guasta sul campo, senza la necessità che un tecnico configuri l'attrezzatura sul luogo. Naturalmente tutto questo comporta un costo iniziale relativamente più alto per le apparecchiature, facendo un paragone con i componenti off-the-shelf.

Dal punto di vista di un architetto di rete, i tre più grandi rischi nascosti quando si scelgono soluzioni commerciali sono il ***vendor lock-in***, le ***linee di prodotti fuori produzione***, e il ***cambiamento dei costi delle***

licenze.

Può essere costoso permettere al richiamo di quelle che sono erroneamente definite "nuove caratteristiche" di comandare lo sviluppo della rete. I costruttori spesso forniranno caratteristiche che sono incompatibili per progettazione con quelle della concorrenza, e poi tireranno fuori materiale di marketing per convincere che non si può vivere senza di loro (al di là del fatto che la caratteristica contribuisca o meno alla soluzione del problema di comunicazione). Quando si inizia a confidare in queste caratteristiche, probabilmente si deciderà di continuare ad acquistare apparecchiatura dallo stesso costruttore in futuro. Questa è l'essenza del "vendor lock-in". Se una grande istituzione utilizza una quantità significativa di apparecchiature proprietarie è poco probabile che la abbandonerà per utilizzare un marchio diverso. Le divisioni commerciali (⚠ sales teams ⚠) lo sanno (e di fatto, alcune ci fanno affidamento) e utilizzano il vendor lock-in come strategia per la negoziazione dei prezzi.

Combinato con il vendor lock-in, un costruttore potrebbe decidere di mettere fuori produzione una linea di prodotti, al di là della loro popolarità. Questo assicura che i clienti, che si affidano alle caratteristiche proprietarie del costruttore, acquisteranno il modello più nuovo (e quasi sempre più caro). Gli effetti di lungo termine del vendor lock-in e dei prodotti fuori produzione sono difficili da stimare quando si progetta una rete, ma dovrebbero essere tenuti a mente.

Infine, se un particolare pezzo dell'apparecchiatura utilizza codice informatico proprietario, potrebbe essere necessario avere la licenza per quel codice per tutto il tempo. Il costo di queste licenze potrebbe variare in base alle caratteristiche, il numero di utenti, la velocità di connessione o altri fattori. Se la licenza non viene pagata, alcune apparecchiature sono progettate per smettere di funzionare fino a quando non viene fornita una licenza valida e pagata! Assicurarsi di capire i termini di utilizzo di qualunque apparecchiatura acquistata, compreso il costo delle licenze.

Utilizzando apparecchiature generiche che supportano standard aperti e software open source, si possono evitare alcuni di questi tranelli. Per esempio, è molto difficile ⚠ to become locked-in ⚠ ad un venditore che utilizza protocolli aperti (come TCP/IP su 802.11a/b/g). Se si incontra un problema con l'apparecchiatura o il venditore, si possono sempre acquistare apparecchiature da un venditore differente che funzionerà con quelle che sono già state acquistate. E' per queste ragioni che raccomandiamo l'utilizzo di protocolli proprietari e frequenze non libere **solo** nei casi in cui i protocolli aperti (come 802.11a/b/g) e le frequenze libere non siano utilizzabili per impedimenti tecnici.

Similmente, mentre i prodotti individuali possono essere messi fuori produzione in ogni momento, si può limitare l'impatto che questo avrà sulla rete utilizzando componenti generici. Per esempio, una particolare scheda madre potrebbe diventare introvabile sul mercato, ma si possono avere a portata di mano un certo numero di schede madri di PC che eseguiranno in maniera efficace lo stesso compito. Vedremo alcuni esempi di come utilizzare queste componenti generiche per costruire un nodo wireless completo più avanti in questo capitolo.

Ovviamente, non ci dovrebbero essere costi continuativi di licenza relativi a software open source (con l'eccezione di un venditore che fornisca supporto esteso o qualche altro servizio, senza far pagare l'utilizzo del software stesso). Ci sono stati alcuni casi di venditori che hanno lucrato sul regalo che i programmatori open source hanno dato al mondo, mettendo il codice in vendita con una licenza, violando i termini di distribuzioni impostati dagli autori originali. Sarebbe saggio evitare questi venditori, e di essere sospettosi sulle dichiarazioni di "software libero" accompagnate da licenza a pagamento.

Lo svantaggio dell'utilizzo di software open source e hardware generico è chiaramente la questione del supporto. Quando sorgeranno problemi sulla rete, bisognerà risolvere i problemi da soli. Questo è spesso realizzato consultando risorse gratuite online e motori di ricerca e applicando patches al codice direttamente. Se non si hanno membri della squadra competenti e dedicati a progettare una soluzione al problema di comunicazione, realizzare un progetto di rete può richiedere una quantità di tempo considerevole. Naturalmente, non c'è mai la garanzia che semplicemente investire soldi nel problema lo risolverà. Mentre

forniamo vari esempi di come fare molto del lavoro da soli, si potrebbe trovare questo lavoro molto difficile. Si dovrà trovare l'equilibrio tra la soluzione commerciale e l'approccio fai-da-te che funzioni per il progetto.

In breve, definire sempre prima gli obiettivi della rete prima, identificare le risorse che possono portare a risolvere il problema, e permettere che la selezione dell'apparecchiatura emerga naturalmente dai risultati. Considerare soluzioni commerciali così come componenti aperte, ma tenendo a mente i costi di lungo termine di entrambe.

1.4 Prodotti Wireless Professionali

C'è abbondanza di apparecchiature sul mercato per i collegamenti punto-punto di lunga distanza. La maggior parte di queste apparecchiature sono pronte per funzionare "out of the box", solo il cavo dell'antenna deve essere collegato e sigillato. Quando si pensa a collegamenti di lunga distanza, ci sono tre fattori principali da considerare: la distanza totale del link, quanto tempo dovrà rimanere in piedi e, naturalmente, della necessaria velocità di collegamento.

