# GUIDA ALLE W-LAN


**lo studio, la realizzazione teorico-pratica,**
**la sicurezza, il modding e l'hacking**
**per il neofita e l'utente evoluto**

**Rev. 0.9.1-5**

**Testo realizzato da Dj Byte con la collaborazione degli utenti del forum di**

**INDICE** Pag.

**INDICE** Pag.

**Installazioni in esterno**



**Hacking degli apparati**



**PC in rete: la creazione**



**Servizi nella W-LAN**



**Sicurezza avanzata**

**INDICE** Pag.

## Prefazione

Lavorare o navigare senza meta nell'infinità di internet, comodamente seduti sulla poltrona o sul divano di casa, sdraiati a prendere il sole nel giardino in una bella giornata estiva, non è più mera fantasia. La comodità di una rete senza fili ha numerosi vantaggi ma, come tutte le cose, esistono anche alcuni aspetti negativi che devono essere presi in considerazione, onde evitare spiacevoli conseguenze.
Con il diffondersi ed il calare del costo d'acquisto degli apparati Wi-Fi, molte persone hanno iniziato a sperimentare l'utilizzo di access point apportando modifiche hardware, estendendo la propria rete casalinga. Gruppi di amici si uniscono tra loro creando celle di reti piuttosto ampie, dove risorse e passioni comuni si uniscono in un'unica entità. Grazie agli appassionati, si assiste al passaggio all'uso "esterno" di apparati che sono nati per un uso "interno" alla propria abitazione.

Questa guida nasce da una passione personale, frutto di molte ore passate a sperimentare e di estenuanti ricerche in internet, spesso infruttuose; non vuole essere una sorta di testo definitivo sulle reti senza fili ma una risposta alle molte domande e perplessità che un utente alle prime armi si pone, aiutandolo a capire i fondamenti, le difficoltà e la risoluzione dei problemi d'installazione e gestione iniziale di questa tecnologia; non si vuole trascurare nemmeno l'utente evoluto che vuole ottenere il massimo dai suoi apparati con realizzazioni al limite della fantasia e della tecnica.

Credendo nella libertà di parola ed espressione, nell'aiuto reciproco, nella divulgazione della conoscenza e nell'open source, questa giuda è resa disponibile a tutti secondo la licenza pubblica generale (GPL), modificabile, integrabile, traducibile in ogni lingua e stampabile infinite volte, indicando sempre l'autore o gli autori del progetto di base. Le informazioni qui contenute hanno il solo scopo didattico e divulgativo. L'autore declina ogni responsabilità circa l'uso improprio delle tecniche descritte all'interno.

Un ringraziamento particolare è rivolto agli utenti del forum di www.nabuk.org, ai LUG (Linux User Group) italiani, che hanno prestato la loro assistenza e competenza, correggendo alcuni "bug" di questa guida e a coloro che hanno suggerito quali argomenti trattare in modo più approfondito; per ultimo ma non ultimo, voglio ringraziare tutte le comunità del software libero e che ci aiutino a creare un mondo migliore...

***Dj Byte***

## Introduzione alla guida e convenzioni utilizzate

Questa guida alle W-LAN non ha pretese di essere o diventare una guida definitava, ma vuole costituire un aiuto e supporto a coloro che vogliono realizzare una propria rete wireless utilizzando lo standard Wi-Fi oppure a coloro che vogliono sperimentare, utilizzando come "base di partenza" quanto già sperimentato da altri... In linea generale, s'è cercato d'utilizzare un linguaggio il più semplice possibile, usando terminologie informatiche e tecniche solamente dove l'uso di parole "alternative" avrebbe compromesso il senso di quanto esposto. In questa guida saranno utilizzate le seguenti note:

Nota interessante, tip, informazione tecnica.

Cautela, potenziali problemi di configurazione.

Attenzione, potenziali rischi sulla sicurezza del sistema.

I nomi dei file ed i percorsi verranno visualizzati con caratteri a spaziatura singola, così come i comandi da digitare a riga di comando verranno visualizzati in questo modo:

**$comando da digitare** [tasto da premere]

I tasti principali utilizzati, quando richiesti, saranno così visualizzati:

| | |
|---|---|
| [Ctrl] | Pulsante Control |
| [invio] | Pulsante invio |
| [Shift] | Pulsante Shift |
| [Alt] | Pulsante Alternate |

La selezione di un'opzione viene visualizzata nel modo "**Scelta opzione**", mentre il listato di un file di configurazione:

**listato**

# *Generalità e informazioni di base*

## 1.1 Cos'è una rete

In ambito informatico una rete viene definita come l'insieme di due o più computer od altri dispositivi in grado di scambiarsi informazioni o dati. Esistono molte tipologie di reti e quindi di suddivisione delle stesse che, generalmente, vengono suddivise in base alla forma dell'architettura:

- **Stella:** in questo tipo di reti c'è un computer centrale, solitamente un server, che si occupa di smistare tutte le comunicazioni tra i vari client. Fisicamente tale rete ha tanti cavi quanti sono i client connessi al centro-stella (server);
- **Bus:** questa configurazione, al contrario di quella a stella, non prevede un server centrale perciò l'informazione generata viene inviata su un cavo (detto appunto bus) che collega in parallelo tutti i computer che sono in grado di ascoltare i dati che vi transitano.
- **Anello:** detta anche "Token Ring", anche questa configurazione prevede, come quelle a bus, la presenza di un solo cavo di collegamento che però collega i vari computer in serie, anziché in parallelo, formando un anello chiuso. La comunicazione tra i computer avviene attraverso l'assegnazione ciclica di un Token, cioè il diritto di un computer a comunicare. Il proprietario immette il dato sulla rete che viene trasmessa al computer successivo che, nel caso sia lui il destinatario, accetterà il dato, altrimenti lo passerà a quello successivo, fino al raggiungimento del destinatario. Quest'ultimo accetterà il dato ma non lo cancellerà dalla rete perché, essendo ad anello, dovrà ritornare al mittente che, alla ricezione, provvederà a passare il Token al computer successivo, in maniera ciclica.
- **Mesh:** in questa configurazione non esistono né una struttura server-client né una vera e propria forma fisica. Ogni computer deve funzionare da server e da client, quindi ripetere i dati ricevuti ma indirizzati ad altri computer. Questo tipo di rete offre notevoli vantaggi in ambito delle tipologie wireless.

Ai fini pratici, le reti di tipo Bus e ad Anello, stanno andando in disuso, mentre quelle a Stella sono preferite in ambito aziendale o casalingo, tramite l'uso di switch. La classificazione di una rete viene anche integrata da quella riguardante le dimensioni della rete stessa. Entrano perciò in gioco i seguenti acronimi:

- **PAN:** detta anche Personal Area Network, indica una rete di ridottissime dimensioni e composta da un paio di elementi poco distanti tra loro (generalmente una stanza);
- **LAN:** detta anche Local Area Network, è una rete di dimensioni più rilevanti rispetto la PAN, sia dal punto di vista geografico (anche un edificio intero) sia in termini di computer collegati;
- **CAN:** detta anche Campus Area Network, è una rete di dimensioni maggiori di una LAN, che permette geograficamente la connessione di qualche edificio;
- **MAN:** detta anche Metropolitan Area Network, indica una rete in grado di coprire geograficamente un'area metropolitana;
- **WAN:** detta anche Wide Area Network, indica una rete in grado di coprire geograficamente intere regioni o nazioni;
- **GAN:** detta anche Global Area Network, indica l'unione di più reti WAN.

La corretta descrizione della rete deve perciò comprendere: architettura, dimensione, tipologia wired o wireless (cablata o senza fili).

## 1.2 Come si riconoscono i PC in rete: ovvero l'indirizzo IP

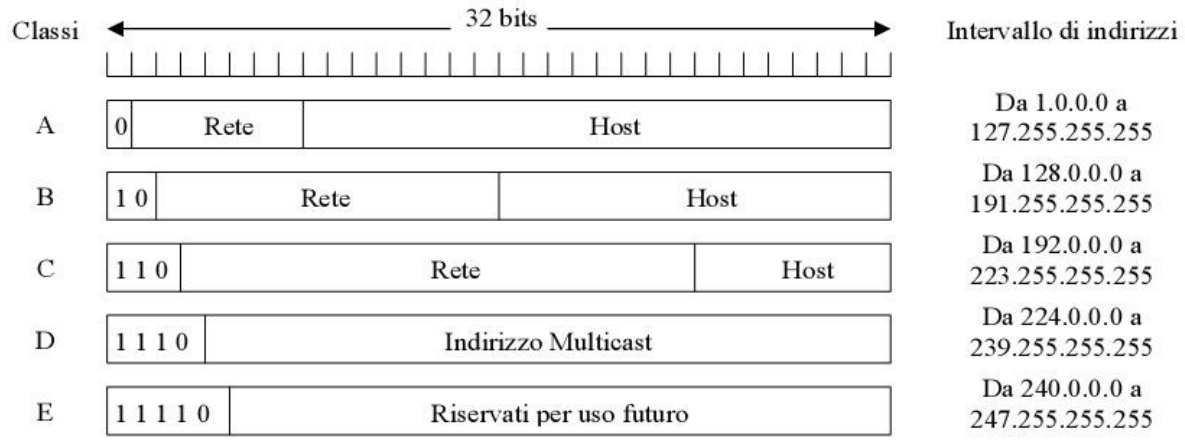
L'indirizzo IP fa parte del protocollo standard TCP/IP che s'è imposto sulle reti e che permette ad ogni dispositivo d'avere un numero univoco. Gli indirizzi sono formati da 4 gruppi di 8 bit con numeri compresi tra 0 e 255 (un esempio è 192.168.1.0) nel quale sono presenti intervalli pubblici e privati; ad esso si affianca la sottorete o Subnet Mask (un esempio è 255.255.0.0) che dev'essere uguale in tutti i dispositivi appartenenti alla stessa rete. Esiste una notevole differenza tra gli indirizzi IP pubblici e privati: se gli indirizzi di un sito internet sono risolvibili da qualsiasi nodo, gli indirizzi privati sono risolvibili solo all'interno della LAN di appartenenza. Nella tabella seguente è possibile apprezzare le differenze tra le classi di indirizzi IP privati possibili:

| Classe | Indirizzi IP<br>Da → A | N° sottoreti<br>possibili | Indirizzi disponibili<br>per sottorete |
|---|---|---|---|
| A | 10.0.0.0 → 10.255.255.255 | 126 | 16.774.214 |
| B | 172.16.0.0 → 172.31.255.255 | 16.384 | 65.534 |
| C | 192.168.0.0 → 192.168.0.255 | 2.097.152 | 254 |

Come s'è visto, l'indirizzo IP si compone dalla numerazione XXX.YYY.ZZZ.UUU ed il numero degli indirizzi privati disponibili per ogni sottorete può essere facilmente spiegato dalla tabella seguente:

| Classe | Rete | Computer (host) |
|---|---|---|
| A | XXX | YYY.ZZZ.UUU |
| B | XXX.YYY | ZZZ.UUU |
| C | XXX.YYY.ZZZ | UUU |

Le due classi comunemente usate sono la B e la C, mentre le grandi organizzazioni preferiscono utilizzare la A che poi suddividono tramite la subnet mask in molte sottoreti; gli indirizzi di classe D ed E sono usati per scopi particolari: la classe D non identifica né la rete né l'host ma un indirizzo di trasmissioni in Multicast; la classe E, invece, serve per scopi futuri.
In alcuni file di configurazione appare la sintassi XXX.YYY.ZZZ.UUU/B. Con /B si indica il numero di byte fissi del network. Quando il valore di B è 8, significa che XXX è fisso; quando è 16, significa che XXX.YYY sono fissi; quando è 24, significa che XXX.YYY.ZZZ sono fissi. Il numero degli host possibili sulla rete dipende quindi dai byte rimasti liberi.
L'immagine riassuntiva a seguire fornisce una visione generale di quanto descritto, considerando sia l'indirizzamento di tipo pubblico, sia privato:



Un esempio pratico potrebbe avere i valori seguenti:

```
IP address (classic): 192.168.183.15/255.255.255.0
 IP address (cisco): 192.168.183.15/24
  IP value (binary): 11000000.10101000.10110111.00001111
 Netmask (binary): 11111111.11111111.11111111.00000000
          Network: 192.168.183.0/24
    Network Class: C
     Total avail. IP: 256
  Network address: 192.168.183.0
Broadcast address: 192.168.183.255
```

L'indirizzo IP oltre che fisso, può essere assegnato attraverso un DHCP server. Esso è il responsabile dell'assegnazione automatica degli indirizzi IP ai dispositivi che vi si collegano. L'indirizzo delle periferiche cambia ad ogni connessione ma resta pur sempre valido perché esso opera in un range prestabilito, escludendo la possibilità d'errore nelle configurazioni generali.

## 1.3 Il wireless

Prima di iniziare l'esposizione riguardante il Wi-Fi, occorre fare una panoramica sul wireless, il cui sviluppo iniziò nel 1970 e si cercò di unire fra loro computer senza l'ausilio di fili... La prima applicazione funzionante derivò dalla necessità di collegare fra loro le isole Hawaii, attraverso la rete AlohaNet. Di recente, nel 1994, la comodità di collegare senza cavo i cellulari al palmare od in generale al personal computer, spinse IBM, Ericsson, Nokia e Toshiba alla creazione dello standard Bluetooth. Esistono diversi gruppi di reti wireless, che si differenziano tra loro non solo per la velocità di trasmissione dati, ma anche dall'uso per la quale sono state create:

- **PAN wireless:** tecnologie ad onde radio sopperiscono all'intralcio delle connessioni tra portatili, PDA, cellulari, lettori MP3 e macchine fotografiche, rendendo semplice la sincronizzazione di dati, fotografie, musiche ed altri contenuti. Le PAN (Personal Area Network) hanno un raggio d'azione tipicamente limitato a pochi metri di distanza. Di questa categoria fanno parte: il **Bluetooth**, che consente una connessione a 721Kbps alla massima distanza di 10 metri e progettato per essere economico, semplice da usare e da integrare, con un consumo ridottissimo; **IrDA** (Infrared Device Application), che consente collegamenti ad infrarosso tra dispositivi posti in visibilità reciproca ad una massima distanza di 1 o 2 metri, con velocità di 4Mbps.
- **LAN wireless:** applicazione di maggior rilievo che consente la connettività ad una LAN cablata, mediante l'uso di dispositivi detti punti d'accesso (o brevemente AP). Agli albori sorsero grossi problemi di interoperabilità a causa delle diverse tecnologie implementate e ci si rese ben presto coscienti che servisse uno standard. Nel 1997, l'IEEE approvò lo standard Wireless Ethernet, 802.11 (2Mbps) la cui variante 802.11b (11Mbps) detta anche Wi-Fi, riscosse notevole successo. Il suo raggio di copertura in campo aperto è nelle condizioni migliori di 400 metri.
- **MAN wireless:** è un campo di applicazione del Broadband Wireless o Wireless Local Loop che consente la distribuzione di dati come internet, telefonia, ecc, su un agglomerato urbano. E' principalmente usato in alternativa al costoso cablaggio dell'*ultimo miglio* nella telefonia. L'architettura fa parte del gruppo di lavoro IEEE 802.16.

- **WAN wireless:** nella categoria delle Wide Area Network fa parte il dominio che prevede la diffusione delle applicazioni previste sia per le reti cablate (LAN) che per le MAN ma con copertura totale, anziché localizzata in prossimità dei punti d'accesso. A questa categoria appartiene per esempio la telefonia GPRS, EDGE, UMTS o superiori e Wi-MAX.

Le classificazioni PAN, LAN, MAN e WAN qui descritte non sono nette, ma solamente indicative per i campi di applicazione delle varie tecnologie.

## 1.4 Il Wi-Fi e gli standard

Detto anche "wireless fidelity", è il marchio che contraddistingue gli apparati conformi allo standard IEEE 802.11x, dove diversi produttori si sono riuniti formando la "Wi-Fi Alliance" con l'obbiettivo di garantire la compatibilità reciproca dei propri dispositivi.
Responsabile della standardizzazione mondiale dei protocolli di scambio dati è l'IEEE (Institute Of Electrical and Electronics Engineers) che ha elaborato gli attuali e futuri standard.
Ad oggi sono state rilasciate le seguenti norme:

- **802.11**: primo rilascio nella banda di frequenza di 2,4GHz, raggiunge una velocità di 2Mbit/s. Usa una modulazione di tipo DSSS (Direct Sequence Spread Spectrum).

- **802.11a**: operante nella banda di frequenza di 5GHz (5,15 – 5,35GHz), raggiunge una velocità di trasferimento dati di 54Mbit/s; potenza massima di 30mW e 8 canali disponibili. Usa una modulazione di tipo OFDM (Orthogonal Frequency Division Multiplexing).

- **802.11b**: operante con una frequenza di 2,4GHz, raggiunge una velocità di trasferimento dati di 11Mbit/s. Sono disponibili diversi canali (in realtà sono solo 3 quelli non sovrapposti: 1, 6 ,11) in base al paese d'appartenenza (USA 11, Francia 8, Europa 13, Giappone 14); potenza massima di 100mW con modulazione HR-DSSS (High Rate - Direct Sequence Spread Spectrum).

- **802.11c**: mai rilasciato all'uso pubblico, s'è trattato solo da ponte tra l'802.11b e l'802.11d.

- **802.11d**: si tratta principalmente dell'internazionalizzazione di 802.11b.

- **802.11e**: migliora l'802.11b nella qualità del servizio per la trasmissione di audio e video.

- **802.11f**: è principalmente la raccomandazione ai costruttori di apparati di migliorare l'interoperabilità e d'implementare il roaming.

- **802.11g**: operante con una frequenza di 2,4GHz, è un'evoluzione di 802.11b e raggiunge una velocità di trasferimento dati di 54Mbit/s. Usa gli stessi canali di 802.11b e mantiene la retro compatibilità; potenza massima di 100mW e modulazione di tipo OFDM.

- **802.11h**: standard allargato di 802.11a, che aggiunge la banda operante a 5,725 – 5,825GHz, con altri 4 canali, potenza di 200mW, selezione dinamica della frequenza (DFS) e regolazione automatica del livello di trasmissione necessario (TPC, Transmit Power Control).

- **802.11i**: evoluzione di 802.11g, ne mantiene le caratteristiche ma introduce il protocollo di cifratura WPA2.

- **802.11j**: modifica ai layer MAC di 802.11 e PHY di 802.11a per la normalizzazione, ovvero la compatibilità, con il mercato Giapponese.

- **802.11k**: tratta il radio resource management, ovvero la standardizzazione della misurazione dei sorgenti radio.

- **802.11n**: evoluzione di 802.11i che verrà ratificato ufficialmente verso la metà del 2008. Secondo quanto riportato su http://arstechnia.com/news.ars/post/20061129-8322.htm, la prima generazione dei moduli 802.11n offrirà velocità pari a 480Mbps e un limite teorico prossimo a 600Mbps. In termini di copertura si afferma che le nuove tecnologie offriranno il 50% di distanza in più rispetto a un link 802.11g permettendo maggior copertura e velocità del link grazie ad un particolare algoritmo e l'impiego simultaneo di più antenne e canali.

- **802.11p**: comunicazione veicolare utilizzando la frequenza di 5,9GHz con velocità del data-link da 6Mbps.

- **802.11r**: dovrebbe introdurre il Fast Roaming, per la gestione del passaggio da un access point all'altro senza introdurre disconnessioni al link.

- **802.11s**: introduzione del supporto alla tipologia di rete Wireless Mesh.

- **802.11t**: è principalmente la raccomandazione ai costruttori di apparati alla "gestione e test".

- **802.11u**: evoluzione che consentirà la connessione alle reti non 802, come le reti cellulari.

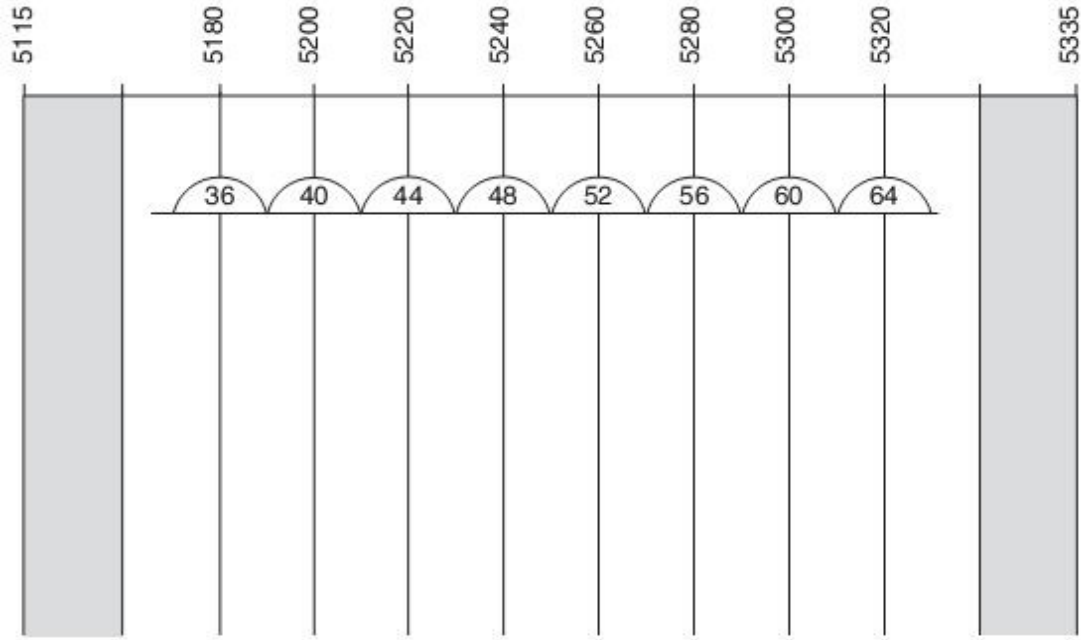
- **802.11v**: introdurrà la "gestione delle reti wireless".

- **802.11y**: è il sinonimo di reti IEEE802.11

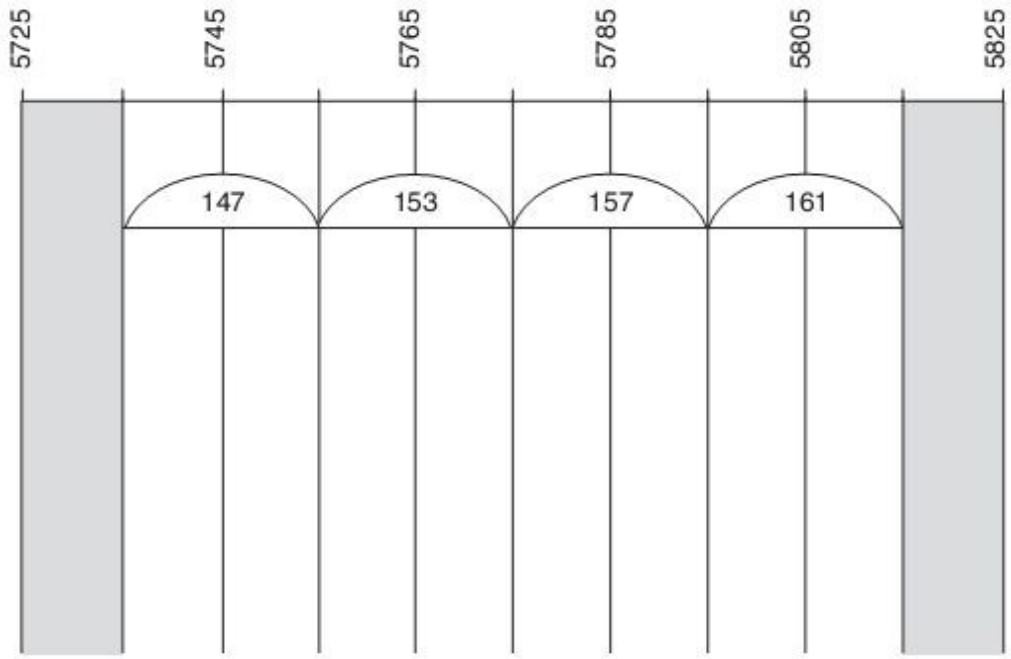
Alcuni produttori offrono tecnologie proprietarie aggiuntive allo standard, con lo scopo di migliorarne le funzionalità o l'efficienza, ma ciò costituisce l'insorgere di problematiche durante l'uso di apparati con chipset diverso.

## 1.5 Canali e frequenze di lavoro

Nella seguente tabella sono elencati graficamente gli 8 canali utilizzati dallo standard 802.11a:



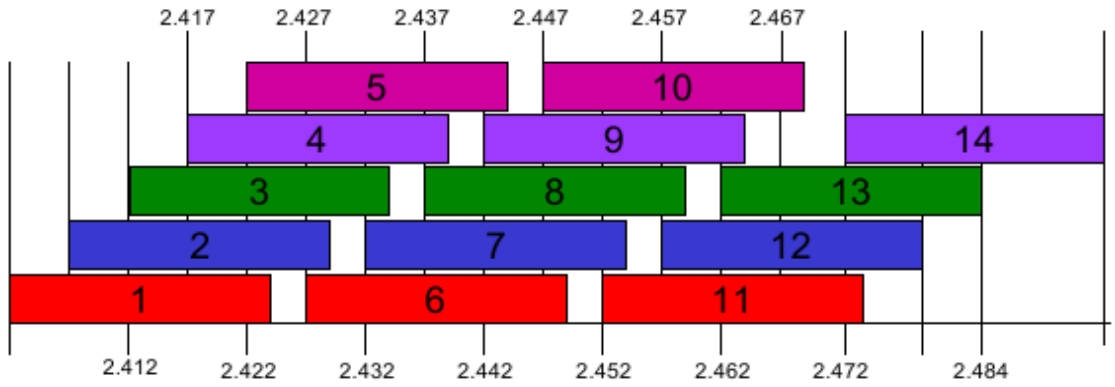

a seguire la tabella riguardante la variante dello standard 802.11a, le aggiunte di 802.11h, che lavora nella banda dei 5,7 Ghz e che aggiunge ulteriori 4 canali:



Attualmente in Europa lo standard 802.11b/g è il più diffuso e di seguito sono rappresentati diversi canali disponibili con relativa frequenza. La sua conoscenza permette d'accordare opportunamente l'elemento irradiante di una antenna in modo d'avere un rendimento migliore ad un particolare canale.

| ***Canale*** | ***Frequenza (MHz)*** | | |
|---|---|---|---|
| | ***inferiore*** | ***centro*** | ***superiore*** |
| 1 | 2401 | 2412 | 2423 |
| 2 | 2406 | 2417 | 2428 |
| 3 | 2411 | 2422 | 2433 |
| 4 | 2416 | 2427 | 2438 |
| 5 | 2421 | 2432 | 2443 |
| 6 | 2426 | 2437 | 2448 |
| 7 | 2431 | 2442 | 2453 |
| 8 | 2436 | 2447 | 2458 |
| 9 | 2441 | 2452 | 2463 |
| 10 | 2446 | 2457 | 2468 |
| 11 | 2451 | 2462 | 2473 |
| 12 | 2456 | 2467 | 2478 |
| 13 | 2461 | 2472 | 2483 |
| 14 | 2473 | 2484 | 2495 |

Se si preferisce, è possibile rappresentare graficamente la tabella precedente nel modo seguente:




Non tutti i canali sono disponibili in tutte le nazioni anche in ambito continentale.
In USA e Canada sono disponibili i canali da 1 a 11; in Europa da 1 a 13 ad eccezione della Francia dove sono disponibili da 1 a 8 e in Spagna da 1 a 11; in Giappone da 1 a 14.

## 1.6 Tipi di apparati disponibili

Trascurando quegli apparati dotati di caratteristiche e funzionalità particolari, la classificazione è così suddivisa:

- **AP**: Access Point è il modo di funzionamento a "punto d'accesso" e cioè quel dispositivo che consente di collegare ad una rete cablata i client Wi-Fi. Esso in pratica è la stazione centrale di trasmissione e ricezione di una rete senza fili.

- **Client**: sono quei dispositivi con interfaccia d'interconnessione PCI, PCMCIA, USB, ecc, che si collegano ed autenticano attraverso le onde radio ad un access point.

- **Apparati multimodalità**: sono dispositivi ethernet che permettono il funzionamento Wi-Fi in modalità multipla come AP, Client, Bridge e Repeater. Non sempre sono garantite l'interoperabilità tra apparati con chipset diverso ed il funzionamento simultaneo di più modalità.

- **Repeater**: il ripetitore è un dispositivo in grado di ripetere il segnale di un access point, permettendo l'estensione della rete Wi-Fi, introducendo però un dimezzamento della banda disponibile. Allo stato attuale non è possibile ripetere più d'una volta il segnale di un AP collegandosi ad un altro repeater; si può comunque collegare più repeater ad un AP purché siano in comunicazione diretta con l'AP base.

- **Bridge wireless-ethernet:** sono apparati particolari, studiati e realizzati appositamente per realizzare un BRIDGE (ponte) wireless tra due reti LAN. L'unica modalità di funzionamento di cui dispongono è quella di bridge. A questa categoria appartengono i D-Link DWL810.

## 1.7 Modalità di funzionamento

- **Infrastructure**: una rete wireless gestita in questa modalità sfrutta un AP come nodo centrale di smistamento dei dati ed ha un raggio d'azione di gran lunga superiore ad una rete Ad-Hoc.

- **Ad-Hoc**: in una rete Ad-Hoc due o più schede client comunicano direttamente tra loro, senza alcun access point che faccia da centro di smistamento dei dati. E' simile ad una rete peer to peer perciò ogni pc è collegato direttamente con un altro. Vi sono alcune problematiche con questo tipo di rete quando si hanno più di tre client. Si consiglia perciò l'uso di IP fissi.

- **Wireless Bridge (o Point To Point Bridge)**: è la modalità di funzionamento che permette l'unione e la connessione di due reti cablate attraverso il Wi-Fi. Tutti i dispositivi ed i pc devono appartenere alla stessa classe e sottorete d'indirizzi IP; i gruppi di lavoro possono essere diversi. Si tratta di una sorta di configurazione ad-hoc fra access point, ed è per questo motivo che le schede client non hanno possibilità di connessione.

- **Wireless Multi Bridge (o Point To Multipoint Bridge)**: è quella modalità che permette

l'unione di tre o più reti cablate attraverso il Wi-Fi. E' un'estensione della modalità bridge, perciò ne eredita da essa le impostazioni e le caratteristiche principali.

- **WDS**: particolare modalità che permette al dispositivo di funzionare simultaneamente sia da bridge sia da access point.

- **Roaming (o Multi AP)**: è quella particolare funzione che permette il passaggio di un client da un access point all'altro senza l'interruzione della comunicazione (per intenderci, è come per i cellulari, passando da un ponte ad un altro, non cade la telefonata). Non tutti gli apparati lo supportano.

- **Hot Spot**: sebbene non sia una modalità di funzionamento, la definizione è qui inserita poiché trattasi di un'area in cui, tramite la W-Lan, si ha accesso alla rete (internet compresa) con vari servizi.

## 1.8 Compatibilità

Sebbene oggigiorno esistono, e si tende ad usare, apparati multi-standard, è buona norma utilizzare quanto più possibile apparati appartenenti alla stessa famiglia o al limite che usino lo stesso chipset. Da tutto questo trarrà certamente vantaggio la "semplicità" della gestione degli apparati e della rete, evitando di passare notti insonni nel tentativo di capire cosa non funziona nella rete stessa.
Come si è potuto notare nel paragrafo relativo al Wi-Fi (1.4), non tutti gli standard sono compatibili tra loro perciò l'802.11h sarà retro compatibile con l'801.11a e l'802.11g e sue evoluzioni sono attualmente retro compatibili con l'802.11b. Questa compatibilità è comunque garantita solo quando gli apparati funzionano in modalità AP/Client (certificata con la presenza del marchio Wi-Fi), considerando che il bit-rate generale della rete si attesterà sul livello del client più lento presente.

## 1.9 Velocità di una rete wireless

Gli standard di fatto presenti sul mercato sono tre e precisamente l'802.11a,b,g le cui velocità dichiarate dai costruttori sono:

| ***801.11a*** | |
|---|---|
| **Velocità (Mbit/s)** | **Portata (m)** |
| 54 | 10 |
| 48 | 17 |
| 36 | 25 |
| 24 | 30 |
| 12 | 50 |
| 6 | 70 |

| *801.11b* | | |
|---|---|---|
| **Velocità (Mbit/s)** | **Distanza indoor (m)** | **Distanza outdoor (m)** |
| 11 | 50 | 200 |
| 5,5 | 75 | 300 |
| 2 | 100 | 400 |
| 1 | 150 | 500 |

| *802.11g* | | |
|---|---|---|
| **Velocità (Mbit/s)** | **Distanza indoor (m)** | **Distanza outdoor (m)** |
| 54 | 27 | 75 |
| 48 | 29 | 100 |
| 36 | 30 | 120 |
| 24 | 42 | 140 |
| 18 | 55 | 180 |
| 12 | 64 | 250 |
| 9 | 75 | 350 |
| 6 | 90 | 400 |

Il bit-rate indicato per ogni standard è comunque quello massimo teorico e mai corrisponde alla velocità reale raggiungibile. Esso dipende da molti fattori ambientali ed alcuni standard risentono più di altri del livello di crittografia applicato; questo è il caso di 802.11b che rallenta in modo percepile quando la codifica WEP è attiva (insignificante invece nell'evoluzione fuori standard 802.11b+). Da notare che durante i test pratici s'è evidenziata una netta differenza della velocità della rete utilizzando apparati multifunzione, dove il massimo s'è sempre ottenuto utilizzando la modalità di funzionamento come ponte (o Bridge). E' comunque possibile stilare la velocità reale di una rete in presenza di condizioni ottimali di funzionamento:

| | |
|---|---|
| 802.11a | Circa 20Mbit/s |
| 802.11b (802.11b+) | Circa 5,5Mbit/s (7-8Mbit/s) |
| 802.11g,i (802.11g+ o super g) | 15-20Mbit/s (30Mbit/s) |

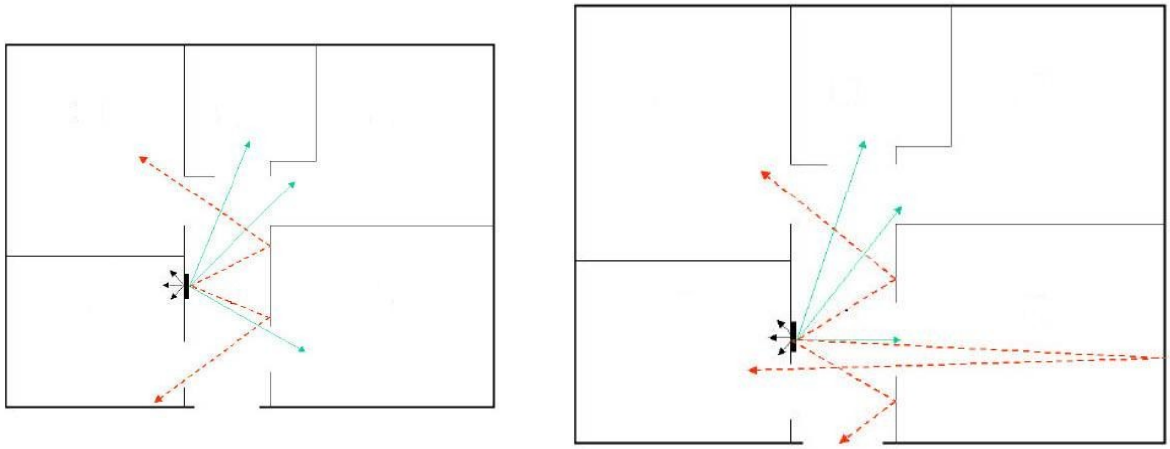
## 1.10 Installazione generica e disturbi ambientali

Le reti Wi-Fi sono relativamente facili sia nell'installazione che nell'utilizzo ma, nel caso si presentino dei problemi, è meglio sapere a cosa prestare particolare attenzione.
In questa sezione si tratterà l'installazione classica indoor di un access point. Tipi di installazioni particolari, come ad esempio quella della realizzazione di un ponte esterno, verranno trattate in modo dettagliato in altra sezione.
Siccome la trasmissione dei dati avviene per mezzo di onde radio, le reti W-Lan risultano sensibili alle interferenze ed è di primaria importanza scegliere la posizione migliore dove installare l'access point. Una posizione centrale nell'appartamento o nel locale dove diffondere il segnale è la condizione migliore, oltre al fatto che dovrebbe essere posto con l'antenna ad un'altezza sufficientemente alta, onde prevenire riflessioni dovute a mobili o elettrodomestici. E' altresì utile mantenere le antenne distaccate dai muri o dai case dei pc (20 centimetri possono talvolta fare la differenza) e lontano da fonti di disturbo.
Gli apparati conformi agli standard 802.11b/g soffrono particolarmente i disturbi generati dalle apparecchiature che funzionano sulla stessa frequenza (2,4GHz) e dotate di potenza particolarmente elevata come i forni a microonde ed i video-sender (i ripetitori AV che servono per portare il segnale di un decoder o videoregistratore ad un altro televisore). La tecnologia Bluetooth sebbene operante sulla stessa frequenza, non desta particolari problemi poiché impiega potenze nettamente inferiori, oltre ad un tipo di modulazione diversa.

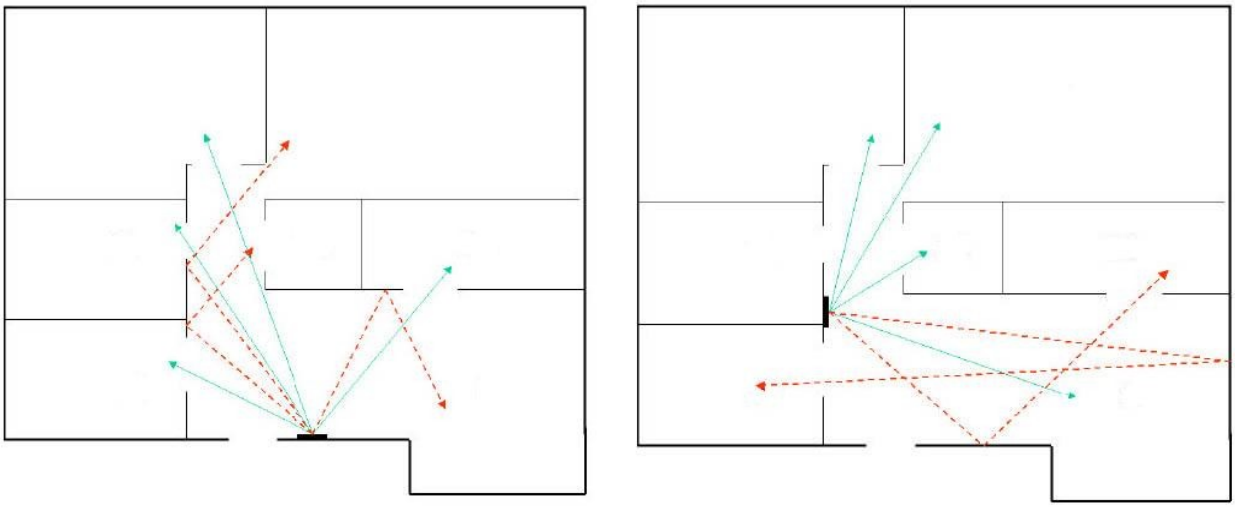
Si hanno notizie riguardanti alcuni tipi di modem xDSL e ricevitori satellitari SKY, che a causa di motivi non del tutto chiari, se posizionati nelle immediate vicinanze, creano diversi disturbi che influiscono sulla velocità del link, fino a decretarne l'inspiegabile caduta.

Non sempre la causa di malfunzionamento di una W-Lan è dovuta a disturbi ed interferenze, molto spesso è dovuto ad un inspiegabile basso livello del segnale ricevuto: le attenuazioni e disturbi dei materiali edilizi.
Le onde radio sono purtroppo sensibili ai tipi di materiali impiegati nella costruzione di opere murarie che ne attenuano il livello fino alla completa schermatura. Muri in cemento armato possono schermare o attenuare completamente il segnale, rendendo praticamente impossibile la realizzazione di una rete wireless; in questa condizione bisogna affidarsi a tecniche alternative, stendendo un cavo ethernet, oppure, se proprio non si vuole intervenire con “la forza bruta” ed esistono finestre adiacenti, posizionare gli access point con relative antenne accostati alle finestre.
Prove pratiche hanno dimostrato che pareti divisorie in cartongesso possono riflettere ed indebolire il segnale. Il fatto è da ricercare nel tipo di minerale usato e dal modo con cui è costruito il telaio interno che, se realizzato mediante griglia metallica, può costituire ulteriore ostacolo al passaggio della radiofrequenza. Tendendo il cartongesso ad assorbire e trattenere l'umidità dell'aria, le onde radio, in particolare modo quelle a 2,4GHz, tendono a comportarsi come un debolissimo forno a microonde e, cedono energia nel tentativo di riscaldare l'acqua presente.
Quest'ultima considerazione è da tener particolarmente presente nelle realizzazioni outdoor, dove la presenza di piante, o peggio ancora d'un bosco, può decretare il fallimento d'un progetto.
Di seguito, è possibile vedere alcuni esempi di come posizionare un router Wi-Fi all'interno di un appartamento.

*Appartamento o ambiente "A"*



*Appartamento o ambiente "B"*



Nelle figure precedenti, le frecce azzurre indicano il percorso diretto delle onde radio, mentre quelle rosse il percorso delle onde radio riflesse. Lo studio del posizionamento di un access point o di un router wi-fi permette una migliore copertura degli ambienti ma bisogna considerare che nella pratica, non sempre la riflessione del segnale porta a concreti benefici poiché il segnale potrebbe risultare attenuato o annullato.

## 1.11 Livelli di protezione

Una trasmissione di dati attraverso onde radio può benissimo essere ascoltata ed intercettata da chiunque possiede l'attrezzatura adatta. Per questo motivo è necessario provvedere ad impedire che malintenzionati o semplici curiosi possano violare la nostra privacy; perciò è bene non sottovalutare mai i problemi di sicurezza di una rete wireless. Sebbene risulta difficile difendersi dai cracker, il cui comportamento è eticamente ben diverso da quello di un hacker, è bene approntare un qualche tipo di codifica che renda almeno difficoltoso o laborioso l'attacco alla vostra rete, cercando così di scoraggiare un curioso di turno... Sembrerà un discorso piuttosto paranoico ma almeno il vostro vicino di casa non "scroccherà" la vostra connessione ad internet e non rovisterà nel contenuto degli hard disk dei pc.
Quando escono dalla fabbrica gli access point o gli apparati multifunzione, sono configurati per consentire qualsiasi connessione e non risulta attiva nessuna chiave di codifica delle informazioni. Ciò non è una dimenticanza o l'indicazione di scarsa qualità del prodotto, ma semplicemente una comodità offerta per essere subito operativi e pronti al funzionamento.

**Nessuna rete dev'essere posta in attività mantenendo le impostazioni originali ed è a carico dell'utente provvedere immediatamente alla sua configurazione.**

Teoricamente la codifica andrebbe attivata dopo aver effettuato le varie prove di comunicazione e impostazioni generali degli apparati, o fintanto che si ha la connessione diretta all'apparato, mediante connessione ethernet. Se questa condizione non viene rispettata, si corre il rischio di escludersi dalla rete. **Si raccomanda l'uso del livello di codifica quanto più elevato possibile.**

- **WEP e WPA**: all'inizio la cifratura dei dati fu affidato al **WEP** (Wired Equivalent Privacy) con chiave di codifica a 64 e 128 bit, una tecnica che prevedeva un livello di privacy equivalente a quello di una rete cablata ma presto si rivelò il suo limite e la sua insicurezza (è infatti possibile ricostruire la chiave di rete semplicemente "ascoltando" il traffico scambiato), ma se ne consiglia sempre l'attivazione. Gli standard 802.11b,g ammettono una codifica WEP fino a 128 bit, con l'802.11a si raggiungono i 152 bit. Esistono tuttavia tecnologie proprietarie che permettono una codifica WEP di 256 bit come nel caso di 802.11b+ che sebbene offre maggior protezione, è compatibile solo con apparati dotati dello stesso chipset. Esiste in molti casi la possibilità d'inserire più chiavi che, associato al metodo **Open Key**, permette il cambio automatico delle chiavi ad intervalli regolari. Con l'introduzione di 802.11g, fece la comparsa il **WPA** (Wi-Fi Protected Access) decisamente più sicuro del WEP e basato sul protocollo **Tkip** (Temporal Key Integrity Protocol), supportando i server di autenticazione, soluzione particolarmente interessante nell'uso aziendale ma onerosa in termini d'uso casalingo o amatoriale. In quest'ultimo caso è bene prendere in considerazione la variante **WPA-Psk** (Pre-Shared Key) dove sarà l'utente stesso ad assegnare la password d'accesso **Master Key** a ciascun apparato, poi sarà il protocollo Tkip che basandosi su essa, genererà altre chiavi sicure. Con l'802.11i, è introdotto il **WPA2** e basato sul protocollo **AES** (Advanced Encryption Standard) con chiavi da 128, 192, 256 bit e teoricamente compatibile con il WPA. Per utilizzare questo standard non è però possibile il solo aggiornamento del software o firmware dell'apparato, serve infatti un nuovo tipo di hardware.

- **MAC**: altro metodo, decisamente sicuro, ma non assoluto, per proteggere la rete wireless, consiste nel filtrare gli indirizzi **MAC** delle schede di rete e far accedere solo quelli autorizzati, semplicemente compilando una lista di controllo. Come tutte le cose elettroniche

ed informatiche, è certamente possibile falsificare un indirizzo MAC con tecniche di spoofing ma richiede scaltrezza e conoscenze più approfondite da parte dei cracker.

- **SSID**: per offrire un ulteriore strato di protezione dei dati trasmessi, la disattivazione della pubblicazione di **SSID** (Service Set Identifier), rende la rete non identificabile ma utilizzando particolari programmi, resta pur sempre visibile il canale utilizzato. In questo modo sarà l'utente a dover fornire lo SSID ai client.

Applicando le informazioni acquisite in questa sezione ed assegnando indirizzi **IP fissi**, disabilitando cioè il server **DHCP** integrato nell'apparato, si mette la rete in condizione d'esercizio con un buon livello di protezione, migliorabile installando su ogni pc un firewall.
Protezione estremamente efficace, sarebbe quella d'implementare un tunnel **VPN**.
La protezione di una W-Lan dev'essere fatta a strati multipli, dove, più strati sono presenti, maggiore è il livello di sicurezza. Applicando quanto descritto sopra, un cracker dovrebbe scoprire il canale utilizzato, SSID, l'intervallo degli indirizzi IP validi, la chiave crittografica ed un indirizzo MAC valido e violare una VPN se presente... Certamente nulla è impossibile ma è estremamente laborioso carpire tutte le informazioni.

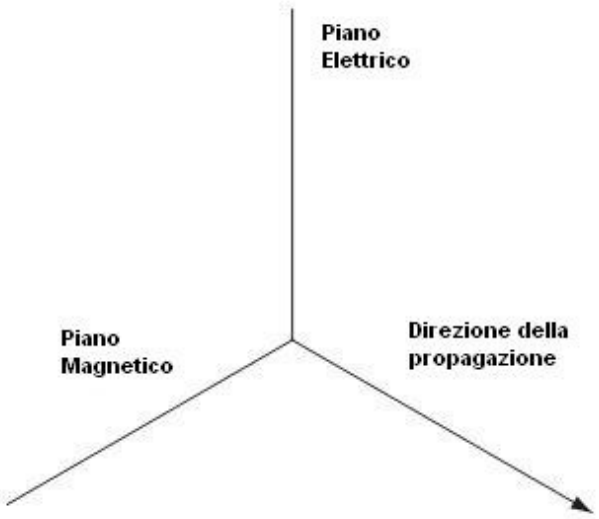
In questa sezione non sono state prese in considerazione le reti Ad-Hoc, ossia quelle reti wireless funzionanti senza access point. In questa modalità non esistono funzioni di sicurezza avanzate e, poiché insicura, se ne sconsiglia l'uso permanente.

# *Introduzione e concetti di base sulle onde radio*

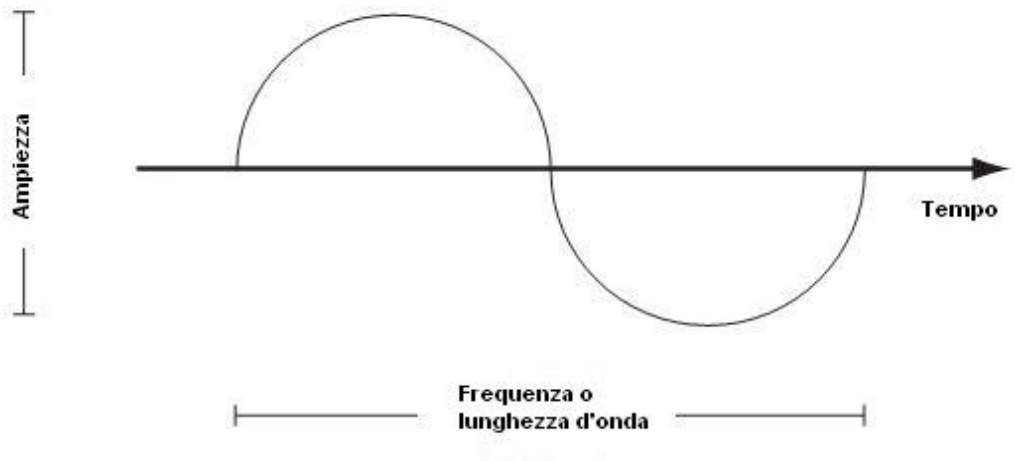
Prima di cimentarsi nell'allestimento di una rete Wi-Fi o comunque wireless, è bene apprendere alcune informazioni di base per stabilirne la fattibilità. In questa sezione, verranno trattate inizialmente informazioni teoriche di base per poi passare a regole di carattere pratico che pur basandosi sulle nozioni teoriche precedentemente esposte, semplificheranno certamente lo studio sulla realizzazione pratica d'un progetto.
La prima norma da tenere sempre presente è che un link (o collegamento) al limite minimo della potenza di funzionamento non sarà mai stabile e al presentarsi delle prime variazioni ambientali critiche (come la pioggia, la neve, ecc.), esso cadrà inesorabilmente. Prove pratiche hanno evidenziato che basta un 30% di potenza in più del minimo indispensabile per prevenire l'insorgere di problemi. Onde evitare di creare confusione è utile procedere a piccoli passi, fornendo i concetti di base...

## 2.1 Energia RF

L'energia a Radio Frequenza, comunemente abbreviata in RF, può essere definita nel modo più semplice possibile come un segnale a corrente alternata che forma un movimento sia sul piano elettrico sia su quello magnetico che, a loro volta, si sviluppano sul piano della propagazione in modo perpendicolare...
La loro posizione rispetto alla terra o alla direzione del piano di propagazione, determina il tipo di polarizzazione che può essere di tipo orizzontale, verticale o circolare. Senza scendere nei dettagli più tecnici, la visione della figura a seguire può facilmente rendere l'idea di quanto esposto, riguardante un segnale RF con polarizzazione verticale:




La RF è definita, oltre dalla polarizzazione, anche dalle caratteristiche di frequenza e di lunghezza d'onda, che sono inversamente proporzionali l'una dall'altra. La frequenza viene indicata con l'Hertz, in onore al suo scopritore Heinrich Hertz, che definì 1Hz come un ciclo completo di un'onda sinusoidale in un secondo. La figura a seguire mostra graficamente quanto esposto:




La lunghezza d'onda è definita tipicamente in metri ed è la lunghezza fisica dell'onda sinusoidale; da essa dipende fortemente la lunghezza dell'elemento irradiante.
L'ampiezza indica il massimo valore sia positivo che negativo che l'onda raggiunge.
Nella paragrafo "formule utili" è possibile trovare la relazione tra frequenza e lunghezza d'onda

## 2.2 Divisione dello spettro radio

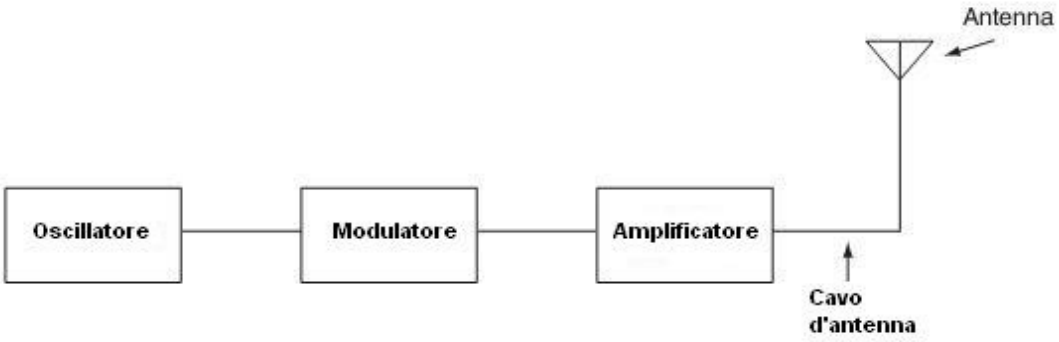
Lo spettro della radiofrequenza è diviso, come accade similmente con lo spettro della luce visibile che viene diviso in colori, in bande radio che sono ulteriormente suddivise in canali. Iniziando da una frequenza di 9KHz si dividono in:

| Designazione | Abbreviazione | Banda di frequenza | Lunghezza d'onda in spazio libero |
|---|---|---|---|
| Very Low Frequency | VLF | 9Khz - 30KHz | 33Km - 10Km |
| Low Frequency | LF | 30KHz - 300KHz | 10Km – 1Km |
| Medium Frequency | MF | 300KHz - 3MHz | 1Km - 100m |
| High Frequency | HF | 3MHz - 30MHz | 100m - 10m |
| Very High Frequency | VHF | 30MHz - 300MHz | 10m - 1m |
| Ultra High Frequency | UHF | 300MHz - 3GHz | 1m - 100mm |
| Super High Frequency | SHF | 3GHz - 30GHz | 100mm - 10mm |
| Extremely High Frequency | EHF | 30GHZ - 300GHz | 10mm - 1mm |
| Infrarossi - Ultravioletti | IR - UV | 1THz - 10000THz | |

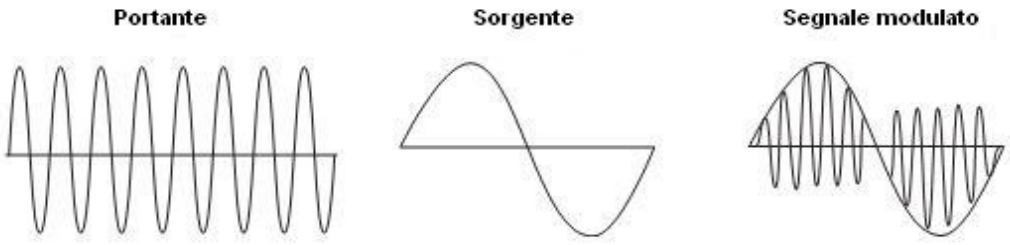
Come già accennato precedentemente, le bande di frequenza sono ulteriormente divise in canali individuali che rappresentano piccoli pezzi della banda disponibile e permettono ad una trasmittente e ad un ricevitore di operare esattamente ad una frequenza ben definita. I canali non sono tutti uguali ma sono in numero diverso e posseggono diversa larghezza di banda in base alla divisione di spettro appartenente ed al tipo di uso o di servizio designato.

## 2.3 Principio di base di un trasmettitore

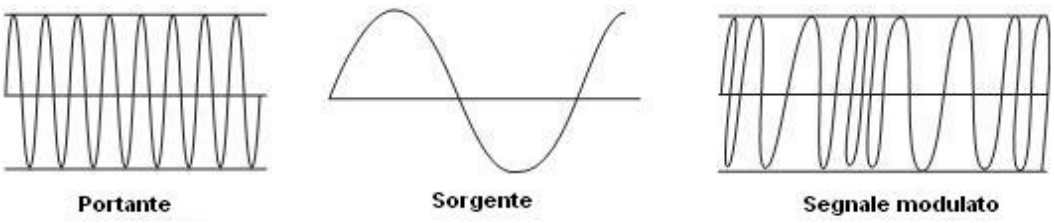
Il compito del trasmettitore è quello di generare e trasmettere nell'aria il segnale a radiofrequenza opportunamente modulato, ed è composto da diversi elementi elettronici, ognuno dei quali ha un compito preciso. Per facilitarne la comprensione, è opportuno utilizzare uno schema a blocchi semplificato:



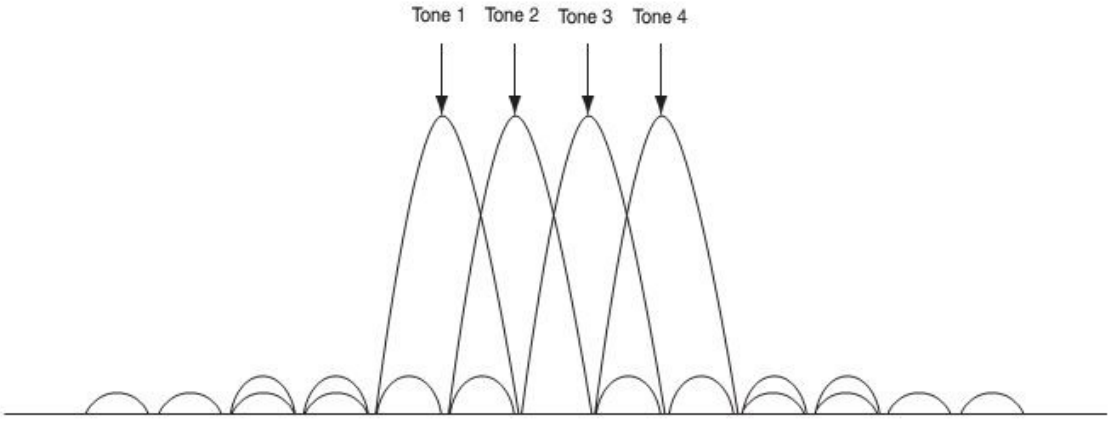

- L'oscillatore ha il compito di generare il segnale a radiofrequenza di base, chiamata anche portante. Nelle moderne radio è sostituito da un sintetizzatore a PLL. Molto si potrebbe dire a riguardo di questo stadio ma siccome lo scopo è dare solo informazioni di base, in parole molto semplici l'oscillatore non è altro che un amplificatore che funziona in regime di risonanza ad una ben definita frequenza.
- Il modulatore ha l'importante compito di "inserire" ovvero miscelare un qualunque segnale, nel nostro caso specifico i dati, nella radiofrequenza di base o portante. Esso determina anche il tipo di modulazione usata che può essere AM (Amplitude Modulation, modulazione d'ampiezza) oppure FM (Frequency Modulation, modulazione di frequenza). La modulazione d'ampiezza è usata principalmente per le trasmissioni audio monofoniche a lunga/lunghissima distanza poiché non è richiesta la visibilità ottica tra trasmittente e ricevitore; il suo lato negativo è che risulta essere suscettibile alle cariche elettriche nell'atmosfera.
La modulazione FM è usata per tutti gli altri tipi di trasmissioni, dove dev'essere garantita maggiore fedeltà di riproduzione su lunghe distanze; il suo lato negativo è che deve esserci visibilità ottica tra trasmettitore e ricevitore, non presenta i difetti della modulazione AM.
Esistono tuttavia molti tipi di modulazione come la DSSS o la OFDM, utilizzate per la trasmissione di dati. Nelle immagini seguenti è possibile vedere alcuni esempi di modulazione:



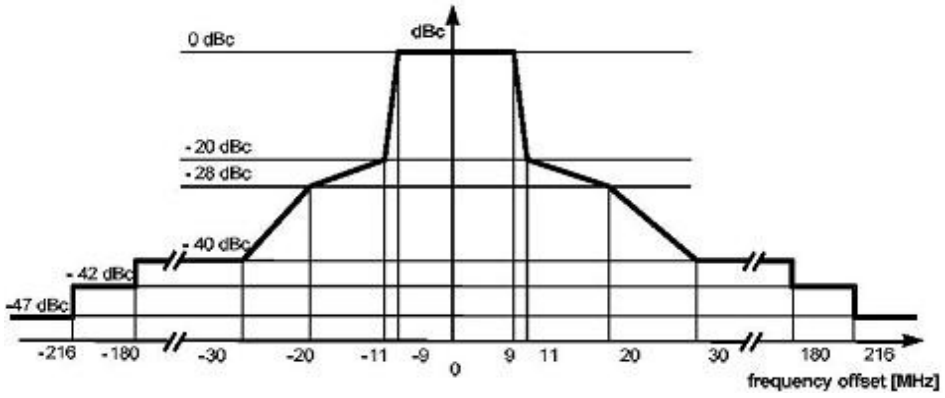

Modulazione AM




Modulazione FM




Modulazione OFDM



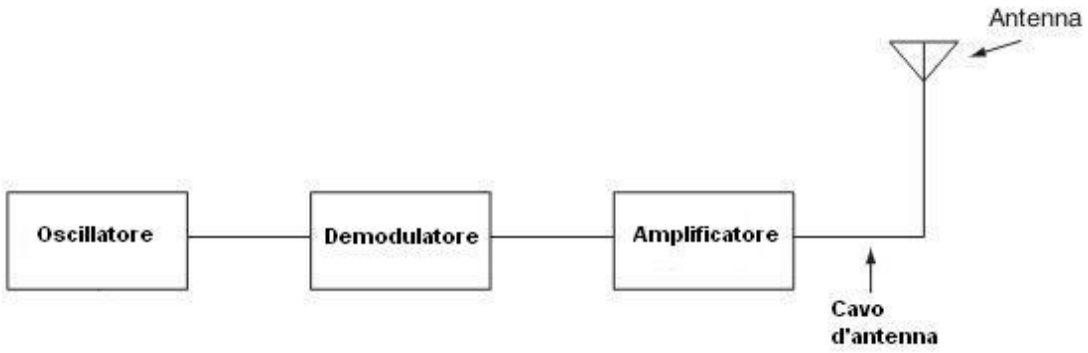

Modulazione DSSS

Nella modulazione DSSS il frequency offset indica lo scostamento in frequenza, in MHz, dal centro del canale utilizzato. Analizzando attentamente la figura, si può capire che segnale in questo occupa più di un canale ed introduce “rumore” in quelli adiacenti.

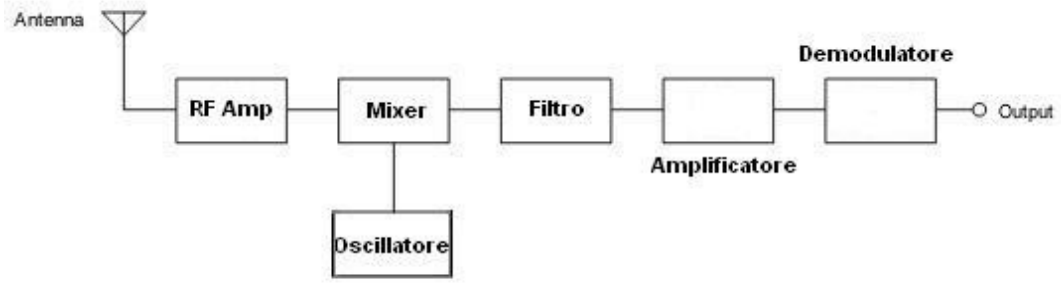
- L'amplificatore ha, come facilmente intuibile, il compito di amplificare e cioè aumentare l'ampiezza del segnale senza però introdurre distorsioni. Alla sua uscita è collegato il cavo d'antenna, possibilmente a bassa perdita (attenuando il meno possibile il segnale) e l'antenna stessa.

## 2.4 Principio di base di un ricevitore

Il compito del ricevitore è quello di ricevere il segnale a radiofrequenza modulato e renderlo all'uscita il più possibile simile all'originale. E' composto da diversi elementi elettronici, ognuno dei quali ha un compito preciso. Per facilitarne la comprensione, è opportuno utilizzare uno schema a blocchi semplificato:




Il ricevitore funziona in modo simile ma contrario al trasmettitore. In realtà il discorso è molto più complesso poiché per spiegare anche a grandi linee come funziona un ricevitore, occorre introdurre alcuni blocchi che permettano di meglio capire lo schema sopra esposto che, risulta essere eccessivamente semplificato. Comunque sia, l'antenna capta il segnale modulato presente nell'etere e lo invia tramite il cavo d'antenna all'amplificatore interno che provvede ad innalzarne l'ampiezza per meglio gestirne le elaborazioni successive. A questo punto però occorre introdurre gli altri blocchi necessari...




Un oscillatore locale crea la stessa frequenza RF di base del trasmettitore e la invia al mixer che provvede a “togliere” dal segnale modulato captato dall'antenna ed amplificato, la frequenza portante. Il segnale ottenuto passa attraverso un filtro che provvede a “ripulire” ulteriormente il segnale risultante che viene poi amplificato. Il demodulatore infine compie l'operazione inversa del modulatore: alla sua uscita si ha praticamente lo stesso segnale che aveva modulato la portante nel trasmettitore, nel nostro caso i dati.

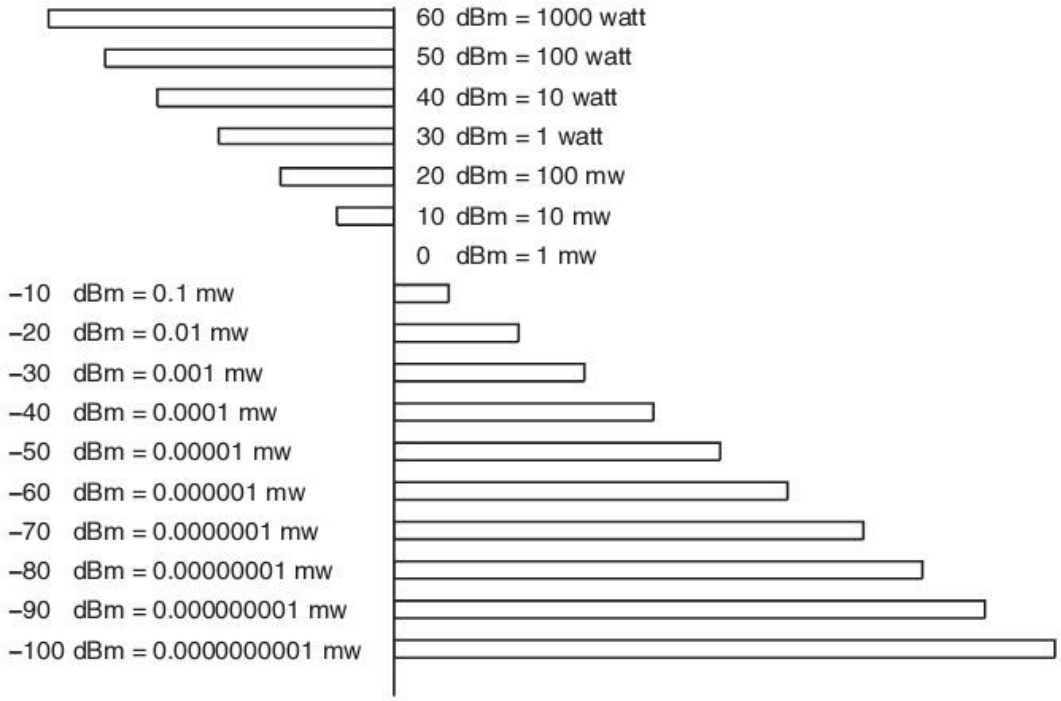
E' utile far notare che per tutti i link a comunicazione bidirezionale, come quelli delle W-LAN Wi-Fi, gli apparati contengono sia trasmettitore che ricevitore. Il trasmettitore ed il ricevitore sono connessi all'antenna attraverso un particolare circuito di commutazione ad alta frequenza.

## 2.5 Il dB

Il decibel è il rapporto tra due valori (uno dei quali di riferimento) e normalmente nel campo delle telecomunicazioni è riferito alle potenze in gioco. Essendo un valore relativo, indica perciò lo scostamento dal valore preso come riferimento, il cui valore è definito dalla formula generica:

**dB = 10 Log (P2/P1)**

P1 indica il valore di riferimento (nel Wi-Fi è di 1 mW) e P2 la potenza dell'apparato preso in esame. Essendo logaritmico, i suoi valori rappresentano una compressione dei valori reali che esprime. Un valore di 3dB indica perciò un fattore 2 (il doppio), -3dB un fattore -2 (la metà). Negli apparati trasmittenti/riceventi è indicato anche un valore in dB **negativi**. Esso indica quel valore inferiore alla potenza di riferimento che il ricevitore è in grado di "sentire". Per meglio capire, il diagramma seguente può essere meglio di mille parole:




In linea generale i termini più comunemente usati sono il **dBm** riferito ad una potenza campione di 1mW; il **dBi** che è riferito al guadagno d'antenna ideale isotropica; il **dBW** che è riferito ad una potenza campione di 1W.

## 2.6 Power (o Link) Budget e l'EIRP

Il Power (o Link) Budget è il termine che indica la somma algebrica dei guadagni e delle perdite che concorrono in un link. Esso è indispensabile per verificare sia la realizzazione pratica sia la corrispondenza dello stesso alle normative vigenti.
Semplificando molto le variabili in gioco, la rappresentazione grafica di una installazione tipica reale, può essere così esposta:


Come si può notare le zone in verde concorrono all'aumento della potenza e quelle in rosso, indicano le perdite di segnale e perciò ad una perdita di potenza. Gli elementi che compongono il Power Budget sono quindi riassumibili in:

- **Potenza radio**: è la potenza d'emissione dello stadio finale del trasmettitore (A e G). E' espresso in W (Watt) ma nel caso degli apparati Wi-Fi, in mW. In quest'ultimo caso, tale potenza viene espressa in dBm ed è un valore positivo.
- **Cavo d'antenna e connettori**: i cavi d'antenna e relativi connettori, introducono delle perdite (B e F). Espresse in dB (riferito al metro di lunghezza o su 100m di cavo), sono sempre di valore negativo e variano anche di molto in base al tipo di cavo e connettore impiegato.
- **Antenna**: sebbene di tipo passivo, in base alla conformazione e geometria, introduce un guadagno positivo (C e E) supplementare espresso in dB. Essa ha il compito d'irradiare e ricevere il segnale.
- **Propagazione nello spazio libero**: è l'attenuazione, espressa in dB, che il segnale subisce attraversando l'aria e lo spazio per raggiungere l'antenna remota (D).

Il Power Budget avrà perciò il valore fornito dalla formula algebrica:

**PB = A (dBm) + C (dB) – B cavi(dB) – B connettori (dB)**

Questo valore non dev'essere mai superiore al limite imposto dalle vigenti leggi (massimo 20dBm **EIRP** per le reti Wi-Fi.). Può essere comunque superiore se le due stazioni trasmittenti/riceventi appartengono a radioamatori, i cui limiti dipendono dal tipo di patente posseduta.
Il limite massimo di 20dBm **EIRP** all'antenna, usando la frequenza di 2,4GHz, indica la ***potenza effettiva isotropica irradiata*** e cioè quella potenza che viene irradiata in ogni direzione dall'antenna.

.

## 2.7 Fresnel Zone

**L'effetto Fresnel** è quell'insieme di fenomeni d'interferenza che sono sempre presenti nelle trasmissioni a radiofrequenza. L'utilizzo di alta frequenza richiede poi che le antenne siano a portata ottica e che non vi siano ostacoli d'ogni genere interposti. Si definisce **LOS** (**L**ine **o**f **S**ight ovvero "linea di visibilità") quella linea ottica diretta e priva di ostacoli tra due punti. Quest'ultima condizione è facilmente verificabile ed in caso di distanze particolarmente elevate, l'utilizzo di un binocolo costituisce valido aiuto. Ostacoli che possono oscurare la LOS possono essere di varia natura:

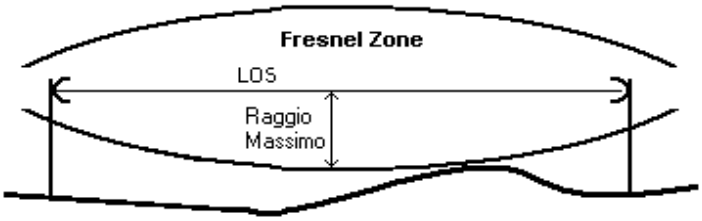
- elementi caratteristici della zona: montagne o colline;
- palazzi o altre costruzioni;
- piante o boschi;
- curvatura terrestre: solo a grandi distanze

In un radio link non basta considerare la sola LOS, parte dell'energia irradiata vi si trova intorno.
Si può immaginare questa zona come un ellissoide o un dirigibile il cui asse è la LOS stessa. Questo spazio viene definito come **ZONA di FRESNEL** e non dovrebbe mai essere attraversato da oggetti o elementi elencati sopra.
Se un oggetto solido come un monte o un palazzo rientra in tale zona, il segnale può essere deviato (per riflessione) e/o attenuato di potenza (per assorbimento o per cammini multipli del segnale). La zona di Fresnel assume dimensioni variabili e dipendenti dalla frequenza e dal percorso del segnale.


L'immagine qui sopra può rappresentare il tipico esempio di zona di Fresnel non libera, sebbene la LOS lo risulti. Fenomeni di diffrazione e riflessione possono deviare parte del segnale originale.
Siccome queste riflessioni non sono mai in fase, il segnale può risultare attenuato in potenza o annullato completamente (tipico nei fenomeni di cammini multipli). Anche la presenza di piante attenua il segnale.

- Da queste considerazioni si intuisce che antenne a "visibilità ottica" diretta **non garantisce** in teoria l'efficienza di un link. Prove pratiche "sul campo" hanno però evidenziato che è sufficiente avere il 60% del raggio massimo della zona di Fresnel libera da occlusioni per avere un link efficiente ed in particolare, il 60% per la modulazione DSSS e l'80% per la FHSS Frequency Hopping Spread Spectrum. Fonte: http://www.radiolan.com/fresnel.html dov'è possibile calcolare una Fresnel di prova.

Il calcolo della zona di Fresnel è usato per dimensionare la posizione in altezza di antenne ed è ricavabile mediante apposite tabelle. In caso di particolari occlusioni, è bene optare nel cambio di posizione dell'antenna in modo tale d'aver almeno il 60% del raggio massimo di tale zona libero o meglio ancora fino ad ottenere le condizioni di funzionamento ottimali come riportate nella figura seguente.




| *Dimensioni del raggio in metri della zona di Fresnel* | | | |
|---|---|---|---|
| ***Distanza (m)*** | ***2,4GHz*** | ***5,25GHz*** | ***5,77GHz*** |
| 500 | 3,95 | 2,67 | 2,55 |
| 1000 | 5,58 | 3,78 | 3,06 |
| 2000 | 7,09 | 5,34 | 5,1 |
| 3000 | 9,68 | 6,54 | 6,24 |
| 5000 | 12,49 | 8,44 | 8,06 |
| 8000 | 15,08 | 10,68 | 10,2 |
| 10000 | 17,67 | 11,94 | 11,4 |
| 15000 | 21,63 | 14,63 | 13,95 |

I raggi d'esempio sono stati calcolati ipotizzando la presenza di un ostacolo esattamente alla metà della distanza del link.

## 2.8 Propagazione nell'aria

Le onde radio sono il mezzo per trasportare e trasferire dati a distanza e supponendo d'usare una antenna omnidirezionale (detta anche isotropica), escono da essa con un Power Budget definito e teoricamente si diffondono nell'aria in modo uniforme in ogni direzione (come una sfera che si espande dal centro, dove risiede l'antenna). In realtà, il segnale è attenuato perché soggetto ad interferenze di vario tipo: colpiscono ostacoli come edifici, alberi ed oggetti in movimento, venendo riflesse, attenuate e deviate dalla LOS dalla gravità, dall'effetto Fresnel, dai percorsi multipli ed altro. L'effetto risultante di tutte queste interferenze è che il segnale radio ideale, partito dall'antenna trasmittente, giunge all'antenna ricevente attenuato, distorto e sfasato.
Da quanto appreso finora, si deduce che nel calcolo totale della potenza del sistema, va considerata anche la potenza minima indispensabile al ricevitore per riconoscere il segnale (sensibilità) che andrà sommata anch'essa algebricamente.
Si definisce **margine di guadagno (MG)** la stima della potenza a cui il ricevitore sarà messo in condizioni di lavoro, le cui prove pratiche hanno dimostrato debba essere di circa 15dB superiore alla soglia minima per avere un link stabile nelle varie stagioni.

**MG = PB (dB) – Perdite propagazione (dB) – sensibilità ricevitore (-dB)**

## 2.9 Quanta distanza?

Quanto lontano si può andare? Molte sono le variabili in gioco ma usando particolari accorgimenti, è possibile aumentarla o almeno sapere quanta potenza è necessaria per raggiungere una distanza definita. Ci sono 4 fattori da tener presente di cui su 3 si può avere una certa padronanza d'intervento:

1. L'EIRP del sistema: aumentando la potenza in uscita o il guadagno delle antenne e limitando le perdite dei cavi e dei connettori, si fa più strada.
2. Linea di visibilità (o LOS): maggiore è l'arco di visibilità migliori sono le condizioni d'esercizio poiché si attenuano i fattori ambientali come la crescita di rami e foglie, l'abbattimento della potenza a causa di ghiaccio, della polvere, ossidazione e guano.
3. La sensibilità del ricevitore: rappresentando "l'orecchio" del sistema, più è bassa, meglio è. Può essere migliorata abbassando la velocità del link. Le caratteristiche di sensibilità generalmente aumentano col diminuire della velocità, non di rado passando da 11Mbit/s a 5,5Mbit/s, si guadagnano 3 dB che passando a 2 Mbit/s diventano 6dB, corrispondenti di fatto ad un raddoppio della distanza mantenendo invariata la potenza.
4. Effetto Fresnel: superati i 2 Km, gli effetti si fanno rilevanti.

## 2.10 Il puntamento

Quando la distanza inizia ad essere rilevante o quando s'impiegano antenne di tipo direttivo, il puntamento delle stesse in modo ottimale assume un carattere importante nella realizzazione del link. Sebbene non sia indispensabile, è sempre bene avere a disposizione ciò che personalmente definisco come "*kit di sopravvivenza Wi-Fi*" che si compone di:

1. Un ap anche economico, con connettore per antenna esterna e piuttosto "elastico" in termini d'alimentazione.
2. Una scheda client possibilmente PCMCIA, per computer portatile, dotata di attacco per antenna esterna e compatibile con il programma Network Stumbler.
3. Una serie di connettori ed adattatori, in particolare da sma o rp-sma ad N.
4. Un computer portatile con il software Network Stumbler.

Questi componenti, oltre a rendere semplice il puntamento, possono tornare utili per fare delle verifiche veloci quando si ha l'impressione che il link realizzato "rallenti" o quando si devono apportare modifiche anche rilevanti.
Accendiamo il portatile e colleghiamo in modo "volante" l'antenna alla scheda client e verifichiamo con Network Stumbler se intorno a noi sono presenti altre reti wireless e su quale canale lavorano.
Si tenga presente, come visto nel capitolo precedente, che i canali disponibili non sovrapposti sono solo 3 ed è bene scegliere uno di questi.
Scegliamo il tipo di polarizzazione, verticale o orizzontale, tenendo presente la morfologia circostante e considerando il fatto che prove pratiche hanno dimostrato che la polarizzazione verticale offre prestazioni migliori ma non sempre è possibile usarla e, siccome ogni impianto fa storia a sé, non è detto che sia oltretutto la più efficiente.

Prima di procedere al montaggio “in esterno” degli apparati, è bene che gli stessi vengano impostati e testati “al banco”, sulla scrivania.

Verificato il funzionamento e la connessione tra gli apparati, si procede al fissaggio di un'antenna da un lato del link ed utilizzando un binocolo, la si punta verso la “destinazione” e vi si collega l'ap del kit di sopravvivenza, impostato per l'uso dell'antenna esterna. Effettuata una rapida verifica delle connessioni, si procede ad alimentare l'apparato.
Spostandoci sull'altro lato (la destinazione del link), si monterà l'antenna avendo cura di mantenere la stessa polarizzazione e vi si collegherà la scheda client.
Accendiamo il portatile ed avviamo il programma Network Stumbler, muovendo l'antenna dall'alto in basso e da destra verso sinistra verifichiamo se c'è disponibilità del link. Quando lo si rileva, serrare leggermente le viti di fissaggio, selezioniamo dal pannello di sinistra del programma il canale dell'ap remoto e far compiere dei piccoli scostamenti all'antenna in modo da ottenere il massimo segnale. Fissare in modo definitivo l'antenna cercando di non farle compiere scostamenti.
Spegnere il computer e scollegare l'antenna dalla scheda. Portandosi sull'altro lato del link, togliere l'alimentazione all'ap del kit e ripetere l'operazione nel senso opposto.
Ultimate queste ultime operazioni, avrete un bel link funzionante.

Si ricorda di non usare tutta la potenza degli apparati ma quanto basta per avere un link stabile. Trasmettere a piena potenza generalmente non è sinonimo di massima velocità ottenibile, spesso si ottiene l'effetto inverso perché è come ascoltare musica a tutto volume utilizzando le cuffie... il risultato finale è che sentirete del gran rumore senza distinguere nulla. Il fatto d'usare poca potenza, garantisce anche ad altri la realizzazione di un proprio link wireless.

# Antenne

## 3.1 Generalità

Le antenne hanno particolare importanza nelle applicazioni radiotrasmittenti-riceventi, ad esse è affidato il compito d'irradiare e di ricevere il segnale nell'etere e per questi motivi, possiedono guadagno sia in trasmissione che in ricezione. La scelta e l'installazione del tipo più opportuno d'antenna può essere particolarmente impegnativo e difficile, dipendente di sovente dalle condizioni morfologiche del territorio. Per comprenderne le differenze tra i vari tipi disponibili è utile capire il concetto principale: la ***direzionalità***, cioè la capacità dell'antenna di diffondere i segnale in determinate direzioni, piuttosto che in altre. Si deduce perciò che i tipi d'antenna possono essere:

1. **Omnidirezionale o isotropica:** diffonde il segnale a radiofrequenza tutt'intorno; idealmente il segnale si propaga come fosse una sfera (in realtà somiglia più ad una mela...) al cui centro risiede l'antenna. Questo tipo d'antenna non possiede generalmente alto guadagno poiché l'energia viene "dispersa" in ogni direzione, rendendola perciò la favorita in applicazioni dove è richiesta la copertura di ambienti non necessariamente estesi. Sebbene ve ne siano di svariati tipi e costruzioni, la sua forma tipica è quella di una stilo.

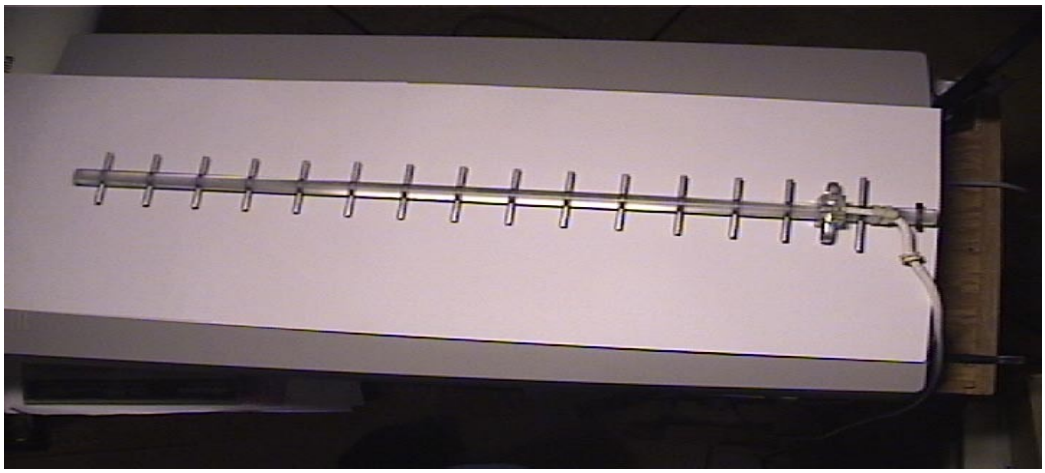
2. **Direzionale e direttiva:** hanno la peculiarità di concentrare il segnale in una zona, nella direzione del suo sviluppo. Dietro di sé, il segnale è fortemente ridotto d'intensità poiché ha scarse condizioni d'irradiazione. Il suo guadagno varia molto dal tipo di costruzione e dal materiale impiegato. Nelle versioni ad alto guadagno, il puntamento è particolarmente impegnativo poiché il segnale viene concentrato in un solo ipotetico punto. Particolare importanza riveste l'angolo d'apertura del segnale e la sua polarizzazione che può essere verticale se il suo campo si propaga sull'asse verticale o orizzontale se si propaga sull'asse orizzontale.

Considerando il fatto che ci sarebbe da dire molto riguardo le antenne, ma poiché questa guida si rivolge essenzialmente all'uso più che alla tecnica delle stesse, si ritiene utile soffermarsi su quelle di tipo direzionale, di ampio uso nei link a media e lunga distanza.

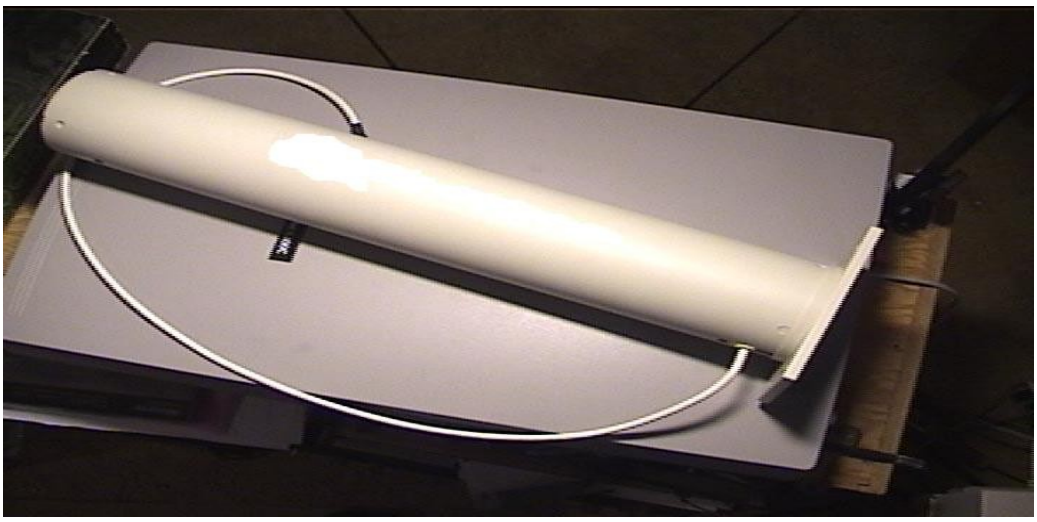
### 3.2 Direzionali e direttive

Da quanto esposto al punto nelle generalità, si evince che le direttive e direzionali posso essere di diverso tipo come per esempio:

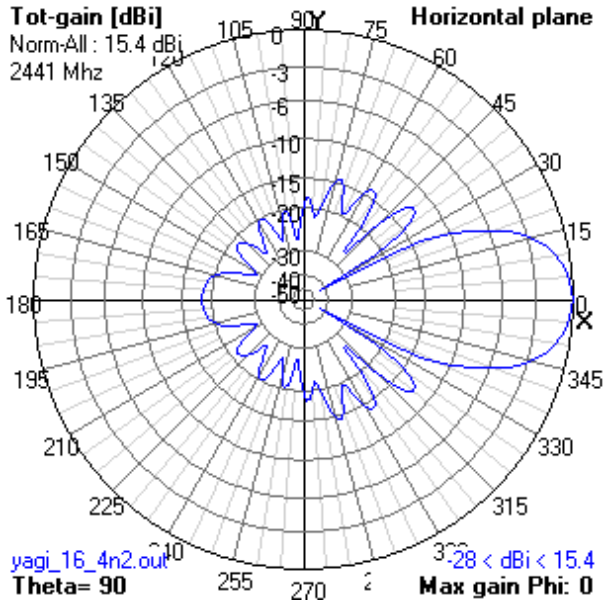
1. **Yagi:** simili in tutto per tutto alle antenne utilizzate per la ricezione dei segnali televisivi, si riconoscono per l'elevato numero di elementi che la compongono (composta cioè da quelli che vengono volgarmente chiamati “baffi”, tanto per intenderci...). Sono delle buone antenne e l'angolo di apertura del segnale diminuisce con l'aumentare del guadagno, come del resto accade con qualsiasi antenna direttiva. Vengono spesso impiegate nei centri urbani, in condomini, poiché si mimetizzano facilmente tra le antenne per la televisione. Ci sono alcune caratteristiche che però ne limitano l'impiego: **A**) più il guadagno è alto, più l'antenna si sviluppa in lunghezza, rendendone difficile l'installazione; **B**) sono piuttosto sensibili alla pioggia e durante la stagione invernale, formazioni di ghiaccio e neve, ne abbattono notevolmente il guadagno rallentando il link, fino ai casi più estremi in cui si perde.

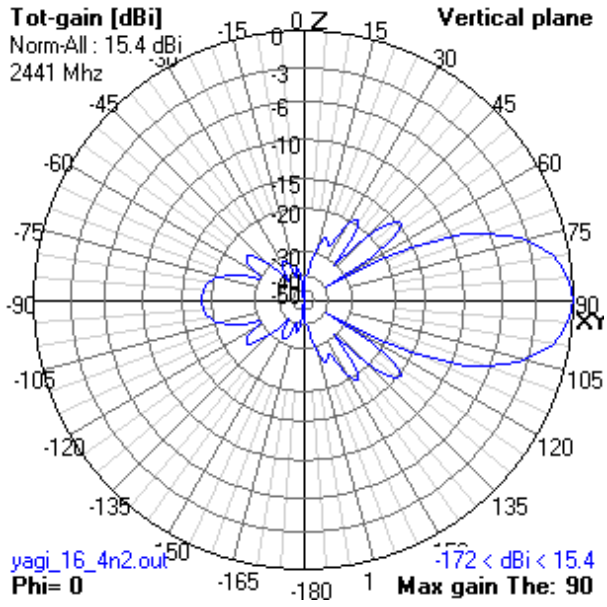


Per limitare le caratteristiche negative elencate al punto B descritto poco sopra, è possibile utilizzare il modello intubato che, purtroppo, la rende terribilmente identificabile:



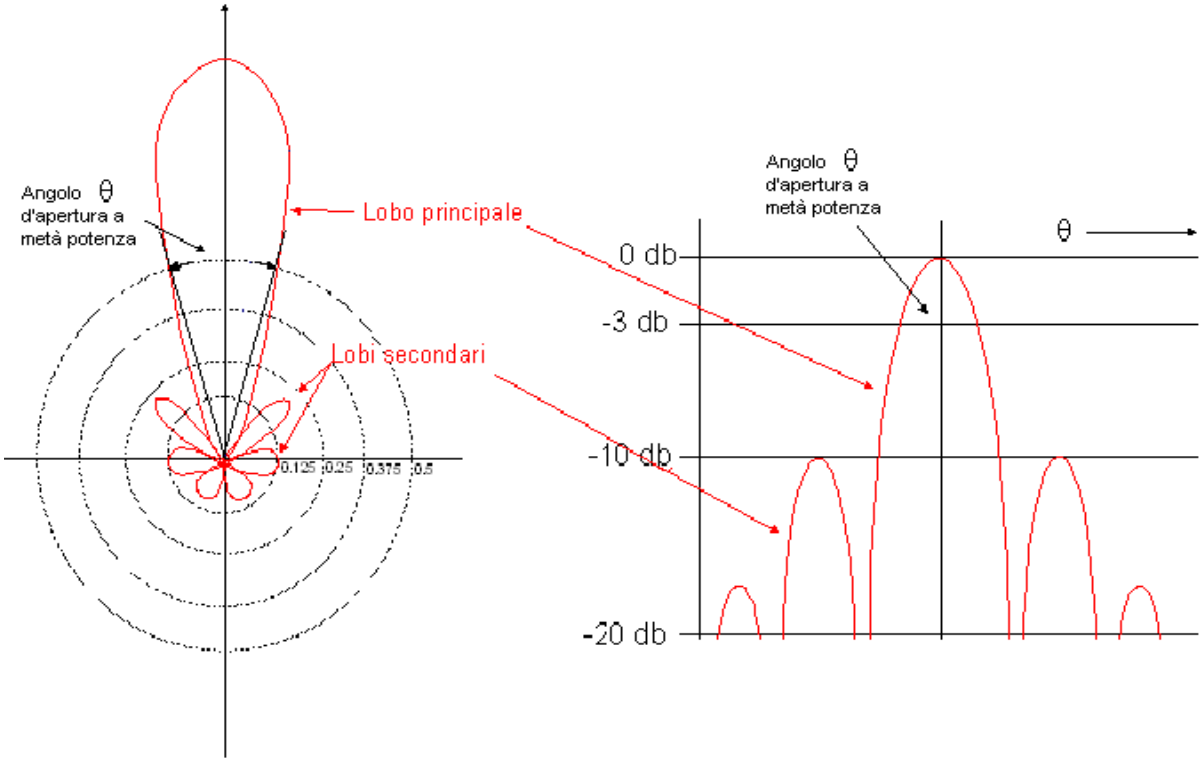
Le Yagi permettono link piuttosto lunghi, intorno ai 10 Km. Utilizzando il programma Nec2, è possibile creare una simulazione grafica dell'irradiazione, sia sul piano orizzontale sia su quello verticale, di una Yagi avente 16 elementi, come quella illustrata sopra e circa 15dB di guadagno:



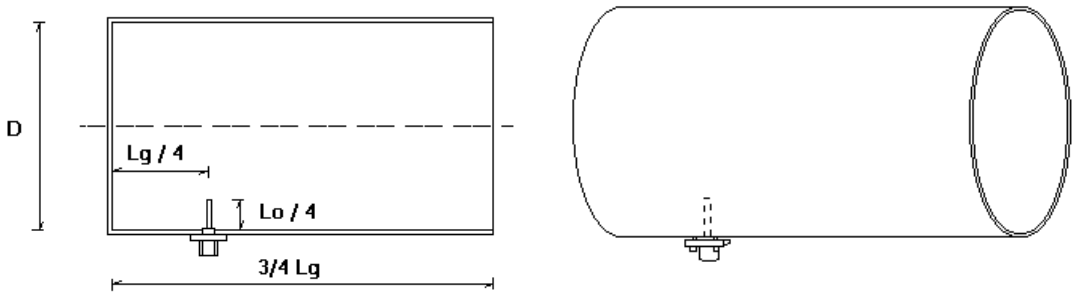
2. **Parabole:** Sono antenne particolarmente indicate quando la distanza inizia ad essere rilevante. Posseggono generalmente grande guadagno con dimensioni piuttosto ridotte che comunque aumentano con l'aumentare del guadagno. Sono composte da un elemento irradiante che si trova fisicamente nel fuoco di una griglia o di un disco parabolico. Queste ultime hanno una resa migliore ma le rendono molto visibili e sensibili alle forze di trazione generate dal vento. Possedendo grande direzionalità e quindi pochi gradi d'apertura del segnale, su grandi distanze, non è semplice il puntamento e spesso ci si aiuta col binocolo.

Il perché del grande guadagno è facilmente spiegabile mostrando i lobi d'irradiazione del segnale di un'antenna di tipo direttivo, come riportato nel disegno seguente:



Generalmente, in commercio, si possono facilmente reperire parabole dai 15 ai 24dB di guadagno ma, se si vuole salire, occorre darsi al modding ed utilizzare dei riflettori offset, normalmente impiegati per la ricezione delle emittenti satellitari. In questo caso basterà posizionare nel fuoco, al posto dell'LNB, una cantenna oppure una BiQuad. Nota particolare riguarda a questo punto il montaggio su palo che andrà eseguito al contrario, in modo che il puntamento non sia verso il cielo… Di seguito è possibile vedere alcuni esempi:

3. **A guida d'onda "Cantenna":** è la più semplice tra le antenne a giuda d'onda, particolarmente amata tra gli appassionati perché di semplice costruzione, con un costo di realizzazione decisamente irrisorio. Fondamentalmente è costituita da un barattolo in metallo e dall'elemento irradiante, il dipolo, che da sperimentazioni effettuate deve avere un diametro di 2 mm. Lo stesso dipolo è generalmente ricavato o saldato direttamente sul connettore d'antenna usato, tipicamente un N femmina. Lo schema di costruzione tipico è il seguente:




Siccome la frequenza utilizzata è di 2,45GHz, "**Lo**" ha valore di 122 mm ed il diametro "**D**" del barattolo dev'essere di circa 10 centimetri. La lunghezza del barattolo non è propriamente critica e dev'essere uguale o superiore a **3/4Lg**. Dati questi valori, si deduce che **Lo/4** è di 31 mm. Il valore di **Lg** dipende invece dal diametro del barattolo scelto. Di seguito sono forniti alcuni valori d'esempio, per l'uso in Wi-Fi:

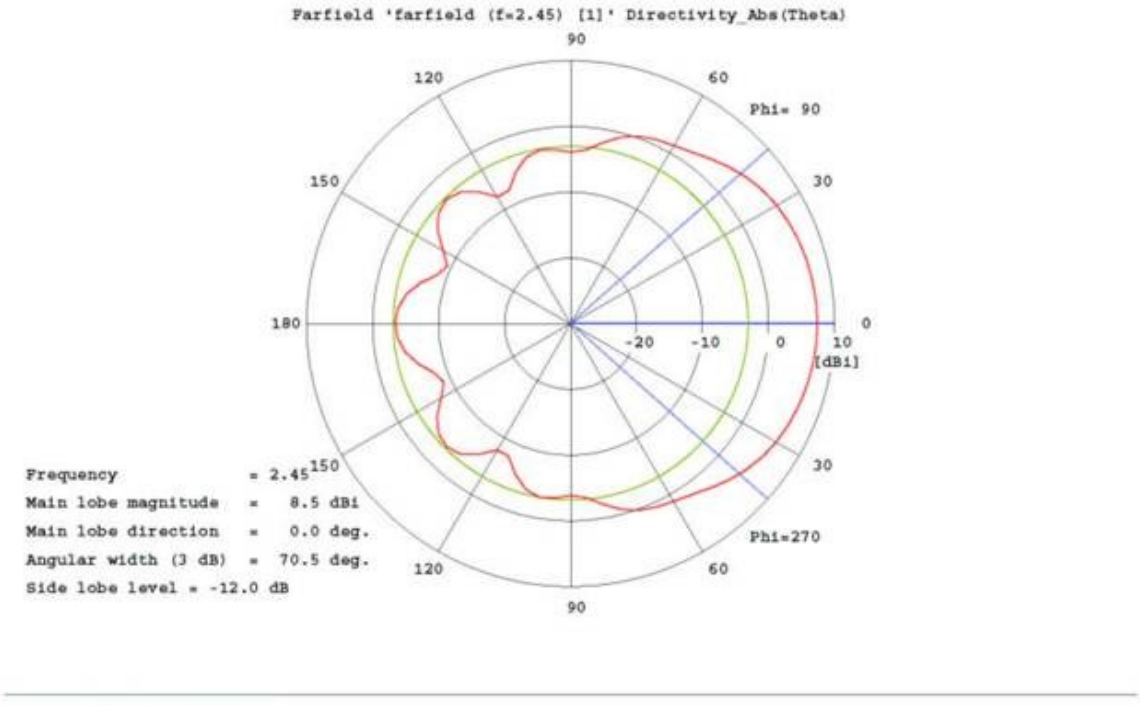
| Diametro del barattolo (mm) | Lunghezza d'onda LG (mm) | Lg/4 |
|---|---|---|
| 90 | 202,7 | 51 |
| 95 | 186,7 | 47 |
| 100 | 175,7 | 44 |
| 105 | 167,6 | 42 |
| 110 | 161,5 | 40 |

Tra le cantenne, la più famosa è la **Pringles Antenna**, costruita con i tubi delle omonime patatine; anche se un po' più corta, la sua estrema semplicità di costruzione la rende estremamente versatile per ogni occasione ma non adatta per l'uso definitivo in esterno (il tubo anche se alluminizzato all'interno, resta pur sempre di cartone). Esempi di Cantenna e di Pringles, sono visibili nelle seguenti foto. La prima montata provvisoriamente su un treppiede, durante una prova di link; la seconda, invece, è mostrata nelle sue componenti d'assemblaggio:

Cantenna

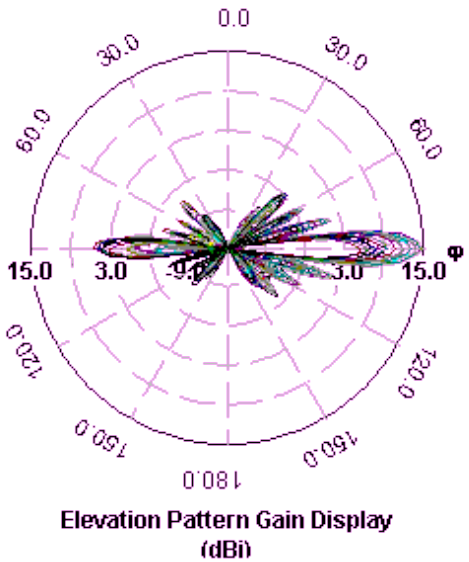
Pringles

Le antenne a barattolo risultano essere buone e con un guadagno stimato dai 7 ai 10dB, consentendo la realizzazione di link da 100 m a 3-4Km. Utilizzando il programma Nec2, è possibile creare una simulazione grafica dell'irradiazione sul piano orizzontale di una cantenna avente il diametro del barattolo di 10 cm:

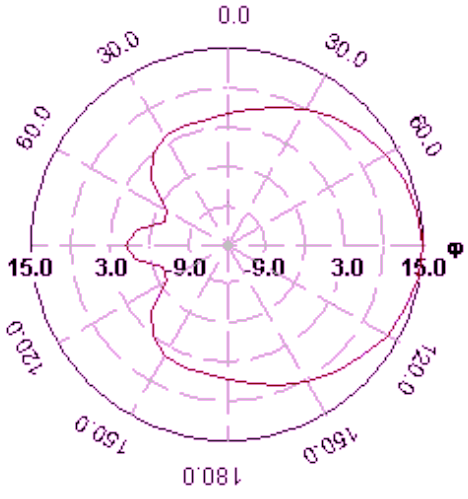


4. **Antenna a guida d'onda "Slotted Waveguide 180°":** Sebbene la sua costruzione richieda una lavorazione tramite macchine a controllo numerico (e quindi alto costo di realizzazione), questo tipo d'antenna è particolarmente utile quando gli angoli d'apertura del segnale devono essere piuttosto elevati (max 160-170°) ed accompagnati da un guadagno d'antenna medio-alto. Il suo sviluppo in altezza dipende dal numero di slot presenti e possiede polarizzazione orizzontale. Superato un certo numero di slot, data l'enorme lunghezza, si preferisce montarla in orizzontale. Questo tipo d'antenna viene anche realizzata con apertura di 360° (omnidirezionale). In figura è possibile vedere un tipico esempio di slotted waveguide con i suoi caratteristici slot, in questo caso sono ben 16:

Come detto in precedenza, a causa dell'elevata precisione della lavorazione richiesta, una realizzazione home-made è quasi impossibile. A titolo informativo, è giusto dire che esistono comunque delle sperimentazioni che utilizzano una barra di polistirolo ricoperta di carta stagnola, ricavando le aperture incidendo la stessa. Utilizzando il programma Nec2, è possibile creare una simulazione grafica dell'irradiazione sui piani di elevazione ed azimutale di una slotted waveguide 180° avente 8 slot:

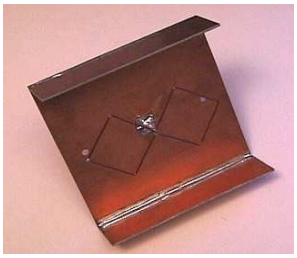


Elevation Pattern Gain Display
(dBi)



Azimuth Pattern Gain Display
(dBi)

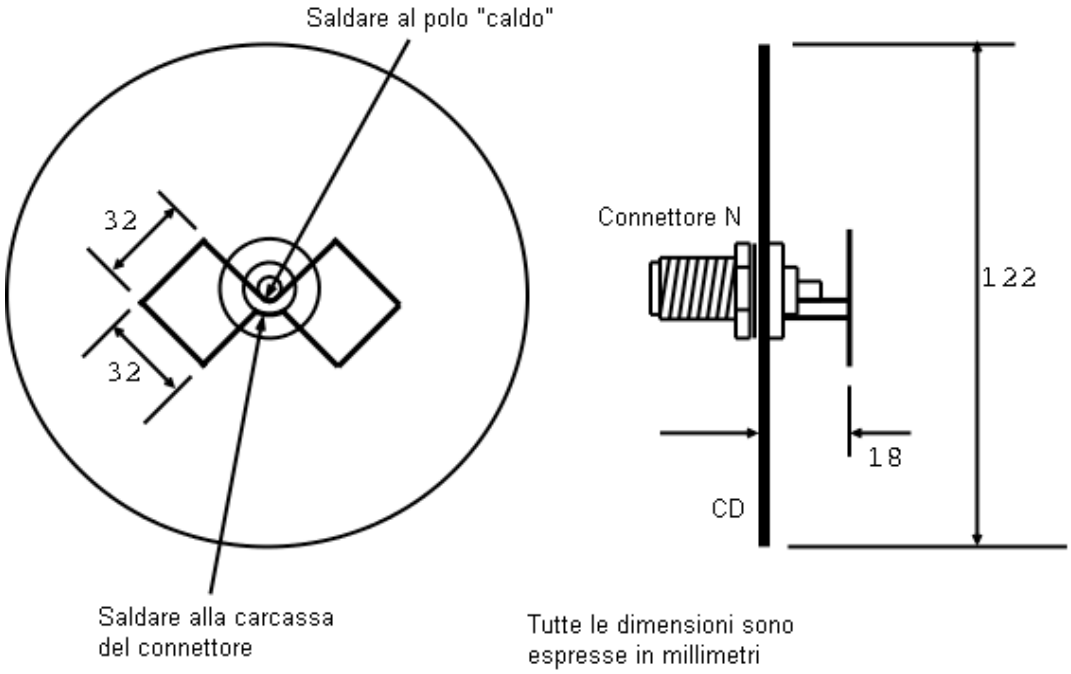
5. **BiQuad:** Esteticamente piccola, la BiQuad vanta grande popolarità grazie alla sua semplicità costruttiva e di puntamento, ha apertura di 180° e guadagno nell'ordine dei 10-11dB. Sebbene il principio di costruzione sia sempre uguale, ne esistono svariate realizzazioni, impieganti materiali e forme diverse (particolare è l'impiego di vecchi cd). Nella foto è possibile vederla nella sua realizzazione tipica, utilizzando lamine di rame.



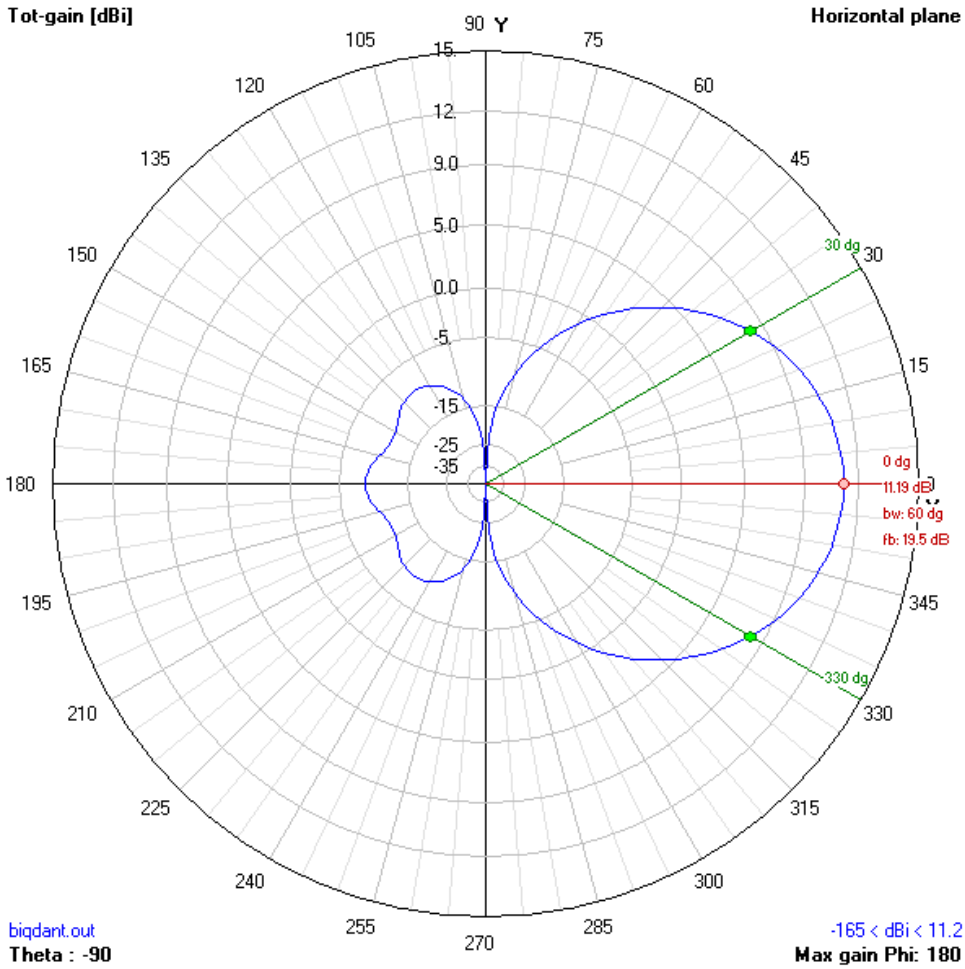
Vediamo ora come realizzarne velocemente una, nella versione "BiQuad CD", dove il materiale occorrente è di facile reperimento e consiste in:

- 2 cd o cd-r inutilizzabili (vi sarà capitato di "bruciarne" qualcuno);
- della carta stagnola;
- un connettore femmina da pannello con fissaggio "a controdado";
- spezzone di cavo di rame con diametro di 2 millimetri.

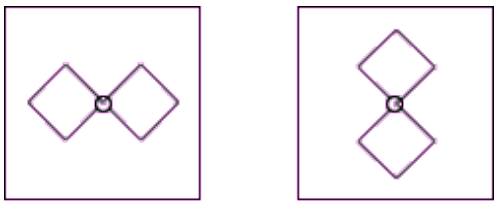
Reperito il materiale, affidarsi al disegno di costruzione seguente che, pur non essendo di carattere tecnico, fornisce sufficienti dettagli per la realizzazione.




Per semplicità di rappresentazione, nello schema è stato disegnato un solo cd che, nella realtà, si compone di due cd con interposti due fogli di carta stagnola che, a sua volta, deve presentare continuità elettrica con la carcassa del connettore N.
Per l'uso esterno, è possibile racchiudere il tutto all'interno di un contenitore di cd spindle.
Utilizzando il programma Nec2, è possibile creare una simulazione grafica dell'irradiazione sul piano orizzontale:




E' altresì opportuno far presente che, come avviene per ogni antenna, in base alla posizione dell'elemento irradiante cambia anche la polarità del segnale:



Verticale Orizzontale

Le BiQuad, senza l'ausilio di un riflettore parabolico, sono antenne che permettono generalmente la realizzazione di link fino a 6-7 Km di distanza.

### 3.3 Formule utili

Sebbene questa sezione non vuole assumere carattere prettamente tecnico, viene fornita una serie di formule matematiche che semplificano lo studio e la realizzazione di un link wireless.

- Lunghezza d'onda **λ** (in metri):

  **$\lambda = 300/f$** f = frequenza in MHz

- La densità di potenza in un punto qualsiasi di distanza (**d**), utilizzando un'antenna di tipo omnidirezionale, è dato dalla formula:

  **$P(d) = EIRP/(4*\pi*d^2)$ [W/mq]**

- La potenza al ricevitore è data dalla formula:

  **$Pr = EIRP * Gar * [\lambda/(4*\pi*d)]^2$** Gar = guadagno antenna ricevente

- L'attenuazione dovuta alla distanza (**d**)**:**

  **$Ad = [\lambda/(4*\pi*d)]^{-2}$**

- Power o Link Budget (PB):

  **PB = Papp (dBm) + Gant (dB) – Pcavi(dB) – Pcon (dB)**

  Papp = potenza apparato
  Gant = guadagno antenna
  Pcavi = perdita cavi
  Pconn = perdita connettori

- Margine di guadagno (MG):

  **MG = PB (dB) – Perdite propagazione "Ad"(dB) – sensibilità ricevitore (-dB)**

# Attacco alla (propria) rete wireless

Un esempio classico che fa sempre venire dei dubbi sull'affidabilità e sicurezza della propria rete wireless può essere il seguente: “siete comodamente seduti all'interno della vostra casa, davanti a voi il fidato portatile e state svogliatamente navigando in internet attraverso la rete wi-fi, incuranti di ciò che sta avvenendo all'esterno dell'appartamento. Vostra madre alla finestra vede un'auto che accosta e si ferma sotto casa ma non presta più di tanto attenzione... in fin dei conti sono molte le auto che affollano le città. Sarebbe tutto normale se i tizi in macchina non fossero indaffarati ad armeggiare con un portatile... In effetti, stanno facendo del WARDRIVING, cioè stanno girando la città alla ricerca di reti wireless e dopo qualche minuto, hanno violato la vostra rete, sfruttandone come parassiti la connessione a banda larga o, peggio ancora, rovistando nelle vostre risorse.”

Sembra un paradosso ma, per difendersi e testare la propria rete, bisogna pensare come un hacker e sapere come vengono condotti gli attacchi. Solo così ci si può difendere e capire di quali falle di sicurezza soffre la propria rete. Le informazioni date di seguito sono da considerarsi di carattere didattico ed usate per testare la propria rete wireless. E' doveroso far presente che violare una rete è una pratica illegale e punibile secondo le vigenti leggi. Questa sezione ha motivo d'esistere poiché ogni installazione deve garantire nel miglior modo possibile un’adeguata sicurezza e rendere quantomeno difficile un tentativo d'intrusione. L'autore declina ogni responsabilità sull'uso diverso dalla “conoscenza didattica” ad opera dei lettori.

## 4.1 L'hardware

Gli strumenti che tipicamente usa un wardriver non si discostano molto dall'hardware utilizzato da un utente comune. In effetti, alcuni componenti hardware (e software) vengono comunemente impiegati per il puntamento delle antenne direttive: un portatile con scheda wireless pcmcia dotata di connettore per antenna esterna, un'antenna omnidirezionale o direttiva (nello specifico una cantenna, impiegata per condurre attacchi o rilevamenti “a distanza”) e un ricevitore GPS, il cui uso è facoltativo ed utilizzato per risalire alle coordinate geografiche di un ap attraverso l'intensità del segnale rilevata da alcuni software... questa soluzione risulta eccellente se si desidera verificare la portata in trasmissione. Non mancheranno certamente dal suo corredo cavi ed adattatori d’ogni tipo, per fronteggiare qualsiasi tipo di esigenza.
Sebbene l'attrezzatura descritta sopra può sembrare a prima vista piuttosto costosa, il wardriver è anche un esperto di modding, cioè possiede conoscenze che gli permettono di modificare alcuni componenti hardware per renderli fruibili e operanti in condizioni diverse da quelle per cui sono stati concepiti. E' così che schede dal costo contenuto, diventano un ottimo strumento adatto alle sue esigenze.

## 4.2 Il software

Nell'infinità di internet è possibile trovare molto materiale adatto allo scopo. Molto di questo software è disponibile solo per Linux e quindi per utenti un po' evoluti, dove molte volte è richiesta la ricompilazione del kernel con driver opportuni. Sebbene quest'affermazione può demoralizzare quegli utenti abituati al "punta e clicca" tipico di Windows, anche per loro esiste del software che bene si adatta allo scopo e sebbene la quantità di utility sia inferiore, presenta notevole facilità di configurazione.
I pacchetti che ben rappresentano la categoria, più conosciuti e relativamente semplici da usare sono, **Network Stumbler** (conosciuto anche come **NetStumbler), Kismet, Ethereal, AirSnort, Look@Lan, AiroPeek NX.**
Questi software vengono considerati strumenti a "doppio taglio" e cioè possono essere usati per studiare la propria rete, osservandone le sue debolezze, e per il fine meno glorioso: l'attacco! Bisogna però sempre tener presente che questi strumenti sono stati concepiti come base di conoscenza per impostare una linea difensiva ed aumentare il livello di sicurezza della propria rete wireless. Vengono altresì indicati per ogni software la **diffusione**, cioè la frequenza d'uso verso bersagli reali (1 = raro, 10 = utilizzato spesso), la **semplicità d'uso** (10 = esperto, 1 = principiante), l'**impatto sul sistema** (1 = poco rilevante, 10 = compromissione) ed il **fattore di rischio** (1 = basso, 10 = alto).

- **Network Stumbler:**

  O.S.: Windows Sito: www.netstumbler.com
  Diffusione: 10
  Semplicità d'uso: 1
  Impatto sul sistema: 9
  Fattore di rischio: 9,7

  Considerato erroneamente uno sniffer, si limita ad effettuare il parsing degli header dei pacchetti wireless. Il wardriving degli access point ha inizio con la localizzazione, tramite il metodo passivo di ascolto dei *Broadcast Beacon* trasmessi oppure utilizzando il metodo più aggressivo, consistente nella trasmissione di *Client Beacon*, in modo da ottenere risposte dagli AP con la configurazione della rete. Dispone di un'interfaccia grafica opportunamente progettata, mostrando in tempo reale i dati relativi la posizione (se usato in concomitanza con un ricevitore GPS), identificazione SSID, lo stato del WEP, l'indirizzo MAC, il canale usato, il modo di funzionamento del dispositivo (AP, Bridge...), produttore e rapporto segnale/rumore (anche graficamente). Se NetStumbler non rileva reti dove si è sicuri ve ne siano, è utile verificare che nelle impostazione di rete, lo SSID o il nome della rete sia impostato su ANY. Questa impostazione indica al driver di utilizzare un SSID di lunghezza 0 (zero) nelle richiesta di *probe.* La maggior parte degli access point risponderà alle richieste con *probe* contenenti il loro SSID o con SSID di lunghezza 0 (zero).

  *Contromisure:* poiché NetStumbler si basa su una sola forma di rilevamento delle reti, attraverso la richiesta di probe di tipo broadcast, può essere accecato disabilitando questa funzionalità che normalmente viene offerta dai produttori di access point. E' sempre buona norma disabilitare lo SSID broadcast e cambiare il suo valore di default.

- **Kismet:**

  O.S.: Linux Sito: www.kismetwireless.net
  Diffusione: 8
  Semplicità d'uso: 3
  Impatto sul sistema: 9
  Fattore di rischio: 8

  E' uno sniffer per reti wireless a rilevamento passivo, dotato di molte funzionalità. Come NetStumbler consente d'identificare gli accesss point, la posizione mediante GPS, il tipo di modalità di funzionamento, il canale usato. Il rilevamento avviene in modalità ciclica, tramite la scansione dei canali disponibili alla ricerca di pacchetti 802.11. Per funzionare necessita di driver personalizzati facendo funzionare la scheda wireless in modalità *monitor*, la cui procedura d'abilitazione varia in base al chipset usato.
  Subito dopo l'avvio, l'interfaccia mostra tutte le reti disponibili nel raggio di copertura disponibile evidenziando, nei dettagli, la classe d'indirizzo usata (**IP Range**), tramite richieste ARP o ascoltando il traffico normale. Al suo interno è presente il programma GPSMap, in grado di creare mappe dai dati rilevati. Supporta la maggior parte delle schede disponibili per Linux.

  *Contromisure:* purtroppo non esistono molte contromisure poiché allo stato attuale risulta essere il miglior tool per il wardriving. Dalla sua descrizione si evince che è in grado di rilevare reti che normalmente sfuggono a NetStumbler di cui ha in comune molte funzionalità. E' altresì in grado di registrare automaticamente i pacchetti WEP con punti deboli **IV**, utilizzabili da AirSnort.

- **Ethereal:**

  O.S.: Linux, Windows Sito: www.ethereal.com
  Diffusione: 9
  Semplicità d'uso: 4
  Impatto sul sistema: 8
  Fattore di rischio: 8

  E' uno strumento per il monitoraggio delle reti e sebbene non studiato appositamente per le reti 802.11x, ne supporta la cattura e la decodifica attraverso la libreria *libpcap* solo sui sistemi *nix. Siccome tale opportunità non è presente nella versione per Windows, è possibile aggirare il problema utilizzando la versione *nix per la cattura ed elaborando poi i dati salvati con quella per Windows. Come per Kismet, necessita l'uso di driver personalizzati per far funzionare la scheda wireless in modalità monitor. La sua interfaccia è suddivisa in tre sezioni: in quella superiore c'è il riepilogo dei pacchetti catturati; quella intermedia mostra il dettaglio del pacchetto selezionato nella sezione superiore; la *data view* è nella sezione inferiore ed è il dumping dei dati esadecimali e ASCII.

- **AirSnort:**

  O.S.: Linux Sito: airsnort.shmoo.com
  Diffusione: 7
  Semplicità d'uso: 3
  Impatto sul sistema: 9
  Fattore di rischio: 8

  E' uno strumento che sfrutta i punti deboli del WEP, consentendo e semplificando l'automazione degli attacchi, sfruttando tecniche di cattura e crack dei pacchetti. E' l'insieme di tool più popolare, specificatamente impiegato per il crack dei pacchetti wireless, grazie alla rapida configurazione sia del canale da esplorare sia della lunghezza (in bit) della chiave WEP. Grazie alla sua semplice interfaccia grafica, è possibile catturare una certa quantità di pacchetti di diverso tipo affinché si possano condurre vari attacchi alla rete wireless.

  *Contromisure:* per tutti gli sniffer e cracker di pacchetti wireless, le contromisure usate sono piuttosto semplici. Per prima cosa bisogna attivare il WEP su tutti gli apparati, impiegando una lunghezza della chiave almeno da 128 bit. Scegliere una chiave segreta che non sia presente in un dizionario, la cui lunghezza sia superiore a 8 caratteri e che contenga un insieme di caratteri alfanumerici e speciali. Tutto ciò non garantisce la massima sicurezza ma permette d'aumentare notevolmente il tempo necessario per l'esecuzione di attacchi basati sulla tecnica della *"forza bruta"*, rispetto ad una semplice chiave da 6 caratteri. Adottare, se possibile, implementazioni proprietarie (come WEP a 256 bit) o fixate del WEP, cambiando spesso la chiave. Non usare mai l'impostazione di fabbrica di SSID e se possibile (molto spesso), disabilitarne il broadcast.

- **Look@Lan:**

  O.S.: Windows Sito: www.lookatlan.com
  Diffusione: 6
  Semplicità d'uso: 2
  Impatto sul sistema: 8
  Fattore di rischio: 8

  Software diagnostico che permette di visualizzare in modo dettagliato tutte informazioni, compresi i servizi attivi della rete che si sta analizzando, sebbene non è concepito per l'analisi dei pacchetti wireless. E' utilizzato spesso in abbinamento ad altri pacchetti. Una volta avviato, dalla schermata iniziale si seleziona un profilo e dopo qualche istante appaiono tutti i computer con rispettivi indirizzi IP, O.S., Hostname, posizione e stato della rete a cui si è collegati. Particolarmente interessante è la possibilità di richiamare ed analizzare facilmente i dettagli di ogni singolo componente della rete, mostrandone i servizi e le porte aperte.