La maggior parte dei prodotti commerciali disponibili per collegamenti di raggio più lungo ora utilizzano la tecnologia OFDM e operano nella banda dei 5.8 GHz. Sono disponibili alcuni prodotti che utilizzano standard aperti, ma la maggior parte fa uso di un protocollo proprietario di qualche tipo. Questo significa che per creare un collegamento, gli apparati radio da ambo le parti devono provenire dallo stesso costruttore. Per i collegamenti di importanza più critica è una buona idea utilizzare un sistema che utilizzi le stesse identiche apparecchiature a tutt'e due i capi del collegamento. In questo modo solo un'unità di scorta deve essere immagazinata e, in caso di bisogno, può rimpiazzare uno dei capi del collegamento. Ci sono alcuni buoni prodotti sul mercato che utilizzano apparecchiature differenti ad uno dei capi del collegamento. Questi possono essere utilizzati in una rete fintanto che sia fatto con attenzione, o altrimenti sarà necessario avere apparati di scorta per entrambi i tipi di apparecchiature radio.

Ciò che segue non vuole essere né la buona né la cattiva pubblicità di nessun apparato. Queste sono solo alcune note che sono venute fuori da più di cinque anni di esperienza sul campo in tutto il mondo con prodotti commerciali senza licenza. Sfortunatamente non c'è modo di recensire ogni prodotto, perciò segue l'elenco di alcuni dei preferiti.

1.4.1 Redline Communications

La Redline ha esordito sul mercato con la sua linea di prodotti AN-50. Questo è stato il primo prodotto punto-punto disponibile con velocità di trasmissione superiore a 50 Mbps che i piccoli operatori potevano permettersi. Utilizzano solo 20 MHz di spettro per canale. Ci sono tre differenti modelli disponibili nella linea AN-50. Tutti e tre hanno lo stesso insieme di caratteristiche di base, solo la larghezza di banda totale cambia. Il modello standard ha 36 Mbps di throughput, il modello ecnomico ha 18 Mbps e la versione completa ha 54 Mbps. Il controllo della larghezza di banda è aggiornabile via software e può essere aggiunto al sistema quando la domanda di larghezza di banda aumenta.

Gli apparati radio della Redline sono composti da un'unità da indoor, un'unità da outdoor e un'antenna. L'unità da indoor entra in un rack standard da 19 pollici, ed occupa ⚠ 1U ⚠ . L'unità da outdoor si monta sullo stesso sostegno che regge l'antenna. Questa unità outdoor è il vero apparato radio. Le due unità sono collegate da un cavo di interfaccia coassiale. Un cavo Beldon RG6 o RG11 è utilizzato a questo scopo, ed è lo stesso che viene utilizzato per la TV satellitare. Non è caro, è facile da trovare, ed elimina il bisogno di costosi cavi a bassa perdita, quali il Times Microwave serie LMR o l'Heliax dell'Andrew Corporation. Inoltre, tenere la radio montata così vicina all'antenna limita la perdita relativa al cavo al minimo assoluto.

Ci sono due caratteristiche che spiccano negli apparati Redline. La prima è la ***modalità di allineamento generale*** (General Alignment Mode), che accende un avvisatore acustico che cambia di tonalità quando cambia la tecnica di modulazione. "Beep" più veloci corrispondono ad una connessione più veloce. Questo permette un più facile allineamento, visto che il collegamento può essere allineato quasi interamente con

l'utilizzo dei segnali acustici. Solo un tuning finale sarà necessario, ed un'applicazione grafica per Windows è disponibile per questo scopo. L'altra caratteristica è un pulsante ***Test***. Quando si effettuano modifiche radio ma non si è sicuri della loro correttezza, premendo il pulsante test invece del pulsante ***Save*** attiverà i cambiamenti per cinque minuti. Dopo cinque minuti, la configurazione torna nello stato in cui si trovava prima della pressione del pulsante test. Questo permette di provare dei cambiamenti, e se le cose non funzionano e il collegamento cade, il collegamento tornerà dopo cinque minuti. Una volta che i cambiamenti sono stati provati, si possono confermare semplicemente le nuove impostazioni premendo il pulsante di salvataggio invece di quello di test.

La Redline dispone di altri modelli. L'AN-30 ha quattro porte T1/E1, oltre ad una connessione Ethernet da 30 Mbps. L'AN-100 segue lo standard 802.16a, ed è di prossima uscita il RedMax, che promette di essere conforme al WiMax.

Per maggiori informazioni sui prodotti della Redline Communications, visitare http://www.redlinecommunications.com/

1.4.2 Alvarion

Uno dei maggiori vantaggi del lavorare con prodotti Alvarion è la sua solida rete di distribuzione. Hanno anche una delle più grandi fette di mercato mondiale dell'hardware wireless per la connessione ad Internet. Ci sono distributori e rivenditori nella maggior parte delle regioni del mondo. Per collegamenti di lunga distanza ci sono due prodotti di interesse: la serie VL, ed il Link Blaster.

La serie VL è in pratica un sistema punto-multipunto, ma un singolo client radio che si connette ad un singolo access point funzionerà benissimo come collegamento punto-punto. L'unica cosa che dovrebbe essere considerata è l'utilizzo di un'antenna più direzionale sull'access point, a meno che non si progetti in futuro di creare un altro collegamento con quell'access point. Ci sono due velocità disponibili per la serie VL: 24 Mbps e 6 Mbps. Il budget, quanto tempo il link deve funzionare, e le esigenze di velocità guideranno la decisione su quale ⚠ CPE ⚠ utilizzare.