  *Contromisure:* contro questo tipo di analisi si può fare ben poco. L'unico consiglio è quello di tenere i sistemi aggiornati, evitando d'esporre i pc ad inutili exploit. Utilizzare firewall selettivi, anche perimetralmente, in modo da filtrare tutto il traffico sulla rete, evitando di lasciare inutili porte aperte.

- **AiroPeek NX:**

  O.S.: Windows  Sito: www.wildpackets.com
  Diffusione: 3
  Semplicità d'uso: 2
  Impatto sul sistema: 8
  Fattore di rischio: 6

  E' uno strumento appositamente studiato per la diagnostica, il monitoraggio e l'analisi dei pacchetti 802.11x, decifrandone il contenuto in tempo reale. E' veramente valido ed efficiente, raggruppando i nodi in base al loro indirizzo MAC. Ne visualizza gli indirizzi IP, i protocolli e nella *peer map* mostra tutti gli host rilevati sulla rete mediante le loro connessioni reciproche. Quest'ultima particolarità permette di semplificare di molto la relazione tra access point e client. Come tutte le cose, presenta dei lati negativi: non funziona con tutte le schede wireless e necessita di driver appositi e gira solo su Windows 2000/XP. E' un tool commerciale (attualmente per Windows non esistono tools gratuiti), il cui costo è comunque contenuto rispetto ad altri software simili. Al suo interno, sono presenti opzioni per aumentare la sicurezza della rete.

  *Esiste tuttavia un altro eccellente tool simile ad AiroPeek disponibile al link www.thc.org e che risponde al nome di THC-Wardrive. Consente di condurre test di penetrazione alla rete.*

### 4.3 Da MAC a IP e ritorno. L'ARP (Address Resolution Protocol)

L'indirizzo MAC rappresenta l'identificatore fisico univoco di un adattatore di rete, che permette a livello di datalink, ovvero al layer 2 ISO/OSI, di accedere al livello fisico per la comunicazione in rete (la scheda di rete). L'indirizzo IP rappresenta l'indirizzo logico dell'adattatore nella rete del protocollo internet. Utilizzando sistemi operativi GNU/Linux è possibile scoprire entrambi i valori dando da shell il comando:

```
$ifconfig [invio]
```

Come sarà spiegato in seguito, la staticità del MAC può essere violata in molteplici modi, causando pesanti problemi di sicurezza attraverso le vulnerabilità di ARP (Address Resolution Protocol), una feature interna al protocollo IP, che permette la "traduzione" dall'indirizzamento IP ad indirizzamento MAC, e che sta alla base della comunicazione nelle reti di tipo broadcast; non è comunque possibile effettuare l'operazione inversa poiché ARP non è stato creato per funzionare in altre "direzioni".
Prima di capire il funzionamento di ARP, è utile capire cosa sia una comunicazione di tipo broadcast. Nella definizione più semplice è la trasmissione di informazioni da un sistema trasmittente ad un insieme di ricevitori numericamente non definito.
Non esiste un metodo universale per determinare l'indirizzo IP da un indirizzo MAC conosciuto e comunque sia, può essere possibile solo in specifiche condizioni. Il protocollo ARP tiene traccia, in una sorta di lista, di entrambi gli indirizzi nella **ARP cache** che è disponibile nei pc, negli adattatori di rete ed in alcuni router IP.
Per comprendere il principio di funzionamento di ARP è utile analizzare le varie fasi che permettono di stabilire una comunicazione tra due amici in un gruppo numeroso... Colui che intende avviare la comunicazione (A), deve determinare in modo univoco il destinatario (B) all'interno del gruppo e che possiede un certo attributo, il nome. Quindi le varie fasi si possono così riassumere:

- "A" si rivolge al gruppo e chiede chi è "B";
- Il gruppo riceve la domanda ma solo "B" risponde;
- Ora è possibile la comunicazione diretta tra "A" e "B".

Come avviene nel mondo umano, ARP non fa altro che determinare quale interfaccia di rete tra quelle presenti sulla LAN possiede un determinato indirizzo IP. Traducendo in termini più tecnici, ARP opera effettuando una riduzione da broadcast ad unicast, rendendo così possibile la comunicazione nelle reti informatiche.
Riprendendo l'esempio precedente, è possibile analizzare le vari fasi:
Per prima cosa, un'applicazione richiede l'invio di ad un determinato host, il cui nome dev'essere risolto (ovvero tradotto) in un numero IP verso cui stabilire una connessione e, infine, il sottosistema di rete tenta di stabilire una corrispondenza tra IP ed il MAC della scheda fisica che lo possiede, rendendo possibile la successiva comunicazione.
Per stabilire questa corrispondenza IP/MAC di destinazione, il mittente, cerca prima la presenza nella propria ARP cache l'eventuale presenza di questo accoppiamento; ciò è vero quando i due computer hanno comunicato di recente. Se non fosse presente, l'informazione va reperita dalla LAN: il primo pc (A) invia in broadcast a tutti i pc presenti un pacchetto chiamato "ARP Request", all'interno del quale si trovano il proprio IP, il proprio MAC e l'IP del destinatario (B). Tutti i pc ricevono la richiesta e verificano se sono loro i destinatari; solo chi possiede l'IP giusto (B) invia in unicast verso il MAC di A uno speciale pacchetto chiamato ARP Reply dove inserisce il suo MAC; tutti gli altri pc scartano semplicemente la richiesta.
A questo punto, "A" inserisce nella sua cache la corrispondenza e può finalmente avviare la

comunicazione. Dando da shell il comando ARP, verrà visualizzato il contenuto della ARP cache e presente nel file **/proc/net/arp** di cui si riporta un esempio generico:

**$arp** [invio]

| **Address** | **HWtype** | **HWaddress** | **Flags** | **Iface** |
|---|---|---|---|---|
| **192.168.0.1** | **ether** | **00:40:A1:BF:F3:EB** | **C** | **eth0** |
| **192.168.0.2** | **ether** | **00:40:A1:BF:F3:DF** | **C** | **eth0** |

Si può apprendere l'indirizzo IP (Address), il tipo di link che porta all'host (HWtype), il MAC (HWaddress), i vari Flags (C = valido; M = permanente; ed altri ancora) e l'interfaccia.

E' possibile rimuovere manualmente una entry dando il semplicissimo comando:

**$arp -d indirizzo_ip** [invio]

Esiste anche un comando per inviare richieste ARP ad un host appartenente alla propria rete:

**$arping indirizzo_ip** [invio]

Riassumendo quanto detto finora, ARP è il protocollo di basso livello su cui poggiano le comunicazioni di rete: nel momento in cui due pc devono comunicare, ad ARP è affidato il delicatissimo compito di metterli in contatto. La fiducia sulla quale ARP sottende, fa sì che il bind tra gli indirizzi IP/MAC di destinazione avvengano senza nessun tipo di controllo su chi ha inviato l'ARP Reply (cosa che viene invece effettuata con l'introduzione del protocollo IPv6). Tutto ciò espone i computer a falle di sicurezza per effetto di contraffazioni (spoofing) od avvelenamento (poisoning). Ma vediamo come può accadere una cosa simile...

- L'IP spoofing:

Un computer può impersonarne un'altro solitamente presente sul suo stesso segmento di rete semplicemente acquisendone l'indirizzo IP ed inserendosi quando quest'ultimo è spento o non raggiungibile perché isolato dalla stessa a causa di un attacco DoS andato a buon fine. L'IP spoofing può essere realizzato semplicemente e può portare anche alla compromissione del routing della rete, quando l'IP contraffatto è quello del gateway. Questo tipo di attacco dovrebbe far riflettere su quanto sia estremamente debole, insicuro e da evitarsi, il diffusissimo approccio di autenticazione degli utenti basato sull'indirizzo IP; quando possibile, conviene affidarsi all'autenticazione basata su certificati e chiavi crittografiche.

- L'ARP spoofing:

Conosciuto anche come ARP poisoning, ovvero avvelenamento, consiste nella compromissione della ARP cache del computer, del router o altro apparato sotto attacco. Purtroppo questo tipo di attacco è piuttosto semplice da realizzare se viene utilizzato il programma “ettercap”, che permette di realizzare pacchetti di tipo ARP Reply ed inviarli al target stabilito, ingannando così gli accoppiamenti IP/MAC.
Per completezza d'informazione, occorre dire che la ARP cache ha dimensioni finite e limitate; ogni computer tende a rimuovere dalla cache i dispositivi con cui non “parla” da un certo periodo di tempo, in modo da lasciare spazio a nuove entry. La conseguenza devastante è che se un ramo della rete viene letteralmente inondato di ARP flood, ovvero di pacchetti appositamente creati, il server (o altri pc) tenderà a svuotare la cache e si sarà in grado di creare delle nuove entry a piacimento; è così possibile inserirsi nella comunicazione tra due nodi, avvelenando la loro cache in modo da far

credere ad entrambi di parlare con la corretta controparte, mentre invece il MAC con cui dialogano è quello registrato sulla scheda di rete del computer avvelenatore... Per questo motivo, questo attacco prende il nome di **Man in the Middle (MitM)**, uomo nel mezzo.
Un attacco MitM è talmente grave da permettere lo sniffing anche delle reti switched: quando uno switch viene sottoposto ad un ARP flood, non è più capace di mantenere le associazioni e passa ad uno stato di funzionamento chiamato "fail open", in cui si comporta come un HUB, e replica i pacchetti del traffico su tutte le porte, rendendo terribilmente banali operazioni di sniffing. Gli apparati professionali o comunque seri, dispongono di contromisure adeguate.

- Esempio pratico:

Solamente per far capire come sia semplice sfruttare le debolezze strutturali di ARP, vediamo come fare un attacco Man in the Middle utilizzando ettercap...
Supponendo che il client con IP 192.168.10.1 voglia scambiare dati con un server avente IP 192.168.10.100 e che il pc attaccante, con IP 192.168.10.20, desideri intromettersi tra i due in modo tale da far credere che entrambi che stanno veramente comunicando con la legittima controparte, se non sono state prese opportune misure precauzionali, l'attaccante non dovrebbe far altro che digitare da shell il seguente comando:

**$ettercap -T -M arp /192.168.10.1/192.168.10.100/** [invio]

La cache di clent e server saranno avvelenate dopo pochi istanti. Tutto il traffico transiterà attraverso il pc attaccante e sarà sufficiente uno sniffer per verificarlo, compromettendone l'integrità dei dati per quanto riguarda la privacy e la sicurezza...

**NOTE:** Per completezza d'informazione, è utile far presente che esiste anche un protocollo inverso: **RARP** (**R**everse **A**ddress **R**esolution **P**rotocol), che permette ad un host di risolvere il proprio indirizzo IP a partire da MAC address tramite una richiesta ad un server RARP.
Utilizzando ad esempio il sistema operativo Microsoft Windows ed alcuni altri, il comando **"ARP"** permette l'accesso alla cache locale, il cui risultato si ottiene dando (da shell) il seguente comando:

**$arp -a** [invio]

è comunque da ricordare che un'operazione simile è fattibile solo nel caso in cui il computer sia correttamente connesso alla rete, altrimenti la cache resterà vuota e che, nel caso migliore, mostrerà solo l'indirizzamento dei computer e dei dispositivi connessi alla propria LAN. Tale opportunità è altresì inclusa in alcuni router a banda larga che la rendono visibile attraverso una "comoda" interfaccia web-based.

## 4.4 Dalla teoria alla pratica

In questo paragrafo si sperimenterà l'attacco ad una rete wireless (di proprietà) partendo da zero (detto anche conoscenza-zero o zero-knowledge), dove non si conosce decisamente nulla del network preso in esame. Naturalmente ci si deve dotare dello stretto necessario, che corrisponde al *"Kit di sopravvivenza Wi-Fi"* e descritto in precedenza; un portatile sul quale gira un sistema operativo GNU/Linux con installato Kismet e AirCrack.
Abilitare la scheda di rete Wi-Fi ed avviare Kismet che chiederà in quale directory salvare il file di dump del traffico ricevuto; per esempio è possibile salvarlo in /tmp/kismet. E' altresì possibile indicare quale prefisso debba avere il file di log; anche il valore di default è sufficiente. Cliccando su OK, Kismet verrà avviato e dopo qualche istante appariranno le reti Wi-Fi alla nostra portata. Prima di iniziare è bene aprire il menù *Sorting* (con il tasto "s") e premere il tasto "f" per dire a Kismet di ordinare le reti in ordine di rilevamento. Scegliere a questo punto la rete da "testare". Dalla schermata principale è immediatamente possibile notare di quale tipo (type, colonna "T") di network si tratta (A = access point; P = peer; B = bridge), se la codifica WEP (colonna "W") è attiva (Y = yes; N = no), il canale usato (colonna Ch), i pacchetti trasferiti, ecc... Premere il tasto "i" per avere informazioni più dettagliate e segnare da qualche parte i parametri che più interessano:

- *SSID*: Service Set Identifier, il nome della rete, che costituisce un primo livello di protezione;
- *BSSID*: trattasi dell'indirizzo MAC (aa:bb:cc:dd:ee:ff) della scheda di rete dell'access point;
- *Encrypt*: è l'algoritmo di cifratura usato. Bisogna sapere se WEP o WPA.

Ora che abbiamo a disposizione le informazioni principali, non resta che catturare, ascoltando, il maggior traffico possibile e perciò bisognerà dotarsi di pazienza fino a quando si saranno raccolti da 200 a 800 Mbyte di dati per tentare di recuperare la chiave usata per la cifratura... Per dovere di cronaca, se il network è attivo, dopo 30 minuti, si avranno abbastanza dati (poco più di 300 Mbyte) per tentare un attacco, detto in gergo "test preliminare"... Si è così pronti a "dare in pasto" il contenuto ad un altro tool: AirCrack. Questo programma implementa moltissimi attacchi contro WEP e WPA, è flessibile e permette molte opzioni, inseribili nel caso si conoscano maggiori dettagli sul network. Per funzionare, necessita di tre opzioni fondamentali che sono quelle annotate in precedenza. Aprire una sessione a linea di comando ed inserire quanto segue:

**$aircrack -ng -a 1 -e SSID -b BSSID -n 64 /tmp/file.dump** [invio]

il primo parametro indica che si vuole crackare una chiave WEP, il secondo l'SSID, il terzo lo BSSID, il quarto (-n) indica che si vuole cercare una chiave a 64 bit; se non si ottiene risultati apprezzabili, provare inserendo 128, 256 o 512. L'ultimo parametro indica il file contenente il dump del traffico del network. Dando l'invio, si dovrà attendere qualche istante e, se tutto procede per il verso giusto, si otterrà la risposta *"KEY FOUND"*, segno che è stata trovata la chiave...
A questo punto è utile provare ad associarsi all'access point, dando da consolle i comandi:

**$ifconfig ethx up** [invio]
**$iwconfig ethx essid "SSID" ap ESSID** [invio]
**$iwconfig ethx key open WEPKEY** [invio]
**$iwconfig ethx** [invio]

naturalmente “ethx” andrà sostituito con la scheda di rete Wi-Fi, per esempio eth1; SSID con il valore rilevato in precedenza; ESSID con il valore rilevato in precedenza (del tipo: aa:bb:cc:dd:ee:ff); WEPKEY con il valore rilevato tramite AirCrack.
L'ultimo comando serve per verificare se ci si è associati correttamente all'access point. Se è presente un ulteriore “strato” di sicurezza, come il controllo sui MAC dei client associati, è facile imbattersi nella dicitura *“UNASSOCIATED”*. Sebbene conferisce maggior grado di sicurezza, non costituisce un problema per il test, poiché è possibile recuperarne facilmente uno valido attraverso la tecnica di spoof. Tornare alla finestra di Kismet e premere il pulsante “c” (client list) sulla schermata del network prescelto, ottenendo in questo modo la lista dei client associati. Scegliere quello che genera il minor traffico (colonna Data e Size) e segnarsi da qualche parte il MAC. Con un semplice comando, assegnarlo alla propria scheda wireless:

**$ifconf ethx hw ether MAC** [invio]

ricontrollare lo stato della connessione con il comando

**$iwconfig ethx** [invio]

se tutto è andato a buon fine, si sarà associati con successo all'access point. Tutti i dispositivi della rete saranno ora raggiungibili.

### 4.5 Altri tipi di attacchi

Il particolare tipo di struttura di una rete wireless, si presta alla possibilità di agire con diversi tipi di attacchi. Utilizzando ad esempio **FakeAP**, è tranquillamente possibile fingersi un access point ma bisogna tener presente che servirà una scheda che utilizza un trasmettitore avente lo stadio finale rf con potenza maggiore di un ap ed un'antenna di tipo direttivo è consigliata. Questo tipo di attacco prevede di posizionarsi tra l'ap reale ed il client. I computer che si connetteranno “all'esca” di FakeAP sveleranno la loro chiave che si potrà riutilizzare in seguito. In alternativa è possibile disassociare i client connessi utilizzando l'ottimo **Void11**, causando un DoS sul network e rallentando a tutti il link. Questa tipologia di attacco è difficilmente arginabile e gli amministratori del network dovrebbero monitorare costantemente la rete per verificare la presenza di falsi access point.

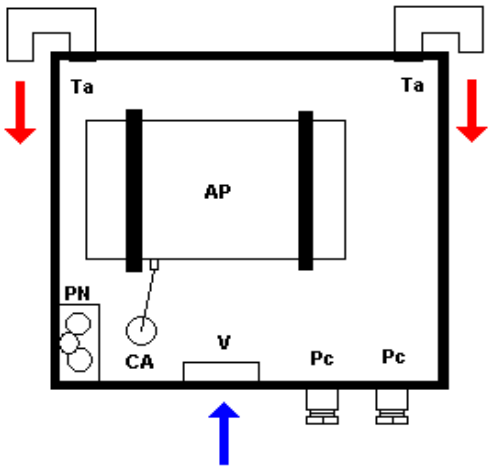
# Installazioni in esterno

## 5.1 Generalità

In commercio esistono dispositivi creati appositamente per l'uso esterno ma il costo risulta ai più proibitivo o eccessivamente oneroso per l'uso amatoriale. Anche in questo caso, l'arte dell'hacking e del modding ha portato alla realizzazione di soluzioni alternative che bene si adattano allo scopo.
Può sembrare ridicolo ma il passaggio dall'uso interno a quello esterno non è cosa di poco conto. Le variabili in gioco cambiano di molto e se nell'uso interno, umidità, variazione della temperatura di funzionamento, polvere ed insetti non sono un problema, all'esterno assumono un fattore decisamente rilevante.
La scatola dove l'apparato sarà alloggiato deve possedere caratteristiche che la rendano stagna e contemporaneamente sufficientemente areata in modo da evitare pericolosi ristagni d'aria calda. Prove pratiche hanno dimostrato che il surriscaldamento dovuto all'esposizione solare della scatola provocano instabilità e blocchi dell'apparato, mentre l'umidità provoca con il passare del tempo corrosioni che danneggiano irrimediabilmente i componenti elettronici.

## 5.2 Installazione tipica

Esistono diverse applicazioni che permettono di realizzare quanto sopra e la più diffusa è quella che impiega tubi ricurvi a manico d'ombrello, secondo l'esempio riportato di seguito:



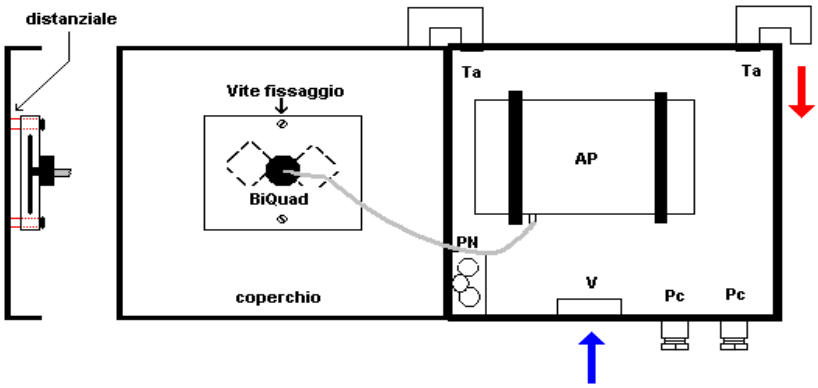

La scatola impiegata spesso è del tipo GW44-208 della Gewiss, piccola a sufficienza per contenere un access point (AP), una ventola (V) per forzare la circolazione dell'aria (non è indispensabile ma in alcuni casi è fortemente consigliata), alcuni pressa-cavi (Pc), un connettore N (indicato con CA) femmina da pannello per esterni, i due tubi ad ombrello (Ta) montati in modo che l'acqua non entri, ed uno scatolino con molti fori, contenente alcune palline di naftalina (PN).
Sembrerebbe assurdo ma per prevenire che insetti s'annidino all'interno, la naftalina è un vero toccasana e si suggerisce inoltre d'inserire della retina a maglia fine nell'uscita dei tubi ad ombrello.

In questo tipo di realizzazione s'è usata una ventola termoregolata da 4x4 centimetri alloggiata nel punto più basso dove in precedenza sono stati praticati molti fori, favorendone così l'aspirazione d'aria fresca proveniente dall'esterno. L'apparato è fissato all'interno della scatola mediante fascette di plastica, facilmente sostituibili in caso di upgrade o manutenzione.
Realizzazioni pratiche hanno dimostrato che se l'alimentatore viene inserito all'interno della scatola, la formazione di calore aumenta di molto. Onde evitare problemi, è bene realizzare i tubi ad ombrello con diametro interno da almeno 20mm.
Nelle installazioni tipiche, la scatola, è montata nelle immediate vicinanze dell'antenna, in modo d'utilizzare un cavo RF il più corto possibile, limitando in questo modo le perdite dovute ad eccessiva lunghezza.

## 5.3 Installazioni particolari

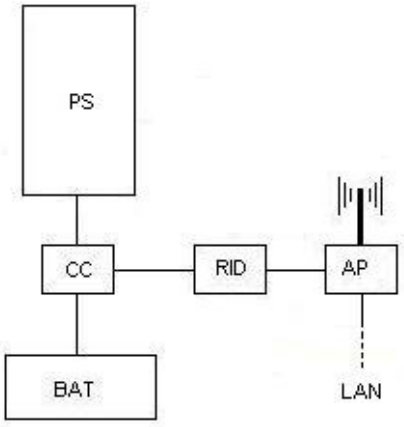
La passione e la ricerca di coloro che vengono definiti "smanettoni" porta in alcuni casi a realizzazioni particolarmente fantasiose che permettono di mimetizzare visivamente una rete o estendendola mediante ponti radio isolati.
Sebbene per alcune di esse esiste una controparte commerciale, gli appassionati preferiscono costruire da sé i vari componenti necessari, diminuendo il costo di realizzazione impiegando materiali alternativi, garantendone elevata personalizzazione e soddisfazione personale.
Quando ci si cimenta in tali realizzazioni, particolare attenzione va prestata al materiale usato per la scatola stagna. Molte volte accade infatti d'aver realizzato un'opera d'arte ma il risultato finale è che la rete wireless non funziona e non si capisce bene dove risiede il problema. Prove pratiche hanno dimostrato che alcune scatole utilizzano materiali "schermanti" per la radiofrequenza, sebbene sembrano realizzate di sola plastica. Una rapida verifica consiste nel mettere la scatola appena acquistata nel forno a microonde per qualche secondo... se la scatola scalda, significa che non è adatta all'uso che intendiamo farne se, invece, resta fredda, significa che è composta di sola plastica.

- **<u>Scatola stagna con antenna incorporata</u>:** è tipicamente la realizzazione che permette il massimo mimetismo (in effetti si nota solo una strana scatola montata su un palo) e non si discosta molto dall'installazione tipica in esterno. La differenza principale consiste nell'applicare sul lato interno del coperchio della scatola stagna di una antenna del tipo BiQuad. Lo schema di principio di montaggio è simile a quanto riportato in figura:



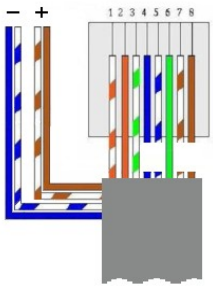
- **<u>Installazione in ponti radio isolati</u>:** è la realizzazione più originale e costosa ed impiega fonti d'alimentazione alternative come i pannelli fotovoltaici. In questo tipo di realizzazione, il risparmio energetico assume carattere di vitale importanza poiché l'autonomia di servizio non è infinita ma ben definita e limitata. In casi particolari, ai pannelli fotovoltaici si aggiunge un generatore eolico che permette un'autonomia di funzionamento in condizioni "critiche" ben superiore. Simili realizzazioni richiedono la presenza di circuiti elettronici particolari per la gestione della carica della/e batteria/e tampone e gestione dei dispositivi presenti nel ponte. Da quanto qui esposto, si capisce che pochi si affidano a questo tipo d'impianto e la causa è da ricercare nella difficoltà del dimensionamento delle singole parti che richiedono competenza tecnica. In rete si trovano comunque progetti validi allo scopo, ed un esempio di installazione è visibile nella foto a seguire.

Il principio di funzionamento dell'impianto ad energia solare è riassumibile nel seguente schema a blocchi, da cui si evince il livello di complessità costruttivo:




Per mezzo del circuito di carica (CC), l'energia prodotta dal pannello solare PS (o dai pannelli solari, in questo caso servirebbe un circuito particolare di accoppiamento) viene fornita alla batteria che in questo modo viene caricata. L'alimentazione dell'apparato è generalmente prelevata dal circuito di carica che deve altresì gestire i carichi, evitando di sottoporre la batteria a condizioni di funzionamento dannose come lo sono l'eccessiva carica o scarica. Un riduttore di tensione (RID) si occupa d'adattare la tensione fornita dalla batteria a quella richiesta dall'apparato. Di sovente vengono impiegati riduttori di tipo switching che garantiscono elevata efficienza e rendimento con poco calore prodotto.

- **<u>Installazione con singolo cavo per dati e alimentazione</u>:** è il tipo d'installazione più gettonato ed utilizzato quando non si vuole stendere un cavo aggiuntivo per l'alimentazione dell'apparato e si vuole limitare l'uso di pressa-cavi nella scatola. Questa tecnica prende il nome di **PoE (Power Over Ethernet)**. La sua realizzazione è possibile grazie al cavo utilizzato per lo standard ethernet che fino a 802.3u (fast ethernet, 100Mbit/s) non usa tutte le coppie presenti ed è così possibile destinare quelle libere ad altro scopo.




Non sempre il PoE risulta essere la soluzione migliore a causa dei suoi limiti:

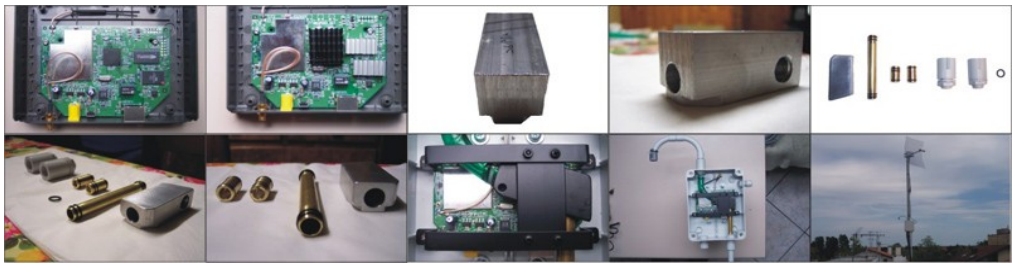
- la piccola sezione dei conduttori presenti impone dei limiti sulla massima corrente circolante;
- la caduta di tensione che si viene a creare a causa del precedente fattore limitante e la lunghezza del cavo, sottopone l'apparato a stress da sotto-alimentazione, rendendolo instabile. Questo problema aumenta con l'aumentare della lunghezza della linea ethernet.

Esiste tuttavia il modo per ovviare a questi fattori limitanti, ricorrendo all'uso di tensione d'alimentazione, a monte del PoE, più alta di quanto necessario ed usare un circuito di riduzione a valle, interno alla scatola, nei pressi dell'apparato. Questa tecnica è spesso utilizzata ma, oltre a concorrere nell'aumento del costo di realizzazione, introduce, a causa del riduttore di tensione, una fonte di calore all'interno della scatola che può essere notevolmente ridotto grazie all'uso di riduttori switching. Il sito http://www.gweep.net/~sfoskett/tech/poecalc.html fornisce uno script per il calcolo della tensione da applicare in ingresso del PoE e la dissipazione della linea; prestare comunque attenzione perché i risultati offerti seguono lo standard americano.

- **<u>Installazioni in scatola perfettamente stagna:</u>** è il tipo d'installazione utilizzata in quei luoghi dove l'aria è addizionata di sostanze corrosive. Alcune prove pratiche hanno dimostrato che l'esposizione all'aria ricca di salsedine tipica delle zone rivierasche, provoca malfunzionamenti dovuti alla corrosione delle piste di rame dei circuiti stampati degli apparati. In questo caso, sebbene sia consigliato l'uso di dispositivi nati per esterno, è ancora possibile l'utilizzo di apparati comuni, affidandosi all'arte del modding estremo. La linea di principio di tale realizzazione prevede l'apertura dell'apparato ed il montaggio sui chip che generano calore, di particolari dissipatori cilindrici con interno cavo, costruiti su misura, al cui interno viene fatta circolare l'aria prelevata dall'esterno della scatola stagna tramite una serie di tubazioni che costituisce un vero e proprio sistema a pompa di calore.

Riprendendo il discorso sulla descrizione della soluzione artigianale studiata e realizzata da **Absolute**, membro del forum di Nabuk.org, nel suo ponte utilizzante apparati D-Link DWL2100ap in scatola perfettamente stagna, egli dice: *"Per raffreddare questo AP, un normale dissipatore passivo o attivo che fosse, non avrebbe risolto il problema del surriscaldamento complessivo della scatola in quanto sigillata. L'interno avrebbe semplicemente impiegato più tempo a raggiungere una temperatura critica, creando instabilità dell'apparato... il sistema chiuso avrebbe prima o poi raggiunto*

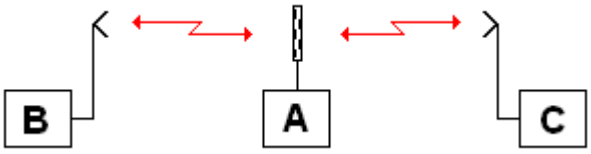
*approssimativamente la temperatura del microprocessore, con o senza aletta, perché non poteva essere raffreddato da aria "fresca" proveniente dall'esterno. Si è perciò impiegata una soluzione dedicata, utilizzando un sistema a pompa di calore, con ventilazione a camino e dissipatore appositamente costruito. Ovviamente fattore irrinunciabile era il fatto che comunque, l'interno della scatola fosse sigillato dall'esterno, al fine di evitare pericolosi effetti condensa ed il ristagno della salsedine..."*
Nella figura seguente, è possibile vedere il numero dei componenti utilizzati ed il risultato finale:



Dall'angolo in alto a sinistra si vede in sequenza: l'apparato originale aperto, una modifica impiegante dissipatori passivi e nelle restanti immagini, i dettagli relativi alla realizzazione in oggetto il cui componente principale non è altro che un cilindro in alluminio con foro passante. In questo modo l'aria si riscalda passando attraverso il dissipatore e, tendendo a "salire", viene espulsa attraverso la tubazione esterna montata nella parte superiore della scatola, richiamando contemporaneamente aria fresca dalla parte bassa.

- **<u>Installazioni di più reti:</u>** non di rado accade di dover creare una rete wireless che unisca più reti lan, la cui posizione è opposta ad un punto centrale, dove risiede il nodo principale della rete stessa. Un tipico caso, è quello di due reti laterali geograficamente poste a 180° rispetto ad una centrale, particolarità che viene aggravata dalla distanza che separa i vari apparati. Questa condizione rende il link piuttosto impegnativo, richiedendo ulteriori studi poiché la soluzione può avvenire in modi diversi, alcune volte fantasiosi, o come esercizio di stile...

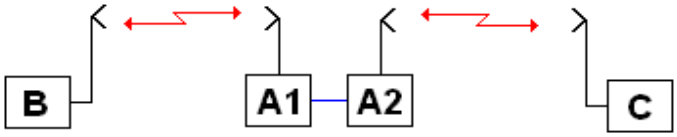
  **Soluzione 1: apparato centrale con antenna slotted waveguide con apertura di 360°:** è la soluzione classica che monta nel punto centrale (A) una antenna omnidirezionale ad alto guadagno, mentre gli apparati laterali (B e C) montano antenne di tipo direttivo.




Questa soluzione offre l'indubbio vantaggio d'avere grande copertura geografica del segnale ma, se gli apparati laterali coinvolti sono solo due, posti a 180° rispetto ad A, con lunghezza del link medio-lunga, si è costretti ad utilizzare una slotted waveguide di dimensioni ragguardevoli e di parabole ad alto guadagno su B e C. Si deve altresì considerare che a causa della slotted stessa, il segnale viene irradiato in ogni direzione, sottoponendo il link a probabili e continui attacchi oltre che interferire con la regola del "buon vicinato": segnale a 360° potrebbe disturbare altre reti, magari anche importanti come ospedali e aeroporti, rendendo di fatto la rete molto più visibile, inoltre le antenne oltre a spedire segnale a 360°, lo ricevono anche da 360°, insieme ai vari disturbi ambientali... Nella sua impostazione

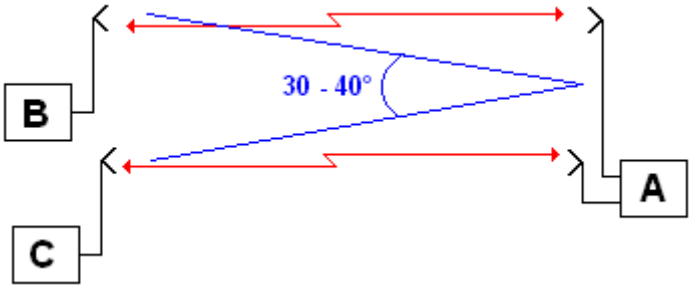
tipica, gli apparati B e C saranno impostati come BRIDGE verso A che, settato in MULTIPOINT, permetterà alle lan collegate agli apparati stessi (lan A, lan B e lan C) di colloquiare fra loro. ***Non tutti gli apparati permettono questo tipo di configurazione ed il risultato ottenuto sarà che la rete "A" comunicherà bidirezionalmente con "B" e "C" ma, "B" e "C" non potranno comunicare tra loro passando per "A".***

**Soluzione 2: uso di 2 apparati centrali con antenne direttive:** è la soluzione più dispendiosa poiché nel punto centrale saranno posti 2 apparati (A1 e A2) collegati insieme dalla LAN e dotati di propria antenna direttiva. Garantisce maggiore efficienza e flessibilità alla rete, grande distanza raggiunta dal link wireless e maggiore sicurezza poiché, il segnale è irradiato in sole due direzione e, grazie alle direttive, con angolo d'apertura ridotto.




Nella sua configurazione tipica, gli apparati saranno impostati come due singoli BRIDGE, in modo tale che B sarà in bridge con A1 e C con A2.

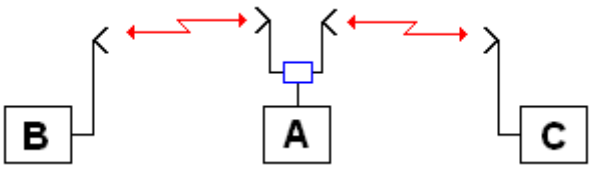
**Soluzione 3: apparato centrale con due antenne direttive e diversity attivo:** è il caso in cui le reti reti da collegare (B e C) sono poste con un'apertura angolare di 30 – 40° rispetto ad una terza (A). Sfruttando l'elevata frequenza di funzionamento del diversity, è possibile unire le reti applicando all'apparato centrale (opportunamente modificato, se necessario) due antenne di tipo direttivo che, puntano ognuna un apparato remoto. Si hanno comunque notizie riguardo la possibilità di stabilire un link con apparati remoti posti a 180° rispetto al centrale, solo nel caso in cui si ha limitato traffico generato sulla connessione wireless.




La configurazione tipica degli apparati prevede B e C in BRIDGE con A in MULTIPOINT. Da prove pratiche, con apparati D-Link DWL2100ap, è emerso che utilizzando questo schema, si ha un sensibile decadimento delle prestazioni, in presenza di trasferimenti multipli tra apparati.

**Soluzione 4: apparato centrale con due antenne direttive e splitter d'antenna:** l'utilizzo di uno splitter d'antenna, chiamato anche "power divider-combiner", permette il collegamento di due antenne ad una sola connessione d'antenna. Questa soluzione presenta il difetto d'introdurre una attenuazione di trasmissione e ricezione di poco inferiore ai 3 dB e

perciò può ritenersi valida per link di lunghezza media. Il costo piuttosto alto di questo dispositivo, ha spinto gli appassionati alla realizzazione casalinga che, rispetto alla versione commerciale, introduce una perdita di poco superiore ai 3 dB, quando fatto a regola d'arte. Una rete wireless utilizzante lo splitter per l'apparato centrale (A), alla quale sono collegate due antenne direttive, ed apparati laterali posizionati a 180°, provvisti anch'essi di antenne direttive, può essere così rappresentata secondo il seguente schema:




La configurazione tipica, prevede che l'apparato A sia settato per il funzionamento in modalità MULTIPOINT e che gli apparati laterali B e C settati in BRIDGE con A. Nelle seguenti figure in tabella, è possibile vedere l'immagine di uno splitter commerciale con diagramma di connessione ed installazione tipica, una realizzazione "home-made" dello stesso fatta dall'utente **Midori** (anch'egli membro del forum di Nabuk.org), che dovrà poi essere chiuso in un contenitore metallico. Prove pratiche hanno dimostrato che saldando direttamente i connettori allo stampato, si riducono le perdite d'inserzione ma si ricorda che 3 dB equivalgono a metà intensità del segnale. Dall'immagine dello stampato si deduce che ad ogni antenna giungerà metà del segnale perciò, per compensare le perdite, è indispensabile l'uso di antenne con guadagno superiore. L'utilizzo dello splitter è da considerarsi valido quando la distanza del link non obbliga all'uso della massima potenza.

- **Installazioni con antenna originale migliorata:** essenzialmente consta d'un riflettore applicato dietro l'apparato nel cui fuoco è posizionato l'antennino originale. Questo tipo di realizzazione, se fatta a regola d'arte, permette d'incrementare il guadagno d'antenna di 8dB con i seguenti vantaggi:

  - non richiede nessun connettore d'antenna aggiuntivo;
  - nessuna modifica all'apparato;
  - nessun problema d'elevato livello di onde stazionarie (SWR);
  - costruzione estremamente semplice con bassa probabilità di errori;
  - riduzione delle interferenze.

  Di riflettori ne sono stati realizzati di forme al limite della fantasia, impiegando materiali diversi. Nelle seguenti foto è possibile vedere il progetto base di www.freeantennas.com sulla quale si basano tutte le evoluzioni.

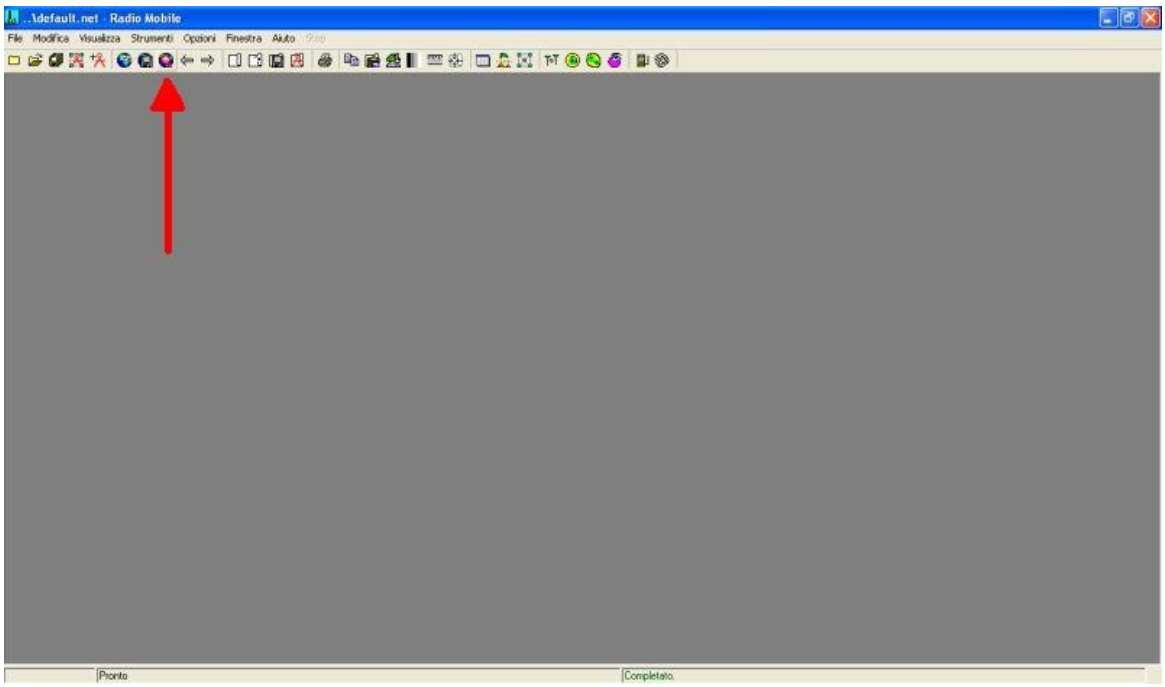

LINKSYS

## 5.4 Progettazione avanzata utilizzando RMW

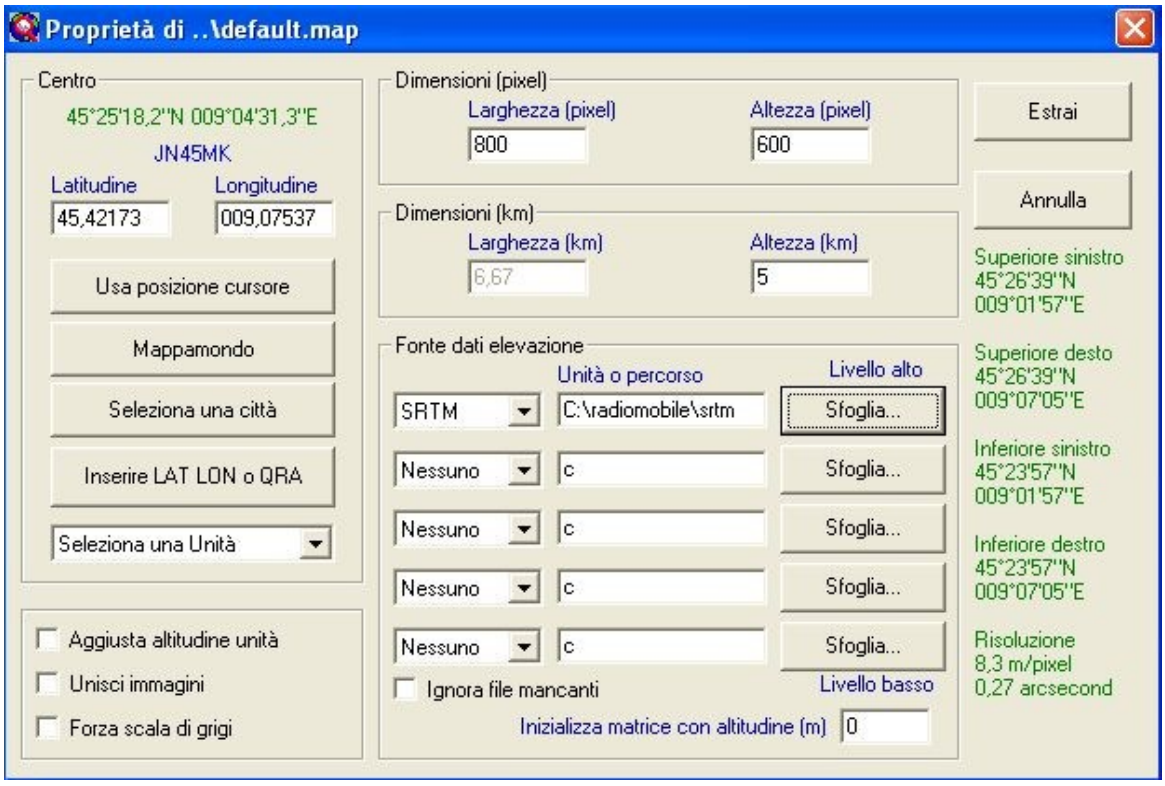
Esistono diversi modi per progettare un link wireless esterno, ma tutti si basano sul calcolo matematico algebrico delle potenze in gioco, le cui formule utili sono rese disponibili in questa guida. Per una progettazione avanzata, esiste un particolare software che prevede il comportamento del link stesso attraverso un ambiente simulato, restituendo visivamente il risultato sia in modalità 2D che 3D.
Questo software prende il nome di *Radiomobile for Windows,* sviluppato da Roger Coudé (VE2DBE), rilasciato come freeware per uso radioamatoriale e scopo umanitario, liberamente scaricabile da www.cplus.org/rmw/english1.html oppure dal mirrior e sito dell'autore stesso www.ve2dbe.com/english1.html. Procedere al download ed installare il programma, che ricordo gira sotto OS Windows, nella speranza che, prima o poi, l'autore o qualcun'altro, faccia il porting verso OS liberi come GNU/Linux, senza usare WINE o derivati, seguendo semplicissimi passi:

- per revisioni "vecchie" di Windows, occorre installare prima le runtime di VB6;
- il software è multilinguaggio, perciò occorre spacchettare prima rmwcore.zip nella cartella voluta, ad esempio C:\radiomobile;
- scaricare il pacchetto rmwupdate.zip e scompattarlo sempre nella cartella precedente;
- scaricare il pacchetto relativo al linguaggio voluto e scompattarlo nella directory precedente;
- creare la directory necessaria al sistema per memorizzare le mappe digitali del terreno, come ad esempio C:\radiomobile\srtm.

Cosa serve per poter sfruttare al meglio le funzionalità offerte? Fondalmentali sono i dati del link, come le potenze in gioco, trasmittenti, ricevitori, antenne e cavi; trasposizione digitale del terreno dove s'intende realizzare il link; dati per sovrapporre alle mappe gli elementi topografici.
Le trasposizioni digitali del terreno, effettuate con rilevamenti laser dalla nevetta saziale Shuttle, con risoluzione 100 metri (3 arcosecondi di risoluzione), sono liberamente scaricabili dall'ftp della Nasa: ftp://e0srp01u.ecs.nasa.gov/srtm/version2/SRTM3/Eurasia/ per quanto riguarda l'Europa e l'Asia, all'interno della quale troverete molti pacchetti con estensione zip. Per sapere quale sia quello giusto, dovrete armarvi di GPS rilevando latitudine e longitudine di dove si crea il link.
Tanto per fare un esempio pratico, se attraverso il GPS si ottengono al centro del link le coordinate del tipo N 45° 42' 17,3" e E 09° 07' 53,7", si dovrà scaricare il file N45E009.hgt.zip e scompattarlo nella cartella C:\radiomobile\srtm. Siamo ora in grado di poter fornire al programma tutti i dati necessari.
Avviare il programma cliccando due volte sull'eseguibile rmwita.exe nel caso si utilizza la lingua italiana e, se preferite, creare un collegamento sul desktop, per rendere l'accesso al programma più diretto. La finestra principale di lavoro si presenterà come segue:

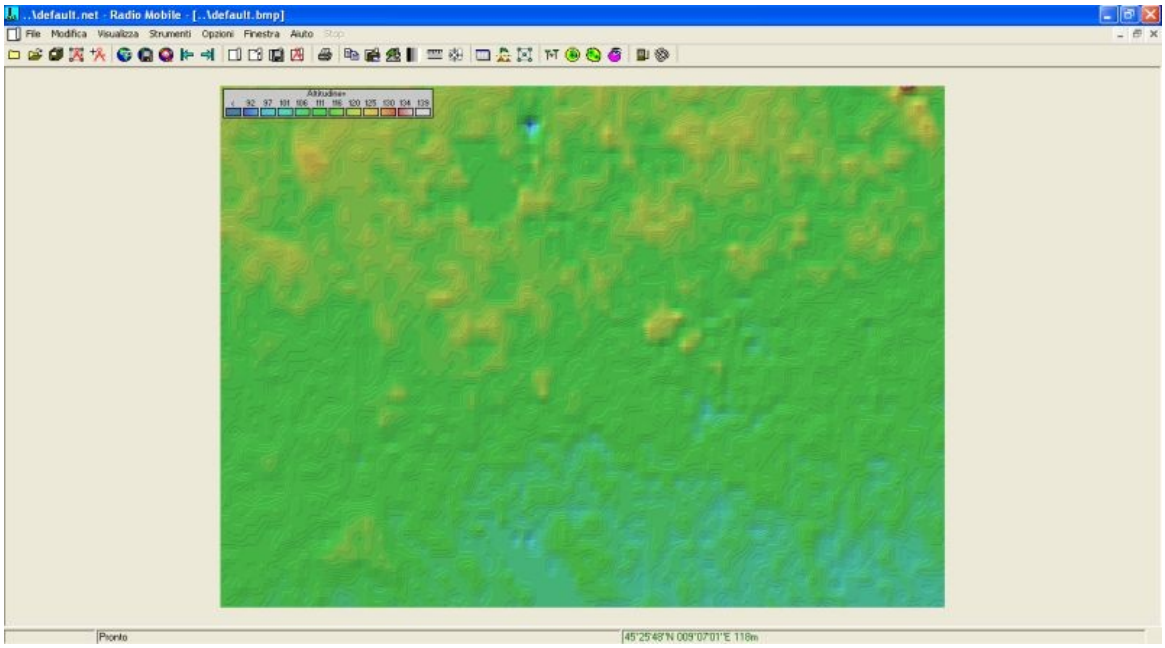



Evidenziata dalla freccia è l'icona a cui bisognerà cliccare per definire le proprietà della mappa, in modo tale da inserire i dati principali dell'ubicazione del link, la cui finestra è simile a quanto segue:

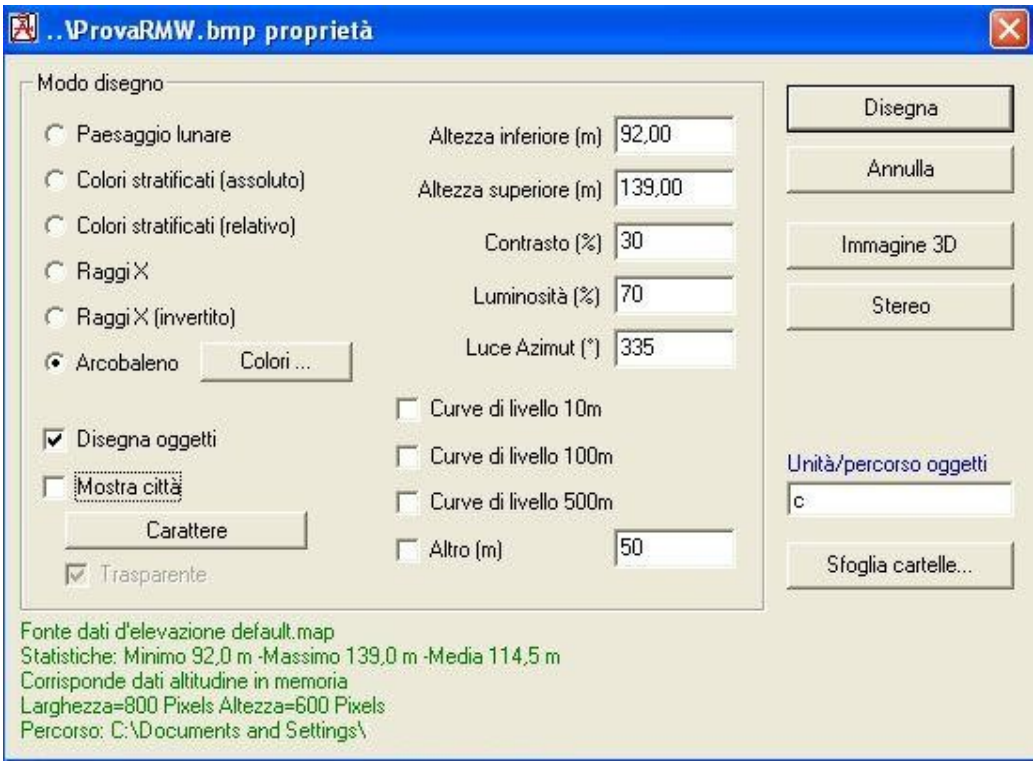



Inizieare inserendo nel lato sinistro, nei box relativi la latitudine e longitudine del luogo; al centro inserire le dimensioni dell'immagine di lavoro ed i chilometri che deve avere al massimo l'asse Y della stessa. Per quanto riguarda la "fonte dati elevazione", selezionare "srtm" ed il percorso relativo ai file estratti dal pacchetto delle mappe digitali. Premere sul pulsante "Estrai" per ottenere l'immagine di lavoro. Se per errore di coordinate GPS o per dimensioni chilometriche selezionate

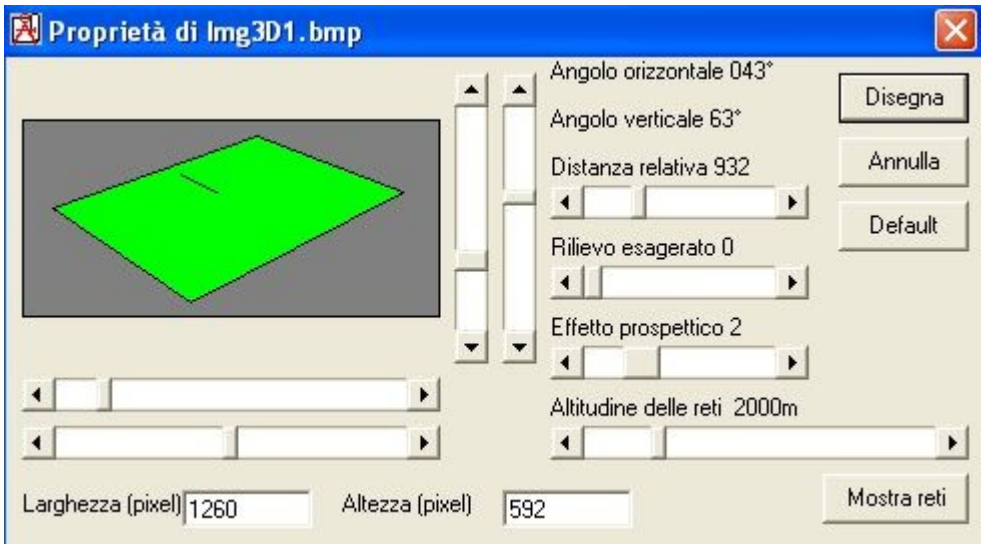
superiori a quanto visualizzabile entro il pacchetto scaricato precedentemente, il software si collegherà ad internet e scaricherà i pacchetti aggiuntivi per il completamento della mappa, che verrà automaticamente visualizzata appana finita la computazione.




A questo punto è già possibile salvare l'immagine ottenuta cliccando su *Salva immagine* dal menù *File*. Dallo stesso menù, è anche possibile aggiungere ulteriori dettagli all'immagine, cliccando su *Proprietà immagine* (oppure attraverso la sequenza di tast CTRL+I ):



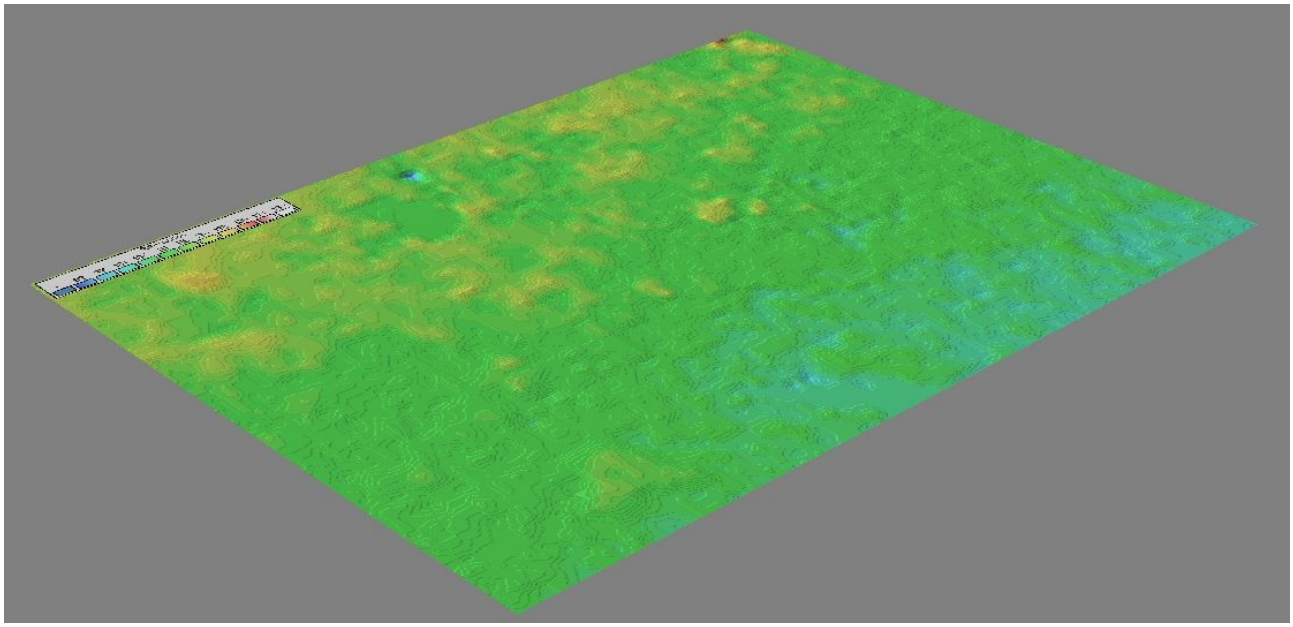
In questa finestra è possibile selezionare come si preferisce visualizzare l'immagine, dal paesaggio lunare fino al modo arcobaleno. La funzione di maggior interesse riguarda il pulsante “Immagine 3D” sulla destra, che permette una migliore visione prospettica.




Regolare i cursori secondo vostro piacimento, tenendo presente che:

- l'angolo orizzontale e verticale ruotano l'immagine dei gradi voluti;
- la distanza relativa rappresenta la distanza virtuale alla quale si guarda l'immagine;
- il rilievo esagerato crea una sorta di piedistallo sulla quale viene adagiata l'imagine;
- effetto prospettico definisce 5 livelli 3D predefiniti.

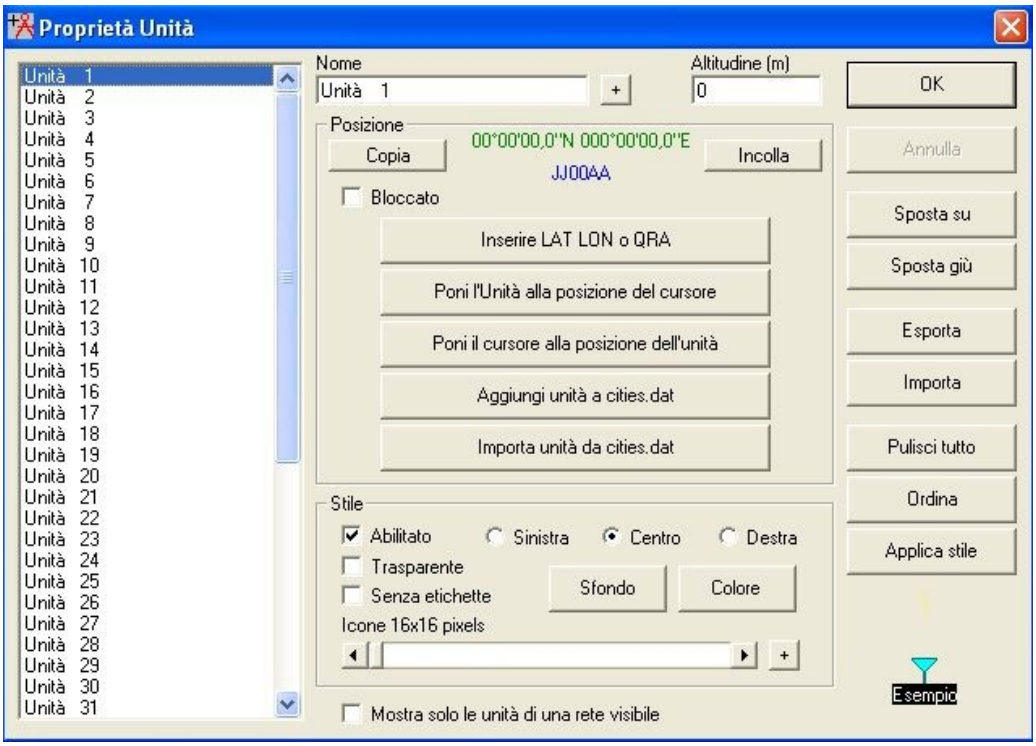
Cliccare sul punsante “Disegna” per apprezzare il risultato:



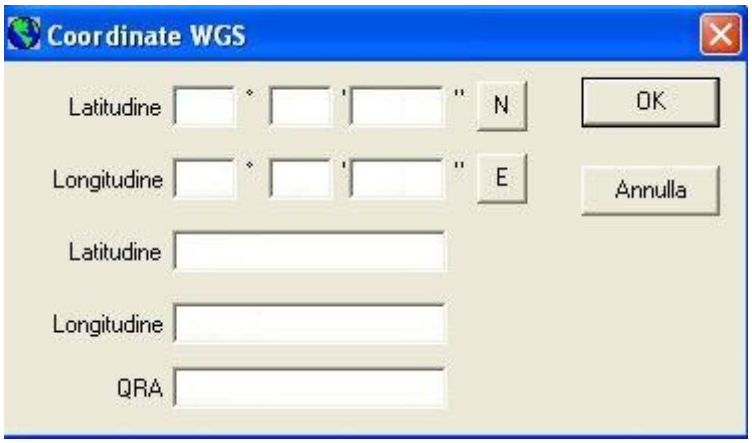
In RMW le immagini 2D e 3D saranno sempre disponibili, il passaggio da una all'altra avviene selezionandole nel menù “Finestra”.

si tenga presente che l'inserimento dei falsi colori, ovvero la modalità di visualizzazione “arcobaleno” e le curve di livello, migliorano di molto l'aspetto visivo.

A questo punto passiamo all'inserimento delle posizioni delle stazioni radio, ovvero le “Unità”. Selezionare “Proprietà unità” (CTRL+U) da menù “File” dove si aprirà una finestra simile a quanto visualizzato in figura:

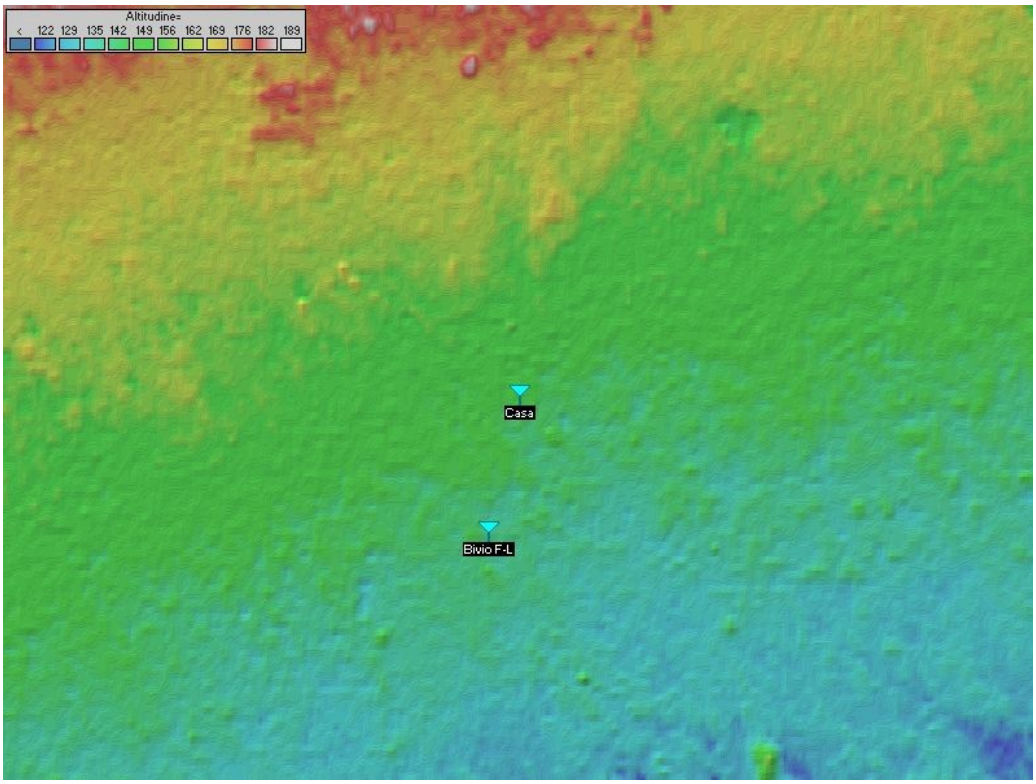



Dare un nome un po' più consono all'”Unità 1” nel box “Nome” ed assegnare l'altitudine. In basso, nel riquadro “Stile”, è possibile abilitare o meno la visualizzazione sulla mappa, nonché altri attributi estetici come la mancanza di etichette, icona a destra, al centro o sinistra della posizione GPS inserita. Proseguire poi con l'inserimento della latitudine e longitudine cliccando sul pulsante centrale “Inserire LAT LON o QRA”:

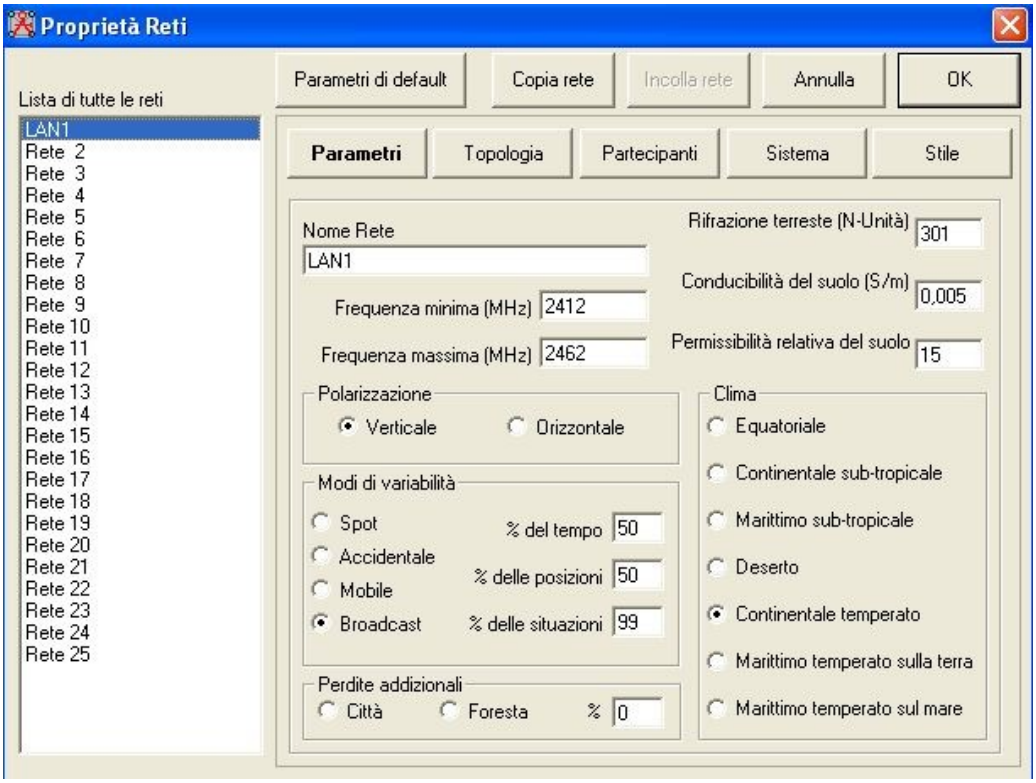



Cliccare su OK per confermare i dati inseriti. Ora sulla mappa comparirà la stazione relativa all'unità 1. Per posizionare la seconda stazione, occorre ripetere lo stesso procedimento appena

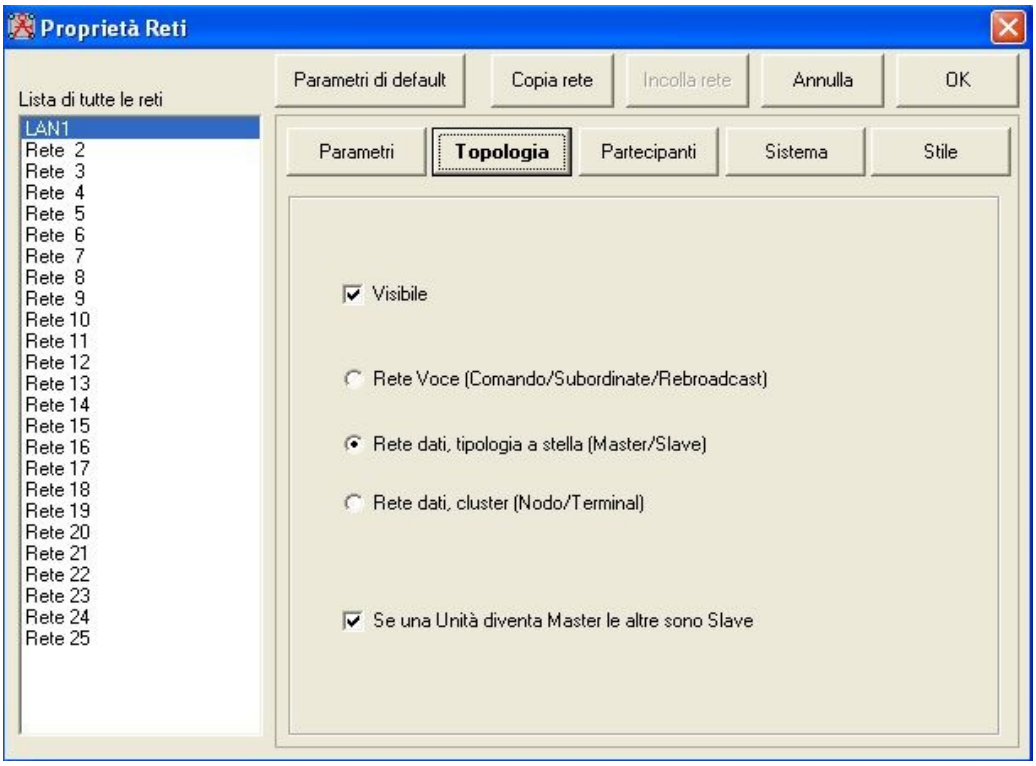
visto, andando a modificare ed inserire i valori relativi alla “Unità 2”. Se si clicca sul pulsante “Poni l'Unità alla posizione del cursore”, è possibile inserire automaticamente i dati relativi alle unità radio, semplicemente cliccando sull'immagine. Finito l'inserimento delle unità, si avrà la mappa completa delle posizioni delle due stazioni radio:



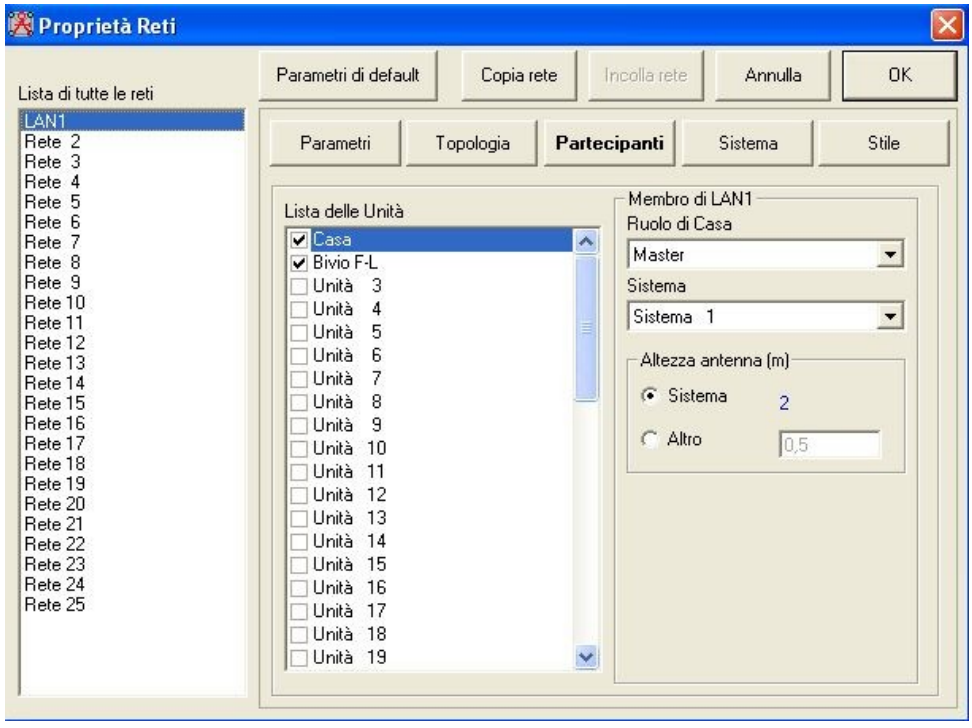

Fissate le posizioni geografiche delle unità radio, bisogna impostare le caratteristiche fisiche della rete wireless, selezionando dal menu “File” la voce “Proprietà rete” (CTRL+N):



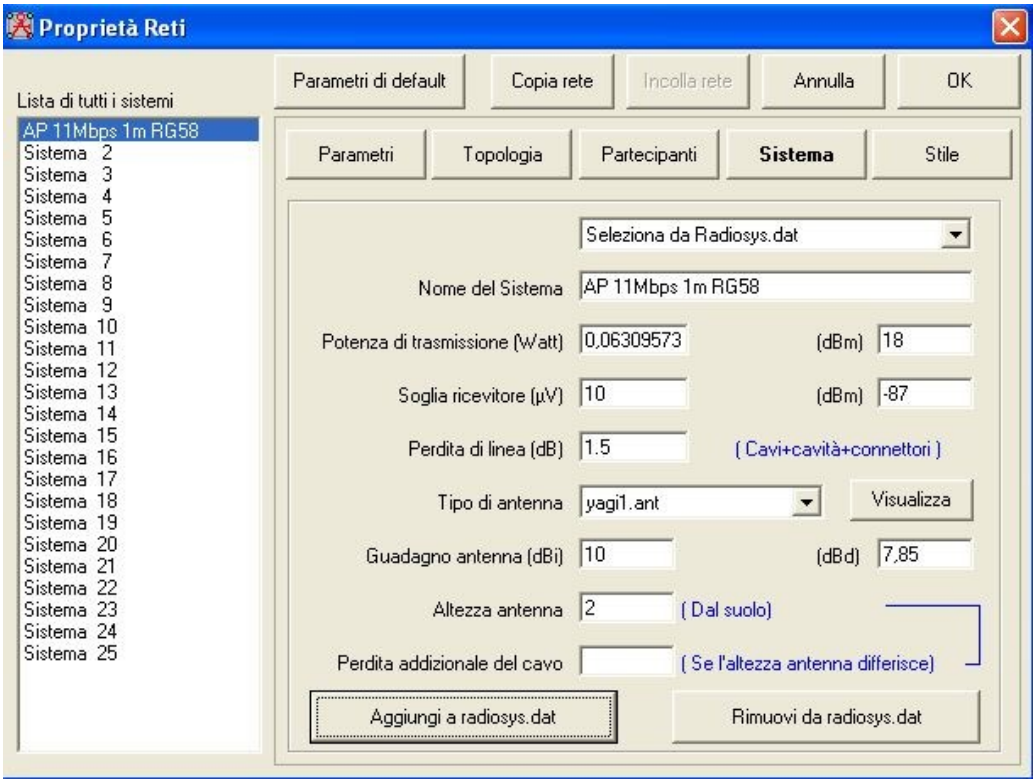
Diamo il nome alla rete, la frequenza utilizzata (per connessioni Wi-Fi è 2412 – 2462), la polarizzazione utilizzata. Nei "modi di variabilità" selezionare "Broadcast" e dare il valore 99% ed in "Clima" selezionare quello più opportuno, in linea generale, per l'Italia, "Continentale temperato" pare essere adeguato. Esistono poi ulteriori atributi per meglio definire in quali condizioni deve operare la rete, come le perdite addizionali relative ad ambienti cittadini o forestali.
Cliccare ora sul pulsante "Topologia" e definire quanto segue:




selezionare la rete dati, spuntare la visibilità e se una rete diventa aster le altre sono slave.
Passare poi a "Partecipanti" e spuntare le unità coinvolte.



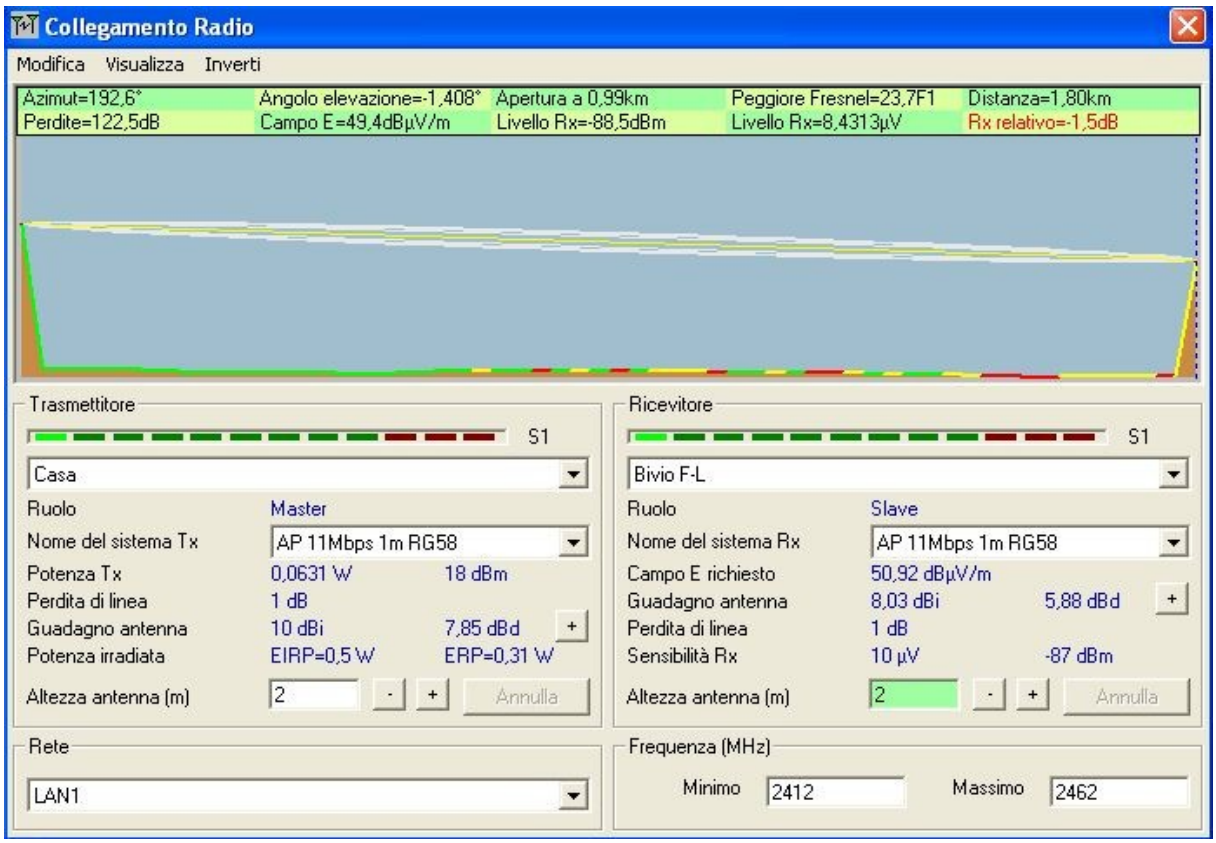
Passare ora al pulsante “Sistema” e definire l'hardware del sistema da simulare:




Inserire nelle relative caselle i dBm di trasmissione, soglia minima relativa al ricevitore dell'ap, tenendo presente che questa soglia varia a seconda della tecnologia utilizzata, le perdite in dB relative ai cavi e connettori, il tipo d'antenna e relativo guadagno. Cliccare sul pulsante OK per confermare quanto inserito.
Finalmente si sono definiti i punti del link sulla mappa, si è data loro un'appartenenza e definite le caratteristiche degli apparati impiegati. Ora nella mappa, sarà rappresentato il link.
Selezionare “Collegamento Radio” dal menù “Strumenti” per vedere se il link è fattibile.
Dalla finestra che appare, visibile nell'immagine a seguire, si ha subito la visione completa di tutti i dati inseriti, nonché i calcoli eseguiti dal programma, riportati nella parte superiore:

- l'azimuth dell'antenna;
- l'elevazione dell'antenna;
- il campo perdite in dB del link in campo libero;
- il campo perdite in µV del link in campo libero;
- il campo distanza, calcolata sulla base delle coordinate GPS inserite;
- l'angolo d'apertura del segnale irradiato dall'antenna;
- il livello in dB di segnale al ricevitore;
- il livello in µV di segnale al ricevitore;

Nella parte inferiore è invece possibile vedere tutte le caratteristiche degli apparati impiegati, il loro ruolo nella rete (master o slave), la potenza di trasmissione ed il campo elettrico richiesto per il link, la perdita di linea, la potenza irradiata (EIRP), guadagno d'antenna, sensibilità del ricevitore, ecc...




Con le nozioni esposte, è possibile stabilire a priori se un link sia realizzabile o meno. Nell'immagine sopra, è possibile altresì notare dove non il segnale è scarso od assente, esattamente dove il terreno è marcato con linea gialla o rossa.

Per acquisire maggiore padronanza di RMW, si consiglia di consultare la guida in linea del programma stesso e fare ricerche mirate in internet.

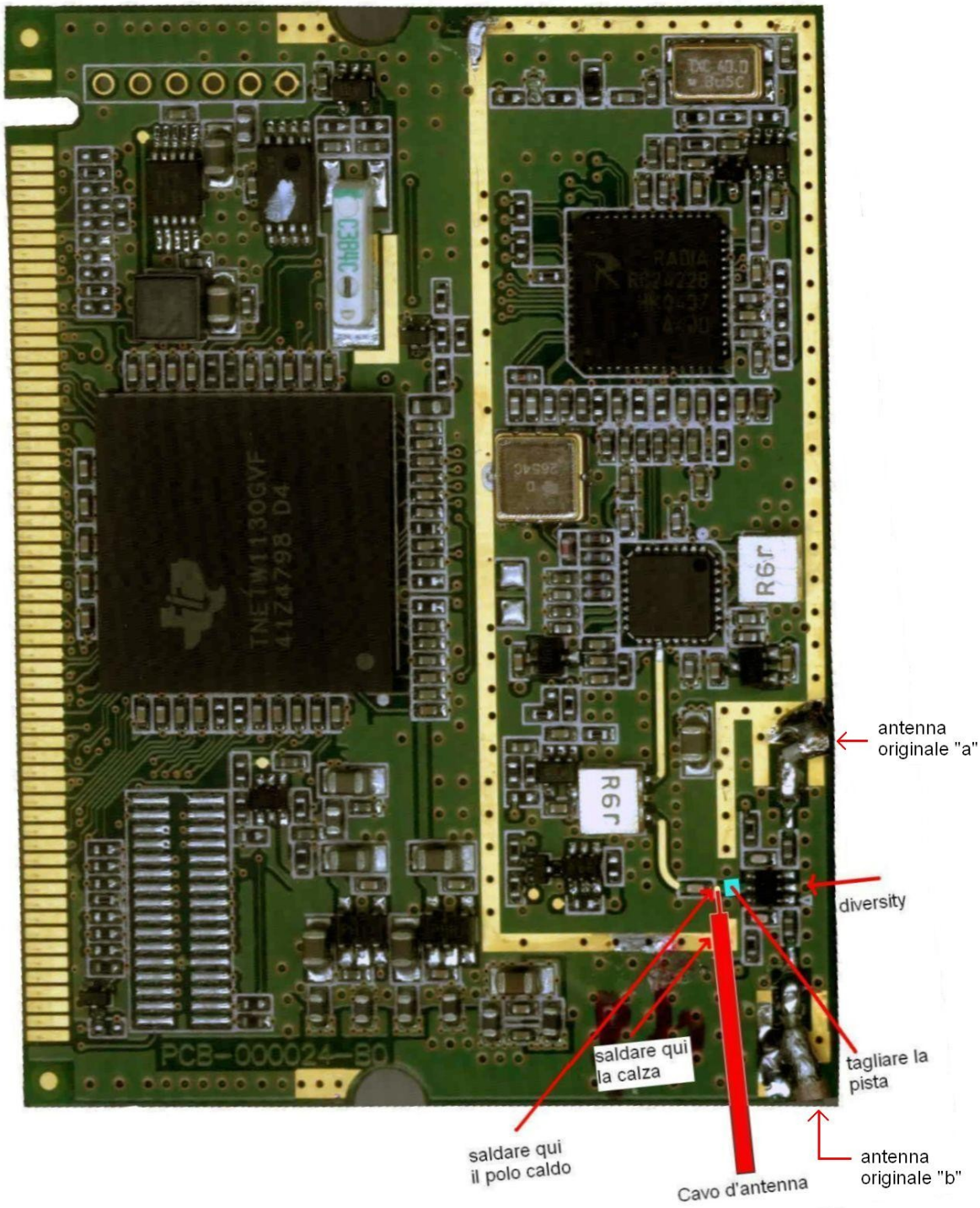
# Hacking degli apparati

## 6.1 Generalità

L'arte dell'hacking degli apparati, sia che si tratti di access point che di schede PCI o PCMCIA, s'è sviluppata parallelamente alla diffusione del Wi-Fi, permettendone un aumento delle prestazioni, funzionalità o stabilità. Esistono diverse tecniche ma, in generale, si ricorre all' hacking di tipo hardware, software oppure di tipo combinato, che fa cioè uso di entrambe le tecniche per ottenere ulteriori vantaggi in termini di flessibilità.

## 6.2 Hacking hardware

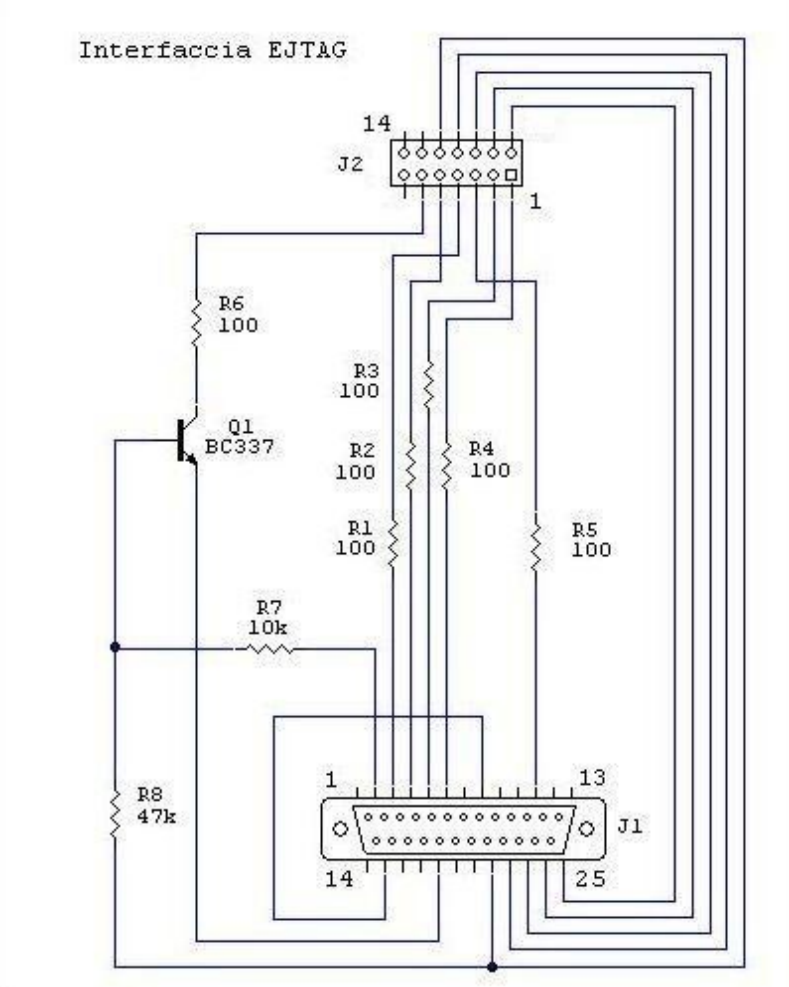
Questo tipo di modifica viene utilizzata generalmente per aumentare la potenza d'uscita in antenna di **1,5 dB** togliendo o bypassando il diversity, quel particolare chip che operando ad alta frequenza, sceglie l'antenna che ha maggior segnale tra le due sempre presenti, garantendo così il miglior rendimento in ogni condizione d'utilizzo. In applicazioni fisse come ad esempio in ponti radio, l'uso del diversity è pressoché inutile poiché all'apparato viene collegata un'antenna fissa di tipo direttivo. Sebbene sia più o meno sempre possibile operare questa modifica, la sua realizzazione richiede un minimo di conoscenza delle apparecchiature elettroniche ed un minimo di abilità nell'uso di saldatori a stagno poiché si andrà ad operare su componenti SMD (cioè a montaggio superficiale, di dimensioni ridotte) e piste del circuito stampato dove, di sovente, si ricorre all'uso di lenti d'ingrandimento. Nella pagina seguente è possibile vedere l'immagine ingrandita riguardante l' eliminazione del diversity alla scheda mini-PCI contenuta nel DWL2000AP alla quale è stata ovviamente rimossa la copertura metallica di schermatura del circuito a radiofrequenza che sarà poi adeguatamente modificata e reinstallata, permettendo l'uscita del cavo d'antenna nella nuova posizione. Questa tecnica è applicabile in modo simile a tutti i dispositivi wireless ed è possibile dissaldare i cavi d'antenna originali, indicati in figura con “antenna originale a e b”. Per una migliore riuscita della modifica, spesso si riutilizza uno degli originali, già dotati di connettore che dà all'esterno dell'apparato. Dalle esperienze fatte dai modders, le schede che creano maggiori problemi sono quelle degli adattatori Wi-Fi USB, le cui dimensioni ridotte impediscono l'inserimento di un connettore di tipo SMA direttamente sulla scocca, rendendo l'aspetto finale non propriamente “pulito” e compatto.
Nella sequenza d'immagini illustrata più avanti, è infatti possibile notare quanto sia difficile, ma non impossibile, effettuare una modifica per mettere un'antenna esterna ad un adattatore di tipo USB della D-Link modello DWL 122.


antenna
originale "a"
diversity
tagliare la
pista
saldare qui
la calza
saldare qui
il polo caldo
Cavo d'antenna
antenna
originale "b"

L’antenna originale, perfettamente visibile in questa pagina, è da rimuovere. In queste foto è presente per il solo scopo di far capire come dev’essere effettuata la modifica.

## 6.3 JTAG

JTAG è l'acronimo di **J**oint **T**est **A**ction **G**roup, un consorzio di 200 imprese produttrici di circuiti stampati ed integrati con l'intento di definire un protocollo standard per i test funzionali di apparati, sempre più complessi e difficili da controllare, rendendo impossibile il tradizionale metodo manuale. Le aziende principali che hanno aderito sono IBM, AT&T, DEC, Texas Instruments, Philips, Siemens. Questo consorzio si è costituito tra il 1985 e il 1990, dando vita a quello che poi è diventato lo standard lo IEEE1149.1, noto come standard JTAG dal nome del consorzio promotore.
Esistono diversi tipi di circuiti amatoriali per la connessione ma il più semplice è quello a seguire:

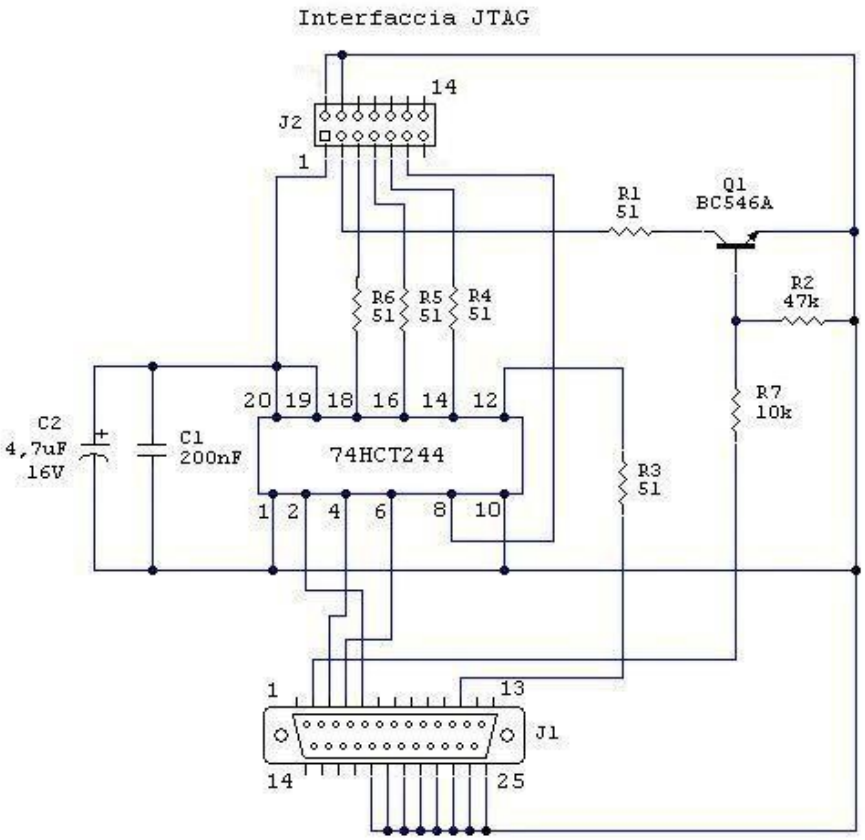



si compone di pochi componenti ed il necessario è:

- R1, R2, R3, R4, R5, R6: resistenze da 100 Ohm ¼ W;
- R7: resistenza da 10K Ohm ¼ W;
- R8: resistenza da 47K Ohm ¼ W;
- Q1: transistor NPN tipo BC 337;
- J1: connettore DB25 maschio (per l'interfaccia parallela);
- J2: connettore IDC14 femmina (in seguito si vedrà come realizzarne uno in alternativa);
- Piattina con 11 fili (recuperabile da un cavo IDE).

Questo tipo d'interfaccia sembra funzionare in modo molto efficace sul D-Link DWL2100ap.

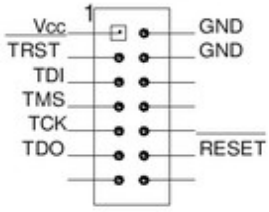
Questo secondo schema è decisamente più complesso e funziona da adattatore alle JTAG generiche, dove la presenza dell'integrato buffer 74HCT244 permette una migliore gestione:




Gli elementi che compongono questo “semplice” circuito di buffer sono:

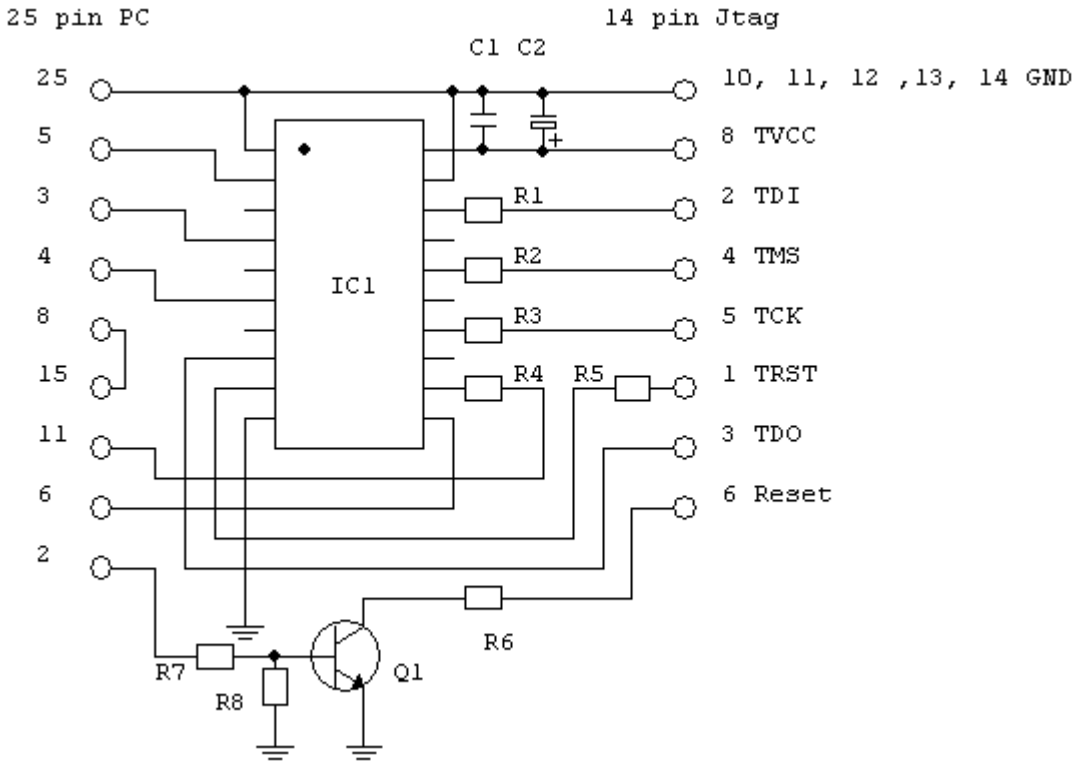
- Un integrato 74HCT244;
- C1: condensatore ceramico da 200 nF;
- C2: condensatore elettrolitico da 4,7 uF 16V;
- R1, R3, R4, R5, R6: resistenza da 51 Ohm ¼ W;
- R2: resistenza da 47K Ohm ¼ W;
- R7: resistenza da 10K Ohm;
- J1: connettore DB25 maschio (per l'interfaccia parallela);
- J2: connettore IDC14 femmina (in seguito si vedrà come realizzarne uno in alternativa);
- Piattina con 8 fili (recuperabile da un cavo IDE).

E' possibile notare che l'alimentazione dell'integrato 74HCT244 viene presa direttamente dal connettore JTAG che, avendo connessioni standardizzate, ogni PIN assume il seguente significato:



Dello schema proposto in precedenza, esiste una variante adatta per l'uso “universale” con gli apparati D-Link e chiamata “LiquidSky”. Onde evitare infruttuose ricerche nella grande rete di internet, si riportano gli schemi di realizzazione, comprensivi di circuito stampato e disposizione dei componenti richiesti. Prima di cimentarsi nella realizzazione occorre fare delle precisazioni su IC1.
In commercio esistono diverse versioni e, se quello reperito ha una tensione di alimentazione di 5 V anziché 3,3 V, occorre non realizzare la connessione con il piedino numero 8 della JTAG ed alimentare esternamente con tensione di 5 Volt. Generalmente l'integrato M74HC244B1 accetta tensioni d'alimentazione da 2 a 6 Volt; fare riferimento ai datasheet per ricavare la piedinatura di eventuali integrati equivalenti.

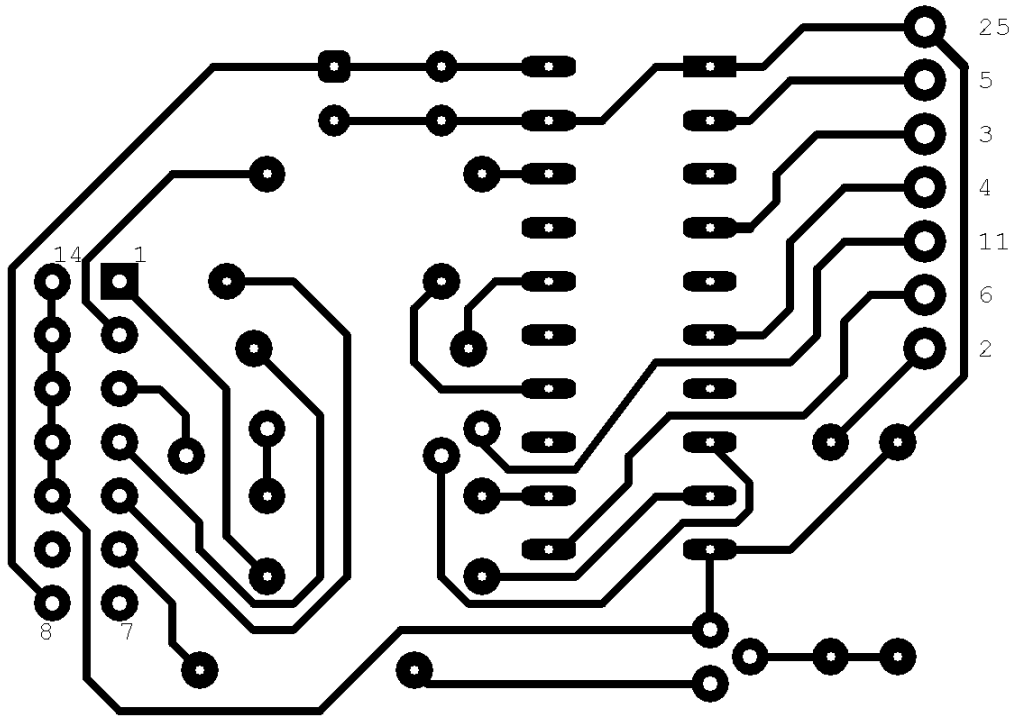
Lo schema elettrico:



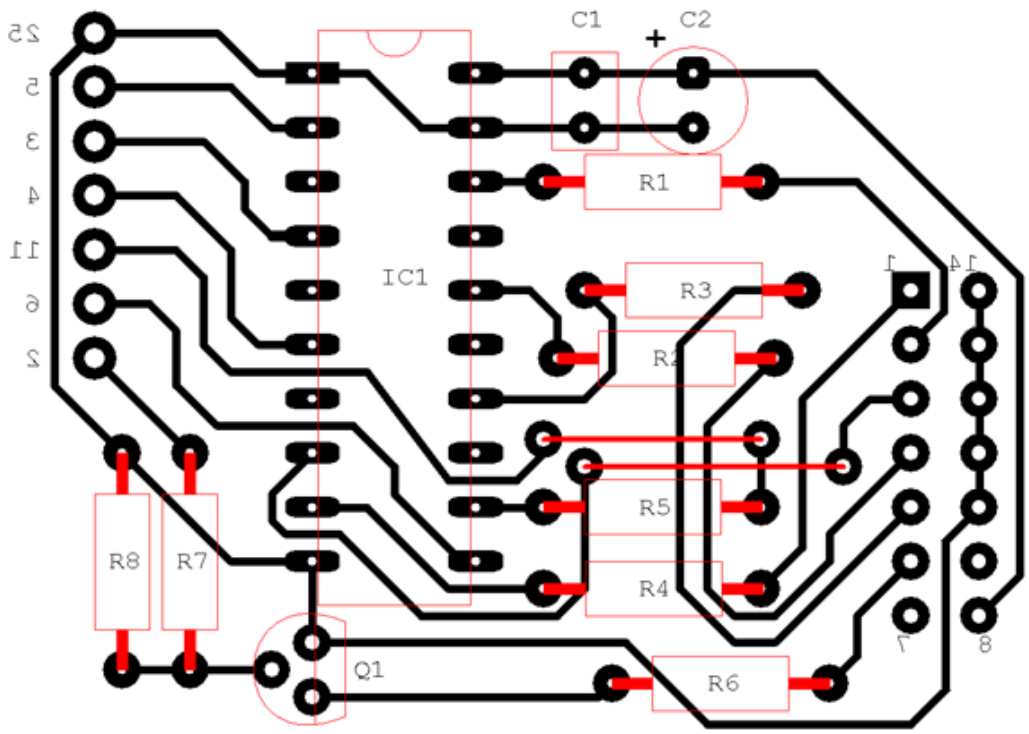

Lista dei componenti:

- IC1: M74HC244B1;
- Q1: BC337;
- R1-R6: 51 Ohm ¼ od ⅛ W (in alternativa anche 41 Ohm);
- R7: 10 Kohm;
- R8: 47 Kohm;
- C1: 200 nF;
- C2: 4,7 uF 10V.

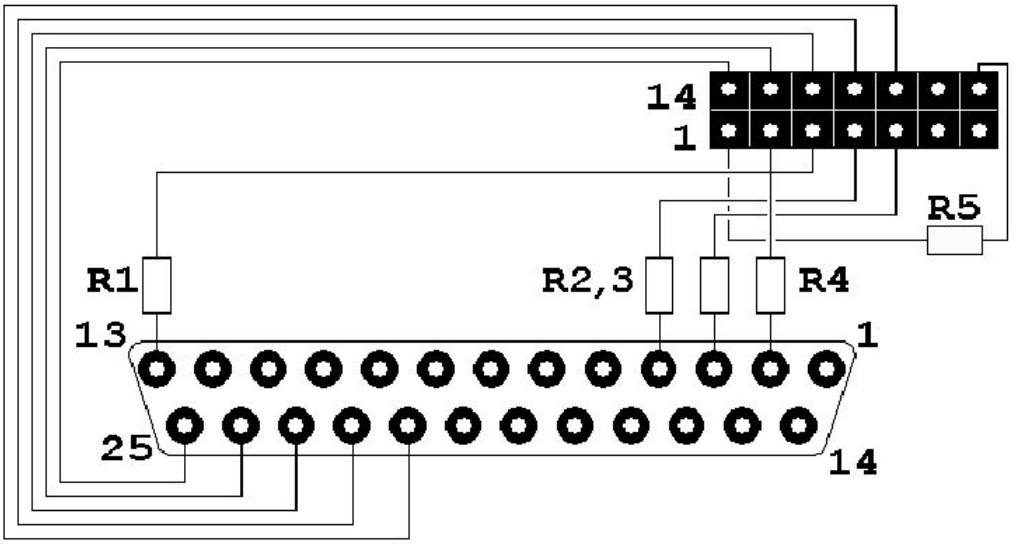
Il circuito stampato non a grandezza naturale:




La disposizione dei componenti:



L'arte del “fai da te” di coloro che non masticano propriamente elettronica ha portato alla creazione di un circuito d'interconnessione chiamato “interfaccia JTAG dei super poveri” od anche detto “Very Poor Man”, presentato anch'esso sul sito di LiquidSky e chiamato “Xilinx”:




Per la sua realizzazione occorrono soltanto pochissimi componenti, ed è estremamente consigliata a coloro che non posseggono di nessuna dimestichezza con saldatore e componenti elettronici. Il materiale occorrente è:

- R1, R3, R4, R5: resistenza da 100 Ohm ¼ W;
- Connettore DB25 maschio a saldare (per l'interfaccia parallela);
- Connettore IDC14 femmina (in seguito si vedrà come realizzarne uno in alternativa);
- Piattina con 8 fili (recuperabile da un cavo IDE).

In internet è possibile trovare una quantità di schemi veramente impressionante ed utilizzabili su apparati di diverso tipo. Analizzando attentamente gli schemi reperiti attraverso una ricerca su Google, è possibile apprezzarne le differenze, che portano ad una conclusione disarmante... Esistono, allo stato attuale, diverse versioni di connettori JTAG, le cui specifiche, sebbene standard, vengono cambiate dai produttori in base alle esigenze necessarie. Poiché le stesse non vengono solitamente corredate da adeguata documentazione, in fondo non dovrebbe essere una interfaccia utilizzata da un utente comune, conviene effettuare ricerche sulla scheda e sul tipo di processore utilizzato. Un consiglio di carattere generico è quello di utilizzare il pin TVcc per avere la tensione di riferimento e limitare la corrente circolante nella JTAG a soli 2mA. A seguire è possibile vedere il significato dei pin delle versioni più diffuse tenendo conto che le abbreviazioni utilizzate indicano:

- ➔ o = output dal processore all'interfaccia debugger;
- ➔ i = input al processore dall'interfaccia debugger;
- ➔ p = pin d'alimentazione (+V o GND);
- ➔ oc = collettore aperto comandato dall'interfaccia debugger;
- ➔ nc = non collegato o non comandato dall'interfaccia debugger;
- ➔ k = chiave, questo pin è tipicamente mancante sulla scheda madre.

1) **“COP” Motorola PowerPC 6xx, 7xx, 8xx e IBM PowerPC 6xx, 7xx. (IBM chiama questa connessione anche col nome RISCWatch):**

| | | | | | |
|---|---|---|---|---|---|
| TDO | o | 1 | 2 | i | QACK |
| TDI | i | 3 | 4 | i | TRST\ |
| HALTED | o | 5 | 6 | p | TVcc |
| TCK | i | 7 | 8 | nc | |
| TMS | i | 9 | 10 | nc | |
| SRESET | i | 11 | 12 | p | GND |
| HRESET\ | oc | 13 | 14 | nc | |
| CKSTP_OUT | o | 15 | 16 | p | GND |

2) **“COP” IBM PowerPC 4xx (IBM chiama questa connessione anche col nome RISCWatch):**

| | | | | | |
|---|---|---|---|---|---|
| TDO | o | 1 | 2 | nc | |
| TDI | i | 3 | 4 | i | TRST\ |
| HALTED | o | 5 | 6 | p | TVcc |
| TCK | i | 7 | 8 | nc | |
| TMS | i | 9 | 10 | nc | |
| HALT | i | 11 | 12 | p | GND |
| SRESET\ | oc | 13 | 14 | k | KEY |
| | nc | 15 | 16 | p | GND |

3) **“BDM” Motorola MCP8xx, MCP5xx:**

Note: prima di descrivere il significato dei pin è di vitale importanza far notare che i pin 1 e 6 mostrino perfettamente lo stato del processore dopo l'esecuzione del reset. Alcuni processori, come lo MPC8xx ecc, hanno dei pin configurabili dopo il reset della configurazione. Questi pin devono essere settati propriamente e comunque bisognerà sempre verificare che lo stato del processore sia corretto.

| | | | | | |
|---|---|---|---|---|---|
| FRZ o VFLS0 | o | 1 | 2 | o | SRESET\ |
| GND | p | 3 | 4 | i | DSCK |
| GND | p | 5 | 6 | o | FZR o VFLS1 |
| RESET\ | oc | 7 | 8 | i | DSDI |
| TVcc | p | 9 | 10 | o | DSDO |

**4) "OnCE", ovvero On Chip Emulation per Motorola DSP, M-CORE:**

| | | | | | |
|---|---|---|---|---|---|
| TDI | i | 1 | 2 | p | GND |
| TDO | o | 3 | 4 | p | GND |
| TCK | i | 5 | 6 | p | GND |
| | nc | 7 | 8 | nc | |
| RESET\ | oc | 9 | 10 | i | TMS |
| TVcc | p | 11 | 12 | p | GND |
| | nc | 13 | 14 | i | TRST\ |

5) **ARM:**

Note: ci sono due standard per processori ARM, la vecchia a 14 pin e la nuova a 20 pin.

| | | | | | |
|---|---|---|---|---|---|
| TVcc | p | 1 | 2 | p | GND |
| TRST\ | i | 3 | 4 | p | GND |
| TDI | i | 5 | 6 | p | GND |
| TMS | i | 7 | 8 | p | GND |
| TCK | i | 9 | 10 | p | GND |
| TDO | o | 11 | 12 | oc | RESET\ |
| TVcc | p | 13 | 14 | p | GND |

| | | | | | |
|---|---|---|---|---|---|
| TVcc | p | 1 | 2 | nc | |
| TRST\ | i | 3 | 4 | p | GND |
| TDI | i | 5 | 6 | p | GND |
| TMS | i | 7 | 8 | p | GND |
| TCK | i | 9 | 10 | p | GND |
| | nc | 11 | 12 | p | GND |
| TDO | o | 13 | 14 | p | GND |
| RESET\ | oc | 15 | 16 | p | GND |
| | nc | 17 | 18 | p | GND |
| | nc | 19 | 20 | p | GND |

6) **MIPS – EJTAG 2.5:**

Note: sono in uso molte connessioni per le schede MIPS. Questa, specifica solo quella utilizzata da MTI per la EJTAG 2.5.

| | | | | | |
|---|---|---|---|---|---|
| TRST\ | i | 1 | 2 | p | GND |
| TDI | i | 3 | 4 | p | GND |
| TDO | o | 5 | 6 | p | GND |
| TMS | i | 7 | 8 | p | GND |
| TCK | i | 9 | 10 | p | GND |
| RESET\ | oc | 11 | 12 | k | KEY |
| DINT | i | 13 | 14 | p | TVcc |

**7) Toshiba MIBS:**

| | | | | | |
|---|---|---|---|---|---|
| TRST\ | i | 1 | 2 | p | GND |
| TDI | i | 3 | 4 | p | GND |
| TDO | o | 5 | 6 | p | GND |
| TMS | i | 7 | 8 | p | GND |
| TCK | i | 9 | 10 | nc | |
| TVcc | p | 11 | 12 | nc | |
| RESET\ | oc | 13 | 14 | nc | |
| | nc | 15 | 16 | nc | |
| | nc | 17 | 18 | nc | |
| | nc | 19 | 20 | nc | |

**8) Philips MIPS:**

| | | | | | |
|---|---|---|---|---|---|
| TRST\ | i | 1 | 2 | p | GND |
| TDI | i | 3 | 4 | p | GND |
| TDO | o | 5 | 6 | p | GND |
| TMS | i | 7 | 8 | p | GND |
| TCK | i | 9 | 10 | p | GND |
| RESET\ | oc | 11 | 12 | p | GND |
| | nc | 13 | 14 | p | GND |
| | nc | 15 | 16 | p | GND |
| | nc | 17 | 18 | p | GND |
| | nc | 19 | 20 | p | GND |

**9) AMD – Elan SC520:**

| | | | | | |
|---|---|---|---|---|---|
| GND | p | 1 | 2 | p | TVcc |
| TCK | i | 3 | 4 | o | CMDACK |
| TMS | i | 5 | 6 | i | BR/TC |
| TDI | i | 7 | 8 | o | STOP/TX |
| TDO | o | 9 | 10 | o | TRIG/TRACE |
| SRESET\ | i | 11 | 12 | k | KEY |

**10) AMD – Athlon:**

| | | | | | |
|---|---|---|---|---|---|
| TVcc | p | 1 | 2 | i | TCK |
| | nc | 3 | 4 | i | TMS |
| | nc | 5 | 6 | nc | |
| | nc | 7 | 8 | i | TDI |
| | nc | 9 | 10 | i | TRESET\ |
| GND | p | 11 | 12 | o | TDO |
| DBREQ\ | i | 13 | 14 | o | DBRDY |
| RESET\ | p | 15 | 16 | i | PLLTEST\ |

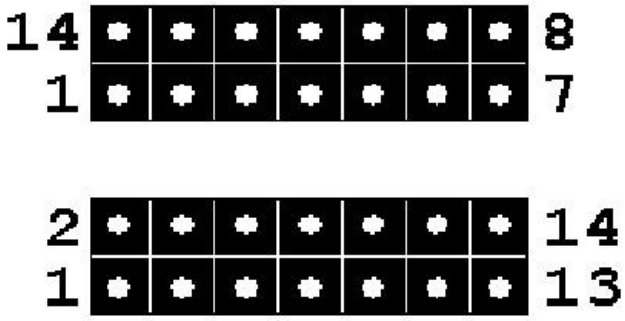
**11) AMD – Opteron:**

| | | | | | |
|---|---|---|---|---|---|
| GND | p | 1 | 2 | p | GND |
| RSVD1 | o | 3 | 4 | p | GND |
| RSVD0 | i | 5 | 6 | p | GND |
| DBREQ\ | i | 7 | 8 | p | GND |
| DBRDY | o | 9 | 10 | p | GND |
| TCK | i | 11 | 12 | p | GND |
| TMS | i | 13 | 14 | p | GND |
| TDI | i | 15 | 16 | p | GND |
| TRST\ | i | 17 | 18 | p | GND |
| TDO | o | 19 | 20 | p | GND |
| TVcc | p | 21 | 22 | p | GND |
| TVcc | p | 23 | 24 | nc | |
| KEY | k | 25 | 26 | nc | |

Il significato delle principali sigle utilizzate e riportate di fianco alla numerazione è:

| Dicitura segnale | Funzione | Direzione |
|---|---|---|
| | | |
| TAP | Test Access Port | --- |
| TCK | Test Clock | Ingresso |
| TMS | Test Mode Select | Ingresso |
| TDI | Test Data Input | Ingresso |
| TDO | Test Data Output | Uscita |
| TRST | Test Reset | Ingresso |
| SRESET\ | Soft Reset | --- |
| HRESET\ RESET\ | Hard Reset | --- |
| TVcc | Test Vcc | + Vcc |
| GND | Ground | Ground |

Malgrado siano state esposte sopra le connessioni più utilizzate per l'interfaccia JTAG, occorre precisare che esistono due diversi tipi di “numerazione” del connettore, la cui conoscenza evita l'insorgere di dubbi e/o errori di realizzazione dei cavi di connessione. Nell'esempio illustrato a seguire, è possibile notare le differenze di numerazione di una interfaccia JTAG di 14 pin:




Il significato dei pin resta comunque il medesimo.

Come ogni circuito o dispositivo connesso al computer, non serve a nulla senza il software di gestione che dipende fortemente dal tipo di processore che fa uso dell'interfaccia JTAG. E' per questo motivo che ad esempio i processori Altera necessitano del software “Free JAM” disponibile al download presso il sito di Altera stessa, ed è perfettamente compatibile con il secondo schema sopra presentato; i processori ARM9 necessitano del software JTAG-ARM9 ed anche in questo caso la seconda interfaccia presentata risulta essere perfettamente compatibile.
Il consiglio finale, prima di cimentarsi in operazioni di test e riprogrammazione, è quello di sincerarsi su quale sia il tipo di processore adottato dal vostro dispositivo, onde evitare danni che potrebbero essere fatali.

## 6.4 Hacking software

Questo tipo di modifica non è di facile attuazione e molte volte richiede conoscenze tecniche avanzate. Esistono però alcune soluzioni "già pronte" che i neofiti possono utilizzare tranquillamente.

- **Driver modificati per DWL650+ e DWL520+:** sono speciali driver rilasciati da V0r[T3X] (utente del forum di Nabuk) per le schede PCI serie DWL520+ e PCMCIA serie DWL650+ della D-Link, che utilizzano lo standard 802.11b e la sua variante fuori specifica b+, dove ha unito la stabilità di una precedente versione dei driver ufficiali con l'efficienza degli ultimi. Tutto questo lavoro ha portato un grande miglioramento nelle più varie condizioni d'utilizzo di tali schede e, quella che ne ha tratto maggiori benefici è stata la DWL650+ utilizzata molto spesso per i test dei link a media e lunga distanza. I driver moddati sono disponibili per il download nel sito dell'utente **Alnath**: http://alnath.supereva.it

- **Firmware modificati per D-Link DWL900AP+:** sono speciali firmware resi pubblici in internet da coloro che vengono definiti "smanettoni". Queste versioni moddate permettono nelle revisioni B di tali apparati, l'aumento della potenza erogata dallo stadio finale. Per le revisioni C è disponibile un particolare firmware ad opera di un gruppo d'appassionati noti come Acinonyx che permette, nella sua ultima versione, la 3.06.06, lo sblocco di tutti i 14 canali, permettendone inoltre l'uso a piena potenza. Di questo firmware però si hanno notizie riguardante il malfunzionamento della cifratura WEP se gli apparati vengono fatti funzionare in modalità bridge, ereditato dalla versione ufficiale da cui deriva. Anche questi firmware sono disponibili per il download nelle pagine di Alnath.

- **Firmware USA su apparati UE (D-Link DWL2100ap e DWL7100ap):** normalmente gli apparati venduti negli USA non hanno lo stesso firmware di quelli venduti in UE, sebbene l'hardware sia sempre lo stesso. Questo fatto è da ricercare nelle diverse normative che regolano il Wi-Fi. Tentare il passaggio da un firmware all'altro con un semplice aggiornamento non è comunque possibile ma un articolo pubblicato nel forum tedesco della D-Link, spiega come fare (un ringraziamento particolare va all'utente Bicio che dopo settimane di ricerca è riuscito a trovarlo, facendo i test di circostanza):

  **A)** Danneggiare il firmware dell'apparato facendo un aggiornamento con un firmware valido, togliendo l'alimentazione (staccare la spina) durante l'aggiornamento stesso.
  **B)** Ricollegando l'alimentazione, l'apparecchio risponde con la pagina di recovery, dove chiede il file per aggiornare correttamente la flash.
  **C)** Controllato che sia in recovery, cioè che ci sia la pagina recovery collegandosi via browser all'indirizzo IP originale, 192.168.0.50, si procede ad un reset hardware per 15 secondi.
  **D)** A reset effettuato, l'apparecchio non sarà più' sull'IP di default 192.168.0.50 (o quello impostato) ma si trova su 10.0.0.1. Cambiando IP sul computer (esempio 10.0.0.2) ci si collega alla pagina web dell'apparato su 10.0.0.1, dove sarà presente ancora la pagina di recovery, con la differenza che questa volta l'apparato ACCETTA firmware anche USA.

  Si rende noto che l'autore non si assume nessuna responsabilità riguardo ad eventuali danni o anomalie imprevedibili che possono crearsi. Il link diretto alla pagina di questa modifica è:

  http://forum.dlink.de/topic.asp?TOPIC_ID=33916&SearchTerms=7100,2100

# PC in rete: la creazione

## 7.1 Generalità

Mettere in rete due o più PC è una operazione abbastanza semplice ma, di tanto in tanto, si presentano alcuni problemi che a prima vista sembrano insormontabili. Questa affermazione appare ancora più vera quando si ha a che fare con le connessioni utilizzanti apparati di tipo wireless.
Questa sezione è dedicata a coloro che sono a digiuno di nozioni informatiche ma che vogliono unire i loro PC in una rete casalinga, condividendone le risorse disponibili. Si inizierà con la descrizione su come realizzare una semplice rete composta da due PC, collegati fra loro mediante apparati wireless di tipo Wi-Fi client, utilizzando la modalità Ad-Hoc, continuando poi con reti via via più complesse.

## 7.2 Configurazione Ad-Hoc


E' il tipo di rete più semplice da realizzare ma, a causa del basso livello di protezione di cui soffre, è bene non usarla in "pianta stabile" ma solo in condizioni saltuarie di estrema necessità. Gli "ingredienti" per la sua realizzazione sono 2 PC e 2 schede wireless Wi-Fi client (PCI, USB, PCMCIA) di qualsiasi standard (a, b, g) o multi standard, ma ovviamente la velocità del link si attesterà alla velocità dello standard più lento tra quelli disponibili (se le due schede presenti sono una in standard b e l'altra in g, il link userà lo standard b). Vediamo ora in dettaglio come approntare la configurazione dei PC :

**A)** Per una corretta installazione, è bene iniziare con l'installazione del software o dei driver a corredo della scheda e poi procedere all'inserimento o alla connessione degli apparati wireless. Sebbene questa procedura sia ricorrente, è meglio dare una veloce lettura dei manuali a corredo, onde evitare spiacevoli conseguenze. Se tutto è andato per il verso giusto, le nuove periferiche saranno riconosciute e se state utilizzando Windows come sistema operativo, noterete nella system tray una icona raffigurante un piccolo schermo con delle onde ai lati e una crocetta rossa in basso a destra.