Il Link Blaster è molto simile al Redline AN-50. E infatti lo è. Appena il Redline AN-50 è sbarcato sul mercato, è stato firmato un'accordo tra le due compagnie, ed è nato il Link Blaster. Nonostante la unità indoor sia in un case differente, e le antenne siano ⚠ marked ⚠ in maniera diversa, l'elettronica all'interno delle unità è identica. Il Link Blaster costa più di una Redline; questo denaro in più compra un design più ruvido ed un livello di supporto addizionale. In molti casi un rivenditore Alvarion può essere più raggiungibile per le spedizioni di un rivenditore Redline. Questo deve essere ricercato localmente. Il costo in più può essere ripagato se il prodotto è disponibile e supportato localmente.

La Alvarion dispone anche di prodotti da 2.4 GHz punto-punto. La maggior parte della loro linea di prodotti nella banda di 2.4 GHz utilizza FHSS (Frequency Hopping Spread Spectrum) e creerà molto rumore su apparati DSSS (Direct Sequence Spread Spectrum) nella stessa torre. Se è in progetto l'installazione di un sistema di distribuzione basato su DSSS, allora FHSS non sarà una scelta efficace.

Per maggiori informazioni sui prodotti Alvarion, visitare http://www.alvarion.com/

1.4.3 Rad Data Communications

La linea di prodotti Rad Airmux è relativamente nuova nel mercato, ed ha grande potenziale. L'Airmux 200 è un'apparato radio a 48 Mbps, utilizza un cavo CAT5, ed ha uno dei prezzi più amichevoli tra le soluzioni commerciali. Le unità sono piccole e facili da maneggiare su una torre. Il lato negativo che potrebbe essere trovato è la mancanza di un sistema di distribuzione locale nel mondo in via di sviluppo. Ci sono due modelli disponibili nella linea Airmux. Una utilizza antenne interne, e l'altra utilizza antenne esterne.

L'esperienza con gli apparati radio Airmux all'inizio del 2005 mostra che c'è un problema nella configurazione del timing. Problema che si mostra quando la distanza del collegamento è maggiore di 12 miglia, o 19 km. Non importa quali antenne si utilizzino. Fino a quando questo bug non verrà aggiustato, questi apparati radio dovrebbero essere utilizzati solo per collegamenti sotto il 19 km. Quando si segue questo consiglio, questi apparati hanno prestazioni molto buone, specialmente per la loro fascia di prezzo.

Per maggiori informazioni sui prodotti della Rad Data Communications, visitare http://www.rad.com/

1.4.4 Cisco Systems

Le soluzioni wireless della Cisco hanno due grandi punti di forza. Hanno una rete di distribuzione, supporto e addestramento ben cosolidati nella maggior parte del mondo. Ci sono distributori e rivenditori dapertutto. Questo può aiutare molto quando giunge il momento di procurarsi le apparecchiature, e soprattutto, se le apparecchiature si guastano e devono essere rimpiazzate. L'altro grande punto di forza è che per la maggior parte, utilizzano standard aperti. La maggior parte delle loro apparecchiature segue gli standard 802.11a/b/g.

L'esperienza ha dimostrato che i loro strumenti di configurazioni web-based non sono facili da capire come quelli di molti altri prodotti, e le apparecchiature tendono ad avere un prezzo che rendono altre soluzioni non commerciali a standard aperto più percorribili.

Maggiori informazioni sulla Cisco possono essere trovate su http://www.cisco.com/

1.4.5 Altre?

Ci sono molte altre soluzioni disponibili sul mercato ora, e ce ne sono sempre in uscita. Buone soluzioni sono disponibili da compagnie come la Trango Broadband (http://www.trangobroadband.com/) e la Waverider Communications (http://www.waverider.com/). Quando si considera quale soluzione utilizzare, ricordarsi sempre i tre fattori principali; distanza, velocità e per quanto tempo deve funzionare il collegamento. Controllare ed assiscurarsi che gli apparati radio operino su una frequenza libera prima di installarli.

1.4.6 Protezione professionale dai fulmini

L'unico predatore naturale dell'attrezzatura wireless è il fulmine. Ci sono due modi in cui un fulmine può colpire o danneggiare l'attrezzatura: colpirla direttamente o colpirla tramite induzione. I colpi diretti accadono quando il fulmine effettivamente colpisce la torre o l'antenna. I colpi indotti sono causati da fulmini che cadono vicino alla torre. Immaginiamo un fulmine carico negativamente. Dal momento che le cariche si respingono, quel fulmine farà allontanare gli elettroni nei cavi lontano dal punto colpito, creando corrente nelle linee. Questa, però, sarà più corrente di quella che le sensibili apparecchiature radio sono in grado di gestire. Tutt'e due i tipi di colpo normalmente distruggeranno le apparecchiature che sono senza protezione.

Figura 5.2: Una torre con un massiccio cavo metallico di messa a terra.

Proteggere le reti wireles dai fulmini non è una scienza esatta, e non c'è garanzia che non possa capitare che l'apparecchiatura venga colpita da un fulmine, anche se si prende ogni singola precauzione. Molti dei metodi utilizzati aiuteranno a prevenire sia i colpi diretti che quelli da induzione. Mentre non è necessario utilizzare ogni metodo di protezione dai fulmini, l'utilizzo di più metodi aiuterà a proteggere meglio le apparecchiature. La quantità di fulmini storicamente osservata nell'area che si intende servire sarà la migliore guida per sapere quanto lavoro debba essere fatto.

Cominciamo dalla base della torre. Non dimentichiamo che la base della torre si trova sotto il livello del suolo. Dopo aver steso le fondamenta della torre, ma prima che il buco venga riempito, un massiccio anello di cavo intrecciato dovrebbe essere installato con ⚠ the lead = un capo? del piombo? ⚠ che arrvi fino alla superficie del suolo vicino ad una gamba della torre. Il cavo dovrebbe essere del tipo American Wire Gauge (AWG) #4 o più spesso. In aggiunta, dovrebbe essere piantato un paletto di messa a terra di riserva, ed un cavo di messa a terra portato dal paletto al ⚠ lead = capo? ⚠ dell'anello interrato.