**B)** Per impostare il primo PC, si entrerà in ***Pannello di controllo → Connessioni di rete***, richiamando le proprietà (cliccando col tasto destro del mouse) sull'icona della connessione senza fili che si è aggiunta. Cliccare sulla linguetta ***Reti senza fili*** e su ***Aggiungi***. Nel box del SSID mettete il nome della rete che volete creare (per esempio HOME_NET), come autenticazione

selezionate ***APERTA***, in crittografia dati ***WEP*** ed infine spuntate la check-box in fondo alla pagina dove c'è scritto ***RETE AD HOC***. Spostatevi sulla linguetta ***Connessione*** e spuntate la check-box ***Connessione automatica quando a distanza di rilevamento***. Cliccando su ***OK***, si dovrà attendere che la rete venga reinizializzata.

**C)** Per impostare il secondo PC, ripetere quanto descritto per il primo PC, immettendo nei campi richiesti gli stessi valori.

Se tutto è andato a buon fine, i due PC dovrebbero ora "sentirsi" ed una semplice verifica consiste nel notare un cambiamento di stato della connessione wireless mostrata nella system tray. Infatti ora il piccolo monitor non avrà più la crocetta rossa in basso a destra ma al suo posto vi saranno delle piccole onde di colore verde. Sebbene i PC si "sentano", attualmente non sono in grado di "vedersi", infatti....

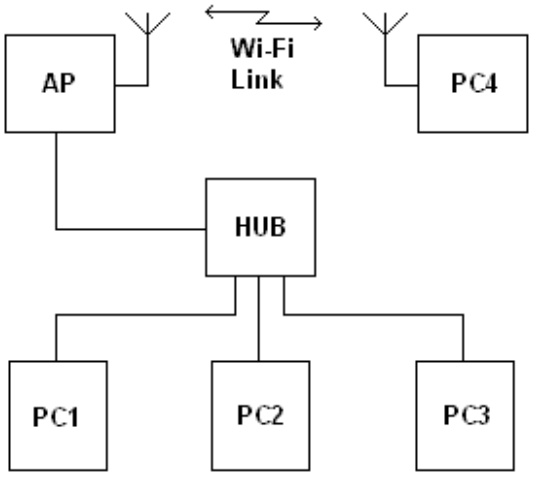
**D)** Torniamo sul primo PC ed apriamo il ***Pannello di controllo → Connessioni di rete***. Richiamiamo le proprietà della connessione senza fili e nella sezione ***Generale*** selezioniamo la voce ***Protocollo Internet TCP/IP***. Richiamandone le proprietà, assegniamo un indirizzo IP valido (per esempio 192.168.0.1) e la maschera di sottorete (in questo caso 255.255.255.0). Se questo PC è collegato fisicamente ad internet e si vuole condividerla, inseriremo nei campi relativi i DNS del nostro provider.

**E)** Sul secondo PC, ripetiamo lo stesso procedimento fatto sopra (punto D) solo che inseriremo un indirizzo IP diverso ma appartenente alla stessa classe (nel nostro caso 192.168.0.2), nel campo ***Gateway*** inseriamo l'indirizzo IP del primo PC (192.168.0.1), per il resto tutto identico.

La condivisione della connessione ad internet sarà completata quando, sul primo PC, si richiameranno le proprietà della vostra connessione da ***Pannello di controllo → Connessioni di rete → Vostra connessione***. Nella sezione ***Avanzate***, spuntate la check-box relativa a ***Consenti ad altri utenti in rete di collegarsi tramite la connessione internet di questo computer***. Si fa presente che è meglio non abilitare le funzioni delle altre check-box ora disponibili, poiché si abiliteranno gli utenti dell'altro PC al controllo completo della connessione internet.

**F)** Tutte le risorse sono ora disponibili? No, direi proprio di NO! Si crei o si scelga una cartella che non contiene dati importanti o sensibili nei due PC e condividiamola semplicemente richiamandone le proprietà (tasto destro del mouse sulla cartella stessa) e spuntare la check-box ***Condividi la cartella in rete***. Riavviate poi entrambi i pc.

### 7.3 3 PC in LAN e 1 Wi-Fi




E' la condizione tipica che si presenta in un piccolo ufficio dove più PC (in questo esempio tre: PC1, PC2, PC3) sono collegati alla rete LAN mediante un HUB o molto spesso da uno SWITCH e si da la possibilità ai portatili (in questo caso uno, PC4, ma il ragionamento non cambia se fossero di più) di collegarsi alla rete mediante connettività Wi-Fi offerta da un access point. Molto spesso i PC nella LAN funzionano in regime d'indirizzamento ad IP fissi, mentre i portatili ad IP dinamici.
Vediamo in dettaglio come fare una configurazione del genere, dando per scontato che gli adattatori ethernet ed interfacce wireless siano stati correttamente installati e riconosciuti dal sistema operativo:

**A)** Iniziamo la configurazione di PC1: entrando in ***Pannello di controllo → Connessioni di rete***, si richiamino le proprietà dell'interfaccia ethernet relative alla ***Connessione alla rete locale (LAN)***. Nella sezione ***Generale***, spuntare la casella in prossimità di ***Mostra un'icona sull'area di notifica quando connesso***, poi evidenziare ***Protocollo internet TCP/IP*** e cliccare sul pulsante ***Proprietà***. Cliccare sul pulsante radio ***Utilizza il seguente indirizzo IP*** ed inserire nel campo ***Indirizzo IP*** un indirizzo privato valido (per esempio 192.168.0.1) ed un indirizzo di sottorete (in questo caso 255.255.255.0) nel campo ***Subnet mask***. Il campo ***Gateway*** per il momento non è necessario ma verrà ripreso più avanti... Cliccare su ***OK***, attendere la reinizializzazione dell'interfaccia di rete e si noterà la comparsa nella system tray di una icona con due piccoli schermi con una croce rossa in basso a destra.

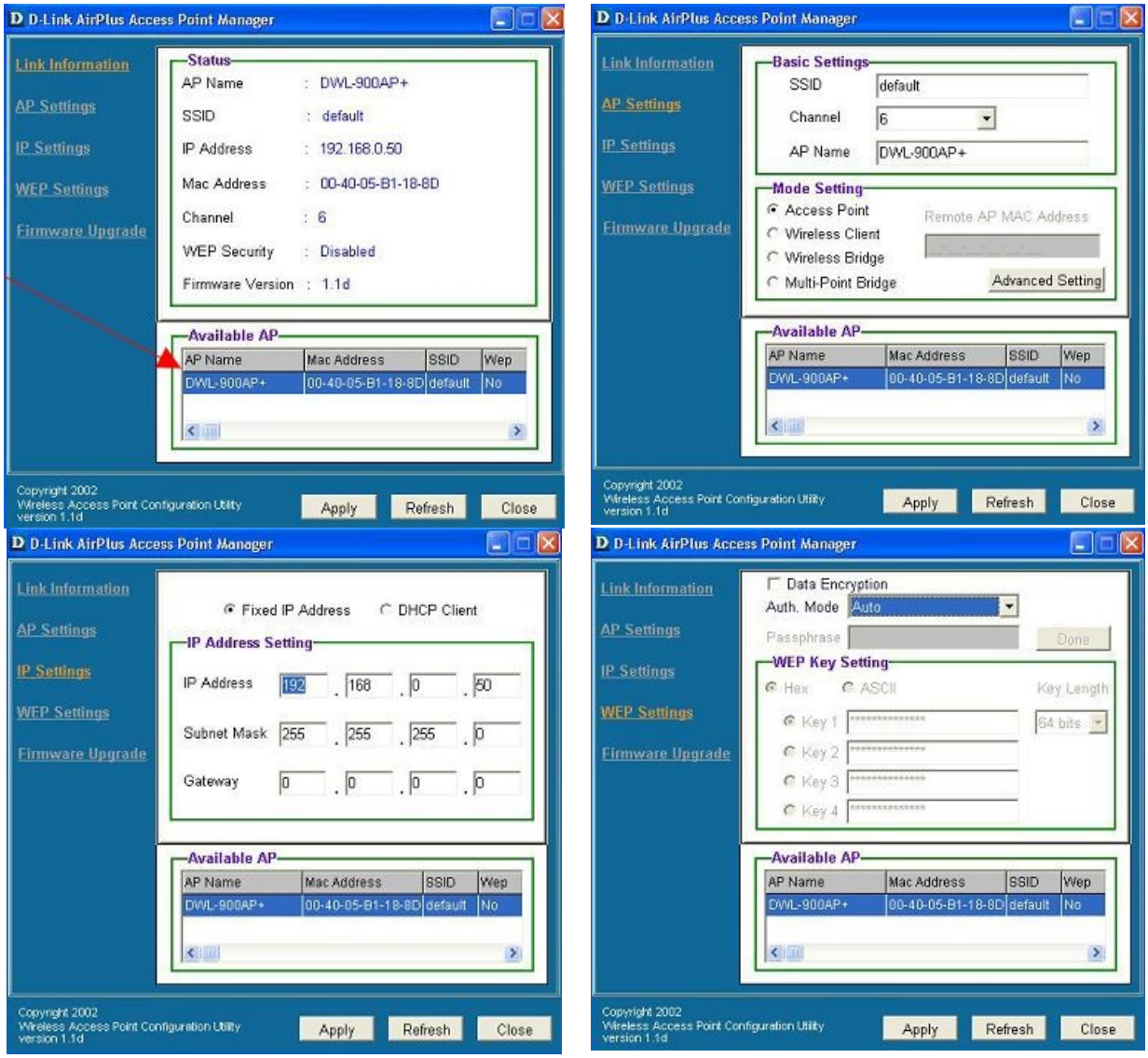
**B)** Configurazione PC2: ripetere la procedura vista sopra ma inserire un indirizzo IP diverso ma valido (per esempio 192.168.0.2).

**C)** Configurazione PC3: ripetere la procedura vista sopra ma inserire un indirizzo IP diverso ma valido (per esempio 192.168.0.3).

**D)** Colleghiamo ora i PC all'HUB o allo SWITCH mediante cavi ethernet. Se tutto è andato per il verso giusto, sulla mascherina dell'HUB si accenderanno delle luci che indicano la presenza del link sulle porte utilizzate, mentre nella system tray dei PC si noterà il cambiamento dell'icona con i due piccoli schermi che ora non avrà più la crocetta rossa. Ora i computer sono in grado di comunicare tra loro.

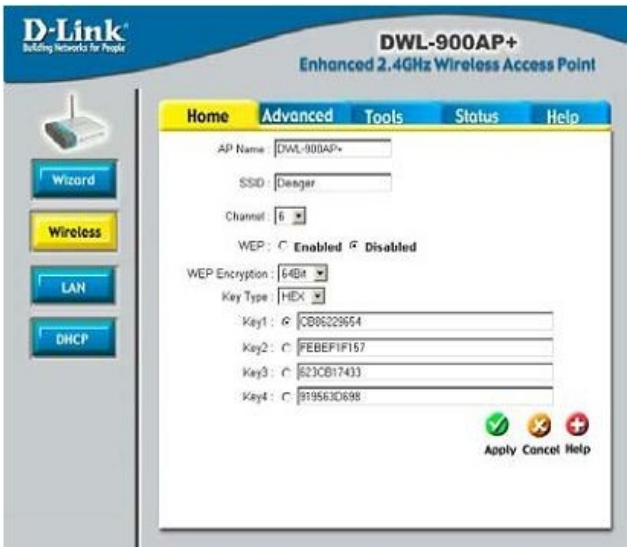
**E)** Configurazione dell'Access Point (AP): per prima cosa colleghiamo l'alimentazione e poi

tramite cavo ethernet, lo si collega all'HUB o allo SWITCH. Solitamente l'ap è fornito impostato sull'uso di un indirizzo IP fisso predefinito, perciò occorre dare una veloce lettura al manuale, per poterlo identificare. Se così non fosse, occorre installare una apposita utility di gestione presente nel compact disc a corredo e, dopo averla avviata, verranno rese disponibili alcune funzioni per l'impostazione dell'AP. Impostiamo a questo punto un indirizzo IP fisso valido per la rete LAN creata (per esempio 192.168.0.4) con relativa maschera di sottorete (255.255.255.0), cambiamo le credenziali di accesso standard (user e password di accesso alle impostazioni), diamo un SSID (per esempio SOHO_LAN), facciamolo funzionare in modalità AP se l'apparato è un multifunzione e salviamo le impostazioni appena fatte. Nelle figure seguenti è possibile avere una visione d'insieme dell'utility fornita a corredo di un apparato D-Link DWL900AP+:

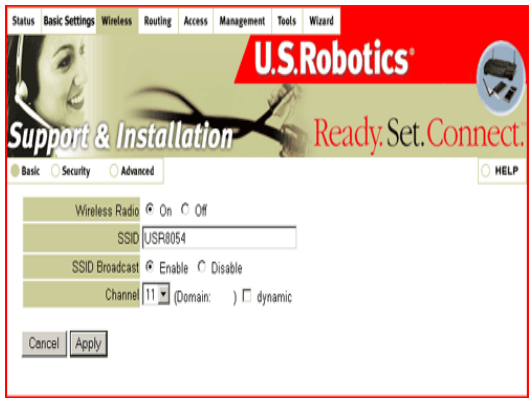



Chiudiamo l'utility di gestione ed avviamo il browser preferito, mettendo come URL l'indirizzo IP dell'access point che risponderà con una finestra di login dove si immetteranno user e password per amministrare l'apparato. Siccome in commercio esistono una grande varietà di apparati, è praticamente impossibile descrivere dettagliatamente la procedura d'impostazione, perciò si daranno le linee guida, fornendo come esempio la configurazione di un DWL900AP+ e del router USR80-805450 utilizzato in modalità "solo AP", ma dovranno essere integrate dalla lettura del manuale fornito col vostro apparato. Se avete dimenticato di settare qualche parametro precedentemente illustrato, non è un problema poiché attraverso l'interfaccia web saranno ancora disponibili, con livello di dettaglio maggiore.

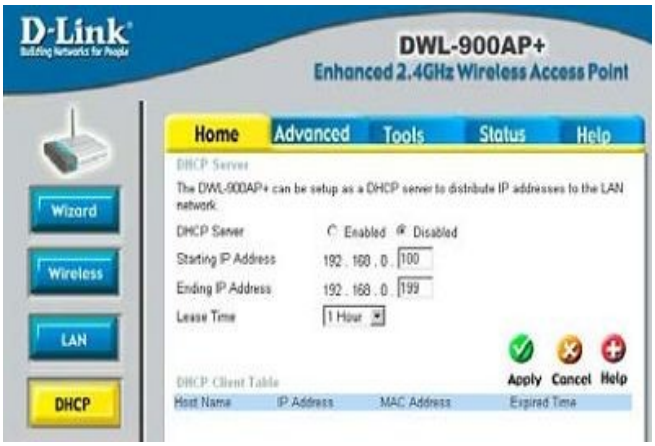
*D-Link DWL900AP+*




*US-Robotics USR80-5450*



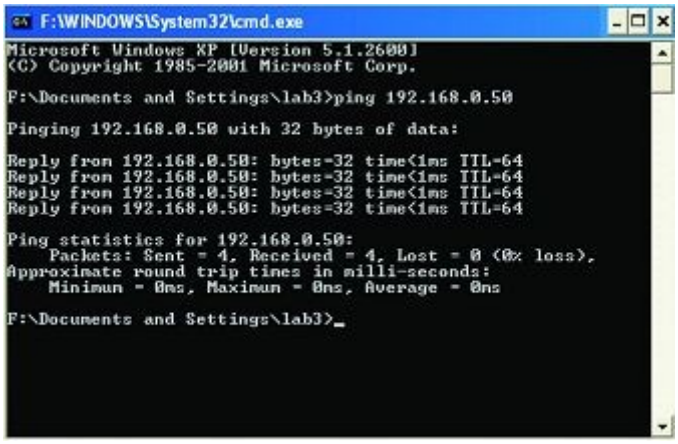

Qui sopra si possono notare la struttura dei menù ed il livello di personalizzazione possibile. Verificare che tutto corrisponda alle nostre esigenze di base descritte nel paragrafo. In questa sezione, è possibile settare il canale che si vuole ed il server DHCP, in modo da permettere ai portatili una connessione veloce senza agire troppo sulle loro impostazioni. E' bene specificare in quale **range** di indirizzi IP far lavorare il DHCP. Ciò permetterà di evitare errori d'assegnazione degli indirizzi, perciò in ***Starting IP Address*** inseriremo l'indirizzo IP 192.168.0.10 ed in ***Ending IP Address*** l'indirizzo IP 192.168.0.20. Si darà così la possibilità di connessione simultanea fino ad un massimo di 11 portali, anche se in questo caso ve n'è uno solo (PC4).





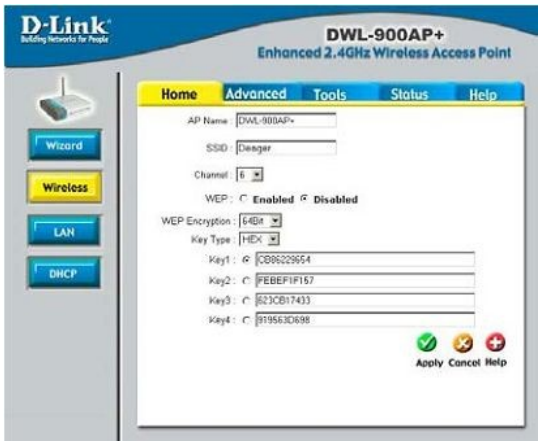
Salviamo le impostazioni cliccando su ***Apply*** ed attendiamo che l'apparato si riavvii. Lasciamo per ora invariate tutte le altre impostazioni presenti poiché al momento non interessano e si deve facilitare l'autenticazione del portatile e verificare l'intero funzionamento della LAN.

**F)** Ritorniamo al PC1 ed apriamo una sessione a "riga di comando" tramite menù ***Avvio → Esegui***, digitando ***cmd***. Nella finestra DOS, utilizziamo il comando ***ping*** seguito dall'indirizzo IP di PC2 e diamo l'invio. Osserviamo la risposta e ripetiamo lo stesso comando utilizzando gli indirizzi IP di PC3 e dell'access point AP. Se tutte le operazioni sono andate a buon fine, cioè nessun pacchetto è stato perso, significa che i computer e l'AP sono correttamente impostati ed in grado di "sentirsi". Di seguito si può vedere un esempio di sessione di ping nella quale sono stati inviati, con esito positivo, 4 pacchetti ad un preciso indirizzo IP: dovreste poter ottenere quattro sessioni con risposta simile.




**G)** Procediamo con l'impostazione del portatile (PC4): entrate in ***Pannello di controllo*** → ***Connessioni di rete*** e richiamate le proprietà (cliccando col tasto destro del mouse) sull'icona della connessione senza fili. Dalla linguetta ***Generale***, spuntate la check-box ***Mostra un'icona sull'area di notifica quando connesso*** poi selezionate ***Protocollo internet TCP/IP*** e richiamatene le proprietà. Verificate che il pulsante radio selezionato sia quello relativo a ***Ottieni automaticamente un indirizzo IP*** e cliccate su ***OK***. Passate alla linguetta ***Reti senza fili*** e cliccate sul pulsante ***Visualizza reti senza fili***. Se siete a distanza di rilevamento (è consigliato stare vicino all'AP in questa fase) sarete in grado di "vedere" lo SSID cioè il nome della vostra rete Wi-Fi (se avete seguito tutto dovreste leggere SOHO_LAN). Selezionate e cliccate sul pulsante ***Connetti***. Dopo qualche istante, il tempo necessario per la reinizializzazione della periferica, il link sarà attivo. Un test veloce di conferma del funzionamento della LAN consiste nel fare dei ping verso gli altri PC. I risultati ottenuti, dovranno essere simili a quanto visto sopra.

**H)** Siccome la rete Wi-Fi creata non è sicura, si opererà ora sulle impostazioni di AP per garantire un minimo di protezione. Da un PC in rete (questa condizione è d'obbligo poiché se lo facessimo dal portatile, al primo errore, non ci si potrà più connettere) entriamo nelle pagine di configurazione relative alla "sicurezza"… Ogni produttore utilizza un menù diverso ma in linea generale dovrebbe proporsi come qualcosa del genere:





Utilizzare la chiave ***WEP*** che permette maggiori bit di profondità, utilizzare quanto più possibile il maggior numero di chiavi disponibili (saranno utilizzate ciclicamente dal sistema ad intervalli regolari), scegliendo un formato secondo preferenza: ***HEX*** per numeri esadecimali o ***ASCII*** per valori alfanumerici. Bisogna tuttavia considerare che a diversi bit di profondità del WEP, corrispondono diverse lunghezze in caratteri della chiave.
La seguente tabella riassuntiva faciliterà la scelta della frase adatta.

| *WEP Key* | *HEX* | *ASCII* |
|---|---|---|
| 64 bit | 10 caratteri | 5 caratteri |
| 128 bit | 26 caratteri | 13 caratteri |
| 256 bit | 58 caratteri | 29 caratteri |

Non tutti gli apparati garantiscono una chiave WEP profonda 256 bit poiché non ratificata dagli attuali standard ma presente su diversi AP, comunque mai presente nella maggior parte dei portatili. Data la debolezza della cifratura WEP, è meglio orientarsi sulla codifica ***WPA-PSK*** che, quando selezionata, consentirà l'inserimento di una ***Pass-Phrase*** sulla quale saranno generate le chiavi di codifica. Cliccare su **Apply** ed attendere la reinizializzazione dell'apparato.
E' possibile incrementare il livello di sicurezza all'accesso, inserendo in una particolare sezione denominata spesso ***Filter*** gli indirizzi ***MAC*** dei dispositivi wireless autorizzati all'autenticazione. Sebbene questo sistema non sia infallibile, consente di creare una ulteriore barriera di sicurezza.

**I)** Tornare al portatile ed inserire la chiave o la pass-phrase scelta in questo modo: aprire ***Pannello di controllo → Connessioni di rete*** e richiamare le proprietà della ***Connessione senza fili***. Nella linguetta ***Reti senza fili*** selezionare la rete preferita (in questo caso SOHO_LAN) e cliccare sul pulsante ***Proprietà***. Nella finestra che si è aperta, in ***Associazione***, selezionare il tipo di crittografia dati scelto ed inserire la chiave nel box ***Chiave di rete***. Dare l'***OK*** due volte ed attendere che la connessione si reinizializzi.

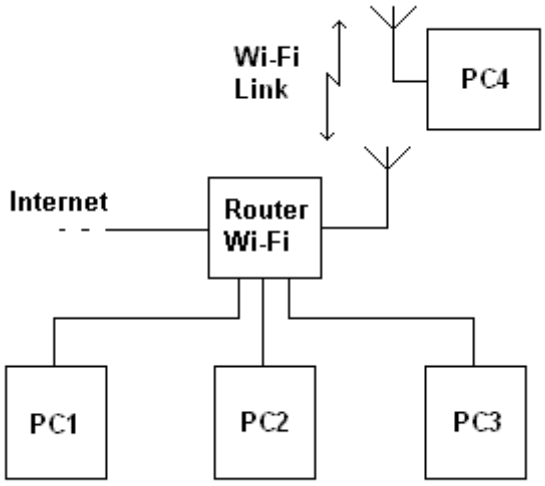
**L)** Effettuare ora il test della rete dal portatile utilizzando il comando ping, come precedentemente descritto. Se tutte le impostazioni sono andate a buon fine, l'intera rete sarà disponibile.

**M)** Le risorse di tutti i PC sono ora disponibili? No! Si crei o si scelga una cartella in ogni PC che non contiene dati importanti o sensibili e condividiamola semplicemente richiamandone le proprietà (tasto destro del mouse sulla cartella stessa) e spuntare la check-box ***Condividi la cartella in rete***. Riavviate i pc e godetevi la vostra rete.

Se ad esempio si ha a disposizione una connessione ad internet sul PC1 e si desidera condividerla, apriamo il ***Pannello di controllo → Connessioni di rete*** di PC2, PC3 e della connessione senza fili di PC4. Nella sezione ***Generale*** evidenziare la voce ***Protocollo Internet TCP/IP*** visualizzandone le proprietà. Nel campo ***Gateway*** inseriamo l'indirizzo IP di PC1 (192.168.0.1) e nei campi ***DNS*** gli indirizzi forniti dal provider. Abilitare su PC1 la condivisione della connessione internet.

### 7.4 Wireless router xDSL con 3 PC in LAN e 1 Wi-Fi

Questa soluzione non si discosta molto da quella presa in esame precedentemente ed in effetti utilizzeremo un router xDSL Wi-Fi dotato di 4 LAN in luogo dell'access point e dell' HUB. Nella figura, è possibile apprezzare la notevole somiglianza della rete al caso precedente.




La presenza del router xDSL Wi-Fi permette di semplificare al massimo la rete, rendendo altresì relativamente semplice la sua configurazione, poiché racchiude al suo interno un modem xDSL, uno switch con quattro porte LAN, un access point, un server DHCP ed il firewall con opzioni di base oppure avanzate (non è comunque detto che il vostro apparato abbia tale opzione)… il tutto perfettamente configurabile attraverso una sola e "comoda" interfaccia Web-Based.
Prima di collegare il tutto conviene dare una veloce lettura al manuale del router in modo da capire come accedere alle sue impostazioni tenendo presente che in questo tipo di configurazione i PC nella LAN funzionano in regime d'indirizzamento ad IP fissi, mentre i portatili ad IP dinamici.
Vediamo in dettaglio come fare una configurazione del genere, dando per scontato che gli adattatori ethernet ed interfacce wireless siano stati correttamente installati e riconosciuti dal sistema operativo:

**A)** Impostazioni PC1: in linea teorica basta seguire le indicazioni spiegate nella configurazione precedente poiché questa soluzione adotta impostazioni similari. Dal manuale del router cerchiamo di carpirne la classe e l'indirizzo IP utilizzato. Supponendo che il router faccia uso dell'indirizzo IP 192.168.1.1, entriamo in ***Pannello di controllo → Connessioni di rete***. Si richiamino le proprietà dell'interfaccia ethernet relative alla ***Connessione alla rete locale (LAN)***. Nella sezione ***Generale***, spuntare la casella in prossimità di ***Mostra un'icona sull'area di notifica quando connesso***, poi evidenziare ***Protocollo internet TCP/IP*** e cliccare sul pulsante ***Proprietà***. Cliccare sul pulsante radio ***Utilizza il seguente indirizzo IP*** ed inserire nel campo ***Indirizzo IP*** un indirizzo privato valido (per esempio 192.168.1.2) ed un indirizzo di sottorete (in questo caso 255.255.0.0) nel campo ***Subnet mask***. Il campo ***Gateway*** per il momento non è necessario ma verrà ripreso più avanti... Cliccare su ***OK***, attendere la reinizializzazione dell'interfaccia di rete e si noterà la comparsa nella system tray di una icona con due piccoli schermi con una croce rossa in basso a destra.
Colleghiamolo alla prima porta LAN del router.

**B)** Impostazioni Router: colleghiamo il cavo d'alimentazione ad accendiamolo. Noteremo che nella system tray di PC1 i due piccoli schermi indicanti la connessione di rete, non presentano più la croce rossa. PC1 ed il router si "sentono".

**C)** Ritorniamo su PC1 e lanciamo il browser preferito ed inseriamo nel campo indirizzi l'IP del router. Alla richiesta, inseriamo le credenziali di amministrazione del router. Da questa interfaccia abbiamo pieni poteri di modifica di tutte le sue impostazioni: si inizi con l'immettere le impostazioni di connessione ad internet fornite dal proprio provider ed impostare l'access point integrato, tenendo presente quanto detto nel ***paragrafo E di 7.3*** ma considerando che si sta lavorando su una diversa classe di indirizzi IP. Cambiare le password di amministrazione e riavviare il router.

**D)** Configurazione PC2: ripetere la procedura vista sopra (punto A) ma inserire un indirizzo IP diverso ma valido (per esempio 192.168.1.3).

**E)** Configurazione PC3: ripetere la procedura vista sopra (punto A) ma inserire un indirizzo IP diverso ma valido (per esempio 192.168.1.4).

**F)** Procediamo con l'impostazione del portatile (PC4): entrate in ***Pannello di controllo*** → ***Connessioni di rete*** e richiamate le proprietà (cliccando col tasto destro del mouse) sull'icona della connessione senza fili. Dalla linguetta ***Generale***, spuntate la check-box ***Mostra un'icona sull'area di notifica quando connesso*** poi selezionate ***Protocollo internet TCP/IP*** e richiamatene le proprietà. Verificate che il pulsante radio selezionato sia quello relativo a ***Ottieni automaticamente un indirizzo IP*** e cliccate su ***OK***. Passate alla linguetta ***Reti senza fili*** e cliccate sul pulsante ***Visualizza reti senza fili***. Se siete a distanza di rilevamento (è consigliato stare vicino all'AP in questa fase) sarete in grado di "vedere" lo SSID cioè il nome della vostra rete Wi-Fi (se avete seguito tutto dovreste leggere SOHO_LAN). Selezionate e cliccate sul pulsante ***Connetti***. Dopo qualche istante, il tempo necessario per la reinizializzazione della periferica, il link sarà attivo. Un test veloce di conferma del funzionamento della LAN consiste nel fare dei ping verso gli altri PC.

**G)** Siccome la rete Wi-Fi creata non è sicura, si opererà ora sulle impostazioni del router per garantire un minimo di protezione. Da un PC in rete (questa condizione è d'obbligo poiché se lo facessimo dal portatile, al primo errore, non ci si potrà più connettere) entriamo nelle pagine di configurazione relative alla "sicurezza"… Ogni produttore utilizza un menù diverso ma in linea generale dovrebbe proporsi come qualcosa del genere:


Utilizzare la chiave ***WEP*** che permette maggiori bit di profondità, utilizzare quanto più possibile il maggior numero di chiavi disponibili (saranno utilizzate ciclicamente dal sistema ad intervalli regolari), scegliendo un formato secondo preferenza: ***HEX*** per numeri esadecimali o ***ASCII*** per

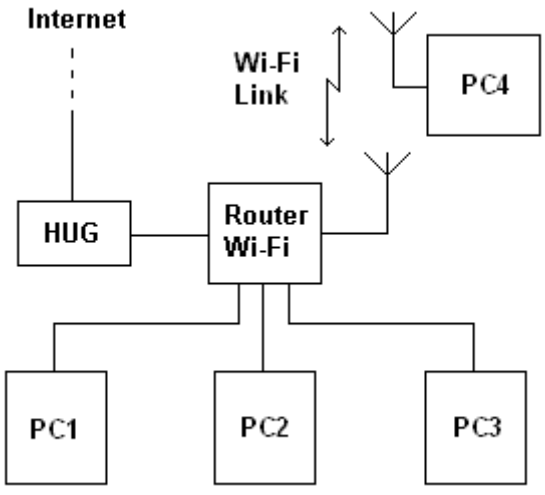
valori alfanumerici. Bisogna tuttavia considerare che a diversi bit di profondità del WEP, corrispondono diverse lunghezze in caratteri della chiave. Non tutti gli apparati garantiscono una chiave WEP profonda 256 bit poiché non ratificata dagli attuali standard ma presente su diversi AP, comunque mai presente nella maggior parte dei portatili. Data la debolezza della cifratura WEP, è meglio orientarsi sulla codifica ***WPA-PSK*** che, quando selezionata, consentirà l'inserimento di una ***Pass-Phrase*** sulla quale saranno generate le chiavi di codifica. Cliccare su **Apply** ed attendere la reinizializzazione dell'apparato.
E' possibile incrementare il livello di sicurezza all'accesso, inserendo in una particolare sezione denominata spesso ***Filter*** gli indirizzi ***MAC*** dei dispositivi wireless autorizzati all'autenticazione. Sebbene questo sistema non sia infallibile, consente di creare una ulteriore barriera di sicurezza.

**H)** Tornare al portatile ed inseriamo la chiave o la pass-phrase scelta in questo modo: aprire ***Pannello di controllo → Connessioni di rete*** e richiamare le proprietà della ***Connessione senza fili***. Nella linguetta ***Reti senza fili*** selezionare la rete preferita (in questo caso SOHO_LAN) e cliccare sul pulsante ***Proprietà***. Nella finestra che si è aperta, in ***Associazione***, selezionare il tipo di crittografia dati scelto ed inserire la chiave nel box ***Chiave di rete***. Dare l'***OK*** due volte ed attendere che la connessione si reinizializzi.

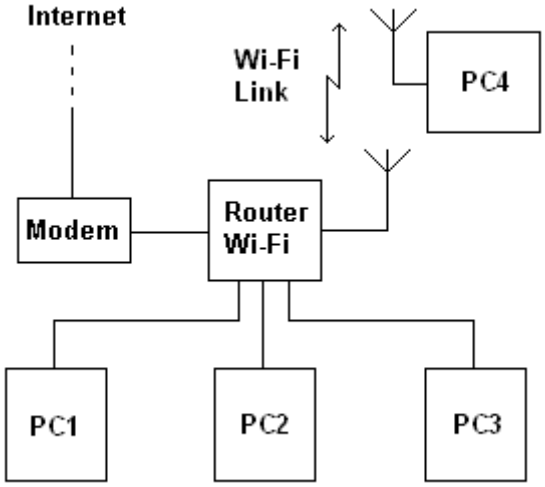
**I)** Effettuare ora il test della rete dal portatile utilizzando il comando ping, come precedentemente descritto. Se tutte le impostazioni sono andate a buon fine, l'intera rete sarà disponibile.

**L)** Le risorse di tutti i PC sono ora disponibili? No! Si crei o si scelga una cartella in ogni PC che non contiene dati importanti o sensibili e condividiamola semplicemente richiamandone le proprietà (tasto destro del mouse sulla cartella stessa) e spuntare la check-box ***Condividi la cartella in rete***. Apriamo il ***Pannello di controllo → Connessioni di rete*** di PC1, PC2, PC3 e della connessione senza fili di PC4. Nella sezione ***Generale*** evidenziare la voce ***Protocollo Internet TCP/IP*** visualizzandone le proprietà. Per utilizzare la connessione ad internet, nel campo ***Gateway*** inseriamo l'indirizzo IP del router (192.168.1.1) e nei campi ***DNS*** gli indirizzi forniti dal provider.

**NOTE:** non tutti i router dispongono all'interno di un modem xDSL. Chiamati anche ***Router Gateway,*** sono usati quando si ha a disposizione una connessione di tipo "via cavo". Un esempio può essere quello della rete di FastWeb che nei centri ad alta densità di popolazione, porta nelle abitazioni la fibra ottica alla quale fa capo un ***HUG***, molto simile ad un HUB. Collegare una porta libera dell' HUG alla presa ***WAN*** del router mediante cavo ethernet. Nella seguente figura è possibile vedere uno schema di connessione:

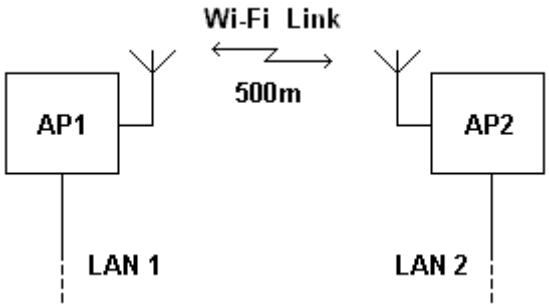


Molto spesso i router gateway vengono usati per l'installazione descritta in questo paragrafo e collegati, tramite la porta WAN ad un modem xDSL ethernet. Questo tipo di configurazione offre il vantaggio di garantire facile upgrade della connessione internet, semplicemente sostituendo il modem ma, aggiunge un ulteriore elemento da configurare sempre attraverso interfaccia web-based.




## 7.5 Bridge tra due LAN

La configurazione che verrà qui descritta è quella "classica" che si trova quando due amici che abitano nelle vicinanze decidono di unire le proprie reti di computer attraverso un link wireless. Prima di acquistare il materiale necessario alla messa in opera del link, è bene valutarne la fattibilità come insegnato nei capitoli precedenti. Visibilità ottica tra i due punti da collegare, non garantisce il 100% della fattibilità, ma offre comunque ottime speranze. Si approntì perciò il "*kit di sopravvivenza Wi-Fi*" e verificare, "annusando" l'aria intorno le due abitazioni, che non vi siano altre eventuali reti wireless; se presenti, scegliete un canale libero possibilmente non sovrapposto.
Dopo le verifiche del caso, passiamo alla realizzazione, tenendo presente che serviranno due access point che diano la possibilità di funzionare in modalità **Bridge**, due cantenne, due scatole stagne e cavo ethernet di adeguata lunghezza per collegare i dispositivi alle relative reti LAN.
Lo schema generico, semplificato alla sola rete wireless, assume le sembianze della seguente figura:

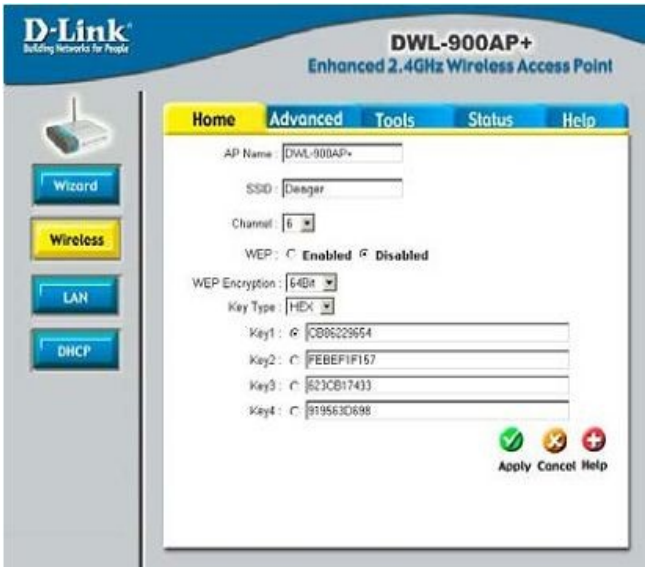



Come è possibile notare, la modalità Bridge non è altro che una versione perfezionata della modalità Ad-Hoc, solo che in questo caso coinvolge access point, rendendo di fatto la rete inaccessibile alle schede client, a tutto vantaggio della sicurezza. Questo è il principale motivo

percui viene largamente usata e preferita questa “speciale” modalità di funzionamento, unita a fatto di permettere un migliore posizionamento degli apparati, la cui distanza dai PC è limitata solo dallo standard ethernet: 100 metri.
Prima di procedere alle impostazioni degli apparati, è bene scegliere la classe di IP sulla quale i PC dovranno lavorare, destinando ed esempio alla LAN 1 un range di IP tra 192.168.0.1 e 192.168.0.10 ed alla LAN 2 un range di IP tra 192.168.0.11 e 192.168.0.20, garantendo in questo modo adeguato “spazio” di crescita alle LAN casalinghe. Per comodità, daremo agli apparati wireless due indirizzi lontani da tali range, ed esempio 192.168.0.201 ad AP1 e 192.168.0.202 ad AP2. Tutta la rete lavorerà con la medesima maschera di sottorete, in questo caso 255.255.255.0.

**A)** Impostazione degli apparati wireless (AP1): si fa presente che è bene effettuare le impostazioni degli AP “al banco”, a poca distanza, in modo da evitare inutili “trasferimenti” tra una casa e l’altra, qualora si verificassero problemi. Alimentiamo AP1 e colleghiamolo con un cavo ethernet ad un PC, lanciamo il browser preferito ed inseriamo alla richiesta le credenziali di amministrazione. E’ bene ricordare di cambiare subito le impostazioni predefinite in modo da rendere la rete meno “visibile”. Vediamo come fare, prendendo come esempio un apparato D-Link DWL900AP+ ed un DWL2100ap:

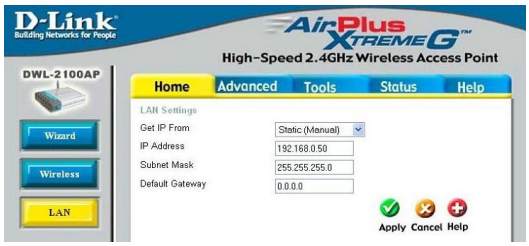
***DWL 900AP+***




***DWL 2100ap***


Cambiamo subito lo SSID con il nome che si vuole dare al link wireless (ad esempio ALFALAN), impostiamo il canale scelto in base ai rilevamenti fatti prima e cambiamo anche il nome assegnato all’apparato in modo da capirne in seguito l’ubicazione (in questo caso daremo il nome AP1 all’apparato che andrà collegato alla LAN 1 e AP2 a quello della LAN 2). Cliccare su ***Apply***.
Disabilitiamo lo ***SSID Broadcast*** in modo da non rendere “visibile” a tutti il nome della nostra W-Lan. Sostituiamo l’indirizzo IP di default con quello che abbiamo scelto in precedenza (in questo caso 192.168.0.201) e cliccare su ***Apply***.
Per il momento non è il caso di inserire alcun tipo di cifratura, lo scopo attuale è di facilitare la comunicazione tra gli apparati.
Impostiamo la modalità di funzionamento in modo che si operi in ***Bridge Mode*** detta anche ***Point To Point Bridge*** (oppure come nel caso del nuovo firmware per DWL2100ap, ***WDS***) ed inserire l’indirizzo ***MAC*** dell’apparato opposto. Attenzione a ciò che inserite! Leggete accuratamente il manuale a corredo degli apparati poiché i MAC disponibili sono due: quello relativo all’interfaccia wireless e quello relativo all’interfaccia ethernet. Nel caso venga inserito il MAC errato, il link non funzionerà. Trattandosi in questo caso di apparati D-Link, andremo ad inserire quello relativo all’interfaccia ethernet dell’apparato opposto. Non tutti gli apparati operano allo stesso modo,

infatti, alcuni richiedono l'inserimento del MAC relativo all'interfaccia wireless.




Settiamo l'apparato per l'uso dell'antenna esterna ed applichiamo le impostazioni cliccando su ***Apply*** ed attendiamo la reinizializzazione dell'apparato.

**B)** Scollegare AP1 dall'alimentazione e da ethernet. Collegare il secondo apparato (AP2) e ripetere le stesse operazioni fatte, ad accezione dell' indirizzo IP che dovrà essere 192.168.0.202. Daremo altresì AP2 come nome ed inseriremo il MAC di AP1.
Attendere la reinizializzazione e scollegatelo dalla ethernet.

**C)** Ricollegare AP1 al PC ed aprite una sessione a linea di comando. Fate un ***ping*** verso AP2 e se tutto è andato bene, otterrete una risposta… Bene, tutto qui? Nemmeno per sogno!

**D)** Ricollegatevi alle pagine di amministrazione dell'apparato e settate il livello di cifratura più alto possibile ed impostate la relativa chiave. Cliccare su ***Apply*** ed attendere la reinizializzazione.

**E)** Scollegate AP1 da ethernet e collegate AP2, ripetere le stesse operazione per abilitarne la cifratura ed inserite le stesse chiavi.

**F)** Ripetere il comando di ping… Se si ottiene risposta, gli apparati sono configurati correttamente.

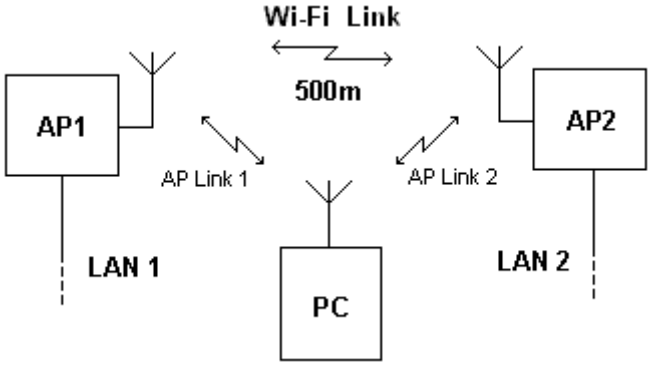
**G)** Potete ora montare gli apparati all'esterno, entro scatole stagne. Montate le antenne e fate il puntamento come descritto nel capitolo riguardante ***"Il Puntamento"***.
Collegate le antenne e la linea ethernet, date alimentazione agli apparati ed andate su un PC. Fate un ping verso l'ap remoto e se risponde, tutta la rete sarà online.

**H)** Siccome gli apparati di default sono settati per usare tutta la potenza concessa, indicata solitamente come 100% o 20dB, l'abitudine al **buon vicinato**, richiede che ne venga utilizzata quanto basta per "tenere in piedi" un link wireless stabile. Per questo motivo, si è scelto l'uso di

antenne direttive, in modo che il segnale venga irradiato solo dove serve, evitando in questo modo di recare disturbo ad altre reti e dando la possibilità ad altri di realizzare un proprio link wireless.

## 7.6 Bridge e WDS

Questa configurazione rappresenta la soluzione ideale per coloro che desiderano realizzare un link in bridge tra due reti LAN, mantenendo la possibilità di "agganciarsi" con un portatile quando si entra nel raggio di copertura, senza dover installare apparati aggiuntivi.
Dal punto di vista "esteriore", la realizzazione della rete, non si discosta molto dal caso preso precedentemente in considerazione (7.5); in effetti, in figura è possibile valutarne la somiglianza.




Questo tipo di configurazione si è resa di "facile" realizzazione con l'introduzione nel mercato di apparati in grado di gestire la modalità di funzionamento ***WDS***.
Vediamone ora la realizzazione pratica prendendo come base il caso precedente (7.5), utilizzando come apparati due DWL 2100ap della D-Link ed un portatile con funzionalità wireless. Alla LAN 1 sarà disponibile un range di IP tra 192.168.0.1 e 192.168.0.10; alla LAN 2 da 192.168.0.11 a 192.168.0.20; alle LAN saranno collegati computer con indirizzo IP fisso.
Ad AP1 si assegnerà l'IP 192.168.0.201 e ad AP2 l'IP 192.168.0.202; la maschera di sottorete dell'intera rete sarà 255.255.255.0.
Per l'indirizzo IP del portatile, si farà invece affidamento al server DHCP incorporato in uno dei due AP, dando come range gli IP compresi tra 192.168.0.30 e 192.168.0.35. Dato per scontato che le due reti LAN siano configurate e funzionanti perfettamente, ci si soffermerà alle sole impostazioni degli apparati wireless, elementi chiave per questa realizzazione.

**A)** Impostazione degli apparati wireless (AP1): si fa presente che è bene effettuare le impostazioni degli AP "al banco", a poca distanza, in modo da evitare inutili "trasferimenti" tra una casa e l'altra, qualora si verificassero problemi. Alimentiamo AP1 e colleghiamolo con un cavo ethernet ad un computer, lanciamo il browser preferito ed inseriamo alla richiesta le credenziali di amministrazione. E' bene ricordare di cambiare subito le impostazioni predefinite in modo da rendere la rete meno "visibile". Cambiamo subito lo SSID con il nome che si vuole dare al link wireless (ad esempio ALFALAN), impostiamo il canale scelto in base ai rilevamenti fatti in loco e cambiamo anche il nome assegnato all'apparato in modo da capirne in seguito l'ubicazione (in questo caso daremo il nome AP1 all'apparato che andrà collegato alla LAN 1 e AP2 a quello della LAN 2). Cliccare su ***Apply***. Disabilitiamo lo ***SSID Broadcast*** in modo da non rendere "visibile" a tutti il nome della nostra W-Lan. Sostituiamo l'indirizzo IP di default con quello che abbiamo scelto in precedenza (in questo caso 192.168.0.201) e cliccare su ***Apply***.
Per il momento non è il caso di inserire alcun tipo di cifratura, lo scopo attuale è di facilitare la

comunicazione tra gli apparati.
Impostiamo la modalità di funzionamento in modo che si operi in ***WDS with AP*** ed inserire l'indirizzo ***MAC*** dell'apparato opposto nel campo relativo al ***Remote AP MAC Address*** ed impostiamo per l'uso dell'antenna esterna. Attenzione a ciò che inserite! Leggete accuratamente il manuale a corredo degli apparati poiché i MAC disponibili sono due: quello relativo all'interfaccia wireless e quello relativo all'interfaccia ethernet. Nel caso venga inserito il MAC errato, il link non funzionerà. Trattandosi in questo caso di apparati D-Link, andremo ad inserire quello relativo all'interfaccia ethernet dell'apparato opposto. Non tutti gli apparati operano allo stesso modo, infatti, alcuni richiedono l'inserimento del MAC relativo all'interfaccia wireless.


Applichiamo le impostazioni ed attendiamo la reinizializzazione dell'apparato.

**B)** Scollegare AP1 dall'alimentazione e da ethernet. Collegare il secondo apparato (AP2) e ripetere le stesse operazioni fatte, ad accezione dell' indirizzo IP che dovrà essere 192.168.0.202. Daremo altresì AP2 come nome ed inseriremo il MAC di AP1 nell'apposito campo.
Attendere la reinizializzazione e scollegatelo dalla ethernet.

**C)** Ricollegare AP1 al computer ed aprite una sessione a linea di comando. Fate un ***ping*** verso AP2 e se tutto è andato bene, otterrete una risposta… Bene, tutto qui? Nemmeno per sogno!
Entrate nella sezione ***Advanced → DHCP Server*** ed abilitarne la funzione, inserendo l'indirizzo IP di partenza nel campo ***IP Assigned from*** (in questo caso 192.168.030 ed inserendo il valore 35 nel campo ***The Range Of Pool***).
Settare la maschera di sottorete con l'indirizzo 255.255.255.0 ed il ***Lease Time*** su 3600 secondi.
Cliccare su ***Apply*** ed attendere la reinizializzazione dell'apparato.


**D)** Occupiamoci del portatile PC: dando per scontato che l'adattatore wireless sia correttamente installato sul sistema, cliccare sul piccolo schermo relativo alla connessione senza fili presente nella System Tray e selezionare ***Cambia impostazioni avanzate***. Selezionare ***Protocollo Internet (TCP/IP)*** e cliccare sul pulsante proprietà, verificando che sia selezionato il pulsante radio ***Ottieni automaticamente un indirizzo IP***. Date l'***OK*** per ritornare al livello superiore.
Selezionare ora la linguetta ***Reti senza fili*** e cliccate sul pulsante ***Aggiungi***. Siccome s'è scelto di disabilitare lo SSID Broadcast, bisognerà inserirlo ora manualmente nell'apposito campo. Cliccare su ***OK***. Selezionare la voce relativa alla rete appena creata e cliccare sul pulsante ***Proprietà***. Nella linguetta ***Connessione*** verificare che sia selezionata la voce ***Stabilisci una connessione quando questa rete è a distanza di rilevamento***. Date OK fino all'uscita dalle impostazioni.
Se tutto è andato per il verso giusto, il portatile sarà ora collegato all'AP ed una veloce verifica consiste nel fare un ping verso gli AP.

**E)** Ricollegatevi alle pagine di amministrazione degli apparati e settate il livello di cifratura più alto possibile ed impostate la relativa chiave. Cliccare su ***Apply*** ed attendere la reinizializzazione.

**F)** Ripetere il comando di ping da un computer nella LAN verso gli apparati… Se si ottiene risposta, gli apparati sono configurati correttamente.

**G)** Impostare la cifratura nelle impostazioni della rete senza fili del portatile ed eseguite la verifica.

**H)** Potete ora montare gli apparati all'esterno, entro scatole stagne. Montate le antenne e fate il puntamento come descritto nel capitolo riguardante ***"Il Puntamento"***.
Collegate le antenne e la linea ethernet, date alimentazione agli apparati ed andate su un PC. Fate un

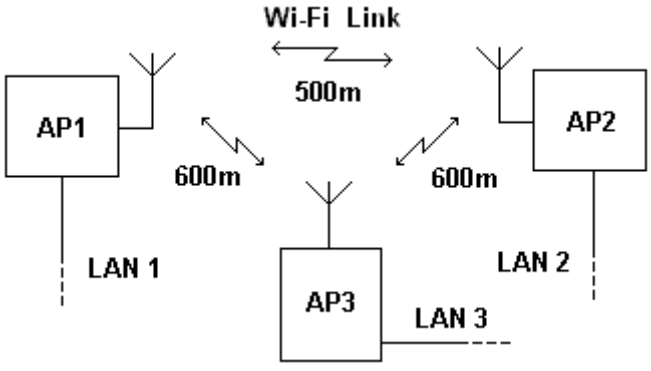
ping verso l'ap remoto e se risponde, tutta la rete sarà online.

**I)** Quando sarete nell'area di copertura di uno qualsiasi degli apparati, avrete la possibilità di collegarvi col portatile alla rete wireless creata.

**L)** Le risorse di tutti i computer sono ora disponibili? No! Si crei o si scelga una cartella in ogni PC che non contiene dati importanti o sensibili e condividiamola semplicemente richiamandone le proprietà (tasto destro del mouse sulla cartella stessa) e spuntare la check-box ***Condividi la cartella in rete***.

## 7.7 Bridge tra più LAN (Multipoint)

La configurazione di questa rete è molto simile a quella descritta nel paragrafo 7.5 ed è il tipo di configurazione "classica" che si trova quando più amici che abitano nelle vicinanze decidono di unire le proprie reti di computer attraverso un link wireless. Prima di acquistare il materiale necessario alla messa in opera del link, è bene valutarne la fattibilità come insegnato nei capitoli precedenti. Visibilità ottica tra i punti da collegare, non garantisce il 100% della fattibilità, ma offre comunque ottime speranze. Si approntì perciò il "*kit di sopravvivenza Wi-Fi*" e verificare, "annusando" l'aria intorno le abitazioni, che non vi siano altre eventuali reti wireless; se presenti, scegliete un canale libero possibilmente non sovrapposto.
Dopo le verifiche del caso, passiamo alla realizzazione, tenendo presente che serviranno access point che diano la possibilità di funzionare in modalità **Multipoint** (chiamato talvolta Point to Multipoint), antenne direttive o direzionali (in base alla morfologia del territorio e disposizione dei punti da collegare), scatole stagne e cavo ethernet di adeguata lunghezza per collegare i dispositivi alle relative reti LAN.
Lo schema generico della connessione, per esempio di tre reti LAN, semplificato alle sole reti wireless, assume le sembianze della seguente figura:

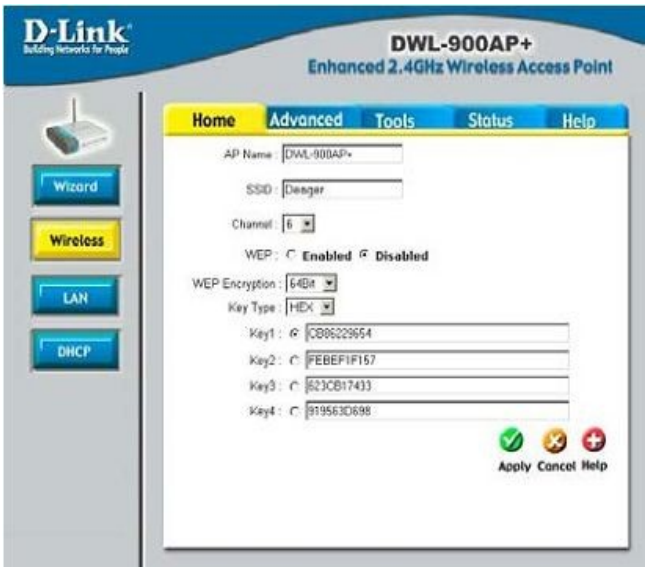



Prima di procedere alle impostazioni degli apparati, è bene scegliere la classe di IP sulla quale i PC dovranno lavorare, destinando ed esempio alla LAN 1 un range di IP tra 192.168.0.1 e 192.168.0.10, alla LAN 2 un range di IP tra 192.168.0.11 e 192.168.0.20, alla LAN 3 un range di IP tra 192.160.0.21 e 192.168.0.30, garantendo in questo modo adeguato "spazio" di crescita alle LAN casalinghe. Per comodità, daremo agli apparati wireless due indirizzi lontani da tali range, ed esempio 192.168.0.201 ad AP1, 192.168.0.202 ad AP2 e 192.168.0.203 ad AP3. Tutta la rete lavorerà con la medesima maschera di sottorete, in questo caso 255.255.255.0.

Tutti i passaggi per la configurazione sono stati descritti nel paragrafo 7.5, percui saranno ripresi effettuando le opportune modifiche per il funzionamento con la modalità multipoint.
Si tenga altresì presente che vi sono casi particolari in cui un apparato vede un solo apparato remoto, percui ci si dovrà informare se il tipo di apparati scelti siano in grado d'effettuare il routing dei dati provenienti dalle altre wireless. E' comunque possibile aggirare l'ostacolo usando installazioni particolari, come descritto nel capitolo 5 paragrafo 5.3, relativo all'installazione di più reti. Si ricorda che è bene effettuare le impostazioni degli AP "al banco", a poca distanza, in modo da evitare inutili "trasferimenti" tra una casa e l'altra, qualora si verificassero problemi

**A)** Impostazione degli apparati wireless (AP1): alimentiamo AP1 e colleghiamolo con un cavo ethernet ad un PC, lanciamo il browser preferito ed inseriamo alla richiesta le credenziali di amministrazione. E' bene ricordare di cambiare subito le impostazioni predefinite in modo da rendere la rete meno "visibile". Vediamo come fare, prendendo come esempio un apparato D-Link DWL900AP+ ed un DWL2100ap:

***DWL 900AP+***




***DWL 2100ap***


Cambiamo subito lo SSID con il nome che si vuole dare al link wireless (ad esempio ALFALAN), impostiamo il canale scelto in base ai rilevamenti fatti prima e cambiamo anche il nome assegnato all'apparato in modo da capirne in seguito l'ubicazione (in questo caso daremo il nome AP1 all'apparato che andrà collegato alla LAN 1, AP2 a quello della LAN 2 ed AP3 a quello della LAN 3). Cliccare su ***Apply***. Disabilitiamo lo ***SSID Broadcast*** in modo da non rendere "visibile" a tutti il nome della nostra W-Lan. Sostituiamo l'indirizzo IP di default con quello che abbiamo scelto in precedenza (in questo caso 192.168.0.201) e cliccare su ***Apply***.
Per il momento non è il caso di inserire alcun tipo di cifratura, lo scopo attuale è di facilitare la comunicazione tra gli apparati.
Impostiamo la modalità di funzionamento in modo che si operi in ***Multipoint Bridge*** detta anche ***Point To Multipoint Bridge*** (oppure come nel caso del nuovo firmware per DWL2100ap, ***WDS***) ed inserire l'indirizzo ***MAC*** degli apparati opposti. Attenzione a ciò che inserite! Leggete accuratamente il manuale a corredo degli apparati poiché i MAC disponibili sono due: quello relativo all'interfaccia wireless e quello relativo all'interfaccia ethernet. Nel caso venga inserito il MAC errato, il link non funzionerà. Trattandosi in questo caso di apparati D-Link, andremo ad inserire quello relativo all'interfaccia ethernet degli apparato opposti. Non tutti gli apparati operano allo stesso modo, infatti, alcuni richiedono l'inserimento del MAC relativo all'interfaccia wireless.





Settiamo l'apparato per l'uso dell'antenna esterna ed applichiamo le impostazioni cliccando su ***Apply*** ed attendiamo la reinizializzazione dell'apparato.

**B)** Scollegare AP1 dall'alimentazione e da ethernet. Collegare il secondo apparato (AP2) e ripetere le stesse operazioni fatte, ad accezione dell' indirizzo IP che dovrà essere 192.168.0.202. Daremo altresì AP2 come nome ed inseriremo il MAC di AP1 e AP3. Attendere la reinizializzazione e scollegatelo dalla ethernet.

**C)** Collegare il terzo apparato (AP3) e ripetere le stesse operazioni fatte, ad accezione dell' indirizzo IP che dovrà essere 192.168.0.203. Daremo altresì AP3 come nome ed inseriremo il MAC di AP1 e AP2. Attendere la reinizializzazione e scollegatelo dalla ethernet.

**D)** Ricollegare AP1 al PC ed aprite una sessione a linea di comando. Fate un ***ping*** verso AP2 ed AP3. Se tutto è andato bene, otterrete una risposta… Bene, tutto qui? Nemmeno per sogno!

**E)** Ricollegatevi alle pagine di amministrazione dell'apparato e settate il livello di cifratura più alto possibile ed impostate la relativa chiave. Cliccare su ***Apply*** ed attendere la reinizializzazione.

**F)** Scollegate AP1 da ethernet e collegate AP2, ripetere le stesse operazione per abilitarne la cifratura ed inserite le stesse chiavi.

**G)** Ripetere il comando di ping… Se si ottiene risposta, gli apparati sono configurati correttamente.

**H)** Scollegate AP2 da ethernet e collegate AP3, ripetere le stesse operazione per abilitarne la cifratura ed inserite le stesse chiavi.

**I)** Ripetere il comando di ping… Se si ottiene risposta, gli apparati sono configurati correttamente.

**L)** Potete ora montare gli apparati all'esterno, entro scatole stagne. Montate le antenne e fate il

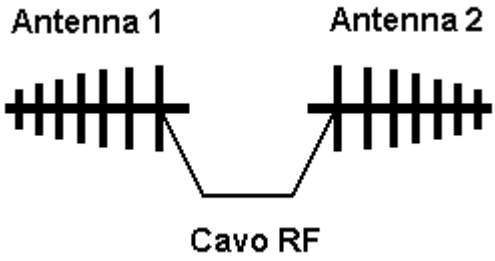
puntamento come descritto nel capitolo riguardante ***"Il Puntamento"***.
Collegate le antenne e la linea ethernet, date alimentazione agli apparati ed andate su un PC. Fate un ping verso gli AP remoti e se rispondono, tutta la rete sarà online.

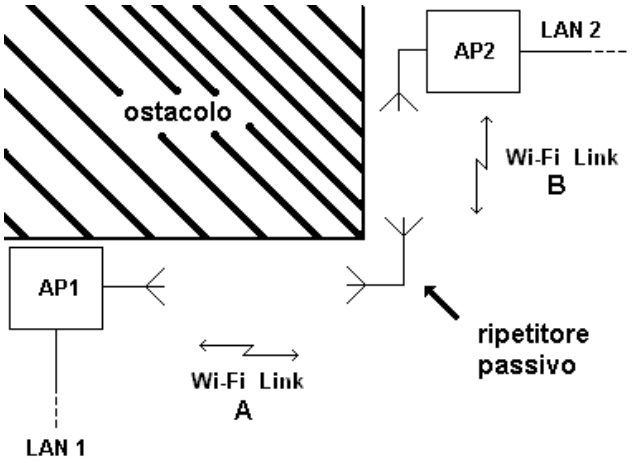
**M)** Siccome gli apparati di default sono settati per usare tutta la potenza concessa, indicata solitamente come 100% o 20dB, l'abitudine al **buon vicinato**, richiede che ne venga utilizzata quanto basta per "tenere in piedi" un link wireless stabile e l'uso di antenne direttive o direzionali fa sì che il segnale venga irradiato solo dove serve, evitando in questo modo di recare disturbo ad altre reti e dando la possibilità ad altri di realizzare un proprio link wireless.

**N)** Le risorse di tutti i computer sono ora disponibili? No! Si crei o si scelga una cartella in ogni PC che non contiene dati importanti o sensibili e condividiamola semplicemente richiamandone le proprietà (tasto destro del mouse sulla cartella stessa) e spuntare la check-box ***Condividi la cartella in rete***.

### 7.8 Bridge con ripetitore passivo

Quando si vuole realizzare un link, può accadere che i punti non siano a portata ottica, con l'aggarvante dell'impossibiltà di realizzare un ripetitore attivo. Quando questa importante condizione non è soddisfatta, difficilmente la realizzazione di un link è fattibile. Prima di rassegnarsi, conviene tentare un "azzardo", ovvero l'uso di un ripetitore passivo, la cui realizzazione ed installazione tipica è schematizzata nel disegno a seguire:



Questo tipo di ripetitore non farà certo miracoli e necessita di calcoli matematici algebrici dopo accurati rilevamenti dei livelli di segnale in gioco. Occorre tener presente che questo ripetitore non amplifica in nessun modo il segnale, anzi, concorre ad aumentarne l'attenuazione e se il rumore o i disturbi ambientali sono troppo "forti", allora è meglio abbandonare...
Supponendo di trovarsi in condizioni più o meno favorevoli, vediamo come affrontare la realizzazione del link, il cui livello di segnale che giunge ad AP2 è, semplificando un poco, dato dalla formula algebrica:

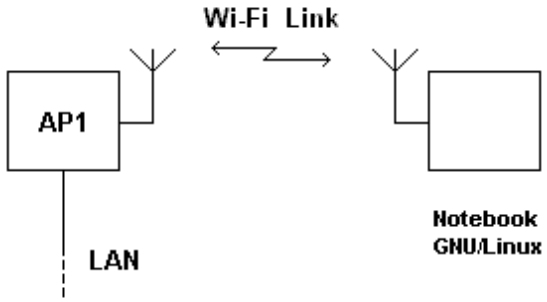
**dB (r) = dB (AP1) – dB (co+ca 1) + dB (ant AP1) – Att (link A) + dB (ar1) – dB (co+ca R) + dB (ar2) – Att (link B) + dB (ant AP2) – dB (co+ca 2)**

dove

**db (AP1)** = è la potenza d'uscita dall'amplificatore dell'apparato trasmittente, qui AP1;
**dB (co+ca 1)** = è l'attenuazione introdotta dai connettori e lunghezza cavo tra AP1 e antenna;
**dB (ant AP1)** = è il guadagno dell'antenna collegata ad AP1;
**Att (link A)** = è l'attenuazione in campo libero dovuto alla distanza tra AP1 e ripetitore;
**dB (ar1)** = è il guadagno dell'antenna del ripetitore puntata verso AP1;
**dB (co+ca R)** = è l'attenuazione introdotta dai connettori e lunghezza cavo tra antenne ripetitore;
**dB (ar2)** = è il guadagno dell'antenna del ripetitore puntata verso AP2;
**Att (link B)** = è l'attenuazione in campo libero dovuto alla distanza tra ripetitore ed AP2;
**dB (ant AP2)** = è il guadagno dell'antenna collegata ad AP2;
**db (co+ca 2)** = è l'attenuazione introdotta dai connettori e lunghezza cavo tra AP2 e antenna;
**dB (r)** = è il livello di segnale che si presenta al ricevitore, in questo caso AP2.

Per la rilevazione di tutti i dati necessari alla realizzazione, è opportuno utilizzare un portatile munito del *"kit di sopravvivenza Wi-Fi"* e studiare "sulla carta" la fattibilità, tenendo conto che il cavo d'antenna utilizzato per la connessione delle due antenne costituenti il ripetitore passivo, dovrà essere il più corto possibile e del tipo a bassa perdita.
La velocità massima che il link potrà raggiungere sarà estremamente dipendente dal livello del segnale disponibile [**dB (r)**], dalla sensibilità delle riceventi integrate negli apparati, dal livello S/N (segnale-rumore) e dai disturbi ambientali presenti; certamente non avrà l'efficienza di un link che utilizza un repeater vero e proprio, ma come spesso viene detto, meglio poco che niente...

## 7.9 Connessione ad un AP con notebook GNU/Linux




La connessione ad una rete Wi-Fi ad opera di un computer di tipo fisso o portatile, con installato il sistema operativo GNU/Linux, non è sempre di facile realizzazione e può mettere in crisi un utente alle prime armi. Siccome con questa guida si vuole offrire la massima versatilità, vediamo come connettersi con un portatile (dove generalmente si trovano le periferiche più ostiche da impostare) ad un AP in modo semplice e veloce attraverso i programmi ***WiFi Radar*** e ***WPA Supplicant***, distribuiti secondo la licenza GNU GPL. Tutti i portatili, dalla generazione "Centrino", sono dotati di scheda Wi-Fi integrata ma, se il vostro non lo fosse, basta utilizzare un adattatore PCMCIA oppure USB. In quest'ultimo caso, non essendo disponibili appositi driver nativi per GNU/Linux, occorre dotarsi del programma ***NdisWrapper***, un software che consente di caricare direttamente i driver Windows presenti nel cd fornito a corredo dell'adattatore, semplicemente lanciando il programma con il comando "**ndiswrapper -i driver.inf**".
Nelle più comuni distribuzioni, per la connessione wireless viene fornito solitamente il programma Network Manager, che risulta essere molto semplice nel suo utilizzo ma che presenta i notevoli difetti: la scarsità di compatibilità ridotta verso le più variegate schede Wi-Fi, dove spesso si presenta una funzionalità ridotta; l'impossibilità allo stato attuale di usare IP statici.
Per ovviare a questo problema, l'uso di WiFi Radar permette affidabilità, completezza ed una compatibilità maggiore, a scapito d'immediatezza d'uso un poco più complicata.
Prima d'iniziare la descrizione delle procedure di connessione, occorre spendere qualche parola sull'uso di WiFi Radar e sui diversi moduli, detti anche driver, che lo stesso richiede per funzionare correttamente con il tipo di adattatore utilizzato.

Come si è già potuto capire nei precedenti capitoli, ogni scheda necessita di driver che dipendono fortemente dal tipo di chipset presente; come accade per i sistemi operativi Windows, nemmeno GNU/Linux sfugge a questo requisito, perciò occorre affidarsi alla tabella a seguire.

| Driver | Tipo di scheda, chipset |
|---|---|
| wext | Driver generico Linux Wireless Extension |
| hostap | Driver Intersil Prism 2, 2.5, 3 |
| ipw | Driver per tecnologia “Centrino” ipw2100, ipw2200 |
| madwifi | Driver MADWIFI 802.11 Atheros |
| hermes | Driver Agere Hermes I, II |
| atmel | Driver Atmel AT76C5XXx |
| Broadcom | Driver chipset Broadcom |
| ndiswrapper | Driver Windows con l'uso di NdisWrapper |

C'è poi da segnalare un piccolo bug che affligge questa utility, rendendo le connessioni impossibili perché non si può accedere all'interfaccia di rete e non compare il pulsante “Connect”. Per ovviare, basta lanciare da root l'editor di testo preferito ed aprire il file **/etc/wifi-radar.conf**, cancellando la riga “**interface=**”. Al successivo riavvio, WiFi Radar rileverà automaticamente e correttamente l'interfaccia di rete, che verrà memorizzata nel file di configurazione definitivamente.
E' possibile fare in modo che WiFi Radar si avvii automaticamente ad ogni avvio del computer, inserendo la linea di codice “**sudo wifi-radar -d**” negli script di avvio, che generalmente si trovano in **/etc/init.d**.

Preliminarmente tutto ciò che bisogna fare è attivare la scheda wireless, considerando che l'uso dei software elencati sopra dipende dal tipo di rete wireless con cui si ha a che fare...

→ Collegarsi ad una W-LAN ad accesso libero:

Avviare WiFi Radar, e selezionare lo SSID della rete wireless desiderata e premere il pulsante “Connect”. E' altresì possibile dare una priorità di connessione alle reti disponibili, semplicemente selezionando un SSID e trascinarlo verso l'alto o il basso, secondo le proprie necessità di priorità. In questo modo, nel caso di più reti wireless, il programma si connetterà al primo SSID disponibile nella lista. Se è la prima volta che ci si connette, è utile creare un nuovo profilo; quindi nella nuova finestra di dialogo che si aprirà, rispondere “**Sì**”, creandone uno. Tipicamente le impostazioni di default funzionano discretamente bene; eventualmente apportare le modifiche di rifinitura e cliccare su “**Salva**”, connettendosi.
Nel caso la connessione non vada a buon fine, attraverso la finestra di configurazione, si può intervenire su alcuni parametri come il “**Manual network configuration**”, i comandi di connessione, lo SSID, il driver dell'adattatore, ecc ecc.

→ Collegarsi ad una W-LAN ad accesso cifrato (WPA):

Quando una rete è cifrata, bisogna per prima cosa installare il pacchetto di rete **wpa_supplicant** e con l'editor di testo preferito modificare il file **/etc/wpa_supplicant.conf** che si presenterà in modo più o meno simile:

```
network={
        ssid=”rete_scelta”
        psk=Passphrase
        key_mgmt=WPA-PSK
        proto=WPA}
```

in SSID bisogna inserire lo SSID della rete;
in PSK bisogna inserire la passphrase, la sequenza di caratteri che protegge la rete e che costituisce una specie di password estesa.
Naturalmente le informazioni da inserire sono contenute nelle impostazioni dell'access point e dovranno essere fornite dall'amministratore della rete.
Siccome la passphrase costituisce l'elemento più importante e delicato, andrebbe perciò protetta e non inserita direttamente in chiaro nel file di configurazione. Per fare ciò, occorre procedere così:

- aprire la shell come utente root e dare il comando wpa_passphrase con argomento lo SSID:

  **$wpa_passphrase SSID** [invio]

- inserire la passphrase.
- La shell restituirà alcune righe e basterà copiare la riga che inizia con **psk=** ed inserirla nel file di configurazione che ora conterrà la passphrase corretta, senza mostrarla.

E' ora possibile avviare WiFi Radar e procedere alla sua configurazione, sfruttando così la cifratura WPA-PSK. Selezionare lo SSID della rete wireless desiderata e seguire come mostrato nel caso precedente, le operazioni di creazione del profilo. Nella finestra di configurazione, cliccare sulla voce “**No WPA**” in modo che cambi in “**Use WPA**” e permetta la selezione del driver utilizzato da wap_supplicant per l'adattatore Wi-Fi usato.

# Servizi nella W-LAN

## 8.1 Server e generalità

Questo capitolo descriverà essenzialmente come abilitare e configurare quelle applicazioni lato server e lato client per accedere alle configurazioni avanzate di cui la maggior parte degli access point sono dotati. Partendo dal presupposto che una rete tra amici non ha le stesse necessità di un provider, anche un computer datato può assolvere ai servizi richiesti e di seguito descritti. Offrendo molteplici servizi aggiuntivi all'interno della LAN o W-LAN, si incrementano le potenzialità della rete stessa! Come sistema operativo, una qualsiasi distribuzione di GNU/Linux può assolvere facilmente e stabilmente quanto richiesto.
Per prima cosa occorre capire bene cosa sia un server. Per ogni servizio di rete esistono almeno due software che lavorano accoppiati: il "server" che fornisce il servizio, il "client" che si collega al servizio server per sfruttarne le risorse. Per poter interagire tra loro, server e client devono interagire seguendo delle regole di comunicazione ben definite, che in gergo prendono il nome di protocolli. La presenza dei protocolli fa sì che esistano diversi server e client per ogni servizio; la cosa fondamentale è che ogni programma che fornisce od utilizza un servizio, segua alla lettera il protocollo che lo caratterizza. Caratteristica molto importante dei servizi di rete è la porta di ascolto, parametro fondamentale che serve a differenziare i diversi servizi di rete attivi su un solo computer.
Ci sarebbe molto da dire al riguardo, ma non essendo lo spirito di questa guida, lascerò al lettore la facoltà di approfondimento attraverso ricerche in internet o la lettura di manuali specifici.
Solitamente si è portati a credere che un server sia un computer costoso, grande e pesante. Nulla di più sbagliato... Ciò che differenzia una workstation da un server è semplicemente il software che ci gira sopra, ma procediamo comunque a piccoli passi, tenendo presente che la maggior parte dei servizi offerti necessita di una piattaforma *LAMP* (ovvero Linux Apache MySQL PHP Perl Python). Essendo questo capitolo di carattere generale e redatto da un neofita del mondo open source, possono essere presenti errori, imprecisioni ed omissioni.

Si raccomanda di tenere collegato il pc al modem-router e di avere attiva la connessione ad internet, durante la fase d'installazione del sistema operativo, in modo da recuperare agevolmente i paccehtti eventualmente non presenti nel cd d'installazione stesso.

### 8.1.1 Requisiti hardware e configurazione

E' davvero necessario acquistare un computer nuovo e fiammante da usare come server? Beh, molto dipende dal numero di client e dei servizi offerti... Certamente una ditta con centinaia di dipendenti, con un sito di e-commerce e molti servizi in rete, necessiterà di specifiche hardware piuttosto elevate; viceversa, per scopi didattici o servizi di rete limitati, anche un vecchio pc può assolvere alacremente a questo compito. Se la macchina deve restare accesa 24 ore su 24, dovrà avere un buon sistema di raffreddamento interno, evitando così pericolosi surriscaldamenti che potrebbero danneggiare in modo irreparabile i delicati componenti elettronici interni. Se durante l'utilizzo si riscontrassero prestazioni basse, l'aggiunta di memoria RAM, la sostituzione del processore con uno più veloce, upgrade del disco fisso, danno generalmente ottimi risultati. A livello "home", anche un computer di classe Pentium con velocità di 300-500 MHz, 128 Mbyte di RAM, disco fisso da 10 Gbyte, lettore di CD o DVD, è più che sufficiente... il componente richiesto nel modo più assoluto è la scheda di rete, senza la quale un server non avrebbe senso...
Dopo aver recuperato il pc, si procederà alla sua configurazione che richiederà una certa dose di "scrematura" dei componenti. Trattandosi di un server, è necessario rimuovere o disabilitare quelle periferiche non necessarie al suo funzionamento. Tutto ciò viene fatto essenzialmente per due motivi: un componente non utilizzato consumerebbe inutilmente energia e concorre, con la sua dispersione di calore, ad aumentare la temperatura del sistema; ogni componente in più, anche se non utilizzato, contribuisce ad aumentare il livello di rischio di malfunzionamenti ed appesantisce il sistema operativo, occupando preziose risorse di sistema e cicli macchina. Discorso analogo verrà fatto anche per il software.
La regola generale per l'installazione (hardware e software) di un buon server è quella di mettere solo ed esclusivamente lo stretto necessario; il superfluo non deve esistere poiché crea solo confusione! Perciò, mano al cacciavite e rimuovere le schede ed i dispositivi superflui:

- il floppy generalmente non serve, perciò è possibile la sua rimozione;
- le schede grafiche 3D sono inutili, una "vecchia" VGA è più che sufficiente;
- le porte seriali e quella parallela sono inutili, tranne che in casi molto particolari;
- la scheda audio è inutile;
- altre schede d'espansione sono inutili (tranne gli adattatori di rete);
- eventuali connessioni "frontali" delle porte USB sono inutili;
- il lettore di CD o DVD è possibile rimuoverlo dopo l'installazione del sistema operativo.

Dopo aver eliminato le periferiche che sono possibili da rimuovere fisicamente, alimentare il computer e rimuovere quelle dette "integrate" sulla piastra madre, entrando nelle impostazioni del BIOS. Se la scheda video è di quelle integrate, che utilizza la condivisione della memoria di sistema, assegnare il quantitativo minore possibile, in modo da limitare al massimo lo spreco di preziosa RAM per operazioni inutili. L'impostazione di altri eventuali parametri dipendenti dalla configurazione "fisica" del sistema, possono essere definiti sempre basandosi sulla solita regola d'oro enunciata prima: "se non serve, conviene toglierlo..."
In caso si sia stati "troppo" selettivi, il computer non partirà più dopo il reboot; in questo caso ripristinare le configurazioni di default, resettando la CMOS, e quindi procedere nuovamente alla configurazione del BIOS, fino a trovare il funzionamento al livello più restrittivo possibile.
Queste operazioni possono risultare senza senso, ma garantiscono una migliore efficienza in termini di utilizzo delle risorse e di sicurezza; quest'ultima è un'arte e in un server va garantita a 360°. Per avere un sistema sicuro, ogni anello dev'essere sicuro e costantemente monitorato; meno driver e programmi saranno caricati in memoria, minori saranno le possibilità che il sistema venga violato.
Terminata la configurazione del BIOS, non resta che installare il sistema operativo GNU/Linux, nella distribuzione preferita, cercando di mantenerlo il più snello possibile, quindi niente Desktop

Environment e front-end grafici (ok, se siete neofiti, sono consentiti solo per fare le prime sperimentazioni e per capire come “muoversi” all'interno dell'OS), ma solo modalità testuale.
In linea teorica, sarebbe possibile fare a meno anche della scheda video poiché è possibile il controllo remoto; tuttavia la sua presenza facilita le operazioni di controllo in loco.

Se siete alle prime armi nell'installazione di una piattaforma server, sarebbe opportuno affidarsi ad una guida che spieghi come effettuare, passo dopo passo, le impostazioni di base, in modo tale da capire cosa state effettivamente facendo.

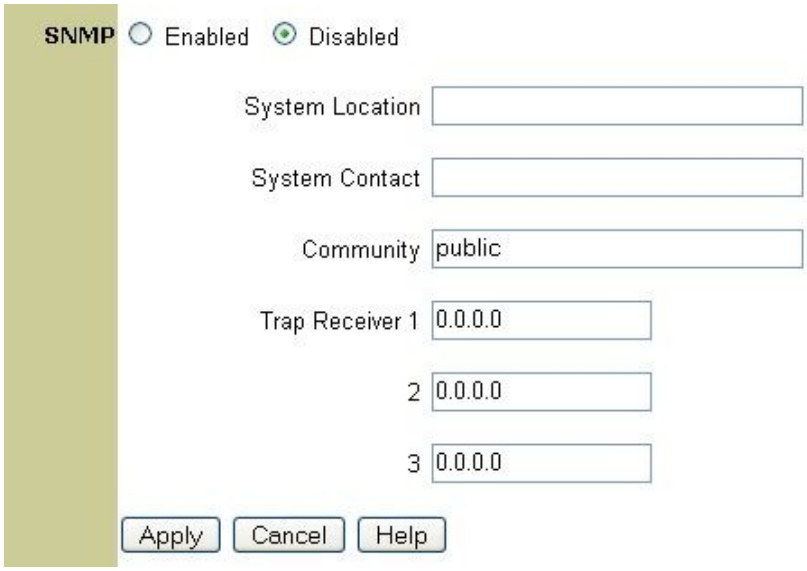
## 8.2 Le statistiche

Su molti apparati esiste la possibilità di monitorare il traffico che passa attraverso la rete wireless, grazie al protocollo **SNMP** che invia ad un computer, solitamente adibito a piccolo server, i dati relativi al traffico stesso. Esistono molti programmi che permettono di raccogliere questi dati e di renderli disponibili e visionabili graficamente attraverso una comoda interfaccia web-based. Il più diffuso tra questi è certamente l'open source **MRTG** (**M**ulti **R**outer **T**raffic **G**rapher), disponibile in rete sia in formato RPM che sorgente. Per il suo utilizzo bisogna avere installati sul server alcuni software aggiuntivi. In particolare devono essere presenti un interprete **Perl** con il quale è stato scritto il programma, le librerie per la creazione e gestione dei grafici, ovvero **zlib**, **libpng** e **gd**. Le fasi essenziali per avere il sistema funzionante sono:

→ configurare una **community** (in sola lettura) sugli apparati da monitorare.
→ installare MRTG.
→ scegliere una directory dove mettere i file (dei log e dei grafici) di MRTG. Se gli apparati da monitorare sono più di uno, si consiglia l'uso di una sottodirectory per ogni host.
→ creare i file di configurazione, uno per ogni apparato, con l'utility **cfgmaker**.
→ creare una pagina di indice dei grafici degli host con **indexmaker**.
→ per rendere visionabili "all'esterno" i grafici sul traffico, è utile configurare il web server **Apache** in modo che la directory di lavoro di MRTG sia raggiungibile via browser.
→ far in modo che MRTG si avvii automaticamente.

Vediamo ora come operare, prendendo come esempio un access point US-Robotics USR80-5450, correttamente configurato per un link funzionante, con indirizzo IP 192.168.0.50 ed una Linux box con indirizzo IP 192.168.0.100, sul quale gira la distribuzione Fedora Core. Si ricorda che quando descritto di seguito è facilmente adattabile a qualsiasi apparato e distribuzione GNU/Linux.

**A)** Accedere alle pagine di configurazione dell'access point puntando il browser preferito all'indirizzo IP dello stesso (in questo caso 192.168.0.50) ed inserire le credenziali di amministrazione quando richieste. Spostarsi nel menù **Tools** e prendere visione della sezione SNMP come mostrato nella seguente figura:



Abilitare la funzione cliccando sul pulsate-radio **Enabled**, nel campo **System Location** inserire la posizione dell'apparato (ad esempio: AP esterno), in **System Contact** inserire ad esempio il nome del gruppo di lavoro dato alla rete dei pc. Sostituire nel campo **Community** la parola **public** con una che ricordi sia la posizione che la velocità… un esempio potrebbe essere **OutsideG**. Siccome con questo apparato è possibile inviare i dati a tre computer che svolgono il compito di monitorare la rete e s'è deciso di usare un solo pc, prenderemo in considerazione solo la voce **Trap Receiver 1** nel cui campo andremo ad inserire l'indirizzo IP del server, in questo caso s'inserirà 192.168.0.100. Le impostazioni riguardanti l'apparato sono ultimate e non resta che cliccare su **Apply** ed attenderne la reinizializzazione.

**B)** Passiamo alle impostazioni del piccolo server e, se non presente, installare MRTG dando il seguente comando da shell con privilegi di ROOT:

**$rpm –ivh mrtg-versione.rpm** [invio]

Una volta installato, dev'essere configurato in modo opportuno e cioè istruito su quali device di rete dovranno essere monitorati. Il file di configurazione è **mrtg.cfg** (presente in /etc/mrtg) e può essere generato grazie all'ausilio dell'utility **cfgmaker** fornita con il programma, dando il seguente comando da shell con privilegi di root:

**$cfgmaker OutsideG@192.168.0.50 --global "WorkDir: /var/www/mrtg" > /etc/mrtg/mrtg.cfg** [invio]

verranno così acquisite le informazioni per la configurazione e generato il relativo file. E' possibile generare un file index.html, molto utile quando si hanno due o più apparati da monitorare, semplicemente dando il comando:

**$indexmaker /etc/mrtg/mrtg.cfg > /var/www/mrtg/index.html** [invio]

A questo punto MRTG ha tutti i dati necessari per il funzionamento e la schedulazione del file mrtg.cfg è già operativa grazie al file di cron (/etc/cron.d/mrtg) installato dal pacchetto RPM.

**C) Affinché** i grafici generati siano visionabili da altri computer nella rete, è opportuno modificare la configurazione di Apache per permetterne l'accesso. Con l'editor di testo preferito, aprire il file **/etc/httpd/conf.d/mrtg.conf** e modificare la direttiva **Allow from 127.0.0.1** in 192.168.0. la quale indicherà che tutti i computer con IP di classe 192.168.0.X potranno accedere ai grafici. Riavviare Apache dando il comando:

**$/etc/init.d/httpd reload** [invio]

Avviare il browser preferito su qualsiasi pc e puntare all'indirizzo **http://192.160.0.100/mrtg**.

**D)** Se i dispositivi da monitorare sono due o più, qualche utile suggerimento può essere utile… Un esempio potrebbe essere quello di monitorare due AP. Per la configurazione degli stessi, la descrizione fatta sopra è sempre valida, fermo restando che l'indirizzo IP debba essere diverso (per esempio 192.168.0.50 per AP1 e 192.168.0.51 per AP2). Si inizi creando due sottocartelle chiamate 1 e 2 in **/var/www/mrtg**. Dalla shell, con privilegi di root diamo il comando per creare il file di configurazione per AP1 che utilizzerà per i risultati la prima sottocartella:

**$cfgmaker OutsideG@192.168.0.50 --global "WorkDir: /var/www/mrtg/1" > /etc/mrtg/mrtg1.cfg** [invio]

verranno così acquisite le informazioni per la configurazione e generato il relativo file. Ripetiamo il comando opportunamente modificato per generare le informazioni per la configurazione di AP2:

**$cfgmaker OutsideG@192.168.0.51 --global "WorkDir: /var/www/mrtg/2" > /etc/mrtg/mrtg2.cfg** [invio]

Abbiamo a questo punto creato i due file di configurazione in **/etc/mrtg/** e dobbiamo istruire il file di **cron** in **/etc/crontab affinché** vengano processati al posto del file di default **mrtg.cfg**. Aprire con l'editor di testo preferito il file **crontab** ed aggiungere i riferimenti ai file di configurazione e commentare (con il carattere #) il riferimento di default, come mostrato nell'esempio seguente:

```
# */5 * * * *  root  /usr/bin/mrtg  /etc/mrtg/mrtg.cfg
*/5 * * * *  root  /usr/bin/mrtg  /etc/mrtg/mrtg1.cfg
*/5 * * * *  root  /usr/bin/mrtg  /etc/mrtg/mrtg2.cfg
```

In alcune distribuzioni nel file **crontab** sono presenti i link alle cartelle di **cron.xxx** dove risiedono la schedulazioni vere e proprie da eseguire. La modifica a questo file ha priorità maggiore e può permettere di evitare l'edit ai file presenti nelle cartelle; comunque sia, il file **crontab** può presentarsi in questo modo:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

In questo caso si può operare aggiungendo una riga come mostrato precedentemente oppure entrare nella directory **/etc/cron.d** ed editare il file **mrtg** la cui direttiva interna si dovrebbe originariamente presentare in modo simile:

```
*/5 * * * * root /usr/bin/mrtg /etc/mrtg/mrtg.cfg --lock-file /var/lock/mrtg/mrtg_l --confcache-file /var/lib/mrtg/mrtg.ok
```

la modifica consiste essenzialmente nell'editare in modo opportuno la direttiva, commentando l'originale ed inserendo le solite due direttive se s'è deciso di non modificare il file **crontab**, permettendo così l'esecuzione dei file di configurazione:

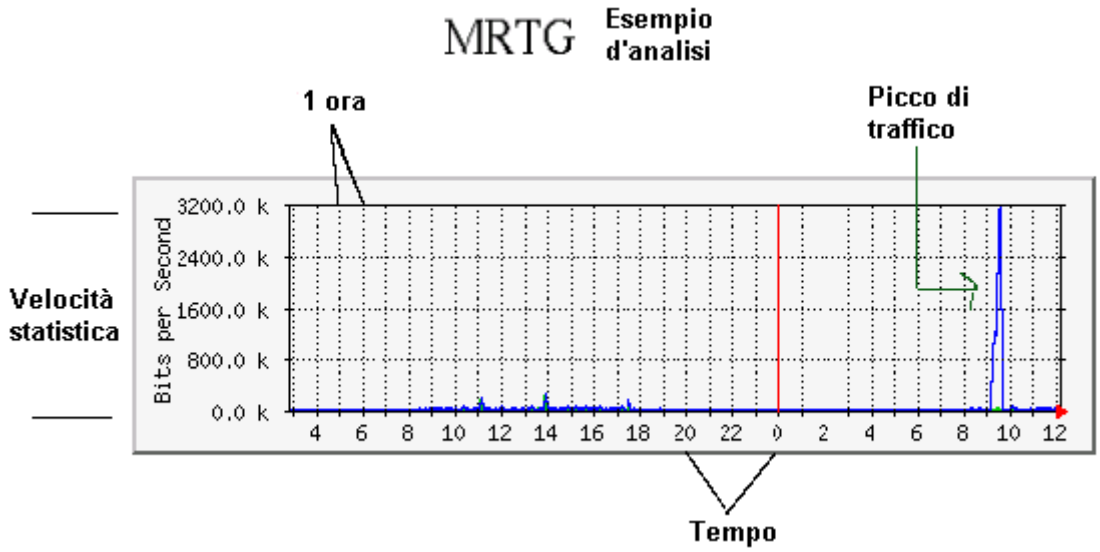
```
# */5 * * * * root /usr/bin/mrtg /etc/mrtg/mrtg.cfg --lock-file /var/lock/mrtg/mrtg_l --confcache-file /var/lib/mrtg/mrtg.ok
*/5 * * * *  root  /usr/bin/mrtg  /etc/mrtg/mrtg1.cfg
*/5 * * * *  root  /usr/bin/mrtg  /etc/mrtg/mrtg2.cfg
```

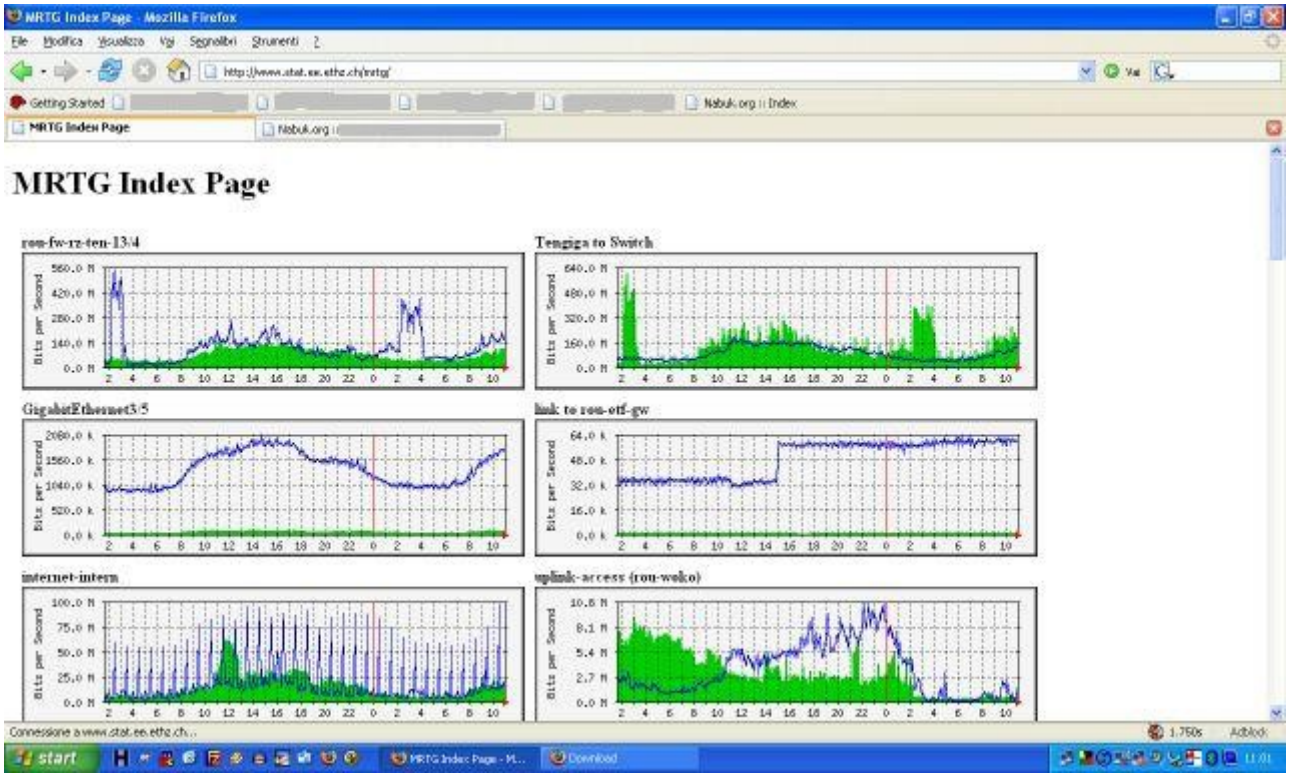
Generare un file di indice “index.html” per gli apparati da monitorare dando il comando:

| **$indexmaker /etc/mrtg/mrtg1.cfg /etc/mrtg/mrtg2.cfg > /var/www/mrtg/index.html** [invio] |
|---|

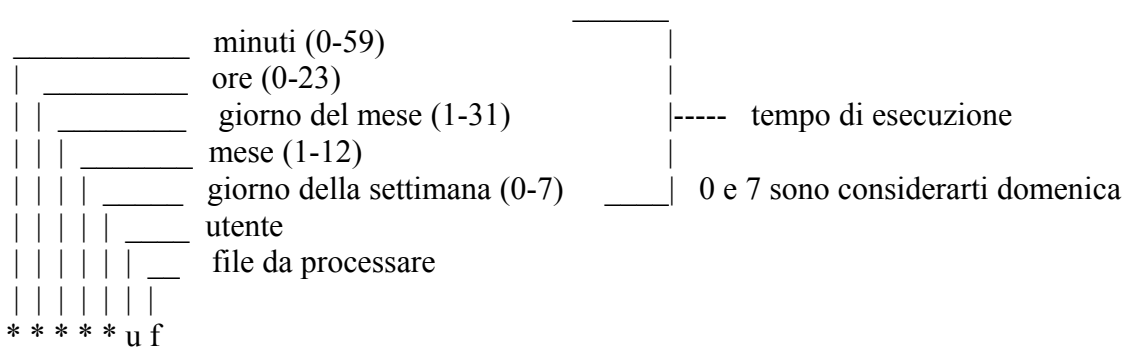
la sintassi generica di indexmaker è “**indexmaker --output=filename device1 device2 ecc**“ ma bisogna considerare che a causa di un non precisato problema dovuto allo stesso, si dovranno correggere nel file index.html generato, i link che puntano ai grafici. Se si desidera rendere visibili i grafici ottenuti ad altri computer in rete, è bene utilizzare quanto descritto nel punto **C**.

**E)** Nelle figure a seguire è possibile vedere un esempio di grafico d’analisi generato da MRTG e dell’indice generale di più apparati. Il monitoraggio della rete permette di rilevare il traffico anomalo generato da un eventuale “intruso”.



**NOTE 1:** i file di cron hanno una sintassi logica del tipo numeri, utente e comando da processare:




Come nel caso del file mrtg.cfg, se un comando dev'essere processato ogni 5 minuti, si inserirà il valore "*/5" nel campo dei minuti e lasciando gli asterischi negli altri. Nel caso in cui si desidera processare un file in due giorni specifici e ad una determinata ora (ad esempio per un backup nei giorni 10 e 20, alle ore 12.30), è possibile inserire nel campo relativo i due giorni separati da una virgola: 30 12 10,20 * * u f. Specificando "root" nel campo utente, il file verrà processato anche se l'utente che usa il computer è diverso.

**NOTE 2:** dando il comando "cfgmaker", MRTG acquisisce le informazioni di configurazione per l'interfaccia ethernet e di loopback (chiamata pseudo-ethernet) del dispositivo da monitorare. Tutto ciò si traduce in due gruppi di grafici per dispositivo. Il gruppo che più interessa è quello relativo alla sola interfaccia ethernet, identificabili dalla sintassi **(indirizzo IP)_1-xxx.html**, mentre quelli di loopback usano la sintassi **(indirizzo IP)_2-xxx.html**. Per evitare confusione e migliorare la semplicità di lettura, è utile editare il file di configurazione ***mrtg.cfg*** in modo che il programma non tenga conto dell'interfaccia di loopback; basterà rimuovere o commentare (aggiungendo il carattere # all'inizio di ogni riga) la parte di codice interessata (tutto il codice relativo alla **Interface 2**), come mostrato nell'esempio di seguito:

```
# Created by
# /usr/bin/cfgmaker OutsideG@192.168.0.50 --global 'WorkDir: /var/www/mrtg/1'
### Global Config Options
#  for UNIX
# WorkDir: /home/http/mrtg
#  or for NT
# WorkDir: c:\mrtgdata
### Global Defaults
#  to get bits instead of bytes and graphs growing to the right
# Options[_]: growright, bits

EnableIPv6: no

######################################################################
# System: WiFiG
# Description: USR 5450
# Contact: server
# Location: USR-5450 (ext)
######################################################################

### Interface 1 >> Descr: 'brecis-msp-ethernet-driver' | Name: '' | Ip: '192' | Eth: '00-c0-49-da-db-45' ###

Target[192.168.0.50_1]: 1:OutsideG@192.168.0.50:
SetEnv[192.168.0.50_1]: MRTG_INT_IP="192" MRTG_INT_DESCR="brecis-msp-ethernet-driver"
MaxBytes[192.168.0.50_1]: 12500000
Title[192.168.0.50_1]: Traffic Analysis for 1 -- WiFiG
PageTop[192.168.0.50_1]: <H1>Traffic Analysis for 1 -- WiFiG</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>WiFiG in USR-5450 (ext)</TD></TR>
   <TR><TD>Maintainer:</TD> <TD>server</TD></TR>
   <TR><TD>Description:</TD><TD>brecis-msp-ethernet-driver  </TD></TR>
   <TR><TD>ifType:</TD>     <TD>ethernetCsmacd (6)</TD></TR>
   <TR><TD>ifName:</TD>     <TD></TD></TR>
   <TR><TD>Max Speed:</TD>  <TD>12.5 MBytes/s</TD></TR>
   <TR><TD>Ip:</TD>         <TD>192 ()</TD></TR>
 </TABLE>


### Interface 2 >> Descr: 'loopback-(pseudo-ethernet)' | Name: '' | Ip: '' | Eth: '4c-50-42-41-43-4b' ###

# Target[192.168.0.50_2]: 2:OutsideG@192.168.0.50:
# SetEnv[192.168.0.50_2]: MRTG_INT_IP="" MRTG_INT_DESCR="loopback-(pseudo-ethernet)"
# MaxBytes[192.168.0.50_2]: 1250000
# Title[192.168.0.50_2]: Traffic Analysis for 2 -- WiFiG
# PageTop[192.168.0.50_2]: <H1>Traffic Analysis for 2 -- WiFiG</H1>
# <TABLE>
#   <TR><TD>System:</TD>     <TD>WiFiG in USR-5450 (ext)</TD></TR>
#   <TR><TD>Maintainer:</TD> <TD>server</TD></TR>
#   <TR><TD>Description:</TD><TD>loopback-(pseudo-ethernet)  </TD></TR>
#   <TR><TD>ifType:</TD>     <TD>ethernetCsmacd (6)</TD></TR>
#   <TR><TD>ifName:</TD>     <TD></TD></TR>
#   <TR><TD>Max Speed:</TD>  <TD>1250.0 kBytes/s</TD></TR>
# </TABLE>

WorkDir: /var/www/mrtg/1
```

Si consiglia tuttavia di rimuovere la parte di codice non interessata, in modo d'avere un file di configurazione "pulito", favorendo così una rapida verifica delle impostazioni.

**NOTE 3:** In sintesi, se si vuole modificare la configurazione, è utile conoscere la struttura generale dei parametri principali:

- **WorkDir: /directory/di/lavoro** specifica quale directory dev'essere usata per salvare i dati e le immagini generate;
- **HtmlDir, ImageDir, LogDir, IconDir** si utilizzano se si vogliono tenere separate le directory dei files html, le immagini, i file di log e le icone;
- **Refresh: x** viene usato per inserire nelle pagine html la direttiva di refresh, in modo da forzare il browser a ricaricare la pagina dopo "x" secondi;
- **Interval: x** specifica ogni quanti minuti deve avvenire la misurazione. Il valore minimo, che è anche quello di default, è 5 minuti;
- **Language: italian** indica in quale lingua devono essere presentati i messaggi di MRTG. Nella directory ***translate*** sono disponibili le traduzioni in diversi linguaggi;
- **RunAsDeamon: Yes/No** indica se deve girare continuamente in background, aggiornando i dati con frequenza stabilita da parametro "interval". Se settato su "No", andrà eseguito ad intervalli regolari via ***cron***;
- **Target[nome]: N_Interfaccia:Community@Indirizzo** viene indicato cosa va letto e da dove;
- **MaxBytes[nome]: xxx** specifica il valore massimo che dev'essere restituito. Serve per determinare la scala del grafico. E' possibile indicare due valori (MaxBytes1 e MaxBytes2) in caso di connessioni sbilanciate, classico nelle connessioni xDSL;
- **Title[nome]: xxx** opzione obbligatoria dove si inserisce la descrizione sintetica del grafico, che apparirà nella pagina generata;
- **PageTop[nome], PageFoot[nome]:** testo in formato HTML che si inserirà in testa e in fondo alla pagina generata;
- **Background[nome]:** il colore dello sfondo in formato HTML (#RRGGBB);
- **YTics[nome]:** indica il numero delle linee orizzontali di riferimento. Di default sono 4;
- **YLegend[nome], ShortLegend[nome], Legend[nome]:** modifica il testo della legenda;
- **Factor[nome]: x** moltiplica tutti i numeri visualizzati sotto il grafico per il fattore "x";
- **YSize[nome], XSize[nome]:** sono le dimensioni in pixel delle immagini. Di default sono 100x400 ed è possibile specificarle da un minimo di 20 ad un massimo di 600;
- **Options[nome]: valore** permette di abilitare o disabilitare per ogni grafico molte opzioni:
  con **growright** si ribalta l'asse orizzontale in modo che il grafico si sviluppa da sinistra verso destra. Di default si sviluppa da destra verso sinistra;
  con **bits/perminute/perhour** si moltiplica per 8, per 60 o per 3600 i valori misurati. Utile per esprimere i valori in bits/secondo, per minuto o per ora;
  con **transparent** lo sfondo delle immagini è trasparente anziché bianco;
  con **gauge** si stabilisce che i dati rilevati sono assoluti e che vanno rappresentati come tali, contrariamente al settaggio di default che li tratta come valori incrementali e che per la rappresentazione viene usata la differenza tra l'ultimo rilevato ed il precedente;
  con **Absolute** si azzera il valore dopo ogni lettura;
  con **Unknaszero** se una lettura fallisce si forza un valore a "zero", contrariamente al comportamento di default che ripetere l'ultimo valore conosciuto. Ciò crea un'interruzione nel grafico. L'uso di questa funzione è da valutare con accuratezza poiché crea difficoltà d'interpretazione;
  con **pngdate** si inserisce un "timestamp" nel grafico, includendo anche la "timezone";
  con **noinfo/nopercent/noborder/noarrow/nobanner/nolegend/noi/noo** si disattivano le informazioni di sistema (uptime, system location), le percentuali di utilizzo, la sfumatura del bordo, la freccia indicante il verso, la legenda, la visualizzazione di una delle due variabili.

Alcuni esempi di quanto spiegato potrebbero essere le seguenti sintassi:

```
WorkDir: /var/www/mrtg
RunAsDeamon: Yes
Interval: 10
Language: italian
Target[pc1]: ifInErrors.1&ifOutErrors.1:public@192.168.0.1
MaxBytes[pc1]: 1250000
Title[pc1]: Errori In-Out


Options[memory]: growright, gauge, pngdate
Options[adsl]: bits, transparent
```

### 8.3 Esagerare con MRTG configurando SNMP

MRTG è un programma talmente versatile che lo si può utilizzare per monitorare anche il web-server Apache, le interfacce ethernet e molti altri dispositivi che probabilmente non fanno uso di SNMP. Si proceda comunque a piccoli passi, in modo da rendere la pagina delle statistiche completa ed esauriente nei dettagli… fare gli "sboroni" a volte fa piacere, ma non montiamoci la testa! Attraverso qualche passaggio aggiuntivo di configurazione, è possibile ottenere risultati soddisfacenti anche per un utente neofita attraverso la configurazione del demone ***SNMP***. Aprire il file ***/etc/snmp/snmpd.conf*** con l'editor di testo preferito e senza spaventarsi per la mole di informazioni ed impostazioni presenti, decommentare la riga:

```
com2sec readonly default public
```

è comunque possibile apportare numerose modifiche al file di configurazione per adattarlo alle proprie esigenze ed un aiuto valido "di massima" viene offerto da uno script Perl chiamato ***snmpconf***. Per lo scopo che attualmente interessa, non occorre altro e quindi si può procedere al suo riavvio dando da shell il comando:

```
$/etc/init.d/snmpd restart [invio]
```

Attraverso il centro di controllo dei servizi, è altresì opportuno fare in modo che il demone parta automaticamente ogni volta che il server viene avviato. Ora si è pronti per creare i file di configurazione di MRTG per ogni dispositivo o funzione interessata, saltando la configurazione offerta dallo script e descritta di seguito…
Dalla shell con privilegi di root dare il comando:

```
$snmpconf –g [invio]
```

che funzionando come un wizard, creerà i file di configurazione necessari semplicemente rispondendo alle domande proposte. In particolare, la configurazione di ***snmpd.conf***, si riassume in quattro sezioni principali e cioè:

1. **Informazioni del sistema:** contiene informazioni logistiche come la persona da contattare, la località fisica dove si trova il computer ed informazioni tecniche;
2. **Controllo degli accessi:** prevede la possibilità di limitare l'accesso in lettura o in scrittura di determinate informazioni SNMP solo ad utenti specifici. Se viene usato SNMP v1, la limitazione viene autenticata tramite la Community; Se viene usato SNMP v2-3, l'autenticazione avverrà tramite la giusta combinazione di Utente, Password e Community.
3. **Destinazione delle notifiche (TRAP):** qui si inseriscono gli indirizzi a cui inviare le TRAP generate. Se la raccolta avviene dallo stesso computer, è possibile inserire ***localhost*** e si dovrà avviare il servizio ***snmptrapd***.
4. **Monitoraggio delle risorse:** questo passaggio è specifico per ***net-snmp*** ed è in grado di controllare alcuni aspetti della macchina su cui gira, generando TRAP o rispondendo a richieste SNMP secondo i seguenti aspetti principali:
   A) **Numero di processi:** dov'è possibile scegliere il nome di un processo (come httpd), specificandone il numero minimo e massimo delle istanze in esecuzione;
   B) **Spazio disponibile nelle partizioni:** è possibile scegliere un punto di mount da controllare, dicendo al demone di segnalare se lo spazio libero disponibile scende al di sotto di un certo valore;

C) **Load average:** è possibile fissare una soglia massima per ogni valore del carico medio del sistema (1 minuto, 5 minuti, 15 minuti);
D) **Dimensione dei file:** è possibile specificare uno o più file con relativa dimensione massima in byte. Se questa dimensione viene superata, il demone manderà un avviso.

Terminata la configurazione, lo script avvertirà in quale posizione è stato salvato il file snmp.conf che andrà spostato in ***/etc/smnp*** e riavviando il demone come mostrato in precedenza. E' utile ricordare che per configurazioni approfondite è bene affidarsi al manuale di snmpd.

Se si è disposti a perderci un po' di tempo oppure si preferisce il "fai da te", per approfondire le conoscenze, è comunque possibile affidarsi alla modifica manuale del file di configurazione. Utilizzare l'editor di testo preferito ed aprire il file **/etc/snmp/snmpd.conf**. Dopo la sua modifica di base, dovrebbe apparire simile all'esempio che segue:

```
# First, map the community name "public" into a "security name"
#          sec.name source   community
com2sec public    default   public

# Second, map the security name into a group name.
#          groupName      securityModel    securityName
group    public           v1               public
group    public           v2c              public
group    public           usm              public

# Third, create a view for us to let the group have rights to:
#          name     incl/excl subtree   mask(optional)
view       all      included .1

# Finally, grant the group read-only access to the systemview view.
#          group    context  sec.model         sec.level prefix  read     write    notif
access     public   ""       any               noauth    exact   all      all      all

# System contact information

syslocation        xxxxxxxx
syscontact         me@host
```

Alcune volte può accadere che sebbene le impostazioni siano giuste, non si abbia risposta del/i dispositivi controllati: è bene fare attenzione alle impostazioni di un eventuale firewall interposto poiché il demone SNMP utilizza la porta 161/UDP per l'ascolto, mentre SNMPTrap utilizza la porta 162/UDP.
Una verifica veloce delle impostazione effettuate è quella di dare da shell il comando:

```
$snmpget –v1 –c COMMUNITY localhost IF-MIB::ifInOctests.1  [invio]
```

naturalmente dove "community" e "localhost" bisognerà sostituire quanto inserito nelle impostazioni. Se tutto è andato a buon fine, si otterrà come risposta i byte in ingresso sulla prima interfaccia di rete, solitamente quella di LoopBack (127.0.0.1).

### 8.3.1 Usare MRTG per monitorare Apache:

Finora abbiamo usato il webserver per rendere disponibile i grafici generati da MRTG ed è possibile estendere le sue funzionalità per ottenere graficamente i dettagli di carico delle chiamate, del processore ed altro. Affinché funzioni, è necessario che sia presente il modulo ***MOD_STATUS*** di Apache, il pacchetto ***apache.mrtg.tgz*** (usate un motore di ricerca per trovarlo) e le librerie ***libwww-perl***. Si tenga presente che sul server preso in esame, gira la distribuzione GNU/Linux Fedora Core 3, ma è pur sempre possibile apportare le dovute modifiche per l'impiego in altre distribuzioni, utilizzando un indirizzo IP 192.168.0.100.

**Configurazione di Apache**:

Abilitare nella configurazione di Apache il mod_status, assicurandosi della presenza nel file ***/etc/httpd/httpd.conf*** delle seguenti direttive:

```
ServerSignature On
AddModule mod_status.c
SetHandler server-status
Order deny,allow
Deny from all
Allow from 127.0.0.1
```

Riavviare Apache dando da shell il comando: **/etc/init.d/httpd reload**.
Se mrtg gira su un'altra macchina, inserire l'indirizzo IP nella direttiva ***Allow from***. E' anche possibile indicare gli host abilitati ad accedere al server-status. Se ad esempio la macchina dove gira MRTG ha indirizzo IP 192.168.0.10, inseriremo questo valore e si dovrà accertare il corretto funzionamento dell'autorizzazione immettendo nel browser dell'host l'indirizzo:

**http://192.168.0.100/server-status?auto**

**Configurazioni di apache.mrtg**:

Creare una cartella in ***/var/www/mrtg/*** chiamata server. Scaricare il pacchetto apache.mrtg.tgz e decomprimerlo in una directory a scelta, per esempio in ***/usr/src/apache.mrtg/*** dove si modificherà:

file **batch:**

```
#!/bin/sh
# batch file to create N sites ...
BATCHBIN="./mkapachemrtg.sh"
$BATCHBIN nome_del_server     "-url http://192.168.0.100/server-status?auto"
```

file **mkapachemrtg.sh:**

```
HTMLHOME="/var/www/mrtg/server"   # dove mrtg crea i grafici
SCRIPTHOME="/usr/src/apache.mrtg"   # dove c'è il file apache.mrtg.pl
URLHOME="http://192.168.0.100/mrtg/" # url ...
CONFHOME="/usr/src/apache.mrtg"      # dove c'è il file apache.mrtg.cfg
MRTGBIN="/usr/bin/mrtg"              # percorso del binario di mrtg
```

Salvare tutte le modifiche e provare ad eseguire dalla shell ***apache.mrtg.pl*** per verificare che legga correttamente il valore SERVERS:

**$./apache.mrtg.pl -url http://192.168.0.100/server-status?auto -info SERVERS** [invio]

se il computer risponderà similmente a quanto segue, allora le impostazioni eseguite sono corrette:

**BusyServers: 1**
**IdleServers: 0**

Se il comando non va a buon fine, il problema è dovuto dalla mancanza del modulo perl ***LWP/Simple.pm***.Installare il modulo con:

**#tar -zxvf libwww-perl-x.y.tar.gz** [invio]
**#perl Makefile.pl && make && make check && make install** [invio]

Ora possiamo eseguire il file ***batch*** dando da shell il comando:

**$./batch** [invio]

il server ci informerà su ciò che sta eseguendo:

**[...] now add this to your crontab**
***/5 * * * * /usr/bin/mrtg //nome_del_server.apache.mrtg.cfg**
**[...]**

Per aggiungere le linee di codice basta dare da shell il comando:

**$crontab -e** [invio]

Ora è tutto pronto e l'aggiornamento avverrà ogni 5 minuti. Per visionare i grafici, puntare il proprio browser all'indirizzo:

***http://192.168.0.100/mrtg/nome_del_server/apache.html***

Se preferite, è possibile creare le opportune modifiche al file **/var/www/mrtg/index.html** creato in precedenza per i dispositivi wireless, inserendo un link a questa pagina, affinché tutti i grafici siano disponibili in modo orinato da una sola pagina.

**NOTE e CONSIDERAZIONI:** durante i test, ho notato che bisogna prestare molta attenzione ai riferimenti alle cartelle usate e che saltuariamente lo script fallisce nelle configurazioni. Ho perciò optato per una configurazione di tipo "manuale" che mi ha permesso di capire come funziona lo script stesso. Se optate per questo tipo di configurazione, oltre a permettere una maggiore flessibilità di configurazione evitando di avviare i file **batch** e **mkapachemrtg.sh**. si otterrà maggiore semplicità inserendo i file decompressi nelle rispettive cartelle e precisamente:

- il file ***sample_apache.mrtg.cfg*** in ***/etc/mrtg***.
- il file ***apache.mrtg.pl*** in ***/usr/local/bin***.
- creare una sottocartella cartella chiamata ***srvstat*** in ***/var/www/mrtg*** nella quale andranno create ulteriori sottocartelle, tante quanti sono i server da monitorare, a cui si darà per semplicità lo stesso nome del server monitorato.
- i file **batch** e **mkapachemrtg.sh** si possono eliminare.

Utilizzando il file d'esempio **sample_apache.mrtg.cfg** fornito con il pacchetto, è possibile apportare le modifiche necessarie direttamente al file stesso, che dovrà essere salvato con il nome **server.apachemrtg.cfg** oppure **apachemrtg.cfg** se il server Apache da monitorare è uno solo. I presupposti per la modifica sono pochi e prevedono di sostituire i richiami ai file ed alle directory di lavoro con i percorsi completi e cioè:

***- %%HTMLHOME%%***: sostituire con il percorso alla directory dove si genereranno i grafici. Nel nostro esempio è da sostituire con ***/var/www/mrtg/srvstat/nome_server***.
***- %%SERVER%%***: sostituire con il nome del server monitorato.
***- %%SCRIPTHOME%%***: sostituire con il percorso al file ***apche.mrtg.pl***, in questo caso si sostituisce con ***/usr/local/bin/apache.mrtg***.
***- %%URLSTATUS%%***: sostituire con ***–url*** seguito dall'indirizzo completo del server e la direttiva di chiamata generica. Utilizzando il server preso in esame si dovrà perciò inserire la direttiva ***-url http://192.168.0.100/server-status?auto***.

Per aiutare a capire dove effettuare le modifiche è riportato di seguito il listato del file ***sample_apache.mrtg.cfg*** suddiviso nelle sue sezioni principali:

```
# - 25/08 changed MaxBytes[apache.tkbytes] to 1000000000000 (to apache.org work)

WorkDir: %%HTMLHOME%%
Refresh: 300
Interval: 5
Options[^]: growright, noinfo, integer, nobanner, gauge, nopercent
PageTop[^]: <H1>%%SERVER%% Apache</H1>
Title[^]: %%SERVER%% Apache
Legend3[^]: Maximal 5 Minute
Legend4[^]: Maximal 5 Minute
LegendI[^]:
LegendB[^]:
#Target[^]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%%
XSize[_]: 600
YSize[_]: 100
WithPeak[_]: ymw

###############################################################

Target[apache.cpuload]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info CPULOAD`
PageTop[apache.cpuload]: <H1>CPULoad</H1>
Title[apache.cpuload]: CPULoad
MaxBytes[apache.cpuload]: 100
Unscaled[apache.cpuload]: ymwd
Options[apache.cpuload]: nopercent, noo
LegendI[apache.cpuload]: CPULoad:
Ylegend[apache.cpuload]: %
ShortLegend[apache.cpuload]: %
Legend1[apache.cpuload]: CPULoad
Legend3[apache.cpuload]: CPULoad

#-

Target[apache.taccesses]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info
TACCESSES`
Options[apache.taccesses]: noo
PageTop[apache.taccesses]: <H1>Total: Accesses</H1>
Title[apache.taccesses]: Total: Accesses
MaxBytes[apache.taccesses]: 1000000000
AbsMax[apache.taccesses]: 1000000000000000
LegendI[apache.taccesses]: TAccesses:
YLegend[apache.taccesses]: TAccesses
kilo[apache.taccesses]: 1000
ShortLegend[apache.taccesses]: Hits
Legend1[apache.taccesses]: Total Accesses
Legend3[apache.taccesses]: Hits
kMG[apache.taccesses]: H ,
```

```
#-

Target[apache.tkbytes]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info TKBYTES`
Options[apache.tkbytes]: noo
PageTop[apache.tkbytes]: <H1>Total: kBytes</H1>
Title[apache.tkbytes]: Total: kBytes
MaxBytes[apache.tkbytes]: 1000000000
AbsMax[apache.tkbytes]: 1000000000000000
LegendI[apache.tkbytes]: TkBytes:
YLegend[apache.tkbytes]: TkBytes
kilo[apache.tkbytes]: 1024
ShortLegend[apache.tkbytes]: Bytes
Legend1[apache.tkbytes]: Total kBytes
Legend3[apache.tkbytes]: kBytes
kMG[apache.tkbytes]: k, M, G, T, Z

#-

Target[apache.uptime]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info UPTIME`
Options[apache.uptime]: noo, nopercent
PageTop[apache.uptime]: <H1>Uptime</H1>
Title[apache.uptime]: Uptime
MaxBytes[apache.uptime]: 1000000000
LegendI[apache.uptime]: Uptime:
YLegend[apache.uptime]: Uptime
ShortLegend[apache.uptime]: days
Legend1[apache.uptime]: Days Alive
Legend3[apache.uptime]: Days Running
kilo[apache.uptime]: 1000

#-

Target[apache.reqpersec]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info
REQPERSEC`
Options[apache.reqpersec]: noo
PageTop[apache.reqpersec]: <H1>Requests per second</H1>
Title[apache.reqpersec]: Requests per second
MaxBytes[apache.reqpersec]: 1000000000
LegendI[apache.reqpersec]: ReqPerSec:
YLegend[apache.reqpersec]: ReqPerSec
ShortLegend[apache.reqpersec]: Reqs/s
Legend1[apache.reqpersec]: Requests per second
Legend3[apache.reqpersec]: Hits per second
kilo[apache.reqpersec]: 1000

#-

Target[apache.bytespersec]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info
BYTESPERSEC`
Title[apache.bytespersec]: Bytes per second
MaxBytes[apache.bytespersec]: 1000000000
YLegend[apache.bytespersec]: BytesPerSec
Options[apache.bytespersec]: noo, nopercent
PageTop[apache.bytespersec]: <H1>Bytes per second</H1>
kMG[apache.bytespersec]: B, K , M, G, T
Legend1[apache.bytespersec]: Bytes per second
Legend3[apache.bytespersec]: N*8bits per second
LegendI[apache.bytespersec]: BPS:
Kilo[apache.bytespersec]: 1024
```

```
#-

Target[apache.bytesperreq]: `%%SCIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info
BYTESPERREQ`
Title[apache.bytesperreq]: Bytes per request
MaxBytes[apache.bytesperreq]: 1000000000
YLegend[apache.bytesperreq]: BytesPerReq
Options[apache.bytesperreq]: noo
PageTop[apache.bytesperreq]: <H1>Bytes per request</H1>
ShortLegend[apache.bytesperreq]: B/req
Legend1[apache.bytesperreq]: Bytes per request
Legend3[apache.bytesperreq]: Bytes by request
LegendI[apache.bytesperreq]: BPR:
kMG[apache.bytesperreq]: , k, M, G, T
Kilo[apache.bytesperreq]: 1024

#-

Target[apache.busyservers]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info
BUSYSERVERS`
Options[apache.busyservers]: noo
Title[apache.busyservers]:   Busy Servers
PageTop[apache.busyservers]: <H1>Busy Servers</H1>
MaxBytes[apache.busyservers]: 1000000000
YLegend[apache.busyservers]: BusyServers
ShortLegend[apache.busyservers]: BServers
Legend1[apache.busyservers]: Busy Workers
Legend3[apache.busyservers]: Workers Alive
LegendI[apache.busyservers]: BWorkers:

#-

Target[apache.idleservers]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info
IDLESERVERS`
Options[apache.idleservers]: noo
Title[apache.idleservers]: Idle Servers
MaxBytes[apache.idleservers]: 1000000000
YLegend[apache.idleservers]: IdleServers
PageTop[apache.idleservers]: <H1>Idle Servers</H1>
ShortLegend[apache.idleservers]: IServers
Legend1[apache.idleservers]: Idle Workers
Legend3[apache.idleservers]: Dead Workers
LegendI[apache.idleservers]: IWorkers:

#-

Target[apache.servers]: `%%SCRIPTHOME%%/apache.mrtg.pl %%URLSTATUS%% -info SERVERS`
Options[apache.servers]: nopercent, integer
Title[apache.servers]: Child Status
MaxBytes[apache.servers]: 1000000000
YLegend[apache.servers]: ServStatus
LegendI[apache.servers]: BServers:
LegendO[apache.servers]: IServers:
ShortLegend[apache.servers]: Workers
PageTop[apache.servers]: <H1>Child Status</H1>
Legend1[apache.servers]: Busy Workers
Legend2[apache.servers]: Idle Workers
Legend3[apache.servers]: Busy Workers
Legend4[apache.servers]: Idle Workers
```

Effettuate le modifiche e salvato il file come spiegato sopra, creare una cartella con il nome del server in ***/var/www/mrtg/server***. Dalla shell con privilegi di root daremo, per creare i grafici una prima volta, il seguente comando:

**$env LANG=C /usr/bin/mrtg  /etc/mrtg/server.apachemrtg.cfg** [invio]

aprire con un editor di testo il file di cron in **/etc/crontab** ed aggiungere la direttiva:

**#*/5 * * * *  root  /usr/bin/mrtg  /etc/mrtg/server.apachemrtg.cfg**

salvare le modifiche ed uscire dall'editor. Per finire, occorre generare un bel file di indice chiamato apache_server.html, dando da shell il comando:

**$indexmaker /etc/mrtg/server.apachemrtg.cfg > /var/www/mrtg/srvstat/nome_server /apache.html** [invio]

Per semplicità di consultazione, è opportuno editare la pagina di indice di MRTG creata nei paragrafi precedenti affinché contenga un link alla pagina apache.html.