E' importante notare che non tutto l'acciaio conduce l'elettricità nello stesso modo. Alcuni tipi di acciaio sono conduttori elettrici migliori di altri, e i diversi tipi di ricopertura possono influenzare il comportamento della torre rispetto alla corrente elettrica. L'acciaio inossidabile è uno dei conduttori peggiori, e ricoperture a prova di ruggine come la cromatura o la vernice diminuiscono la conduttività dell'acciaio. Per questa ragione, un cavo di terra intrecciato viene portato dalla base della torre fino in cima. La base deve essere ben fissata ai ⚠ leads=capi? ⚠ sia dell'anello che del paletto di messa a terra di riserva. In cima alla torre dovrebbe essere fissato un parafulmine, la cui punta dovrebbe essere acuminata. Più la punta sarà fina ed acuminata, più sarà efficace. Il cavo intrecciato di messa a terra alla base deve finire su questo parafulmine. E' molto importante assicurarsi che il cavo di terra sia connesso effettivamente al metallo. Ogni tipo di ricopertura, come la vernice, deve essere rimossa prima di fissare il cavo. Una volta fatta la connessione, l'area esposta può essere riverniciata, coprendo il cavo ed i connettori se necessario per proteggere la torre da ruggine e corrosione.

La soluzione sopra esposta riguarda l'installazione del sistema di messa a terra di base. Fornisce protezione

per la stessa torre dai fulmini diretti, ed installa il sistema di base a cui verrà collegata ogni altra cosa.

La protezione ideale per i colpi da induzione indiretta da fulmine sono gas tube arrestors = tubi per il gas a tutt'e due i capi del cavo. Il capo superiore deve essere messo a terra direttamente tramite il cavo di messa a terra installato nella torre. Il capo inferiore deve essere messo a terra tramite qualcosa di elettricamente sicuro, come una lastra o un tubo di rame ben riempito d'acqua. E' importante assicurarsi che il outdoor lightning arrestor = scaricatore per fulmini da esterno sia reso resistente alle intemperie. Molti arresters=scaricatori per cavi coassiali sono resistenti alle intemperie, mentre molti scaricatori per cavi CAT5 non lo sono.

Nell'eventualità che i tubi per il gas non vengano utilizzati, e che il cablaggio sia prevalentemente coassiale, allora fissare un capo del cavo alla schermatura del coassiale e l'altro capo alla messa a terra installata sulle torri fornirà un certo grado di protezione. Questo può fornire un percorso alle correnti indotte, e se la carica è abbastanza debole, non influirà sul filo conduttore del cavo coassiale. Questo metodo non è assolutamente una protezione buona come quella fornita dai gas arrestors /!\, ma è meglio di niente.

1.5 Costruire un AP da un PC

Diversamente dai sistemi operativi commerciali (come Microsoft Windows), il sistema operativo GNU/Linux fornisce all'amministratore di rete potenzialmente l'accesso totale alla pila TCP/IP (networking stack) . Si può accedere ai pacchetti di rete e manipolarli ad ogni livello: dal data-link fino al livello applicativo. Le decisioni di routing possono essere basate su ogni infomazione contenuta in un pacchetto di rete, da indirizzi di instradamento e porte fino ai dati contenuti. Un access point linux-based può funzionare da router, bridge, firewall, concentratore VPN, server applicativo, monitor di rete, o virtualmente ogni altro ruolo al quale si possa pensare su una rete. E' software disponibile gratuitamente e non richiede pagamenti per la licenza. GNU/Linux è uno strumento molto potente che può ricoprire un'ampia varietà di ruoli in un'infrastruttura di rete.

Aggiungendo una scheda wireless ed una ethernet ad un PC sul quale giri Linux, si otterrà uno strumento molto flessibile che può aiutare a fornire larghezza di banda e gestire la propria rete ad un costo molto basso. L'hardware potrebbe essere qualunque cosa, da un portatile o una macchina desktop riciclata fino a un computer embedded, come un Linksys WRT54G o un kit di rete della Metrix.

In questa sezione vedremo come configurare Linux nelle seguenti configurazioni:

- Come wireless access point con masquerading/NAT ed una connessione su filo ad Internet (detta anche configurazione wireless gateway).
- Come wireless access point che si comporti come bridge trasparente. Il bridge può essere utilizzato sa come un semplice access point che come ripetitore con 2 dispositivi radio.

Queste ricette devono essere considerate un punto di partenza. Sopra a questi esempi può essere creato il server che si adatta esattamente ad ogni infrastruttura di rete.

1.5.1 Prerequisiti

Prima di continuare, bisognerebbe avere una certa familiarità come utente linux, ed essere capaci di installare una distribuzione GNU/Linux a scelta. E' richiesta anche una conoscenza basilare dell'interfaccia a riga di comando (terminale) di Linux.

Avremo bisogno di un computer con una o più schede wireless installate, così come un interfaccia Ethernet standard. Questi esempi utilizzano una scheda ed un driver specifici, ma ci sono diverse schede che dovrebbero funzionare altrettanto bene. Le schede wireless basate sui chipset Atheros e Prism funzionano particolarmente bene. Questi esempi sono basati su Ubuntu Linux versione 5.10 (Breezy Badger) con una scheda wireless che è supportata dai drivers HostAP o MADWiFi. Per maggiori informazioni su questi driver

visitare http://hostap.epitest.fi/ e http://madwifi.org/ .

Il seguente software è necessario per completare queste installazioni. Dovrebbe essere incluso nella distribuzione Linux.

- Wireless Tools (comandi iwconfig e iwlist)
- il firewall iptables
- dnsmasq (server di caching DNS e DHCP)

I requisiti di potenza della CPU dipendono da quanto lavoro deve essere fatto oltre al semplice routing e NAT. Per molte applicazioni, un 486 a 133MHz è perfettamente in grado di instradare pacchetti alle velocità del wireless. Se si intende utilizzare molta crittazione (come la WEP od un server VPN), allora si avrà bisogno di qualcosa di più veloce. Se si vuole anche far girare un caching server (come Squid, vedere il capitolo tre) allora si avrà bisogno di un computer dotato di molta RAM ed un hard disk capace e veloce. Un tipico router per il solo NAT funzionerà con soli 64MB di RAM e spazio su disco.

Quando si costruisce una macchina che si intende inserire nell'infrastruttura di rete, bisogna tenere a mente che gli hard disk hanno una durata limitata rispetto alla maggior parte degli altri componenti. Si può spesso utilizzare memoria a stato solido, come un disco flash, invece di un hard disk. Questo potrebbe essere un flash drive USB (assumendo che il PC sia in grado di fare il boot da USB), o una scheda Compact Flash che utilizzi un adattatore da CF a IDE. Questi adattatori sono poco costosi, e faranno apparire una scheda CF come un hard disk IDE standard. Possono essere utilizzate in ogni PC che supporta hard disk IDE. Dal momento che non hanno parti mobili, funzioneranno per molti anni in un intervallo di temperature più grande di quello che può tollerare un hard disk.

1.5.2 Scenario 1: Access point con IP masquerade

Questo è lo scenario più semplice, ed è specialmente utile nelle situazioni in cui si vuole un singolo access point per l'installazione in un ufficio. Questo è più facile in una situazione in cui:

1. E' già presente una macchina Linux dedicata a gateway e firewall e si vuole aggiungere un'interfaccia wireless.
2. Si dispone di un vecchio computer o laptop recuperato, e si preferisce utilizzarlo come access point.
3. Si necessita di più potenza in termini di monitoraggio, logging e/o sicurezza di quella che la maggior parte degli access point commerciali forniscono, ma non si vuole spendere in un access point di livello superiore.
4. Si vorrebbe che una singola macchina si comportasse come 2 access point (e firewall) in modo da poter offrire sia un accesso sicuro all'intranet, che un accesso aperto agli ospiti.

1.5.2.1 Impostazione iniziale

Iniziamo con un computer già configurato su cui giri GNU/Linux. Questa potrebbe essere un'installazione di Ubuntu Server, o Fedora Core. Il computer deve avere almeno 2 interfacce perché questo funzioni, ed almeno una di queste interfacce dovrebbe essere wireless. Il resto di questa descrizione assume che la porta Ehernet "cablata" (eth0) sia connessa ad Internet, e che ci sia un'interfaccia wireless (wlan0) che possa funzionare da access point.

Per capire se il chipset supporta la modalità master, provare a dare il seguente comando come root:

```
# iwconfig wlan0 mode Master
```

...sostituendo wlan0 con il nome dell'interfaccia wireless.

Se si riceve un messaggio di errore, allora la scheda wireless non supporta la modalità access point. Si può comunque provare la stessa configurazione in modalità ad-hoc, che è supportata da tutti i chipset. Questo richiede che si configurino anche tutti i portatili che si collegano a questo "access point" in modalità ad-hoc, e potrebbe non funzionare esattamente nel modo aspettato. Normalmente sarebbe meglio trovare una scheda wireless che supporti la modalità AP. Vedere i siti di HostAP e MADWi-Fi menzionati sopra per una lista delle schede supportate.

Prima di continuare, assicurarsi che dnsmasq sia installato sulla macchina. Si può utilizzare il gestore di pacchetti grafico della propria distribuzione per installarlo. In ubuntu si può semplicemente digitare il seguente comando come root:

```
# apt-get install dnsmasq
```

1.5.2.2 Configurare le interfacce

Configurare il server in modo che eth0 sia connessa ad Internet. Utilizzare lo strumento di configurazione grafico della propria distribuzione.

Se la rete Ethernet utilizza DHCP, si può provare a digitare il seguente comando come root:

```
# dhclient eth0
```

Si dovrebbe ricevere un indirizzo IP e un default gateway. Quindi configurare l'interfaccia wireless in modalità master e scegliere un nome per la rete.

```
# iwconfig wlan0 essid "rete mia" mode Master enc off
```

L'opzione **`enc off`** disattiva la crittazione WEP. Per abilitare il WEP, aggiungere una chiave esadecimale della lunghezza corretta:

```
# iwconfig wlan0 essid "rete mia" mode Master enc 1A2B3C4D5E
```

In alternativa, si può utilizzare una stringa leggibile facendola preponendo "s:"

```
# iwconfig wlan0 essid "rete mia" mode Master enc "s:apple"
```

Ora dare all'interfaccia wireless un indirizzo IP in una sottorete privata, ma assicurarsi che non sia la stessa sottorete del dispositivo Ethernet:

```
# ifconfig wlan0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255 up
```

1.5.2.3 Configurare il masquerade nel kernel

Per fare in modo di poter tradurre gli indirizzi tra le due interfacce del computer, abbiamo bisogno di abilitare il masquerading (NAT) nel kernel Linux. Prima dobbiamo caricare il modulo del kernel che ci interessa:

```
# modprobe ipt_MASQUERADE
```

Ora faremo il flush (cancelleremo) tutte le regole esistenti del firewall per assicurarci che il firewall non ci stia bloccando nell'inoltro dei pacchetti tra le due interfacce. Se si ha un firewall in funzione, assicurarsi di sapere come ripristinare più tardi le regole esistenti prima di procedere.

```
# iptables -F
```

Abilitare la funzionalità di NAT tra le due interfacce

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Infine dobbiamo abilitare il kernel ad inoltrare pacchetti tra interfacce:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Su distribuzioni Linux Debian-based quali Ubuntu, questo cambiamento può anche essere fatto modificando il file **/etc/network/options**, e cambiando la linea

```
ip_forward=no
```

in

```
ip_forward=yes
```

e quindi facendo ripartire le interfacce di rete con:

```
# /etc/init.d/network restart
```

oppure

```
# /etc/init.d/networking restart
```

1.5.2.4 Configurare il server DHCP

A questo punto dovremmo avere un access point funzionante. Può essere testato collegandosi alla rete wireless "rete mia" con una macchina diversa e dando a quella macchina un indirizzo nello stesso intervallo di indirizzi dell'interfaccia wireless sul server (10.0.0.0/24 se si sono seguiti gli esempi). Se il WEP è stato abilitato, assicurarsi di utilizzare la stessa chiave specificata sull'AP.