### 8.3.2 Monitorare le schede di rete del server senza SNMP

Monitorare le schede ethernet presenti nel server, non è sempre cosa facile ed effettivamente é meglio utilizzare delle chiamate al "demone" SNMP. Esiste tuttavia un modo semplice e veloce per fare quanto voluto, grazie ad uno script di configurazione un po' particolare che andrà salvato in ***/etc/mrtg/***. Si ricorda che per poter processare tale file, andrà aggiunta in ***/etc/crontab*** la riga:

```
*/10 * * * * root /usr/bin/mrtg /etc/mrtg/eth0.cfg
```

Lo script utilizza la directory ***/var/www/mrtg/eth0*** per inserire i grafici perciò è bene crearla prima di eseguirlo in automatico ogni 10 minuti.

Di seguito è mostrato il listato del file ***eth0.cfg***:

```
WorkDir: /var/www/mrtg/eth0

# "sar" sembra essere eseguito ogni 10 minuti
# settare l'interval a 10

Interval: 10

Target[eth0]: `perl -e '@a=split(/[:\s]+/,qx(grep eth0 /proc/net/dev));$f="%.0f";$fmt="$f\n
$f\n1\neth0 traffic\n";$s=sprintf $fmt,$a[2],$a[10];print $s; print STDERR $s;'`;
Options[eth0]: noinfo, growright, transparent, dorelpercent
MaxBytes[eth0]: 12500000
# MaxBytes2[eth0]: 12500000
# AbsMax[eth0]: 12500000
kilo[eth0]: 1024
YLegend[eth0]: Bytes al secondo (B/s)
ShortLegend[eth0]: B/s
Legend1[eth0]: Traffico in ingresso B/s
Legend2[eth0]: Traffico in uscita B/s
Legend3[eth0]: Picco in ingresso ogni 10 minuti
Legend4[eth0]: Picco in uscita ogni 10 minuti
LegendI[eth0]:  In:
LegendO[eth0]:  Out:
Timezone[eth0]: GMT
Title[eth0]: Server - Analisi del traffico su eth0
PageFoot[eth0]: Contattare amministratore per maggiori informazioni<p>
PageTop[eth0]: <H1>Server - Analisi del traffico su eth0</H1>
################################################################################
```

Per semplicità di consultazione, è opportuno editare la pagina di indice di MRTG creata nei paragrafi precedenti affinché contenga un link alla pagina di monitoraggio del dispositivo di rete.
La stessa logica è da utilizzare per monitorare le altre ethernet (eth1, eth2, …), ppp (ppp0, …), apportando le dovute modifiche e generando un file per ogni dispositivo.

### 8.3.3 Monitorare le schede di rete del server con SNMP

Monitorare le schede di rete del server utilizzando una chiamata specifica al demone SNMP è discretamente semplice. Il file di configurazione ***ethx.cfg*** può essere generato come se si trattasse di un apparato esterno, dando il seguente comando da shell con privilegi di root:

**$cfgmaker Community@Indirizo_IP_del_server --global "WorkDir: /var/www/mrtg/ethx" > /etc/mrtg/etx.cfg** [invio]

verranno così acquisite le informazioni per la configurazione e generato il relativo file. Come al solito è utile generare un file di indice col none ethx.html, che andrà linkato alla pagina index.html. Il file di configurazione ***etx.cfg*** generato contiene in linea di massima il seguente codice:

```
EnableIPv6: no
WorkDir: /var/www/mrtg/etx

### Interface 1 >> Descr: 'eth0' | Name: '' | Ip: '192.168.x.x' | Eth: '00-50-xx-xx-xx-xx' ###

Target[localhost_1]: 1:public@localhost:
SetEnv[localhost_1]: MRTG_INT_IP="192.168.x.x" MRTG_INT_DESCR="eth0"
MaxBytes[localhost_1]: 12500000
Title[localhost_1]: Traffic Analysis for 1 – "nome del server"
PageTop[localhost_1]: <H1>Traffic Analysis for 1 – "nome del server"</H1>
<TABLE>
<TR><TD>System:</TD> <TD>"Nome del server"</TD></TR>
<TR><TD>Maintainer:</TD> <TD>Me <io@mail.xxx></TD></TR>
<TR><TD>Description:</TD><TD>eth0 </TD></TR>
<TR><TD>ifType:</TD> <TD>ethernetCsmacd (6)</TD></TR>
<TR><TD>ifName:</TD> <TD></TD></TR>
<TR><TD>Max Speed:</TD> <TD>12.5 MBytes/s</TD></TR>
<TR><TD>Ip:</TD> <TD>192.168.x.x</TD></TR>
</TABLE>

### Interface 2 >> Descr: 'eth1' | Name: '' | Ip: '' | Eth: '00-0b-xx-xx-xx-xx' ###

Target[localhost_2]: 2:public@localhost:
SetEnv[localhost_2]: MRTG_INT_IP="" MRTG_INT_DESCR="eth1"
MaxBytes[localhost_2]: 1250000
Title[localhost_2]: Traffic Analysis for 2 – "Nome del server"
PageTop[localhost_2]: <H1>Traffic Analysis for 2 – Nome del server"</H1>
<TABLE>
<TR><TD>System:</TD> <TD>"Nome del server"</TD></TR>
<TR><TD>Maintainer:</TD> <TD>Me < io@mail.xxx ></TD></TR>
<TR><TD>Description:</TD><TD>eth1 </TD></TR>
<TR><TD>ifType:</TD> <TD>ethernetCsmacd (6)</TD></TR>
<TR><TD>ifName:</TD> <TD></TD></TR>
<TR><TD>Max Speed:</TD> <TD>1250.0 kBytes/s</TD></TR>
</TABLE>
```

Dal listato d'esempio, è stata rimossa la parte di codice riguardante l'interfaccia di loopback, di scarso interesse per lo scopo. E' opportuno dividere il codice in modo da ottenere distinti file di configurazione per ogni adattatore di rete, utilizzanti come workdir una sottocartella diversa. Si dovrà aggiungere la schedulazione per processare i file di MRTG ogni 5 minuti attraverso ***crontab***.

### 8.3.4 Monitorare l'utilizzo delle/a CPU senza SNMP

Un altro grafico di sicuro effetto è quello relativo al monitoraggio della CPU che ai più potrebbe sembrare superfluo… Siccome il computer adibito a piccolo server casalingo utilizza componenti per così dire "di recupero", il monitoraggio della CPU aiuta a prevenire inspiegabili blocchi del sistema, permettendo così un upgrade.
Se si è fortunati e si dispone di un server biprocessore, è possibile, creando un file di configurazione ad-hoc per mrtg, ottenere il risultato desiderato. Si crei la cartella **cpu** in ***/var/www/mrtg*** ed il file ***cpu.cfg*** in ***/etc/mrtg*** con il seguente codice:

```
WorkDir:/var/www/mrtg/cpu

Interval: 10

######################################################################
#                                                                    #
# this is the CPU Utilisation % from sar -U ALL -h                     #
# this is unlikely to work if you only have 1 CPU. Forget fixing it    #
# to work for 1 CPU if you're not a perl regexp guru.                  #
#                                                                    #
######################################################################
#Idle time %= Target[cpu]: `perl -e '$f="%.0f";$fmt="$f\n$f\n1\nCPU Idletime\n";$o=sprintf $fmt,
(qx(sar -U ALL -h | tail -8)=~/cpu0\s+%idle\s+([\d\.]+).*?cpu1\s+%idle\s+([\d\.]+)/sm);print $o; print
STDERR $o'`
Target[cpu]: `perl -e '$f="%.0f";$fmt="$f\n$f\n1\nCPU Idletime\n";($c1,$c2)=(qx(sar -U ALL -h |
tail -8)=~/cpu0\s+%idle\s+([\d\.]+).*?cpu1\s+%idle\s+([\d\.]+)/sm);$c1=1000*(100-$c1);
$c2=1000*(100-$c2);$o=sprintf $fmt,$c1,$c2;print $o; print STDERR $o'`
Options[cpu]: gauge, noinfo, growright, transparent, dorelpercent, nopercent
MaxBytes[cpu]: 100000
YLegend[cpu]: Server - utilizzo CPU
ShortLegend[cpu]: % x 1000
Legend1[cpu]: CPU 0
Legend2[cpu]: CPU 1
Legend3[cpu]: Max 10 Min
Legend4[cpu]: Max 10 Min
LegendI[cpu]:  cpu0:
LegendO[cpu]:  cpu1:
Timezone[cpu]: GMT
Title[cpu]: Server - utilizzo CPU (% x 1000)
PageFoot[cpu]: Qui si possono immettere informazioni aggiuntive personali<p>
PageTop[cpu]: <H1>Server - utilizzo CPU (% x 1000)</H1>
######################################################################
```

Aprire il file ***/etc/crontab*** ed aggiungere la riga necessaria per processare il file:

```
*/10 * * * * root /usr/bin/mrtg /etc/mrtg/cpu.cfg
```

Per semplicità di consultazione, è opportuno editare la pagina di indice di MRTG creata nei paragrafi precedenti affinché contenga un link alla pagina di monitoraggio della CPU. Si tenga presente che questo script è configurato per monitorare due CPU ed occorre una certa conoscenza del Perl per adattarlo…

### 8.3.5 Monitorare l'utilizzo delle/a CPU con SNMP

Utilizzando una specifica chiamata "***Target***" al demone SNMP, è possibile monitorare l'utilizzo del processore. Il file di configurazione di MRTG ***cpu.cfg*** d'esempio utilizza il seguente codice:

```
WorkDir: /var/www/mrtg/cpu
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[server.cpu]:ssCpuRawUser.0&ssCpuRawUser.0:public@127.0.0.1+
ssCpuRawSystem.0&ssCpuRawSystem.0:public@127.0.0.1+
ssCpuRawNice.0&ssCpuRawNice.0:public@127.0.0.1
RouterUptime[server.cpu]: public@127.0.0.1
MaxBytes[server.cpu]: 100
Title[server.cpu]: CPU Load
PageTop[server.cpu]: <H1>Carico della CPU in percentuale</H1>
Unscaled[server.cpu]: ymwd
ShortLegend[server.cpu]: %
YLegend[server.cpu]: Utilizzo CPU
Legend1[server.cpu]: CPU attiva in % (Load)
Legend2[server.cpu]:
Legend3[server.cpu]:
Legend4[server.cpu]:
LegendI[server.cpu]:  Active
LegendO[server.cpu]:
Options[server.cpu]: growright,nopercent
```

Essendo un esempio, si sono utilizzati i valori ***public*** e ***127.0.0.1*** come community ed indirizzo IP. Come si è fatto negli esempi precedenti, si dovrà creare la sottocartella ***cpu*** in ***/var/www/mrtg*** ed aggiungere la riga di schedulazione per processare il file in ***crontab*** ogni 5 minuti.

### 8.3.6 Monitorare l'utilizzo della RAM

Monitorare l'utilizzo della memoria RAM può aiutare a capire il perché ad un certo punto il server "rallenta". Poca memoria a disposizione costringe infatti il sistema operativo a ricorrere allo swap, decisamente più lento perché risiede nel disco rigido. Di seguito è possibile vedere il codice del file di configurazione di MRTG ***ram.cfg***, da salvare come al solito in ***/etc/mrtg***:

```
WorkDir: /var/www/mrtg/ram
LoadMIBs: /usr/share/snmp/mibs/HOST-RESOURCES-MIB.txt
Target[server.mem]: .1.3.6.1.4.1.2021.4.6.0&.1.3.6.1.4.1.2021.4.6.0:public@localhost
PageTop[server.mem]: <H1>Memoria libera</H1>
Options[server.mem]: nopercent,growright,gauge,noinfo
Title[server.mem]: Memoria libera
MaxBytes[server.mem]: 1000000
kMG[server.mem]: k,M,G,T,P,X
YLegend[server.mem]: bytes
ShortLegend[server.mem]: bytes
LegendI[server.mem]:  Memoria libera:
LegendO[server.mem]:
Legend1[server.mem]: Memoria libera in bytes
```

Essendo un esempio, si sono utilizzati i valori ***public*** e ***127.0.0.1*** come community ed indirizzo IP. Come si è fatto negli esempi precedenti, si dovrà creare la sottocartella ***ram*** in ***/var/www/mrtg*** ed aggiungere la riga di schedulazione per processare il file in ***crontab*** ogni 5 minuti; modificare i parametri della community e d'indirizzo IP secondo le necessità.

### 8.3.7 Monitorare l'utilizzo dello SWAP

Monitorare l'utilizzo dello SWAP può aiutare a capire il perché ad un certo punto il server "rallenta". La causa può ricercarsi nella scarsa dotazione di memoria di sistema disponibile, che costringe infatti il sistema operativo a ricorrere allo swap, decisamente più lento della RAM, perché risiede nel disco rigido. Di seguito è possibile vedere il codice del file di configurazione di MRTG ***swap.cfg***, da salvare come al solito in ***/etc/mrtg***:

```
WorkDir: /var/www/mrtg/swap
LoadMIBs: /usr/share/snmp/mibs/UCD-SNMP-MIB.txt
Target[server.swap]: memAvailSwap.0&memAvailSwap.0:public@localhost
PageTop[server.swap]: <H1>Swap</H1>
Options[server.swap]: nopercent,growright,gauge,noinfo
Title[server.swap]: Memoria libera
MaxBytes[server.swap]: 1000000
kMG[server.swap]: k,M,G,T,P,X
YLegend[server.swap]: bytes
ShortLegend[server.swap]: bytes
LegendI[server.swap]:  Memoria libera:
LegendO[server.swap]:
Legend1[server.swap]: Memoria Swap disponibile, in byte
```

Essendo un esempio, si sono utilizzati i valori ***public*** e ***localhost*** come community ed indirizzo IP. Come si è fatto negli esempi precedenti, si dovrà creare la sottocartella ***swap*** in ***/var/www/mrtg*** ed aggiungere la riga di schedulazione per processare il file in ***crontab*** ogni 5 minuti; modificare i parametri della community e d'indirizzo IP secondo le necessità.

### 8.3.8 Monitorare le connessioni TCP aperte

Utilizzando una specifica chiamata "***Target***" al demone SNMP, è possibile monitorare le connessioni TCP aperte verso il server. In questo caso, il file di configurazione di MRTG ***tcp.cfg*** d'esempio utilizza il seguente codice:

```
# tcp connections
WorkDir: /var/www/mrtg/tcp
RunAsDaemon:No
Target[tcpopen]: .1.3.6.1.2.1.6.9.0&.1.3.6.1.2.1.6.9.0:public@localhost
Options[tcpopen]: nopercent,growright,gauge,noinfo
Title[tcpopen]: Connessioni TCP aperte
PageTop[tcpopen]: <H1>Connessioni TCP aperte</H1>
MaxBytes[tcpopen]: 1000000
YLegend[tcpopen]: # conns
ShortLegend[tcpopen]: connessioni
LegendI[tcpopen]: Connessioni:
LegendO[tcpopen]:
Legend1[tcpopen]: Connessioni TCP aperte (lettura ogni 5 minuti)
```

Essendo un esempio, si sono utilizzati i valori ***public*** e ***localhost*** come community ed indirizzo IP. Come si è fatto negli esempi precedenti, si dovrà creare la sottocartella ***tcp*** in ***/var/www/mrtg*** ed aggiungere la riga di schedulazione per processare il file in ***crontab*** ogni 5 minuti; modificare i parametri della community e d'indirizzo IP secondo le necessità.

## 8.4 Autenticazione 802.1x

L'autenticazione dei client e la protezione della rete wireless attraverso i soli servizi offerti dagli access point non sono sufficienti a contrastare un hacker "testardo". Molto si è detto riguardo la (in)sicurezza degli apparati wireless e tutto sommato, in ambito casalingo non conviene esasperare la sicurezza fino a raggiungere livelli paranoici, dopotutto non transitano dati "interessanti"… Discorso diverso è quello aziendale dove una eventuale violazione della rete wireless potrebbe causare un furto di dati importanti e rendere vane alcune strategie aziendali. Come s'è detto più volte in questa guida, la sicurezza di una rete wireless aumenta di efficienza con l'aumentare dei livelli di protezione impiegati. Attingendo dal grande bacino di programmi disponibili nel mondo open source, è possibile realizzare un server affidabile e robusto, in grado di veicolare algoritmi di autenticazione verso un database delle credenziali di tutti gli utenti. Tutto questo è possibile grazie a **FreeRadius** (**Free R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice) prelevabile dal sito ufficiale www.freeradius.org. Sono tuttavia disponibili pacchetti precompilati per la maggior parte delle distribuzioni GNU/Linux ma, l'installazione "manuale" è consigliata partendo dai pacchetti tar.gz attraverso questi semplici passaggi:

```
$tar -xfvz freeardius.x.y.z.tar.gz [invio]
$cd freeradius.x.y.z [invio]
$./configure [invio]
$make [invio]
$make install [invio]
```

L'ubicazione dei file eseguibili, di configurazione e di log, cambia in base alla distribuzione usata ma in linea di massima si può dire che si trovano in ***/etc/raddb*** oppure in ***/etc/freeradius***.
FreeRADIUS possiede file di configurazione terribilmente enormi ma i file rilevanti per il corretto funzionamento sono:

***radiusd.conf***: contiene le direttive di configurazione del server;
***clients.conf***: contiene le informazioni dei client, possono trovarsi anche in radiusd.conf;
***sql.conf***: contiene le informazioni d'accesso al database, può trovarsi anche in radiusd.conf.

Procediamo con ordine ed analizziamo i singoli file di configurazione per meglio capirne il funzionamento delle direttive contenute.
Il file ***radiusd.conf*** è diviso in sezioni la cui struttura è del tipo:

```
[opzioni globali]
modules{

}
authorize{

}
authenticate{

}
accounting{

}
```

Nella sottosezione ***modules*** sono definiti i singoli moduli usati per l'autorizzazione, l'autenticazione e l'accounting. In effetti, nelle sottosezioni **authorize**, **authenticate**, **accounting** contengono i "nomi" dei moduli configurati nella sottosezione precedente.
Se per esempio si vuole implementare il modulo pap per l'autenticazione, il file di configurazione conterrà il seguente codice:

```
...
modules{
   pap {
      encryption_scheme = crypt
   }
}
...
authenticate{
   Auth-Type PAP {
      pap
   }
}
...
```

I moduli a disposizione sono molti ma quelli che generalmente vengono usati sono:

```
modules{
   mschap{
   ...
   }
   ldap{
   ...
   }
   sql{
   ...
   }
}
```

Interessante da notare che il modulo ***sql*** può essere usato in tutte le sottosezioni poiché le informazioni possono essere lette o inserite in un database.
Oltre le sezioni appena viste, in radius.conf, possono essere inserite molte altre opzioni come:

→listen{}: si può inserite informazioni per specificare quale ip e quale porta utilizzare per il bind;
→security{}: impostazioni di sicurezza;
→proxy server{}: impostazioni per il proxing;
→client IPADDRESS{}: vengono specificati i criteri per l'accesso da parte dei vari client;
→tread pool{}: stabilisce il numero di spare server ed il loro comportamento;
→instantiate{}: sezione opzionale che contribuisce al caricamento dei moduli;
→preacct{}: sezione di pre-accounting dove si decide quale tipo di accounting si deve utilizzare;
→session{}: per controllare gli utilizzi simultanei;
→post-auth{}: sezione che viene valutata dopo che l'utente è stato autenticato;
→pre-proxy{}: impostazioni utilizzate per passare richieste autorizzative ad un altro server;
→post-proxy{}: cosa deve fare il server quando riceve un responso di proxing.

Il file ***clients.conf*** contiene le informazioni per i client e si può considerare un'estensione del file radius.conf. Alcune volte questo file non esiste poiché le direttive sono contenute in radius.conf. La configurazione assume la seguente sintassi:

```
client  "indirizzo_IP" {
    secret = testpass
    shortname = localhost
    nastype = other
}
```

Tutti i computer che accedono al server radius devono essere indicati con una direttiva per ogni client. Per il riconoscimento dei client è possibile inserire l'indirizzo IP oppure l'host name. I parametri che seguono invece indicano:

→ **secret**: la password in plaintext che i client dovranno utilizzare per connettersi al server radius, la cui lunghezza massima è di 31 caratteri;
→ **shortname**: utilizzato come alias da sostituire all'hostname o all'indirizzo ip. Questo parametro è obbligatorio;
→ **nastype**: specifica il metodo per comunicare con il NAS. Le opzioni valide sono: cisco, computone, livingston, max40xx, multitech, netserver, pathras, patton, portslave, tc, usrhiper, other.

Per creare un sistema di autenticazione basato su PPPoE + FreeRADIUS + openLDAP è necessario un maggiore dettaglio della configurazione dei moduli mschap, ldap e sql. Un esempio potrebbe essere quello d'utilizzare il protocollo MSCHAP per trasmettere i dati di autenticazione, openLDAP per contenere le informazioni degli utenti ed un database Mysql per archiviare le informazioni di accounting. Si tenga presente che MSCHAP, e soprattutto MSCHAP-V2, è un sistema sufficientemente sicuro per trasmettere le password, diversamente dal PAP con cui le stesse vengono trasmesse in chiaro. Se in aggiunta viene sfruttata una connessione crittografica con il protocollo MPPE, si rende ancora più sicura la transazione. L'esempio di configurazione di questo modulo può essere così realizzata con il seguente codice:

```
mschap {
  authtype = MS-CHAP
  use_mppe = yes
  require_encryption = yes
  require_strong = yes
}
```

Come si può intuire, il modulo viene configurato per chiedere al client di instaurare una connessione con MPPE (use_mppe = yes) in modo obbligatorio (require_encryption=yes) e con chiave a 128 bit (require_strong=yes). E' utile ricordare di controllare se il Linux Kernel, del server e del client, sia compilato (o sia presente il modulo) per gestire connessioni MPPE, altrimenti va patchato. Le principali e recenti distribuzioni GNU/Linux danno la possibilità di impiegare kernel precompilati con il supporto MPPE. Come già detto, il server Radius deve andare a prelevare le informazioni di autenticazione su una directory LDAP, che per esempio può essere costituita dal dominio *mio_dominio.it*. Il codice di configurazione del modulo LDAP assume la seguente sintassi:

```
ldap  {
      server = "localhost"
      identity = "cn=admin,dc=mio_dominio,dc=it"
      password = testpass
      basedn = "ou=people,dc=mio_dominio,dc=it"
      filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
      start_tls = no
      dictionary_mapping = ${raddbdir}/ldap.attrmap
}
```

Dall'analisi del codice si evince che i parametri contenuti assumono il seguente significato:

→ **server**: specifica l'hostname o l'ip address del server LDAP. In questo caso il server LDAP è in esecuzione sulla stessa macchina;
→ **identity**: contiene le informazioni di login per accedere sul server LDAP. Non sempre è indispensabile e dipende dalla configurazione del server LDAP stesso. In questo esempio si accede usando l'identificativo dell'amministratore, ma sarebbe meglio usare un utente apposito (magari chiamato radius) i cui permessi siano strettamente indispensabili per la sua interrogazione;
→ **password**: contiene la password in chiaro dell'utente specificato. Per questa ragione bisogna configurare i permessi del file *radiusd.conf* in modo che sia solo l'utente radiusd a poter accedere in lettura su questo file;
→ **basedn**: contiene il riferimento alla struttura LDAP che contiene i dati degli utenti;
→ filter: effettua la ricerca nella directory LDAP cercando tra i campi uid il valore ricevuto come User-Name;
→ **start_tsl**: la connessione con il server LDAP può essere fatta utilizzando la cifratura TSL. In questo caso, trattandosi della stessa macchina, non è stata utilizzata;
→ **dictionary-mapping**: contiene il path e il nome de file che contiene il dizionario relativo a LDAP. Normalmente fornito nella distribuzione di freeRADIUS.

L'autenticazione ***MS-CHAP*** prevede che sia utilizzata non la password contenuta nell'attributo ***userPassword*** nella directory LDAP, ma la password ***sambaNTPassword***. Per utilizzare questo attributo è necessario aggiungere a openLDAP lo schema fornito con Samba 3. Si ricorda che l'utente impostato in ***identity*** deve poter accedere a questo attributo.
Per poter sfruttare queste opzioni è necessario controllare che nel file **ldap.attrmap** siano presenti le seguenti direttive:

```
checkItem     LM-Password     sambaLMPassword
checkItem     NT-Password     sambaNTPassword
```

Se si è stati bravi nella configurazione a questo punto si hanno tutti gli strumenti per autenticare gli utenti contenuti su una directory LDAP con freeRADIUS. E' possibile inserire le informazioni di accounting su un database mysql. Il modulo per configurare l'accesso ad un database dovrebbe trovarsi in un file chiamato ***sql.conf***, ma è possibile anche inserire il modulo direttamente nel file di configurazione principale... Questo modulo ha molte opzioni, che sono normalmente già presenti file di configurazione fornito con FreeRADIUS. Le parti principali da modificare sono le seguenti:

```
driver = "rlm_sql_mysql"
server = "localhost"
login = "mysql"
password = "mysqlpass"
radius_db = "radius"
```

il significato dei parametri è:

→ **driver**: il driver da utilizzare in base al DBMS impiegato. Le opzioni valide sono: rlm_sql_mysql, rlm_sql_postgresql, rlm_sql_iodbc, rlm_sql_oracle, rlm_sql_unixodbc, rlm_sql_freetds. In questo caso abbiamo deciso di impiegare mysql;
→ **server**: l'hostname o l'ip address del server mysql. In questo caso è in esecuzione sullo stesso computer;
→ **login**: username usato per la connessione con il DBMS;
→ **password**: la password di accesso al DBMS in plaintext;
→ **radius_db**: il nome del database che contiene la tabelle usate da FreeRADIUS;

Per configurare il server FreeRADIUS in modo da autenticare con MSCHAP e LDAP e per loggare l'accountig su mysql il file radiusd.conf assumerà la seguente struttura:

```
...
modules {
  mschap {
    authtype = MS-CHAP
    use_mppe = yes
    require_encryption = yes
    require_strong = yes
  }
  ldap {
    server = "localhost"
    identity = "cn=admin,dc=mio_dominio,dc=it"
    password = testpass
    basedn = "ou=people,dc=mio_dominio,dc=it"
    filter = "(uid=%{Stripped-User-Name:-%{User-Name}})"
    start_tls = no
    dictionary_mapping = ${raddbdir}/ldap.attrmap
  }
  $INCLUDE ${confdir}/sql.conf
}
authorize {
  ldap
  mschap
}
authenticate{
  mschap
}
accounting {
  sql
}
```

Quanto fin qui descritto è da considerarsi una breve sintesi delle opzioni principali di configurazione del file ***radiusd.conf***. Maggiori informazioni sono disponibili nella documentazione ufficiale e fornita con FreeRADIUS sul sito ufficiale.

## 8.5 NAGIOS: controllo completo della (W)LAN

Nagios (www.nagios.org) è un software open source per il monitoraggio dei server e dei servizi di rete. Questo software è molto conosciuto in ambito aziendale ed è utilizzato in molte delle più grandi società in tutto il mondo. NAGIOS è progettato per garantire agli amministratori informazioni costanti sulle prestazioni ed eventuali problemi dei sistemi informatici, prevenendo e riducendo i tempi d'intervento. Funziona in ambiente GNU/Linux e gestisce sistemi di notificazione basati su email, messaggistica web, SMS. I risultati ottenuti dal monitoraggio, sono disponibili attraverso una comoda interfaccia web-based, con la possibilità di gestire delle restrizioni d'accesso. Nagios è un ***heartbeat monitor*** che permette di controllare in realtime qualsiasi sistema predisposto e tra le caratteristiche principali, sono compresi il monitoraggio dei servizi di rete (SMTP, POP3, HTTP, ecc), il monitoraggio delle risorse hardware dei/l server (carico del processore, utilizzo dei dischi e della memoria), di situazioni ambientali (temperatura), la gestione di notifiche differenziate per gruppi e utenti, la produzione di log con notevole livello di dettaglio sulle attività svolte.
Dal sito principale è possibile scaricare sia i sorgenti che la versione pacchettizzata per le principali distribuzioni. E' utile ricordare che il semplice download del file nagios-x.y.z-w.rpm non permette il controllo dei vari dispositivi poiché trattasi del programma principale che si occupa di gestire e generare le pagine web-based con i grafici; è perciò estremamente consigliato anche il download dei ***plug-in***, disponibili anch'essi sia come sorgenti sia in versione pacchettizzata.
Per funzionare correttamente il programma necessita della presenza delle librerie **perl**, **zlib**, **libpng, gd** e del web-server **Apache**.
Creare per prima cosa l'utente ed il gruppo per Nagios e aggiungere al gruppo l'utente *apache*, che deve avere accesso all'interfaccia web del programma. Quest'ultimo utilizzerà i permessi dell'utente/gruppo *apache* durante l'esecuzione, aumentando il grado di sicurezza del sistema. Non è sicuro infatti se Nagios viene eseguito con permessi di root poiché in caso di un exploit ad un suo bug, si riuscirebbe a guadagnare il controllo del sistema. Creando un utente ad-hoc il problema viene notevolmente ridotto… dare perciò in shell i comandi:

```
$adduser nagios [invio]
$/usr/sbin/groupadd nagcmd [invio]
$/usr/sbin/usermod –G nagcmd apache [invio]
$/usr/sbin/usermod –G nagcmd nagios [invio]
```

Creare la directory dove si metterà il programma, settandone i permessi per l'utente sopra creato:

```
$mkdir /usr/local/nagios [invio]
$chown nagios.nagios /usr/local/nagios [invio]
```

Installiamo ora il pacchetto. Di seguito è descritta la procedura d'installazione dai sorgenti, questa va eseguita da shell con permessi di root ed è estremamente banale e ben documentata dal manuale in linea. Scompattare i sorgenti dando da shell il comando:

```
$tar -zxvf nagios-x.y.z.tar.gz [invio]
```

spostarsi nella cartella dei file scompattati, compilarli ed installare il pacchetto con i comandi:

**$./configure –prefix=/usr/local/nagios –with-cgiurl=/nagios/cgi-bin --with-htmurl=/nagios –with-nagios-user=nagios –with-nagios-grp=nagios –with-gd- lib=/usr/local/lib –with-gd-include=/usr/local/include** [invio]
**$make all** [invio]
**$make install** [invio]

è tuttavia possibile usare **./configure** senza parametri aggiuntivi, tenendo in questo caso presente che si dovranno apportare delle modifiche affinché si abbiano direttive coerenti con i percorsi del file-system. Installare lo script che costituisce il demone di Nagios in **/etc/init.d/nagios** , il **command-mode** e la configurazione d'esempio con:

**$make install-init** [invio]
**$make install-commandmode** [invio]
**$make install-config** [invio]

l'ultima istruzione installa i file di esempio di configurazione che serviranno poi per avere una base da cui partire senza riscriverli da zero. Compiute queste prime operazioni, spostandosi nella directory di Nagios (**cd /usr/local/nagios**) ci devono essere altre cinque sottodirectory e precisamente:

***/etc***: contiene il file di configurazione di nagios;
***/var***: la directory dei log;
***/share***: file html per l'interfaccia web e la configurazione di Nagios;
***/bin***: l'eseguibile di Nagios;
***/sbin***: i CGI.

Ora è possibile passare all'installazione dei plug-in che, si ricorda, vanno scaricati e compilati separatamente:

**$tar -zxvf nagios-plugins-1.4.2.tar.gz** [invio]

spostarsi nella directory creata (cd nagios-plugins-x.y.z) e dare i comandi:

**$./configure** [invio]
**$make** [invio]
**$make install** [invio]

Si è quasi operativi, e si proceda con la configurazione del web-server. Aprire con un editor di testo il file **/etc/httpd/conf/httpd.conf** e, come riportato dal manuale di Nagios, in fondo aggiungiamo le seguenti linee di codice:

```
ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<Directory "/usr/local/nagios/sbin">
   ScriptAlias /nagios/cgi-bin /usr/local/nagios/sbin
<Directory "/usr/local/nagios/sbin">
   AllowOverride AuthConfig
   Options ExecCGI
   Order allow,deny
   Allow from all
</Directory>


Alias /nagios /usr/local/nagios/share
<Directory "/usr/local/nagios/share">
   Options None
   AllowOverride AuthConfig
   Order allow,deny
   Allow from all
</Directory>

<Directory /usr/local/nagios/sbin>
AllowOverride AuthConfig
order allow,deny
allow from all
Options ExecCGI
</Directory>

<Directory /usr/local/nagios/share>
AllowOverride AuthConfig
order allow,deny
allow from all
</Directory>
```

fra le varie istruzioni inserite, c'è quella di utilizzare dei file locali per la verifica degli accessi. Risulta quindi necessario configurare un file di accesso in **/usr/local/nagios/sbin** ed editare il file **.htaccess** inserendo:

```
AuthName "Nagios Access"
AuthType Basic
AuthUserFile /usr/local/nagios/etc/htpasswd.users
require valid-user
```

creare quindi i permessi per l'utente nagiosadmin in **/usr/local/nagios/etc/htpasswd.user**:

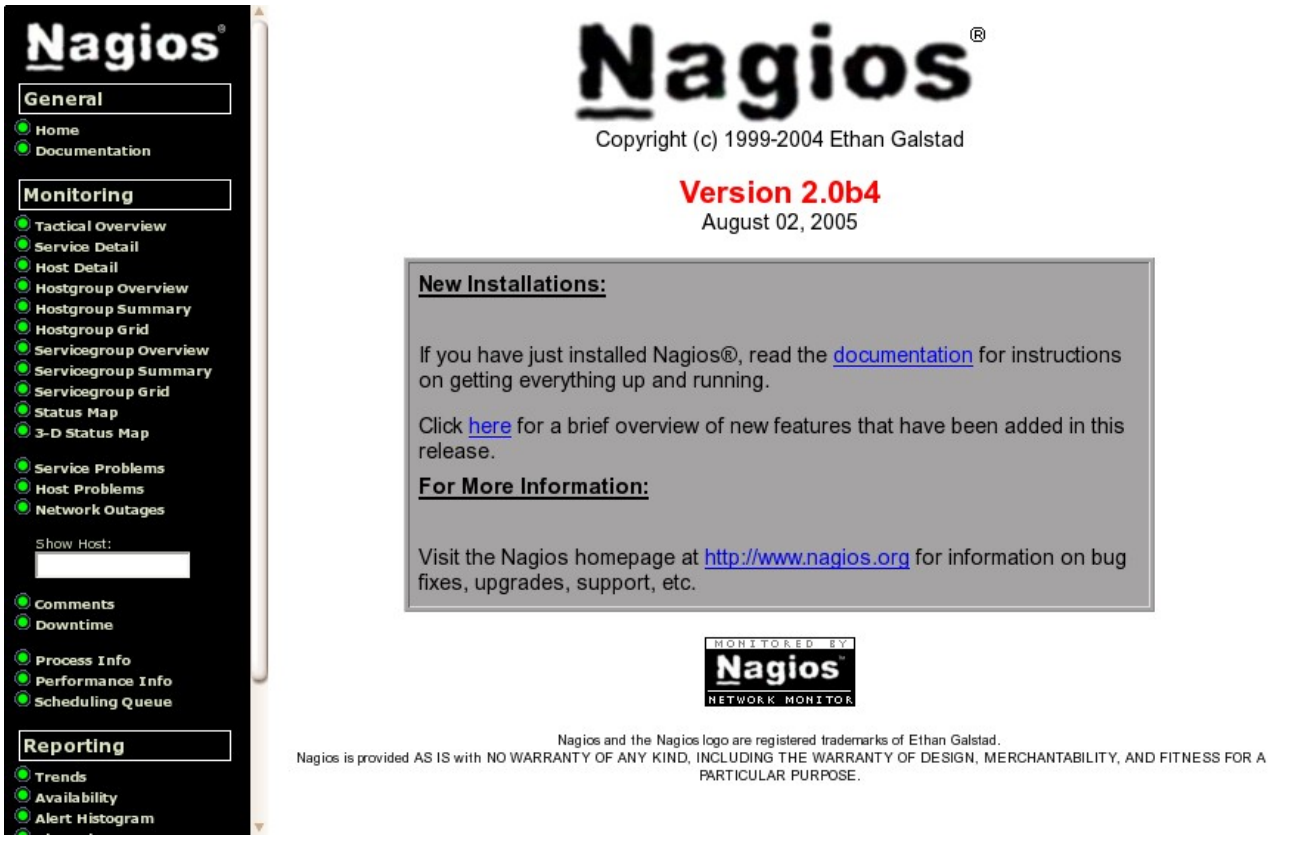
```
$htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin [invio]
```

inserendo e reimmettendo la password dell'amministratore di Nagios quando richiesto. Aggiungere anche l'account dell'utente abituale, ripetendo l'operazione fatta con il comando dato sopra:

**$htpasswd /usr/local/nagios/etc/htpasswd.users user** [invio]

C'è da considerare, ovviamente, che va aggiunto il dovuto permesso per ogni amministratore o utente che deve accedere all'interfaccia web di Nagios.

A questo punto l'installazione è completata e digitando nel browser preferito il percorso ***http://nome_servert/nagios/*** apparirà una finestra simile a questa:




Cliccando sulle voci del menù, si otterranno solo degli errori poiché bisognerà istruire Nagios con delle configurazioni. Se questa pagina viene visualizzata, l'installazione è andata a buon fine.

I file di configurazione d'esempio si trovano nella directory ***/usr/local/nagios/etc/*** ed hanno estensione *.cfg-sample. Dovendo iniziare da essi, si dovrà per prima cosa rinominarli:

**$cp nagios.cfg-sample nagios.cfg** [invio]
**$cp checkcommands.cfg-sample checkcommands.cfg** [invio]
**$cp resource.cfg-sample resource.cfg** [invio]
**$cp misccommands.cfg-sample misccommands.cfg [invio]**
**$cp cgi.cfg-sample cgi.cfg** [invio]
**$cp minimal.cfg-sample minimal.cfg** [invio]

La configurazione di base è nel file **nagios.cfg** e contiene le direttive ai file esterni da processare. In questo caso, l'unica direttiva presente è il collegamento al file **minimal.cfg** che si andrà subito a modificare. Siccome sono presenti un gran numero di opzioni, si procederà ad analizzarne una porzione alla volta, partendo dalla definizione dei tempi di esecuzione:

```
# '24x7' timeperiod definition
define timeperiod{
        timeperiod_name 24x7
        alias           24 Hours A Day, 7 Days A Week
        sunday          00:00-24:00
        monday          00:00-24:00
        tuesday         00:00-24:00
        wednesday       00:00-24:00
        thursday        00:00-24:00
        friday          00:00-24:00
        saturday        00:00-24:00
        }
```

```
# 'workhours' timeperiod definition
define timeperiod{
        timeperiod_name workhours
        alias           "Normal" Working Hours
        monday          08:00-18:00
        tuesday         08:00-18:00
        wednesday       08:00-18:00
        thursday        08:00-18:00
        friday          08:00-18:00
        }
```

```
# 'nonworkhours' timeperiod definition
define timeperiod{
        timeperiod_name nonworkhours
        alias           Non-Working Hours
        sunday          00:00-24:00
        monday          00:00-08:00,18:00-24:00
        tuesday         00:00-08:00,18:00-24:00
        wednesday       00:00-08:00,18:00-24:00
        thursday        00:00-08:00,18:00-24:00
        friday          00:00-08:00,18:00-24:00
        saturday        00:00-24:00
        }
```

```
# 'none' timeperiod definition
define timeperiod{
        timeperiod_name none
        alias           No Time Is A Good Time
        }
```

Come detto sopra, all'inizio del file vengono definiti i ***Time Periods***, cioè le finestre temporali nelle quali verranno gestiti gli eventi o spedite le notifiche. Il periodo è definito come "24x7", ovvero ventiquattro ore per i sette giorni della settimana. Per iniziare si consiglia di definire altri due periodi, uno relativo alle ore lavorative, l'altro relativo alle ore non lavorative. Se nel vostro caso si tratta di turni di lavoro nelle ventiquattro ore o simili, può essere utile definirli ora. Al termine della definizione del periodo “24x7” si aggiungano altri due periodi, più un periodo per definire un “periodo vuoto”, utile per indicare la non esecuzione di un evento come mostrato nel listato sopra. Passare ora alla modifica dei contatti ovvero l'elenco delle persone che verranno contattate ogni volta che viene rilevato un problema. Si noti che Nagios permette di definire dei contatti diversi per ogni macchina, gruppo di macchine, servizio, gruppi di servizi. Nell'esempio che segue si inserirà un solo nominativo come contatto, eliminando quindi i contatti standard inseriti. Inserire perciò i riferimenti come da esempio:

```
# 'nome_account' contact definition
define contact{
        contact_name                    account                 #nome dell'account
        alias                           Nome Cognome            #nome esteso
        service_notification_period     workhours               #si vuole ricevere le notifiche
        host_notification_period        workhours               #solo durante l'orario di lavoro
        service_notification_options    c,r
        host_notification_options       d,r
        service_notification_commands   notify-by-email         #riceveremo la
        host_notification_commands      host-notify-by-email    #notifica via email
        email                           account@localhost
        }
```

Come si vede la definizione del precedente periodo temporale "workhours" è già utile in quanto impiegato per indicare gli orari nei quali si desidera ricevere la notifica. Le direttive ***service_notification_options*** e ***host_notification_options*** sono utilizzate per indicare quali stati del sistema controllato vengono notificati. I valori possibili sono:

**u** = unreachable (irraggiungibile);
**d** = down (spento o assente);
**r** = recoveries (ripristino del servizio);
**f** = flapping (intermittente o instabile);
**w** = warning (avvisi);
**c** = critical (condizione critica o di guasto);
**n** = none (nessuna segnalazione).

Occorre poi modificare anche i gruppi dei contatti inserendo i nominativi aggiuntivi come da esempio seguente:

```
define contactgroup{
        contactgroup_name       admins
        alias                   Nagios Administrators
        members                 account
        }
```

In questo esempio è sufficiente un solo gruppo, ma se si gestisce un'azienda molto ampia con personale molto specializzato, è opportuno definire un gruppo da contattare per i problemi relativi a GNU/Linux, un gruppo per i database, uno per il gestionale e via discorrendo... Un passo ulteriore consiste nel cancellare la definizione dei comandi dal file ***minimal.cfg*** poiché sono un duplicato di quelli presenti nel file ***checkcommands.cfg*** che viene usato dal file ***nagios.cfg***.

Ora c'è la parte più importante, ovvero la definizione di cosa controllare. Si suggerisce di leggere il contenuto del file di esempio e mettere sotto controllo il computer che esegue Nagios stesso. Modificare leggermente l' host ed il gruppo di default ottenendo quanto segue nell'esempio:

```
define host{
        use                     generic-host  ;ci si basa su un template generico predefinito
        host_name               localhost
        alias                   Nagios Server
        address                 127.0.0.1       ;indirizzo per il momento si usa localhost
        check_command           check-host-alive        ; tipo di test da eseguire
        max_check_attempts      10                      ; tentativi massimi
        notification_interval   120
        notification_period     24x7
        notification_options    d,r
        contact_groups          admins
        }


# We only have one host in our simple config file, so there is no need to
# create more than one hostgroup.

define hostgroup{
        hostgroup_name      test
        alias                   Primo test
        members                 localhost
        }
```

Tutto ciò che riguarda i servizi sotto test, si consiglia di mantenere inalterato quanto proposto nei file di esempio. Sistemare i permessi per l'interfaccia grafica editando il file ***cgi.cfg***. Individuare tutte le righe che iniziano con ***authorized_for_***, rimuovendo il commento ed inserendo alla fine il nome definito quando si sono configurati gli accessi alla sezione web. L'esempio seguente può aiutare a capire:

```
authorized_for_system_information=admin,nagios,mio_account
```

verificare la configurazione e fare il test di Nagios dando i comandi:

```
$/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg [invio]
$/usr/local/bin/chechnagios [invio]
```

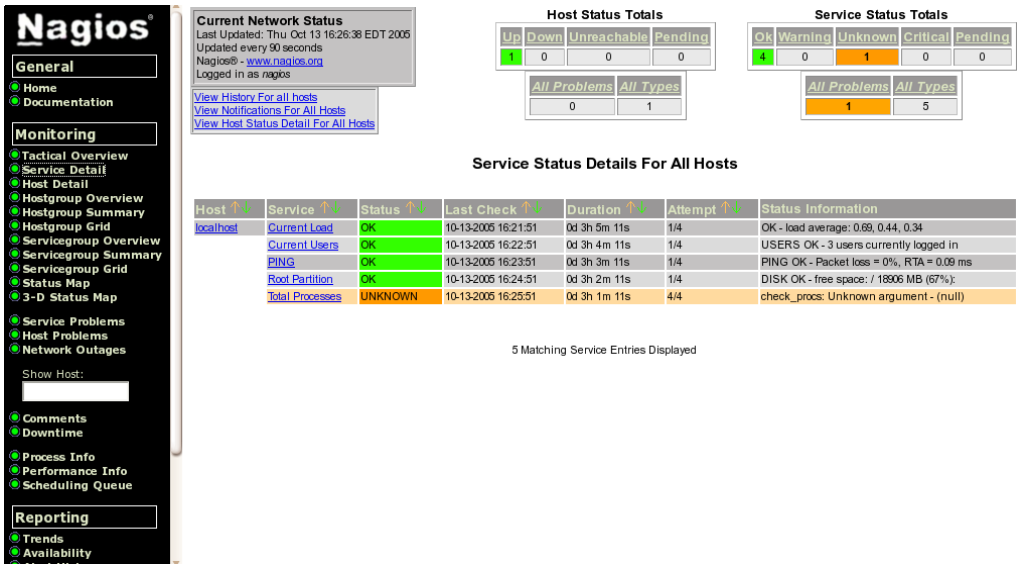
se il computer risponde con quanto segue, la configurazione va bene.

```
Nagios 2.0b4
Copyright (c) 1999-2005 Ethan Galstad (http://www.nagios.org)
Last Modified: 08-02-2005
License: GPL

Reading configuration data...

Running pre-flight check on configuration data...

Checking services...
      Checked 5 services.
Checking hosts...
      Checked 1 hosts.
Checking host groups...
      Checked 1 host groups.
Checking service groups...
      Checked 0 service groups.
Checking contacts...
      Checked 1 contacts.
Checking contact groups...
      Checked 1 contact groups.
Checking service escalations...
      Checked 0 service escalations.
Checking service dependencies...
      Checked 0 service dependencies.
Checking host escalations...
      Checked 0 host escalations.
Checking host dependencies...
      Checked 0 host dependencies.
Checking commands...
      Checked 22 commands.
Checking time periods...
      Checked 4 time periods.
Checking extended host info definitions...
      Checked 1 extended host info definitions.
Checking extended service info definitions...
      Checked 0 extended service info definitions.
Checking for circular paths between hosts...
Checking for circular host and service dependencies...
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors:   0

Things look okay - No serious problems were detected during the pre-flight check
```

Poiché tutto va bene,  è possibile verificare il sistema facendo partire il demone di controllo con:

```
$service nagios start [invio]
```

Avviando il browser preferito, si può finalmente ammirare il risultato controllando i servizi:




**→ Monitorare un server da un host:**

Se ad esempio si vuole monitorare un server GNU/Linux che ospita un servizio web con un database MySQL e un mail server (con indirizzo IP 192.168.0.100) da un altro server sul quale gira Nagios (con indirizzo IP 192.168.0.22) che si trova sulla stessa rete locale, si dovranno operare alcune modifiche. Mantenendo le modifiche fatte precedentemente al file ***minimal.cfg*** contenete le definizioni dei periodi temporali, dei contatti e dei gruppi di contatti, separare le definizioni degli ***hosts*** e dei servizi ***services*** in due file aggiuntivi. Modificare quindi ***nagios.cfg*** rimuovendo il commento dalle righe relative a ***hosts*** e ***services***:

```
#cfg_file=/usr/local/nagios/etc/hostgroups.cfg
cfg_file=/usr/local/nagios/etc/hosts.cfg
cfg_file=/usr/local/nagios/etc/services.cfg
#cfg_file=/usr/local/nagios/etc/timeperiods.cfg
```

Rimuovere dal file ***minimal.cfg*** ogni riferimento a host e servizi; procedere col file ***hosts.cfg***. Prima di inserire le configurazioni degli host e dei servizi è bene capire la tipologia delle definizioni usato da Nagios: esso permette l'uso dei modelli (template) per definire gli host ed i servizi. Si possono cioè inserire delle descrizioni generiche con già preconfigurati tutti i parametri standard. Nella definizione del singolo host o servizio si può indicare di utilizzare il modello e poi aggiungere solo i parametri mancanti o quelli che variano rispetto al modello. E' permesso l'uso di modelli in cascata, come verrà descritto più avanti.

Creare il file ***hosts.cfg*** inserendo il template generico di host già presente nel file ***minimal.cfg*** come visibile nel listato seguente:

```
##############################################################################
# HOST DEFINITIONS
##############################################################################

# Generic host definition template
define host{
        name                    generic-host    ; Il nome di questo template
        notifications_enabled   1               ; Notifiche abilitate
        event_handler_enabled   1               ; Eventi abilitati
        flap_detection_enabled  1               ; Rilevamento stati indefiniti abilitato
        process_perf_data       1               ; Analisi performance abilitata
        retain_status_information       1       ; Mantenimento stato d'errore
        retain_nonstatus_information    1       ; Mantenimento informazioni aggiuntive
        register                0               ; non va registrato poiché non è un host reale
        }
```

a questo modello generico, si accoda il template più dettagliato:

```
# Template più dettagliato
define host{
      use                     generic-host            ; Eredita il template precedente
      name        my_host
      check_command           check-host-alive ; Test di default
      max_check_attempts      10                      ; Numero massimo di tentativi
      notification_interval   120                     ; Intervallo di notifica
      notification_period     24x7                    ; Riferimento al periodo
      notification_options    d,r                     ; Eventi da notificare
      contact_groups          admins                  ; Gruppo da contattare
      register                0                       ; non va registrato poiché non è un host reale
      }
```

definendo poi il server da controllare:

```
# 'web_server' definizione
define host{
      use                     my_host         ; Eredita i modelli
      host_name       web_server              ; Nome del server
      alias           Linux Web & Mail
      address         192.168.0.100           ; Indirizzo IP del server da controllare
      }

# informazioni aggiuntive
define hostextinfo {
      host_name           web_server
      icon_image          linux.png       ; Riferimenti
      icon_image_alt      Linux Host      ; alle
      vrml_image          linux.png       ; immagini da
      statusmap_image     linux.gd2       ; usare
      }
```

creare ora il gruppo, anche se si ha un solo host:

```
##############################################################################
# HOST GROUP DEFINITIONS
##############################################################################
# 'linux-boxes' host group
define hostgroup{
        hostgroup_name  linux-boxes
        alias                Linux Servers
        members           web_server
        }
```

Salvare le modifiche al file ***hosts.cfg*** e passare alla definizione dei servizi nel file ***services.cfg***, definendo i due servizi da controllare ed inviando una notifica al gruppo indicato in caso di errore:

```
##############################################################################
# SERVICE DEFINITIONS
##############################################################################

#  template per un servizio generico
define service{
        name            generic-service              ; Nome del template
        active_checks_enabled       1                ; Controllo di tipo attivo abilitato.
        passive_checks_enabled      1                ; Controllo passivo abilitato
        parallelize_check           1          ; Attiva controlli in parallelo
        obsess_over_service         1              ; Se necessario mantiene il  monitoraggio
        check_freshness             0              ; Non controlla se il dato è fresco
        notifications_enabled       1              ; Notifiche abilitate
        event_handler_enabled       1              ; Abilita la gestione del servizio
        flap_detection_enabled      1              ; Abilita su stato instabile
        process_perf_data           1               ; Abilita controllo performances
        retain_status_information   1              ; Mantiene le informazioni su riavvio
        retain_nonstatus_information    1
        register                    0                ; Non registra il servizio (TEMPLATE)
        }

# Test del mail server
define service{
        use                     generic-service; usa il template precedente
        host_name               web_server      ; nome server
        service_description     SMTP            ; nome servizio
        is_volatile             0                ; non è volatile
        check_period            24x7             ; periodo usato per i test
        max_check_attempts      3                ; massimo numero di tentativi
        normal_check_interval   3                ; intervallo fra i test
        retry_check_interval    1                ; intervallo in caso di errore
        contact_groups          admins; contatti
        notification_interval   120              ; intervallo fra le notifiche
        notification_period     24x7             ; periodo di notifica
        notification_options    w,u,c,r          ; errori notificati
        check_command           check_smtp       ; comando usato per i test
        }
```

```
# Test del web server
define service{
        use                     generic-service         ; usa il template precedente
        host_name               web_server      ; nome server
        service_description     HTTP            ; nome servizio
        is_volatile             0               ; non è volatile
        check_period            24x7            ; periodo usato per i test
        max_check_attempts              3               ; massimo numero di tentativi
        normal_check_interval   3               ; intervallo fra i test
        retry_check_interval    1               ; intervallo in caso di errore
        contact_groups          admins          ; contatti
        notification_interval   120             ; intervallo fra le notifiche
        notification_period     24x7            ; periodo di notifica
        notification_options    w,u,c,r         ; errori notificati (vedi note)
        check_command           check_http
        }
```

le sigle degli errori per il quale si ottiene la notifica sono state esposte in precedenza.

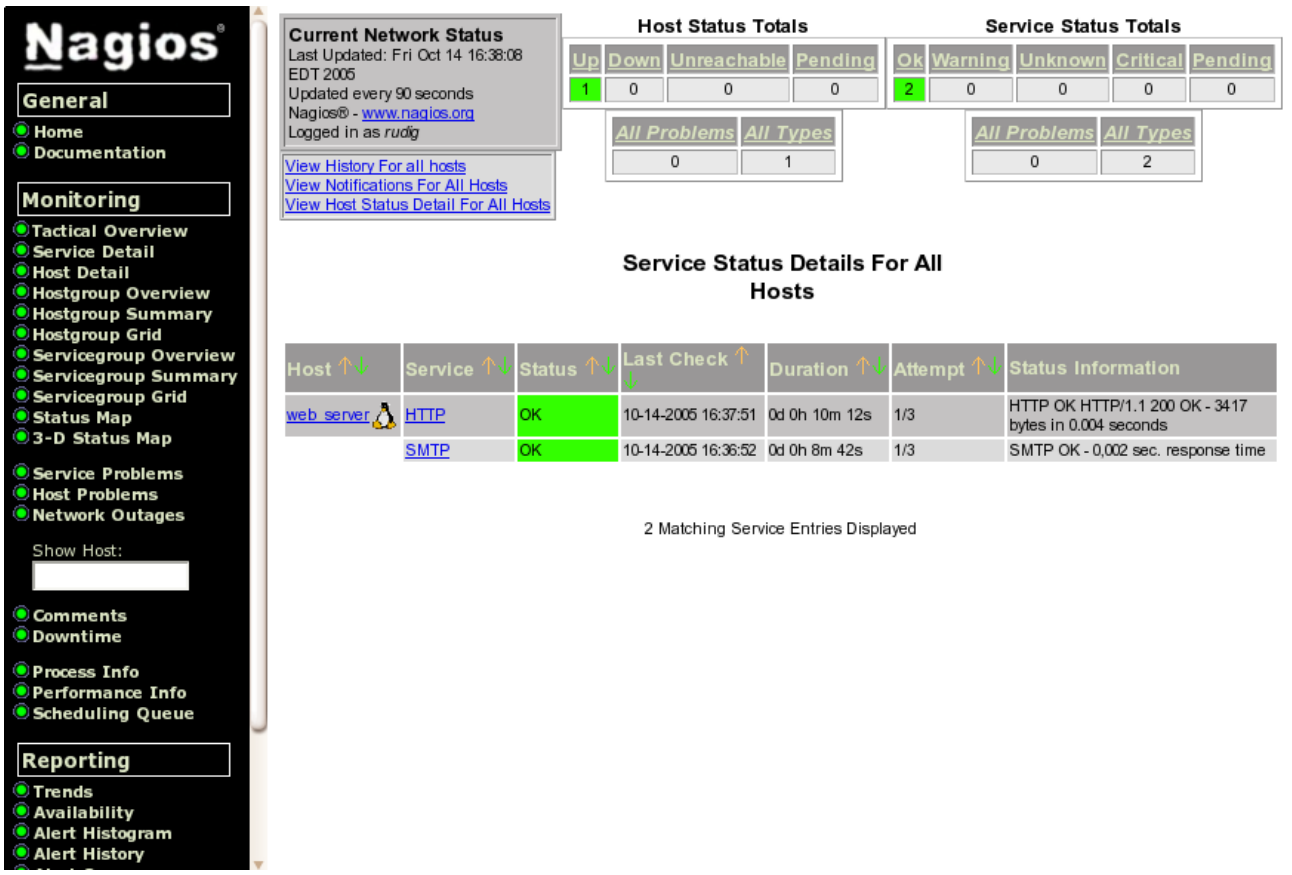
Testare la nuova configurazione con il comando

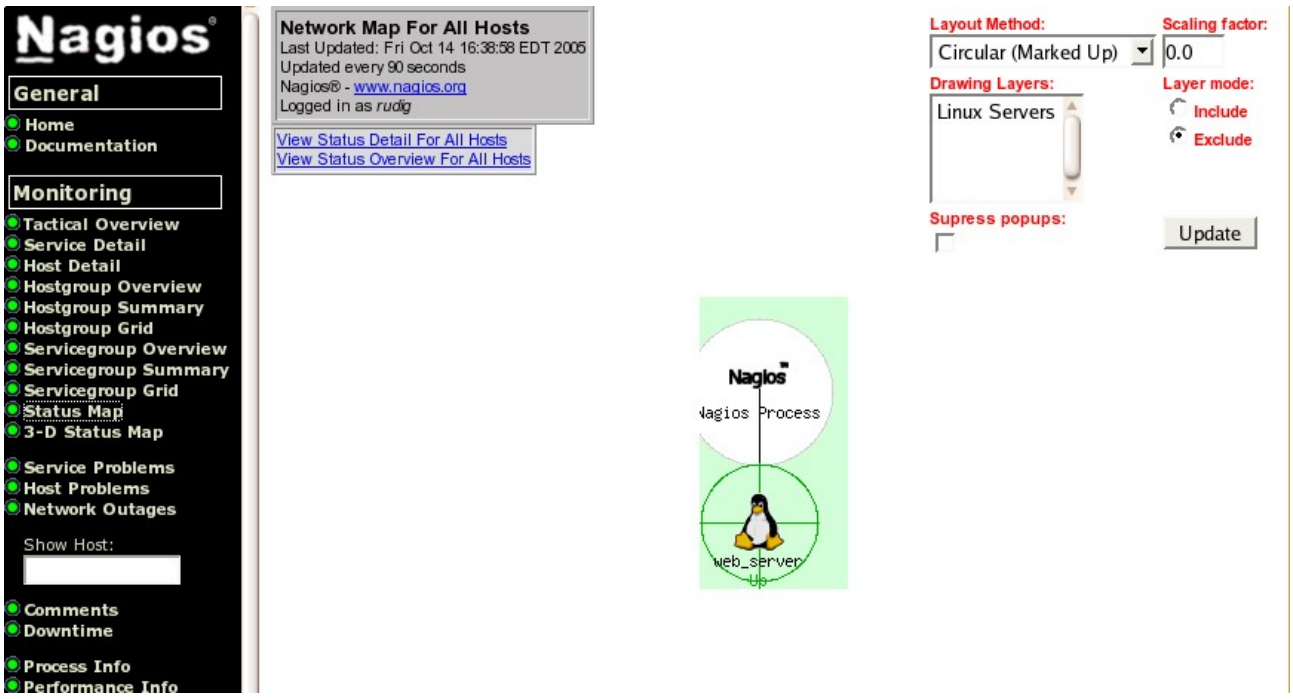
```
$checknagios [invio]
```

Se il computer risponde confermando che sono stati definiti un host e due servizi, è possibile procedere riavviando Nagios con il comando:

```
$service nagios restart [invio]
```

Avviare il browser per ulteriore verifica, si otterrà:




Per monitorare il database MySQL occorre modificare i comandi standard, aggiungendone uno ad-hoc. Nella directory ***/usr/local/nagios/libexec*** si trova il comando ***check_mysql***. Eseguendolo col l'opzione ***- help*** si ottiene l'aiuto in linea che spiega la sintassi e come operare. Tra le varie spiegazioni viene chiaramente indicato che la password inserita è utilizzata ed inviata "in chiaro", perciò è meglio non utilizzare questo modulo in "ambienti a rischio". L'inserimento del comando consiste nel modificare il file ***checkcommands.cfg*** aggiungendo delle semplicissime linee di codice:

```
# 'check_mysql' command definition
define command{
      command_name    check_mysql
         command_line    $USER1$/check_mysql -d my_db -H IP_server_MySQL -u user -p
testpass
      }
```

al file ***services.cfg*** aggiungere:

```
# Test del database
define service{
      use                          generic-service    ; usa il template precedente
      host_name                    web_server         ; nome server
      service_description          MYSQL              ;nome servizio
      is_volatile                  0                  ; non è volatile
      check_period                 24x7               ; periodo usato per il monitoraggio
      max_check_attempts           3                  ; massimo numero di tentativi
      normal_check_interval        3                  ; intervallo fra i test
      retry_check_interval         1                  ; intervallo in caso di errore
      contact_groups               admins             ; contatti
      notification_interval        120                ; intervallo fra le notifiche
      notification_period          24x7               ; periodo di notifica
      notification_options         w,u,c,r            ; errori notificati
      check_command          check_mysql
     }
```

Dopo il riavvio si otterrà il risultato voluto. Con questo paragrafo si sono forniti gli elementi di base per iniziare ad operare con Nagios. Molte di queste informazioni sono state tratte dal manuale del programma, chiaro e completo. La sua lettura è comunque consigliata.