Per facilitare la connessione di persone al server senza conoscere l'intervallo di indirizzi IP, configureremo un server DHCP per passare automaticamente indirizzi ai client wireless.

Utilizziamo il programma dnsmasq a questo scopo. Come il nome indica, fornisce un server di caching DNS ed un server DHCP. Questo programma è stato sviluppato specialmente per l'utilizzo con firewall che fanno NAT. Avere un server di caching DNS è specialmente utile se la connessione Internet di cui si dispone è ad alta latenza e/o si dispone di poca banda, come per un collegamento VSAT o dial-up. Significa che molte query DNS possono essere risolte localmente, risparmiando molto traffico sulla connessione Internet, e dando l'impressione di maggiore velocità a chi si connette.

Installare dnsmasq con il gestore di pacchetti della propria distribuzione. Se dnsmasq non è disponibile come pacchetto, scaricare il codice sorgente ed installarlo manualmente. Si trova su http://thekelleys.org.uk/dnsmasq/doc.html .

Tutto ciò di cui abbiamo bisogno per far girare dnsmasq è la modifica di alcune righe del file di configurazione di dnsmasq, /etc/dnsmasq.conf .

Il file di configurazione è ben commentato, ed ha molte opzioni per vari tipi di configurazione. Per ottenere il funzionamento del server DHCP basilare abbiamo bisogno di scommentare e/o modificare due righe.

Trovare la riga che inizia con:

```
interface=
```

...e farla diventare:

```
interface=wlan0
```

...sostituendo wlan0 con il nome dell'interfaccia wireless. Quindi trovare la riga che inizia con:

```
#dhcp-range=
```

Scommentare la riga e modificarla in modo che corrisponda agli indirizzi utilizzati, per esempio:

```
dhcp-range=10.0.0.10,10.0.0.110,255.255.255.0,6h
```

Quindi salvare il file ed avviare dnsmasq:

```
# /etc/init.d/dnsmasq start
```

Ora dovremmo essere in grado di collegarci al server come access point, ed ottenere un indirizzo IP utilizzando DHCP. Questo dovrebbe permetterci di connetterci ad Internet attraverso il server.

1.5.2.5 Aumentare la sicurezza: Configurare un firewall

Una volta che abbiamo un sistema funzionante e testato, possiamo aggiungere regole extra al firewall utilizzando qualunque strumento di firewall che sia incluso nella nostra distribuzione. Alcuni tipici front-end per configurare le regole del firewall includono:

- *firestarter* - un client grafico per Gnome, che richiede che sul server giri Gnome
- *knetfilter* - un client grafico per KDE, che richiede che sul server gidi KDE
- *Shorewall* - un insieme di script e file di configurazione che renderanno più facile configurare un firewall iptables. Ci sono anche frontend per shorewall, come webmin-shorewall.
- *fwbuilder* - un potente, ma leggermente complicato, tool grafico che permetterà di creare script iptables su una macchina separata dal server, e poi trasferirli più tardi sul server. Questo non richiede che sul server giri un desktop grafico, e questa è una buona scelta per chi si intende di sicurezza

Una volta che tutto sia stato ben configurato, assicurarsi che tutte le impostazioni siano rispecchiate dagli script di avvio. In questo modo i cambiamenti continueranno a funzionare anche se la macchina dovesse necessitare un riavvio.

1.5.3 Scenario 2: Access point con bridge trasparente

Questo scenario può essere utilizzato sia per un ripetitore a doppio dispositivo radio, che per un access point collegato ad un dispositivo Ethernet. Utilizziamo un bridge invece del routing quando vogliamo che tutt'e due le interfacce sull'access point condividano la stessa subnet. Questo può essere particolarmente utile in reti con più access point dove preferiamo avere un singolo firewall, e magari anche server di autenticazione, centrale. Dal momento che tutti i client condividono la stessa subnet possono essere facilmente gestiti con un solo server DHCP e firewall senza il bisogno di utilizzare il DHCP relay.

Per esempio, si potrebbe configurare un server come nel primo scenario, ma utilizzare due interfacce cablate Ethernet invece di una cablata e una wireless. Un'interfaccia potrebbe essere la connessione Internet, e l'altra potrebbe collegarsi ad uno switch. Quindi collegare tanti access point quanti servono allo stesso switch, configurarli come bridge trasparenti, e tutti passeranno attraverso lo stesso firewall ed utilizzeranno lo stesso server DHCP.

La semplicità del bridge va a discapito dell'efficienza. Dal momento che tutti i client condividono la stessa subnet, il traffico broadcast sarà ripetuto su tutta la rete. Questo normalmente va bene per le piccole reti, ma con il crescere del numero di client, più larghezza di banda wireless verrà sprecata in traffico di rete di tipo broadcast.

1.5.3.1 Impostazione iniziale

La configurazione iniziale per un bridging access point è simile a quella di un masquerading access point, senza il requisito di dnsmasq. Seguire le istruzioni per l'impostazione iniziale del precedente esempio.

In più, il pacchetto ***bridge-utils*** è richiesto per il bridging. Questo pacchetto esiste per Ubuntu ed altre distribuzioni Debian-based, così come per Fedora Core. Assicurarsi che sia installato e che il comando **`brctl`** sia disponibile prima di continuare.

1.5.3.2 Configurare le interfacce

Su Ubuntu o Debian configuriamo le interfacce modificando il file /etc/network/interfaces

Aggiungere una sezione come la seguente, ma cambiando i nomi delle itnerfacce e gli indirizzi IP coerentemente. L'indirizzo IP e la netmask devono corrispondere a quelli della rete esistente. Questo esempio assume che si stia costruendo un repeater wireless con due interfacce wireless, wlan0 e wlan1. L'interfaccia

wlan0 sarà un client per la rete "ufficio", e wlan1 creerà una rete chiamata "repeater".

Aggiungere quanto segue a */etc/network/interfaces*:

```
auto br0 ¶
iface br0 inet static ¶
· address 192.168.1.2 ¶
· network 192.168.1.0 ¶
· netmask 255.255.255.0 ¶
· broadcast 192.168.1.255 ¶
· gateway 192.168.1.1 ¶
· pre-up ifconfig wlan 0 0.0.0.0 up ¶
· pre-up ifconfig wlan1 0.0.0.0 up ¶
· pre-up iwconfig wlan0 essid "ufficio" mode Managed ¶
· pre-up iwconfig wlan1 essid "repeater" mode Master ¶
· bridge_ports wlan0 wlan1 ¶
· post-down ifconfig wlan1 down ¶
· post-down ifconfig wlan0 down ¶
```

Commentare ogni altra sezione del file che si riferisca a wlan0 o wlan1 per assicurarsi che non interferisca con la configurazione.

Questa sintassi per configurare i bridge tramite il file *interfaces* è specifico per distribuzioni Debian-based, ed i dettagli dell'effettiva configurazione del bridge sono gestiti da un paio di script: */etc/network/if-pre-up.d/bridge* e */etc/network/if-post-down.d/bridge*. La documentazione per questi script si trova in */usr/share/doc/bridge-utils/*.

Se questi script non esistono nella distribuzione (come, ad esempio, in Fedora Core), qui c'è una configurazione alternativa che raggiungerà lo stesso obiettivo in maniera leggermente più tortuosa:

```
iface br0 inet static ¶
· pre-up ifconfig wlan 0 0.0.0.0 up ¶
· pre-up ifconfig wlan1 0.0.0.0 up ¶
· pre-up iwconfig wlan0 essid "ufficio" mode Managed ¶
· pre-up iwconfig wlan1 essid "repeater" mode Master ¶
· pre-up brctl addbr br0 ¶
· pre-up brctl addif br0 wlan0 ¶
· pre-up brctl addif br0 wlan1 ¶
· post-down ifconfig wlan1 down ¶
· post-down ifconfig wlan0 down ¶
· post-down brctl delif br0 wlan0 ¶
· post-down brctl delif br0 wlan1 ¶
· post-down brctl delbr br0 ¶
```

1.5.3.3 Avviare il bridge

Una volta che il bridge è definito come interfaccia, avviarlo è facile quanto digitare:

```
# ifup -v br0
```

La "-v" significa output verboso e darà informazioni su cosa sta accadendo.

Su Fedora Core (cioè distribuzioni non Debian) c'è ancora bisogno di dare all'interfaccia di bridge un indirizzo IP ed aggiungere una rotta di default al resto della rete:

```
# ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
¶
# route add default gw 192.168.1.1 ¶
```

Ora si dovrebbe essere in grado di collegare un portatile wireless a questo nuovo access point, e collegarsi ad Internet (o almeno al resto della rete) attraverso questa macchina.

Volendo più informazioni sul bridge e su quello che sta facendo, si può dare un'occhiata al comando brctl. Per esempio si può provare questo comando:

```
# brctl show br0
```

Che dovrebbe mostrare alcune informazioni su quello che sta facendo il bridge.

1.5.4 Scenari 1 & 2 in maniera facile

Invece di configurare un computer come access point da zero, si potrebbe utilizzare una distribuzione Linux dedicata che sia fatta apposta per questo scopo. Queste distribuzioni possono rendere il lavoro semplice come fare il boot da un particolare CD su un computer con un'interfaccia wireless. Per maggiori informazioni, riferirsi alla prossima sezione "Sistemi operativi wireless-friendly".

Come si può vedere, è semplice fornire un servizio di access point da un router Linux standard. Utilizzare Linux dà significativamente più controllo sull'instradamento dei pacchetti sulla rete, e aggiunge caratteristiche che semplicemente non ci sono sugli access point commerciali.

Per esempio, si potrebbe iniziare con uno dei due esempi visti prima ed implementare una rete wireless privata dove gli utenti sono autenticati utilizzando un web browser standard. Utilizzando un captive portal quale Chillispot, si possono controllare le credenziali degli utenti wireless rispetto ad un database esistente (per esempio un Windows domain server accessibile via RADIUS). Questa configurazione potrebbe permettere un accesso preferenziale agli utenti nel database, fornendo un livello molto limitato di accesso al resto del mondo.

Un'altra applicazione popolare è il modello commerciale prepagato. In questo modello, gli utenti devono comperare un biglietto prima di accedere alla rete. Questo biglietto fornisce una password che è valida per un tempo limitato (tipicamente un giorno). Quando il biglietto scade, l'utente ne deve comperare un altro. Questa funzionalità di ticketing è disponibile solamente su apparecchiature di rete commerciali relativamente costose, ma può essere implementata utilizzando software libero quale Chillispot e phpMyPrePaid. Vedremo altro sulla tecnologia dei captive portal e dei sistemi di ticketing nella sezione **Autenticazione** del capitolo sei.

1.5.5 Sistemi operativi wireless-friendly

Ci sono vari sistemi operativi open source che forniscono strumenti utili per lavorare con le reti wireless. Questi sono ideati per essere utilizati su PC recuperati o altro hardware di rete (piuttosto che su un laptop o su un server) e sono ottimizzati per costruire reti wireless. Alcuni di questi progetti sono:

- **Freifunk**. Basato sul progetto OpenWRT (http://openwrt.org), il firmware Freifunk porta agli access point MIPS-based, come i Linksys WRT54G / WRT54GS / WAP54G, Siemens SE505, ed altri, un supporto per OLSR di facile utilizzo. ⚠ Flashando ⚠ semplicemente uno di questi AP con il firmware Freifunk, si può rapidamente costruire una rete mesh OLSR autoconfigurante. Freifunk non è attualmente disponibile per macchine con architettura x86. E' mantenuto da Sven Ola del gruppo wireless Freifunk di Berlino. Si può scaricare il firmware da http://www.freifunk.net/wiki/FreifunkFirmware .
- **Metrix Pebble**. Il progetto Pebble Linux è stato iniziato nel 2002 da Terry Schmidt del gruppo NYCwireless. Era originariamente una versione allegerita della distribuzione Debian Linux che includeva wireless, firewall, gestione del traffico e strumenti di routing. Dal 2004, la Metrix Communication ha ingrandito Pebble includendo driver aggiornati, monitoraggio della banda, ed un tool di configurazione web-based. Lo scopo di Metrix Pebble è quello di fornire una piattaforma completa per lo sviluppo wireless. Funziona su hardware x86 con almeno 64MB di memoria flash o hard disk. Si può scaricare Metrix Pebble da http://metrix.net/metrix/howto/metrix-pebble.html .
- **m0n0wall**. Basato su FreeBSD, m0n0wall è un pacchetto firewall molto piccolo ma completo che fornisce servizi da AP. E' configurato da un interfaccia web e l'intera configurazione di sistema è memorizzata in un singolo file XML. Le sue piccole dimensioni (meno di 6MB) lo rendono appetibile per sistemi embedded molto piccoli. Il suo obiettivo è quello di fornire un firewall sicuro, e quindi non include strumenti user-space (non è neanche possibile loggarsi nella macchina attraverso la rete). Nonostante questa limitazione è una scelta popolare tra i "wireless networkers", particolarmente tra quelli familiari con FreeBSD. Si può scaricare m0n0wall da http://www.m0n0.ch/.

Tutte queste distribuzioni sono progettate per macchine con memoria secondaria limitata. Se si sta utilizzando un disco flash molto grande o un hard disk, si può certamente installare un sistema operativo più completo (quali Ubuntu o Debian) ed utilizzare la macchina come router o access point. Probabilmente assicurarsi che tutti i tool necessari siano inclusi, senza installare pacchetti non necessari porterà via molto tempo di sviluppo. Utilizzando uno di questi progetti come punto di partenza per costruire un nodo wireless, si risparmierà notevole tempo e sforzo.

1.5.6 Il Linksys WRT54G

Uno dei più popolari access point commerciali attualmente sul mercato è il Linsys WRT54G. Questo access point dispone di due connettori esterni per antenna RP-TNC, uno switch Ethernet da quattro porte, ed un dispositivo radio 802.11b/g. Viene configurato attraverso una semplice interfaccia web. Nonostante non sia progettato come soluzione outdoor, può essere installato in una grande ⚠ scatola da elettricista (sprinkler box= da annaffiatoio?) ⚠ o in una vasca di plastica ad un costo relativamente basso. Al momento in cui scriviamo, il WRT54G si vende a circa $60 ⚠ (70-80 euro in Italia) [ce l'aggiungiamo?] ⚠ .

Nel 2003, dei network hacker capirono che il firmware del WRT54G era in realtà una versione di Linux. Questo portò ad un grande interesse per la costruzione di firmware personalizzato che allargasse le possibilità del router significativamente. Alcune di queste nuove caratteristiche includono supporto per la modalità client, captive portals e mesh networking. Due popolari pacchetti alternativi di firmware per il WRT54G sono OpenWRT (http://openwrt.org/) e Freifunk (http://www.freifunk.net/wiki/FreifunkFirmware).

Sfortunatamente, nell'autunno 2005, la Linksys ha rilasciato la versione 5 del WRT54G. Questa revisione hardware ha eliminato della RAM e della memoria flash sulla scheda madre, rendendo praticamente impossibile far girare Linux (viene con VxWorks, un sistema operativo molto più piccolo che non permette una personalizzazione semplice). Dal momento che il WRT54G v5 non può far girare firmware Linux personalizzato, questo lo rende un'alternativa meno attrattiva per chi costruisce reti. La Linksys ha rilasciato anche il WRT54GL, che è essenzialmente il WRT54G v4 (sul quale gira Linux) ad un prezzo leggermente più alto.

Linux gira anche su altri access point Linksys, incluso il WRT54GS e il WAP54G. Mentre questi hanno anche prezzi relativamente bassi, le specifiche hardware possono cambiare in ogni momento. E' difficile sapere

quale revisione hardware è utilizzata senza aprire la confezione, facendo diventare rischioso l'acquisto in un negozio al dettaglio e praticamente impossibile da ordinare online. Mentre sul WRT54GL c'è la garanzia che giri Linux, la Linksys ha fatto sapere che non si aspetta di vendere grandi volumi di questo modello, e non è chiaro per quanto tempo rimarrà in vendita.

Se si è in grado di trovare una fonte di WRT54G con revisioni antecedenti o WRT54GL, sono router utili e poco costosi. Con firmware personalizzato possono essere configurati per lavorare come una mesh OLSR o in modalità client, e funzionano molto bene come soluzione lato cliente poco costosa. Mentre il nuovo modello v5 funzionerà come access point, non può essere configurato come client, e si riportano  prestazioni discordanti (mixed reviews)  rispetto al v4 ed ai modelli precedenti.

Per maggiori informazioni, visitare uno dei seguenti siti web:

- http://linksysinfo.org/
- http://seattlewireless.net/index.cgi/LinksysWrt54g