## 8.6 Servizio di posta interna

Sebbene questo argomento non serva in modo specifico alla gestione di una rete wireless, il servizio di e-mail interna alla rete risulta essere molto utile e talvolta voluto da più utenti. Questo servizio è discretamente facile da implementare sul computer che è stato adibito a piccolo server. Grazie all'open source ed al software libero, basterà un po' d'impegno ed avremo questo comodo servizio aggiuntivo, dotato di POP3, SMTP e webmail (utilizzando il pacchetto Squirrelmail). Le procedure di seguito riportate sono state realizzate come al solito sulla distribuzione GNU/Linux Fedora Core 3 (http://fedora.redhat.com), ipotizzando che il server abbia indirizzo IP 192.168.0.1, Subnet Mask 255.255.255.0 e nome Host MioServer.MiaRete.lan.
Prima d'iniziare la configurazione è utile verificare che siano installati i seguenti pacchetti:

→ Database MySQL: MySQL python, mod_auth_mysql, MySQL server, perl_DBD_mysql, php_MySQL.
→ File server Windows: System_config_Samba.
→ Server FTP.
→ Server Mail: cyrus_sasl; dovecot; postfix; spamassasin.
→ Server WEB: crypto utils.

Loggarsi al sistema come root non è mai una bella cosa, ma ai neofiti semplificherà le operazioni di configurazione. Prestare sempre la massima attenzione poiché con i diritti di amministratore è molto facile fare danni anche rilevanti.
Entrare nella directory **/etc/postfix** ed editare il file **main.cf** non prima di aver fatto una copia di sicurezza e d'averla salvata da qualche parte. Le linee di codice che più interessano alle modifiche sono le seguenti:

```
# LOCAL PATHNAME INFORMATION
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix

# QUEUE AND PROCESS OWNERSHIP
mail_owner = postfix
# INTERNET HOST AND DOMAIN NAMES
myhostname = MioServer.MiaRete.lan

# RECEIVING MAIL
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost

# REJECTING MAIL FOR UNKNOWN LOCAL USERS
unknown_local_recipient_reject_code = 550

# TRUST AND RELAY CONTROL
mynetworks_style = class
mynetworks = 192.168.0.0/24, 127.0.0.0/8

# ALIAS DATABASE
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
```

```
# DELIVERY TO MAILBOX
home_mailbox = Maildir/
mailbox_command =

# SHOW SOFTWARE VERSION OR NOT
smtpd_banner = $myhostname ESMTP $mail_name

# DEBUGGING CONTROL
debug_peer_level = 2
debugger_command =
PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
xxgdb $daemon_directory/$process_name $process_id & sleep 5

# INSTALL-TIME CONFIGURATION INFORMATION
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = no
```

Queste sono le opzioni di base e sono successivamente ampliabili con sistemi di protezione TLS e verrà poi descritto come fare si ha necessità del genere. Editare ora il file **/etc/aliases** per assegnare a chi deve ricevere le mail di root, cercando la direttiva:

```
# root: marc
```

che dovrà essere decommentata e, al posto di *marc*, s'inserirà il nome dell'utente a cui dovrà pervenire la posta dell'amministratore. Salvare le modifiche.
Ricreare ora il database ***aliases*** con le modifiche fatte, dando il comando da shell:

**$postaliases hash:/etc/aliases** [invio]

che aggiornerà il file /etc/aliases.db. Verificare ora la corretta configurazione di Postfix dando il comando:

**$postfix check** [invio]

Se nessun errore è mostrato a video, la configurazione è corretta, altrimenti occorre rimettere mano al file **/etc/postfix/main.cf** e verificare che tutto corrisponda come mostrato sopra.
Avviare il gestore dei servizi del computer, spuntare la check-box a fianco di Postfix e, selezionandolo, premere il pulsante avvia per rendere operativo il servizio. Ripetere la stessa operazione con **Dovecot**. Salvare le modifiche fatte e chiudere il gestore.
Una veloce verifica del corretto funzionamento di Postfix e quindi di ***SMTP*** consiste nell'aprire un sessione a riga di comando digitando il comando:

**$telnet MioServer.MiaRete.lan 110** [invio]

se tutto è andato a buon fine, il server risponderà con:

**Connected to localhost.localdomain (127.0.0.1).**
**Escape character is '^]'.**
**220MioServer.MiaRete.lan ESMTP Postfix.**

Uscire dalla sessione telnet con il comando ***quit*** e provare il corretto funzionamento del servizio POP3/IMAP di Dovecot, dando il comando:

**$telnet MioServer.MiaRete.lan 25** [invio]

se tutto è andato a buon fine, il server risponderà con:

**Connected to localhost.localdomain (127.0.0.1).**
**Escape character is '^]'.**
**+OK Dovecot ready.**

Ora è possibile provare un log-in con il nome utente perciò si darà il comando:

**$user NomeUtente** [invio]
**$pass MiaPassword** [invio]

se il server risponderà con il seguente messaggio, tutto è correttamente configurato:

**+OK Logged in**

digitare ***quit*** per uscire dalla sessione telnet.

**ATTENZIONE:** Se il servizio SE-Linux è impostato su “Enforce” e non avete selezionato come “fidato” il servizio POP di Dovecot, il server non vi farà accedere alla vostra casella di posta. Settatelo su “Permessive” e confermate in uscita; ora riprovate il servizio a riga di comando.

### 8.6.1 Configurazione client posta elettronica

La configurazione di un client di posta elettronica non è difficoltosa poiché i parametri da utilizzare sono pochi e semplici:

Protocollo: POP3
User: NomeUtente
Indirizzo del server: MioServer (in alternativa utilizzare l'indirizzo IP del server: 192.168.0.1)

Protocollo: SMTP
User: NomeUtente
Indirizzo del server: MioServer (in alternativa utilizzare l'indirizzo IP del server: 192.168.0.1)

Per il momento si tralasciano le impostazioni di sicurezza perché saranno trattate più avanti. Salvare le impostazioni e provare a collegarsi al mailserver ed inserire la password quando richiesta.

### 8.6.2 Configurazione webserver

In linea di massima, le impostazioni della configurazione di default vanno già bene così come sono ma, qualche opportuna modifica è meglio farla in queste parti significative:

```
Listen 80

User apache
Group apache

ServerAdmin root@localhost

#ServerName www.example.com:80
UseCanonicalName Off

DocumentRoot "/var/www/html"

<Directory />
Options FollowSymLinks
AllowOverride None
</Directory>
```

Nel caso abbiate modificato la DocumentRoot dovete necessariamente modificare anche:

**<Directory "/var/www/html">**
**Options Indexes FollowSymLinks**
**AllowOverride None**
**Order allow,deny**
**Allow from all**
**</Directory>**

Le modifiche sono tuttavia implementabili in seguito. Entrare nel gestore dei servizi, spuntare la check-box di ***httpd***, selezionarlo e premere il pulsante avvia. Salvare le impostazioni ed uscire.
E' ora il momento di testare il web server Apache. Avviare il browser preferito e digitare nella barra degli indirizzi:

***http://MioServer.MiaLan.lan*** oppure ***http://Mioserver***

Se non sono presenti errori di configurazione, la pagina che vi appare è quella di test e di default del web server Apache. Potete sostituire questa pagina con ciò che volete, inserendo un documento html in **/var/www/html**.

### 8.6.3 Configurazione della WebMail

Ora che il web server è impostato, bisogna procurarsi il pacchetto Squirrelmail da www.squirrelmail.org. Creare una cartella chiamata "**webmail**" in **/var/www/html** ed inserire il contenuto dell'archivio compresso. Non è ancora possibile utilizzare la webmail perché bisogna impostare il programma. Dalla shell dare il comando:

**$/var/www/html/webmail/config/conf.pl** [invio]

seguire i pochi e semplici passi guidati per effettuare la configurazione, dove è possibile inserire anche un messaggio di benvenuto… salvare ed uscire. Avviare il browser e puntare all'indirizzo:

***http://MioServer.MiaRete.lan/webmail***

Quella che appare è la pagina principale della webmail di Squirrelmail. Provare a loggarsi inserendo il nome utente e la password. Se tutte le impostazioni sono giuste, immettendo nei relativi campi il nome utente e la password, premendo il pulsante **login**, si accederà alla casella di posta attraverso l'interfaccia web, senza essere costretti ad usare un programma client. A seguire è possibile vedere alcune screen-shot:


Se si vuole, è possibile personalizzare Squirrelmail impostando la lingua italiana o desiderata. Scaricare dal sito la traduzione desiderata e scompattarla in una cartella. Dalla shell dare il comando

**$/percorso_cartella/install** [invio]

seguire le istruzioni richieste oppure spostare manualmente le cartelle presenti nel pacchetto del linguaggio nella directory **/var/www/html/webmail**, sovrascrivendo se necessario quelle già esistenti. Quando ultimato, ridare il comando:

**$/var/www/html/webmail/config/conf.pl** [invio]

entrare nella configurazione del linguaggio ed immettere ad esempio "**it_IT**" se si è installata l'estensione alla lingua italiana. Salvare le impostazioni ed uscire. Per accertarsi del funzionamento, puntare il browser all'indirizzo:

***http://MioServer.MiaRete.lan/webmail/src/configtest.php***.

Se tutto è andato a buon fine, s'è fatto un buon lavoro. Per maggior sicurezza è meglio rimuovere il file ***conf.pl*** dalla directory **/var/www/html/webmail/config**.

### 8.6.4 Implementazione SMTP-AUTH e TLS in Postfix

I pacchetti necessari per tali servizi sono ***cyrus_sasl, cyrus-sasl-devel, cyrus-sasl-gssapi, cyrus-sasl-plain, openssl, bind-chroot***. Oltre a questi, preventivamente aggiunti in fase d'installazione del sistema operativo, è necessaria l'installazione del pacchetto **Fetchmail**.

Dopo la sua installazione, occorre entrare nelle directory **/etc/postfix** e mettere nuovamente mano alle impostazioni contenute nel file **main.cf**, dove andranno inserite le seguenti linee di codice:

```
# IMPLEMENTAZIONE CERTIFICATI SMTP-AUTH E TLS
smtpd_sasl_local_domain =
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_recipient_restrictions =
smtpd_use_tls = yes

broken_sasl_auth_clients = yes
permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination

smtp_use_tls = yes
smtp_tls_note_starttls_offer = yes

smtpd_tls_auth_only = no
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem

smtpd_tls_loglevel = 1
smtpd_tls_received_header = yes
smtpd_tls_session_cache_timeout = 3600s

tls_random_source = dev:/dev/urandom
```

Editare il file **smtp.conf** presente in **/usr/lib64/sasl** in modo tale che contenga le seguenti direttive:

```
pwcheck_method: saslauthd
mech_list: plain login
```

Generare ora i file dei certificati dando i comandi dalla shell:

```
$mkdir /etc/postfix/ssl [invio]
$cd /etc/postfix/ssl/ [invio]
$openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024 [invio]
$chmod 600 smtpd.key [invio]
$openssl req -new -key smtpd.key -out smtpd.csr [invio]
$openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt [invio]
$openssl rsa -in smtpd.key -out smtpd.key.unencrypted [invio]
$mv -f smtpd.key.unencrypted smtpd.key [invio]
$openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650  [invio]
```

Riavviare i servizi interessati (postfix, dovecot, saslauthd) utilizzando se si preferisce la shell con:

```
$chkconfig - -levels 235 NomeDemone on [invio]
$/etc/init.d/NomeDemone start [invio]
```

Per verificare da telnet che tutto funzioni, si dovrà ripetere quanto visto prima e per **SMTP-AUTH** e **TLS**:

```
$ehlo localhost [invio]
```

se le configurazioni sono giuste, il server risponderà con:

```
250-STARTTLS
250-AUTH
```

digitare **quit** ed uscire dalla sessione telnet. Per la configurazione di un programma client di posta, selezionare "***certificati TLS***" nelle proprietà POP3 e SMTP dell'account. Applicare le nuove impostazioni e provare una connessione al mailserver. Si rende noto che ad ogni connessione alla casella di posta, il server rilascerà un nuovo certificato che bisogna per forza di cose accettare sempre per poter accedere al servizio.

# Sicurezza avanzata

## 9.1 Le porte del computer

Senza le cosiddette porte, un computer non potrebbe comunicare con il mondo esterno come potrebbe essere internet o la LAN, tramite i protocolli TCP e UDP. Esse rappresentano gli ingressi e le uscite per i dati che devono essere processati od inviati attraverso la rete. Da questa considerazione si evince che più porte sono aperte più un computer è soggetto a rischi di attacco e per questo motivo devono essere configurati correttamente i firewall, detti anche "port filter". La conoscenza delle porte principali e la loro funzione permettono perciò una corretta ed efficace configurazione. I numeri delle porte fanno parte degli elementi fondamentali per l'uso dei protocolli di rete TCP ed UDP. Senza scendere troppo in dettaglio, vediamo come funziona il trasporto delle informazioni...
Attraverso i singoli livelli della rete, un meccanismo assicura la consegna dei dati al protocollo corretto. L'identificativo del protocollo IP è contenuto in un byte nella prima parola dell'header del datagramma. Questo valore stabilisce la consegna al protocollo di competenza nel livello di trasporto. Alla ricezione, il protocollo di trasporto deve trasferire i dati al processo applicativo corretto. I processi applicativi ai quali devono essere trasferiti i dati dopo l'arrivo sul pc di destinazione, vengono identificati in base al numero della porta; nella prima parola di ogni header TCP o UDP sono perciò contenuti i numeri della porta di origine e di destinazione. Quando un'applicazione dev'essere raggiungibile tramite un numero di porta determinato, lo comunica allo stack del protocollo TCP/IP. La combinazione tra indirizzo IP e numero di porta è detto socket e consente il riconoscimento univoco di ogni singolo processo di rete la cui notazione classica è: Indirizzo IP:porta.
In totale sono disponibili 65535 porte TCP e UDP che, per essere assegnate ad applicazioni determinate, vengono divise in tre gruppi: conosciute (well known), registrate (registered) e dinamiche (dynamically).

- **Porte Well-Known:** trattasi di numeri di porta riservati e standardizzati e vanno da 1 a 1023. Queste porte consentono la connessione dei client ai server senza procedere ad ulteriori configurazioni;
- **Porte Registered:** sono le porte che vanno da 1024 a 49151 e vengono usate da servizi di carattere derivato, come può esserlo ad esempio un servizio proxy http che sempre più spesso utilizza la porta 3128;
- **Porte Dynamically Allocated:** sono porte secondarie, definite anche effimere, assegnate dinamicamente. Vanno da 49152 a 65535. I client possono utilizzare queste porte fintanto che la combinazione tra protocollo di trasporto, indirizzo IP e numero porta è univoco.

Nella seguente tabella sono riportate le informazioni delle principali porte TCP e UDP e quali siano le applicazioni che ne fanno normalmente uso:

| Porta | Protocollo | Servizio | Descrizione | Categoria | Trojan | Cifratura |
|---|---|---|---|---|---|---|
| 20 | TCP/UDP | FTP-dati | File Transfer (dati) | Well-Known | sì | no |
| 21 | TCP/UDP | FTP | File Transfer (controllo) | Well-Known | sì | no |
| 22 | TCP | SSH | SSH Remote Login Protocol | Well-Known | sì | sì |
| 23 | TCP | Telnet | Telnet | Well-Known | sì | no |
| 25 | TCP | SMTP | Simple Mail Transfer Protocol | Well-Known | sì | no |
| 53 | TCP/UDP | Domain | Domain Name Server | Well-Known | no | no |
| 80 | TCP | HTTP | HyperText Transfer Protocol | Well-Known | sì | no |
| 102 | TCP/UDP | ISO-TSAP | X.400, ISO-TSAP Class 0 | Well-Know | no | no |
| 110 | TCP | POP3 | Post Office Protocol V.3 | Well-Known | sì | no |
| 119 | TCP | NNTP | Network News Transfert Protocol | Well-Known | sì | no |
| 135 | TCP/UDP | LOC-srv/epmap | MS Dce Rpc end-point mapper | Well-Known | no | no |
| 137 | TCP/UDP | NetBios-ns | Netbios Name Server | Well-Known | sì | no |
| 138 | TCP/UDP | NetBios-dgm | Netbios Datagram Service | Well-Known | sì | no |
| 139 | TCP/UDP | NetBios-ssn | Netbios Session Service | Well-Known | sì | no |
| 143 | TCP | IMAP4 | Internet Message Access Protocol 4 | Well-Known | no | no |
| 389 | TCP | LDAP | Lightweight Directory Access Protocol | Well-Known | no | no |
| 443 | TCP | SSL | HTTP over TLS/SSL | Well-Known | no | si |
| 445 | TCP/UDP | MS-ds | Windows 200/XP SMB | Well-Known | no | no |
| 554 | TCP | RTSP | Real Time Stream Control Protocol | Well-Known | no | no |
| 636 | TCP | SLDAP | LDAP over SSL | Well-Known | no | sì |
| 993 | TCP | IMAPs | IMAP 4 over TLS/SSL | Well-Known | no | sì |
| 995 | TCP | POP3s | POP3 over TLS/SSL | Well-Knows | no | sì |
| 1214 | TCP | Kazaa | KaZaA/Morpheus | Registered | no | no |
| 1433 | TCP/UDP | MS-SQL-s | Microsoft SQL Server | Registered | sì | no |
| 1434 | UDP | MS-SQL-m | Microsoft SQL Monitor | Registered | sì | no |
| 1755 | TCP/UDP | MS-streaming | Microsoft Media Player | Registered | no | no |
| 1863 | TCP | Msnp | Microsoft MSN Messenger | Registered | no | no |
| 3112 | TCP/UDP | Ksysguard | KDE System Guard | Registered | no | no |
| 3185 | TCP/UDP | Snpppd | SuSE Meta PPPd | Registered | sì | no |
| 4000 | TCP/UDP | ICQ | ICQ/Terabase | Registered | sì | no |
| 4661 | TCP | Non Assegnato | E-Donkey | Registered | no | no |
| 4662 | TCP | Non Assegnato | E-Donkey | Registered | no | no |
| 4665 | UDP | Non Assegnato | E-Donkey | Registered | no | no |
| 5050 | TCP | MMC | Multimedia Conference Control Tool | Registered | no | no |
| 5060 | TCP/UDP | SIP | SIP | Registered | no | no |
| 5190 | TCP | AOL | AOL messenger/ICQ | Registered | no | no |
| 6346 | TCP | Gnutella-svc | Gnutella | Registered | no | no |
| 6347 | TCP | Gnutella-rtr | Gnutella | Registered | no | no |
| 7070 | TCP | Arcp | RealPlayer Server | Registered | no | no |
| 7071 | TCP | Arcp | RealPlayer Server | Registered | no | no |

## 9.2 Introduzione alle VPN

VPN è l'acronimo di **V**irtual **P**rivate **N**etwork (rete privata virtuale) ed è l'insieme delle tecnologie che permettono la connessione tra reti locali private attraverso una rete pubblica come può essere internet. Esistono diversi modi per collegare più reti geograficamente lontane, con facilità di realizzazione decisamente più semplice di una VPN, ma quest'ultima offre indubbi benefici in termini di omogeneità. Non c'è infatti distinzione tra i dispositivi connessi al proprio hub/switch da quelli connessi sulla rete LAN remota: esplorando le risorse di rete si avranno sia i dispositivi locali che quelli remoti. Il punto di forza di questa tecnologia è la trasparenza con cui viene fatta l'intera operazione in modo tale che le applicazioni non percepiscano la "distribuzione" della rete.
Grazie a protocolli particolari si è in grado d'incapsulare il traffico della LAN in specifici pacchetti, inviandoli attraverso una rete di natura insicura alla LAN remota. Questa operazione è sempre sostenuta da almeno due "punti", il client VPN remoto ed il server VPN locale. Da questa affermazione si deduce che deve esserci supporto al VPN da parte dei sistemi operativi, garantito nativamente nei sistemi Unix/Linux like e da Windows 2000 in poi…
La sicurezza è un aspetto fondamentale interno al protocollo, non bisogna mai dimenticare che usando una VPN, si instradano informazioni private all'interno di una rete pubblica dotata per natura di poche garanzie di sicurezza. Per questo motivo devono essere presenti meccanismi atti per realizzare la cifratura del traffico e la verifica delle credenziali. Tralasciare questi aspetti fondamentali equivale ad installare una porta ethernet connessa al proprio hub/switch nel posteggio fuori casa dove chiunque può collegarsi ed "ascoltare" il traffico che vi passa…
L'efficienza di una rete protetta è molto legata alle scelte implementate e, dato l'elevato "traffico" generato, particolare attenzione va prestata alla scelta della velocità di connessione usata poiché tutta la gerarchia OSI a partire dal livello 3 dev'essere isolata, subire il processo di cifratura, incapsulata dentro il protocollo VPN ed inserita in nuovo pacchetto TCP/IP. Tutto questo assume valore maggiormente rilevante quando s'impiegano reti VPN basate su Windows.

Esistono diversi tipi di protocolli VPN che offrono differenti livelli di protezione:

→ **PPTP:** ideato da Microsoft, US-Robotics ed altri produttori, facile da configurare, veloce e supportato da tutti i produttori e dai sistemi operativi. Quest'implementazione è presente a partire da Windows NT 4 Server e da Windows 98 SE, non richiede l'uso di hardware particolare poiché il meccanismo di cifratura è molto semplice e per questo motivo garantisce un livello di sicurezza limitato. Manca di un meccanismo "solido" di verifica delle credenziali e generalmente vengono impiegati i "Log-In" del sistema operativo.

→ **L2TP:** derivato dalla fusione di PPTP e di L2F di Cisco, è una sorta di sintesi delle caratteristiche migliori, con meccanismi avanzati di cifratura ed autenticazione. Questo protocollo è supportato da Windows 2000 e dai sistemi Linux Like.

→ **IP sec:** è il miglior protocollo VPN disponibile, sviluppato da IETF. E' in grado di cifrare i dati e gli header dei pacchetti attraverso una chiave pubblica che è scambiata con un meccanismo evoluto di autenticazione, tramite certificati digitali. Questo protocollo è supportato nativamente a partire da Windows 2000 e nei sistemi Linux Like, per Windows 98/ME/NT serve un client dedicato. Se il traffico IPsec è elevato, potrebbe essere necessario l'acquisto di hardware dedicato alle operazioni di cifratura e apertura dei pacchetti. Complessità d'installazione.
Il funzionamento di una VPN può essere spiegato grossolanamente in questo modo:
Si supponga d'avere due host chiamati A e B, che possiedono una chiave pubblica (pkA, pkB) ed una privata (skA, skB), posti ai lati di un tunnel che rappresenta il "corridoio privato" in una rete pubblica. A invia a B la sua pkA e B invia ad A la sua pkA. Assumendo che A debba mandare un

messaggio a B, prende la pkB, codifica il messaggio e lo invia. B, alla ricezione del messaggio codificato con pkB, utilizza la skB per decodificarlo. Tutto ciò può funzionare solo se in fase di configurazione dei tunnels si inserisce la pkA (o la pkB) del PC opposto. Se la pkA (o la pkB) inserite non sono corrette, l'host opposto non può decodificare il messaggio ed il tunnel non viene aperto.

### 9.3 VPN con IPsec usando FreeSWAN

FreeSWAN (www.freeswan.org) è la più diffusa fra le molte implementazioni di IPsec che girano su piattaforma GNU/Linux ed è possibile gestire diversi tunnel VPN, oltre a permettere la comunicazione con altri dispositivi (non necessariamente computer) utilizzando IPsec. Essenzialmente si suddivide in tre componenti principali:
**Klips**, ovvero il modulo del kernel, estremamente sensibile alle variazioni di versione del kernel stesso ed è bene utilizzare la versione relativa a quello usato;
**Pluto**, il demone che gestisce il protocollo per la negoziazione dei tunnel;
**User Tools**, che invocati da IPsec, permettono tutte le operazioni di gestione delle VPN.
Con questa implementazione si possono configurare tunnel **Net-To-Net**, ai cui estremi del tunnel si trovano dei gateway delle due reti remote da connettere, oppure si possono avere delle singole VPN gateway a cui si collegano client remoti anche con IP variabili (dette anche configurazioni **RoadWarrior**, tipicamente utilizzate per i computer portatili).
L'interoperabilità con altri software e device IPsec è decisamente buona, soprattutto se si usano le patch per il supporto di certificati x.509. Esiste tuttavia una versione parallela a quella ufficiale che si base su di essa e aggiunge tutte le patch più interessanti (supporto NAT, x.509, algoritmi di criptazione alternativi a 3DES ecc) è **Super FreeS/WAN** oppure **OpenSWAN** (www.openswan.org). Fino alla versione 1.99 l'unico protocollo di criptazione supportato è 3DES; DES non viene supportato per la scarsa sicurezza, il supporto AES è previsto nelle successive versioni ufficiali e comunque disponibile nelle patch di Super FreeS/WAN. Molte soluzioni VPN basate su GNU/Linux utilizzano FreeS/WAN, spesso con interfacce grafiche che ne semplificano l'installazione e la configurazione. Ulteriore aiuto all'installazione viene fornita dagli archivi pacchettizzati per la propria distribuzione e revisione del kernel, non resta che effettuare il download dei pacchetti desiderati ed installarli dando i comandi con privilegi di root:

```
$rpm –i freeswan-module-x.xx_xx.x.xx.i386.rpm [invio]
$rpm –i freeswan-x.xx_xx.x.xx.i386.rpm [invio]
```

per avviare il tutto si dovrà riavviare oppure dare il comando sempre con privilegi di root:

```
$service ipsec start [invio]
```

è bene usare il metodo d'installazione a pacchetto solo nel caso in cui il kernel in uso sia "standard" della distribuzione e, dove ricompilato, è meglio affidarsi ad una installazione dai sorgenti.

Di default, FreeSWAN, ha il suo file di configurazione in ***/etc/ipsec.conf*** ed un file ***/etc/ipsec.secrets*** contenente le chiavi RSA o gli elementi per l'autenticazione fra host. I certificati e le revocation lists dovrebbero essere nella directory ***/etc/ipsec.d/.***
Nel file di configurazione vi sono molte direttive, dove si intende generalmente il lato sinistro (**left**) come quello **locale** e quello destro (**right**) come quello **Remoto** (questa è solo una convenzione in quanto i termini possono essere scambiati). Lo stesso file di configurazione prevede diverse sezioni, all'interno delle quali si definiscono direttive con sintassi parametro=valore (una per riga, precedute da almeno uno spazio, anche in presenza di # per i commenti, senza righe vuote all'interno della stessa sezione). Le impostazioni generalmente da fornire per ogni tunnel sono:

- Host ID dei server VPN e il modo con cui si autenticano (**hostid**).
- IP pubblico del server locale (**left**)
- IP del suo default gateway pubblico (**leftnexthop**)
- La rete locale a cui il server è collegato (che dovrà essere messa in comunicazione con la rete remota (**leftsubnet**).
- IP pubblico del server remoto (**right**, può essere un **%any** per indicare un IP arbitrario)
- IP del suo default gateway pubblico (**rightnexthop** può essere un generico **%defaultroute**)
- La rete locale a cui il server remoto è collegato (che dovrà essere messa in comunicazione con la rete locale (**rightsubnet**).
- Il metodo di autenticazione utilizzato (**authby**).

La gestione avviene tramite il comando ***ipsec***, con cui si possono gestire tutte le utility fornite con FreeS/WAN:

**ipsec –help**: mostra tutti i comandi eseguibili, per le quali esiste ottima manualistica con prefisso ***ipsec_*** (esempio: **man ipsec_whack**);

Di seguito sono riportate alcune opzioni particolarmente utili:

***ipsec verify***: verifica se il sistema può gestire un tunnel IPsec. Utile per capire in fretta se ci sono problemi di base che precludono il funzionamento;
***ipsec setup - -start:*** avvia il servizio IPsec (carica il kernek module Klips e lancia Pluto per gestire IKE). Coincide, in installazioni basate su RPM a **/etc/rc.d/init.d/ipsec start**.
***ipsec setup - -stop***: ferma il servizio IPsec, droppando tutti i tunnel eventualmente attivi;
***ipsec whack - -status***: mostra lo stato corrente del sistema IPsec;
***ipsec auto - -listall***: elenca tutte le chiavi PSK, RSA o i certificati x509 che possono essere accettati (leggendo i contenuti da **/etc/ipsec.secrets**)*;*
***ipsec newhostkey - -output /etc/ipsec.secrets - -hostname xxx.xxxx.xxx***: genera una nuova chiave RSA per l'host xxx.xxxx.xxx e la aggiunge al file **ipsec.secrets**
***ipsec barf***: visualizza a video una grande quantità di informazioni utili per il debugging e il troubleshooting in caso di problemi.

per capire come funziona FreeSWAN si suggerisce di dare uno sguardo alla configurazione di base che si trova in ***/etc/ipsec.conf***. Considerando le diverse tipologie di costituzione di una LAN, si suggerisce di fare un disegno a "schema a blocchi" della rete stessa, in modo che sia possibile capirne facilmente il funzionamento e come fare le impostazioni di IPsec.

### 9.4 Tunnel tra 2 LAN con IP fissi e connessione ad internet

Vediamo ora come fare prendendo come esempio lo scenario di una configurazione tipica che utilizza un tunnel VPN per connettere due reti LAN, utilizzanti classi di IP fissi, attraverso una rete tipicamente insicura come internet:


Dallo schema a blocchi si evince che sul lato sinistro del tunnel si ha la LAN "A" composta da un router e da tre computer, interconnessi tra loro tramite un HUB/Switch ed utilizzanti classe di IP 10.0.0.X; sul lato destro si ha invece la LAN "B", fisicamente simile alla LAN "A", ma utilizzante la classe di IP 10.0.1.X. I computer che fungono da server per la gestione della VPN sono in questo caso i **"Router"** ai capi della rete pubblica.
Generare le coppie di chiavi pubbliche e private su entrambi i server dando da shell il comando

**$freeswan-x.xx/utils/newhostkey** [invio]

i server risponderanno con una coppia chiavi del tipo:

**pubkey=0bAEOZLco4X72dbAxSumebLFIg4T…**

che si trovano nel file ***/etc/ipsec.secret*** è bene prenderne nota poiché andranno inserite nel file di configurazione dei server, nelle direttive:

**authby=rsasig**
**leftrsasigkey=**'inserire qui la chiave pubblica del router LAN "A"'
**rightrsasigkey=**'inserire qui la chiave pubblica del router LAN "B"'

Si fa presente che lo stesso valore è presente in entrambi i server router e le diciture "left" e "right" non sono riferite agli hosts ma ai lati della rete. Se sulla "carta" si decide che "left" corrisponde alla LAN "A", lo stesso valore sarà identico su entrambi i server router.

E' buona norma NON utilizzare mai le chiavi predefinite da FreeSWAN ma generarne sempre di nuove, affinché la sicurezza non sia compromessa.

Ultimato l'inserimento delle chiavi, si procede alla configurazione della parte relativa agli IP, tenendo presente che i router utilizzano IP pubblici:

```
# LAN "A"
left=xxx.xxx.xxx.xxx
leftsubnet=10.0.0.0/24
leftnexthop=xxx.xxx.xxx.zzz   # IP"esterno"
# Right security gateway, subnet behind it, next hop torward left.
# LAN "B"
right=yyy.yyy.yyy.yyy
rightsubnet=10.0.1.0/24
rightnexthop=yyy.yyy.yyy.www   #IP "esterno"
```

in questo caso **nexthop** si applica solo se la connessione verso internet passa attraverso un router. E' comunque molto importante che gli indirizzi IP siano corretti e che i dispositivi delle due LAN siano pingabili a vicenda. FreeSWAN non connette come una "bacchetta magica" due dispositivi che non siano stati correttamente configurati ed inseriti nella LAN. Per verificare il tunnel sia effettivamente attivo, da shell dare il comando:

```
$ipsec whack  --status [enter]
```

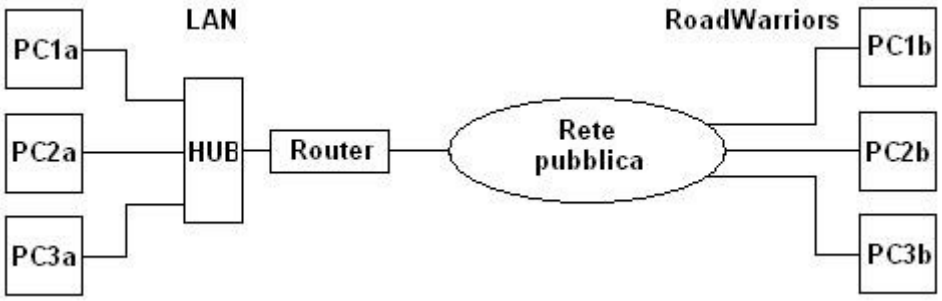
Il codice a seguire, contenuto nel file **/etc/ipsec.conf**, è un esempio di un **tunnel VPN semplice**, ottenuto utilizzando due interfacce di rete: eth0, con IP privato, utilizzata per l'intranet (rete locale) ed eth1, con IP pubblico,  connessa ad internet tramite un router.

```
# basic configuration
config setup
        interfaces="ipsec0=eth1"
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        uniqueids=yes

# defaults for subsequent connection descriptions
conn %default
        keyingtries=0
        spi=0x200
        esp=3des-md5-96
        espenckey=0x01234567_xxxxxx_xxxxxx_xxxxx_xxxxxxx_xxxxxx
        espauthkey=0x12345678_xxxxxxxx_xxxxxxx_xxxxxxx
```

```
conn tunnel
      # Left security gateway, subnet behind it, next hop toward right.
      # LAN "A"
      left=xxx.xxx.xxx.xxx
      leftsubnet=10.0.0.0/24
      leftnexthop=xxx.xxx.xxx.zzz  # Esterna
      # Right security gateway, subnet behind it, next hop toward left.
      # LAN "B"
      right=yyy.yyy.yyy.yyy
      rightsubnet=10.0.1.0/24
      rightnexthop=yyy.yyy.yyy.www # Esterna
      keyingtries=0
      auto=start
      # RSA authentication with keys from DNS.
      authby=rsasig
            leftrsasigkey='chiave pubblica del server-router LAN "A"
            rightrsasigkey='chiave pubblica del server-router LAN "A"
```

### 9.5 Tunnel tra LAN e portatili connessi ad internet

Quella che verrà qui descritta è la tipica situazione che si incontra quando si deve scambiare dati importanti o comunque rendere sicura la connessione tra computer portatili ed una rete locale, passando attraverso internet. Facendo riferimento ad uno schema "a blocchi", l'esempio semplificato può essere così raffigurato:




Il lato LAN (intranet) utilizza IP fissi di classe 10.0.0.X mentre i **RoadWarriors** utilizzano il DHCP, il cui indirizzo viene fornito dal server-router. Procediamo comunque a piccoli passi, specificando cosa viene indicato con RoadWarriors che tradotto letteralmente in italiano significa "guerriero di strada" e si riferisce usualmente a computer (in particolar modo ai portatili) che cambiano spesso indirizzo IP e si collegano da qualsiasi punto della rete.
Non potendo in una situazione del genere contare sull'utilizzo di IP fissi, per l'autenticazione si potranno usare i certificati x509 rilasciati dall'amministratore della intranet a coloro che hanno il permesso di collegarsi da remoto alla LAN. Per usufruire dei certificati x509, FreeSWAN necessita delle apposite patch.
Si supponga che il server GNU/Linux che funge da router ha un IP pubblico del tipo 213.102.0.2 ed è raggiungibile da qualsiasi punto della rete... è molto importante che sia un IP pubblico, non NAT!.
Il file ***ipsec.conf*** conterrà:

```
….
right=%any
rightrsasigkey=%cert
leftid=@server.nome.xx
left=213.102.0.2
leftnexthop=’mettere IP del router se presente’
leftsubnet=10.0.0.0/24
… .
```

Come già visto nel capitolo precedente, a FreeSWAN bisogna dire quali sono i lati del tunnel.
Nella direttiva “right” la variabile ***“%any”*** indica un qualsiasi IP, in questo caso l'eventuale PC che fa da RoadWarriow.
Nella direttiva “left” l'IP pubblico del server. Se il nostro server, che ha come nome canonico ***“server.esempio.it”*** è connesso ad Internet tramite un router è opportuno indicare l'IP di quest'ultimo nella direttiva ***“leftnexthop”***. La direttiva ***“leftsubnet”*** indica a FreeSWAN la classe di indirizzi IP della rete locale a "sinistra" del server, in questo caso 10.0.0.X. Il metodo di autenticazione per la parte a destra (***“right”***) del tunnel è ***“%cert”***, perciò è richiesto un certificato ed è specificata dalla direttiva ***“rightrsasigkey”***.
Il certificato usato sarà specificato nelle direttive del tunnel:

```
conn roadwarrior
        right=%any
        rightid="C=IT, ST=Italy, L=’inserire località’, O=’organizzazione…’"
        rightsubnetwithin=10.0.0.0/23
        leftsubnet=10.0.0.0/24
```

La direttiva ***“rightid”*** contiene i dati del certificato da usare per autenticare il client:
In ***“C=”*** inserire la sigla dello stato di appartenenza;
In ***“ST=”*** inserire lo stato di appartenenza;
In ***“L=”*** inserire la località dove sta il server come ad esempio “Livorno”, “Pisa”, ecc ecc;
In ***“O=”*** inserire il nome dell’organizzazione o un nome di fantasia della rete.
La descrizione delle singole direttive e relativa sintassi sono contenute in ***man ipsec.conf***.

Il codice a seguire mostra il codice delle impostazioni di ***ipsec.conf, dhcp.conf, DHCPRelay e x509 (SSL)*** tenendo presente che sia eth0 che eth1 utilizzano IP pubblici ed eth2 è l’interfaccia della intranet. Ipsec0 è bindato su eth0.

*/etc/ipsec.conf:*

```
# basic configuration
config setup
        interfaces="ipsec0=eth0"
        klipsdebug=none
        plutodebug=none
        plutoload=%search
        plutostart=%search
        uniqueids=yes
        strictcrlpolicy=yes
        dumpdir=/root

# defaults for subsequent connection descriptions
# (these defaults will soon go away)
conn %default
        keyingtries=3
        compress=yes
        disablearrivalcheck=no
        authby=rsasig
        keyexchange=ike
        ikelifetime=240m
        keylife=60m
        pfs=yes
        esp=3des
        right=%any
        rightrsasigkey=%cert
        leftid=@[Nome canonico del server]
        left=[IP del Server]
        leftnexthop=[Eventuale IP del router - Il gateway del server]
        leftsubnet=10.0.0.0/24
        leftupdown=/usr/local/lib/ipsec/updown.x509
        leftcert=/etc/ipsec.d/myCert.pem
        auto=add

conn dhcp
        rekey=no
        keylife=30s
        rekeymargin=15s
        leftprotoport=udp/bootps
        rightprotoport=udp/bootpc

conn roadwarrior
        right=%any
        rightid="C=IT, ST=Italy, L='inserire località', O='organizzazione…'"
        rightsubnetwithin=10.0.0.0/23
        leftsubnet=10.0.0.0/24

conn roadwarrior-sentinel
        right=%any
        rightid="C=IT, ST=Italy, L=Siena, O=....."
        leftsubnet=0.0.0.0/0
        rightsubnetwithin=10.0.0.0/24
```

*/etc/ipsec.secrets:*

```
: RSA   /etc/ipsec.d/private/myKey.pem "mysecretkey"

/etc/dhcpd.conf

# Intranet configuration file for ISC dhcpd
option domain-name "xxxx.it";
option domain-name-servers ns1.xxxx.it, ns2.xxxx.it;
default-lease-time 600;
max-lease-time 7200;
ddns-update-style ad-hoc;
authoritative;
log-facility syslog;

class "vpn-clients" {
      match if option agent.circuit-id = "ipsec0";
}

subnet 0.0.0.0 netmask 0.0.0.0 {
      ddns-updates off;
      ddns-hostname "10.0.0.1";
      option x-display-manager 10.0.0.1;
      option domain-name-servers 10.0.0.1;
      option domain-name "firewall.xxxxx.it";
      option subnet-mask 255.255.255.0;
      option host-name "firewall.xxxx.it";
      option routers 10.0.0.1;
      option broadcast-address 10.0.0.255;
      pool {
         allow members of "vpn-clients";
         range 10.0.0.201 10.0.0.220;
         default-lease-time 3600;
         max-lease-time 7200;
      }
      pool {
         deny members of "vpn-clients";
         range 10.0.0.20 10.0.0.200;
         default-lease-time 7200;
         max-lease-time 14400;
      }
}
```

*/usr/local/etc/dhcprelay.conf:*

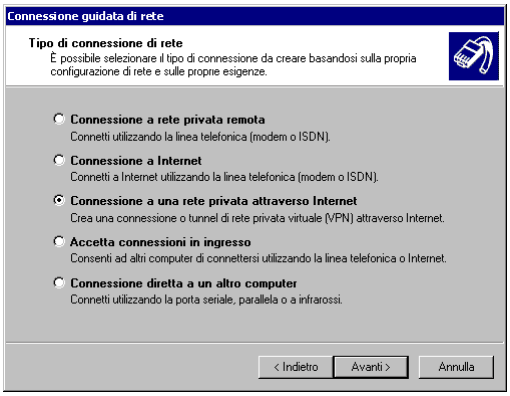
```
# DHCP-Relay configuration file
# $Id: VPN-IPsec-Freeswan-HOWTO.html,v 1.1.1.1 2006/04/16 16:13:49 pragma Exp $

# Logfile
LOGFILE="/var/log/dhcprelay.log"

# IPSec devices (comma separated list including NO spaces)
DEVICES="ipsec0"

# Device over which the DHCP-Server can be reached
SERVERDEVICE="lo"

# Hostname or IP Address of the DHCP-Server
DHCPSERVER="10.0.0.1"
```

## 9.6 PPTP in ambiente Windows (client)

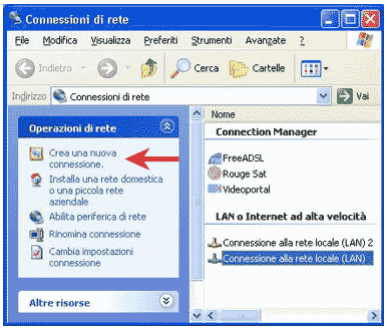
Come già spiegato nell'introduzione alle reti VPN, questo protocollo è stato ideato da Microsoft e risulta quindi di semplice implementazione malgrado le mancanze di cui soffre. Vediamo ora come implementarlo a piccoli passi, per gli O.S. Microsoft Windows 2000 e Windows XP, immaginando di collegarci ad un nostro server:

**A)** Apriamo **Rete e connessioni remote** dal menù **Start → Impostazioni** in Windows 2000; **Start → Impostazioni → Connessioni di rete** in Windows XP.

Win 2000

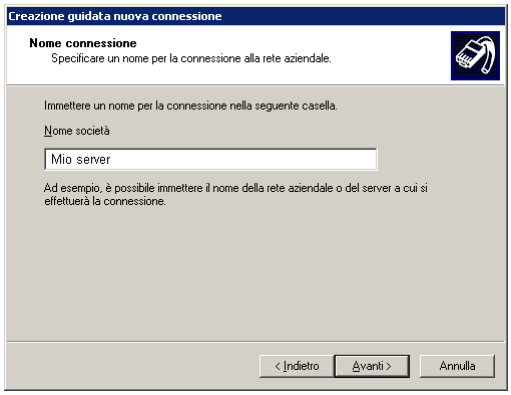


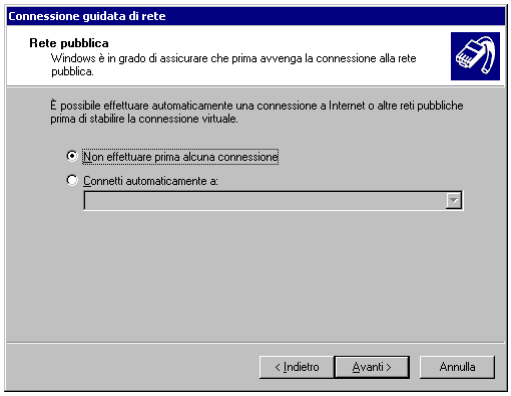

Win XP



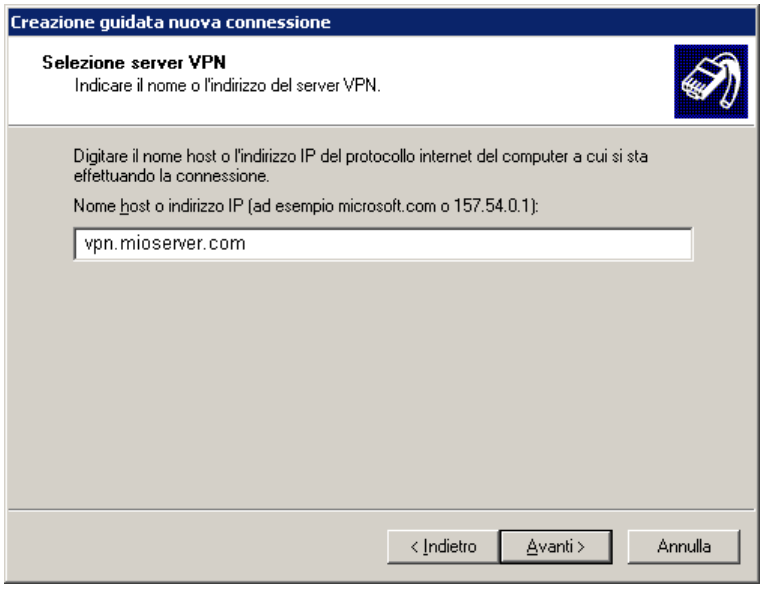

Avviare la creazione guidata ad una nuova rete e selezionare "**Connessione a una rete privata attraverso internet**" in Win 2000. Con Win XP la procedura è leggermente diversa ma molto intuitiva. Cliccare nel menù sulla sinistra "**Crea una nuova connessione**", cliccare sul pulsante **avanti**, selezionare "**Connessione alla rete aziendale**", cliccare su **avanti**, selezionare ora "**Connessione VPN**" ed ancora sul pulsante **avanti**. A questo punto si dovrà immettere il nome della connessione.

**B)** Siccome il tunnel VPN funziona in una connessione tradizionale, sarebbe bene istruire Windows affinché si connetta automaticamente con la stessa. Se non si desidera che ciò avvenga e preferite che siate voi a decidere quando avviarla, selezionate il pulsante radio opportuno:

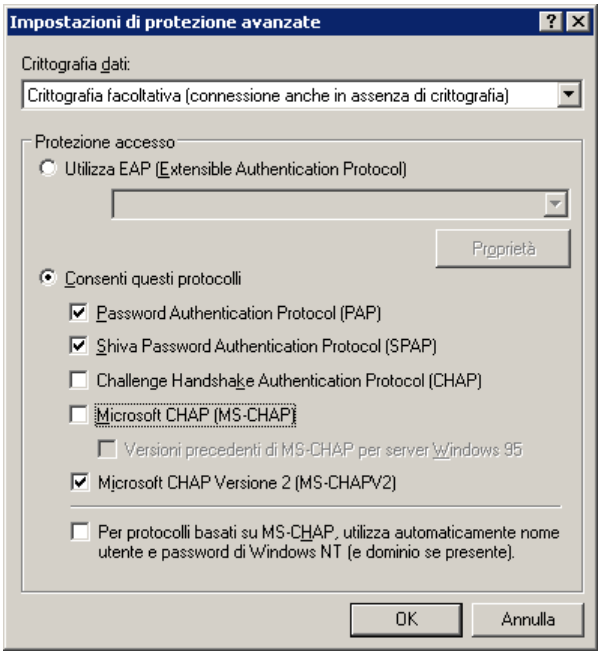


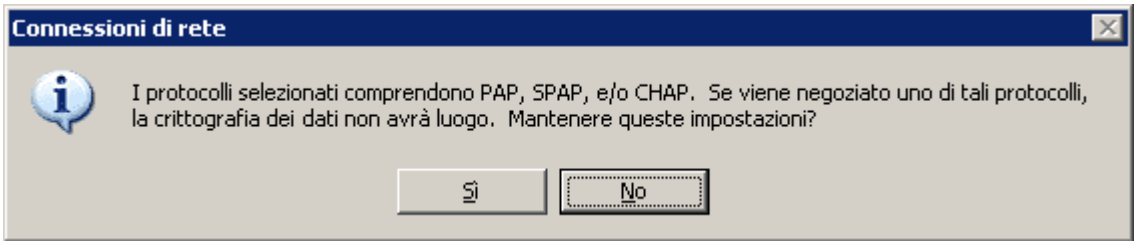
**C)** Affinché sia terminata questa prima fase, immettere il nome dell'host o l'indirizzo IP del server:




**D)** Mancano pochi passi per ultimare la connessione appena creata che sarà ora presente tra l'elenco delle connessioni disponibili. Selezionare e richiamare le proprietà, affinché si possano effettuare le dovute impostazioni. Spostarsi sulla linguetta **Protezione** e selezionare **Avanzate (impostazioni personalizzate)**. Cliccare ora sul pulsante laterale **Impostazioni** per accedere alla crittografia dati:

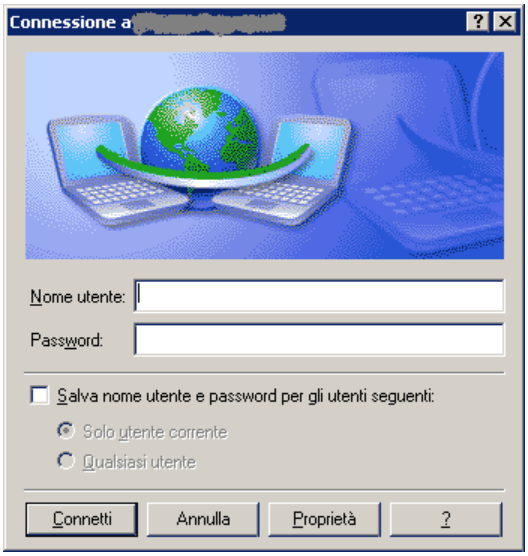



Selezionare ora i protocolli o il protocollo usato dal server per il tunnel VPN tenendo presente che se nel campo **Crittografia dati** viene scelto ***Crittografia facoltativa***, e nella sezione protocolli si spuntano **Password Autentication Protocoll (PAP), Shiva Password Autentication Protocoll (SPAP)** e **Microsoft CHAP Versione 2 (MS-CHAPV2)**, cliccando su **OK** per confermare le impostazioni, apparirà una finestra di avvertimento:




Siccome il tunnel VPN è creato per rendere le connessioni sicure, è bene che tale avvertimento non appaia. Operare quindi in modo da rendere la crittografia sempre abilitata.

**E)** Avviare la connessione, immettere user e password ed avrete un bel tunnel VPN attivo verso il vostro server dopo qualche istante:



## 9.7 VPN PPTP in ambiente GNU/Linux

L'implementazione pptp open source più diffusa è **PopTop** ed utilizzata per permettere ad un sistema GNU/Linux, di fare da server PPTP per client che supportano questo protocollo per VPN che è implementato nativamente su Windows. Per funzionare PopTop si appoggia su **pppd** normalmente disponibile nelle varie distribuzioni GNU/Linux e richiede una configurazione relativamente semplice, ma se si deve operare con client Windows e supportare i suoi metodi di autenticazione (MSCHAP v2) e criptazione (MPPE) è necessario disporre del modulo **mppe** nel kernel, con complicazioni in più per le impostazioni iniziali. Sul sito di PopTop sono presenti diversi tipi di file, dai sorgenti ai pacchetti precompilati per alcune distribuzioni GNU/Linux, che comprendono:

→ **mppe module builder**: serve per avere il supporto mppe e qundi avere piena interoperabilità con client Windows. Vengono utilizzati due componenti come **dkms** che permette di ricompilare "al volo" moduli aggiuntivi del kernel quando questo viene aggiornato (evitando che il modulo mppe diventi inutilizzabile al primo aggiornamento del kernel) ed il modulo mppe, **kernel_ppp_mppe**, pacchettizzato in modo da essere usato con dkms;

→ **ppp**: contenente anche il server pppd in una versione aggiornata e patchata per supportare mppe poiché quella presente nella propria distribuzione potrebbe non esserlo;

→ **pptpd**: il server PopTop in "carne e ossa".

Per l'installazione si possono seguire due strade e cioè compilando i pacchetti sorgenti come spiegato sul sito oppure usare i pacchetti rpm precompilati dei sorgenti (xxx.src.rpm) e generarsi il pacchetto rpm su misura per il proprio computer, dando il comando:

```
$rpmbuild –ba /usr/src/redhat/SPEC/pptpd.spec [invio]
```

Per la distribuzione Debian, pptpd è direttamente disponibile e basta dare il comando:

```
$apt-get install pptpd [invio]
```

I file di configurazione principali sono tre e precisamente:

→ **/etc/pptpd.conf** contenente le informazioni su quali IP assegnare ai client che vi si collegano e qualche altro parametro che normalmente non viene modificato. Solitamente può presentarsi con poche righe di codice del tipo:

***option /etc/ppp/options.pptpd***: la posizione del file delle configurazioni ppp per connessioni pptp; ***localip xxx.xxx.xxx.xxx***: l'indirizzo IP del server pptp sulla rete interna (LAN); ***remoteip xxx.xxx.xxx.zzz-yyy***: il range di IP da assegnare ai client che si collegano alla rete interna; ***bcrelay eth(x)***: viene abilitato il broadcast dai client alla rete interna tramite l'ethernet eth(x). Questa direttiva è necessaria per quei protocolli che si basano sul broadcast per funzionare correttamente; necessario quando si vogliono sfogliare le reti di Windows.

→ **/etc/ppp/option.pptpd** la cui configurazione è di fondamentale importanza poiché contiene i parametri ppp con il metodo di criptazione dei dati ed i metodi di autenticazione. Serve altresì per definire se usare il protocollo mppe e ne esistono due diverse sintassi a seconda della versione del

pppd installata. La sintassi vecchia, che vale per il fork mppe compatibile di **ppp 2.4.1**, prevede parametri come:

***-chap*** rifiuta l'autenticazione CHAP;
***-mschap*** rifiuta l'autenticazione MSCHAP v.2;
***+chapms-v2*** forza l'uso dell'autenticazione basata sul MSCHAP v.2;
***mppe-128*** imposta il supporto mppe con cifratura a 128 bit;
***mppe-stateless*** abilita mppe in modalità stateless.

Questi parametri sono quelli che forzano MSCHAP2 e mppe; sono compatibili con le impostazioni standard delle VPN Windows.
Nella nuova sintassi, valida per **ppp 2.4.2** e successive revisioni, prevede sempre per i parametri di default per client Windows:

***refuse-pap*** rifiuta l'autenticazione PAP (plaintext);
***refuse-chap*** rifiuta l'autenticazione CHAP;
***refuse-mschap*** rifiuta l'autenticazione MSCHAP;
***require-mschap-v2*** forza all'uso dell'autenticazione basata su MSCHAP v.2;
***require-mppe*** imposta il supporto mppe con cifratura a 128 bit;
***nomppe-stateful*** abilita mppe in modalità stateless.

Gli altri parametri presenti e generalmente usati sono comuni a tutte le versioni:

***lock*** crea un file di lock per il server ppd. Se dubbiosi nell'uso, è bene lasciarlo;
***debug*** abilita il debug della connessione ed il log solitamente si trova in **/var/log/messages**;
***name nome_server*** imposta il nome del server pptpd e deve conincidere con quanto inserito nella direttiva presente in **/etc/ppp/chap-secrets**;
***mtu 1500*** imposta la dimensione MTU dei pacchetti;
***auth*** richiede l'autenticazione del client ed è necessario su un server ppp;
***proxyarp*** imposta sul server una arp entry con l'IP assegnato al client ed è necessario per rendere visibile il client agli altri computer nella LAN del server;
***nobsdcomp*** disabilita la compressione BSD;
***ms-wins 10.0.0.10*** imposta l'indirizzo IP (qui 10.0.0.10) del server WINS da assegnare ai client;
***ms-dns 10.0.0.10*** imposta l'indirizzo IP (qui 10.0.0.10) del server DNS da assegnare ai client.

→ **/etc/ppp/chap-secret** contiene i log-in e le password utilizzabili per i collegamenti. La sintassi è semplice e prevede una riga per utente, con i seguenti dati separati da un tab:

nome_utente nome_server password IP

il nome utente dev'essere specificato con l'opzione "name" in /etc/ppp/options.pptpd;
la password dev'essere in chiaro;
IP indica da quale indirizzo il client può collegarsi oppure usare * per non avere restrizioni.

L'esempio classico potrebbe essere:

```
mario     nome_server    mario_password *
```

Se si è compilato pptp con il supporto smbauth, è possibile autenticare gli utenti via samba, con una configurazione tipo:

```
*     nome_server     &/etc/samba/smbpasswd     *
```

E' inoltre possibile autenticare gli utenti usando un server radius.
Per ogni client connesso bisogna creare una nuova porta o interfaccia sul server, a partire da **ppp0** per il primo, **ppp1** per il secondo, **ppp3** per il terzo, eccetera…
A livello di firewall si devono considerare alcuni aspetti importanti come:
- il traffico dev'essere abilitato nella catena di FORWARD, fra la rete interna del firewall e le interfacce ppp(X). Si possono anche configurare le limitazioni che servono come il solo accesso a determinati host interni ecc…
- l'interfaccia esterna del server VPN deve permettere l'accesso dall'IP del client, alla porta tcp 1723 per l'autenticazione, ed il protocollo di trasporto GRE (ip type 47) per il tunnel.
- l'ip forwarding deve essere abilitato sul kernel.

Un esempio di configurazione di iptables su un VPN server dove eth0 è l'interfaccia interna e l'eth1 è quella esterna può essere quello seguente, per due collegamenti ppp contemporanei:

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -p tcp --dport 1723 eth1 -j ACCEPT
-A INPUT -p gre -i eth1 -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A FORWARD -i eth0 -j ACCEPT
-A FORWARD -i ppp0 -j ACCEPT
-A FORWARD -i ppp1 -j ACCEPT
-A FORWARD -m state -state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -m state --state NEW,RELATED,ESTABLISHED -j ACCEPT
COMMIT
```

In genere un server VPN dev'essere accessibile da alcuni IP esterni e avere una interfaccia su una rete interna. Non è il massimo avere le porte su cui si negozia il tunnel sempre accessibili e bisognerà perciò prendere tutte le precauzioni al riguardo.

# Bluetooth

## 10.1 Introduzione e caratteristiche

Sempre più dispositivi portatili vengono forniti equipaggiati di connessione Bluetooth. E' così possibile che lo scambio di dati tra telefono cellulare, PDA, fotocamere e PC sia discretamente semplice da realizzare. Questa tecnologia nasce nel 1998 su iniziativa del SIG (Special Interest Group) di cui inizialmente fanno parte solo Intel, Ericsson, Nokia, IBM e Toshiba, con lo scopo di progettare un dispositivo comune di comunicazione via onde radio, caratterizzato da potenza di trasmissione, consumo energetico e costi di produzione ridotti. Il suo nome, che letteralmente significa “Dente Blu”, deriva da una traduzione non proprio riuscita del nome “Harold Blatand”, re Danese del X secolo (940 circa) che riuscì ad unire le tribù di Danimarca, Norvegia e Svezia, geograficamente vicine ma culturalmente diverse. Data la sua caratteristica principale di bassa richiesta energetica, il Bluetooth viene utilizzato in particolar modo sui dispositivi mobili ma non di rado si trova anche su stampanti, tastiere e mouse. Esistono essenzialmente due tipi di adattatori per PC: i dongle USB (chiamate volgarmente penne USB) e le schede PCMCIA. I computer portatili di fascia alta sono generalmente dotati di questa tecnologia, integrata sulla scheda madre tramite il bus USB. Lo standard Bluetooth utilizza la stessa frequenza del Wi-Fi (2,4GHz, suddivisa però in 79 canali) ma con modulazione FHSS (Frequency Hopping Spread Spectrum, consiste cioè nel saltare di frequenza in frequenza all'interno di una banda molto ampia per 1600 volte al secondo, seguendo una particolare sequenza generata da un algoritmo noto al trasmettitore ed al ricevitore associato) e potenze che raramente superano i 2,5mW; per questo motivo, comunicazioni Bluetooth e Wi-Fi non interferiscono tra loro. Di questo standard esistono tre classi che si differenziano essenzialmente per la potenza usata:

| Classe | Potenza mW | Potenza dBm | Distanza (m) |
|---|---|---|---|
| 1 | 100 | 20 | 100 |
| 2 | 2,5 | 4 | 10 |
| 3 | 1 | 0 | 1 |

Facendo parte delle PAN (Personal Area Network), il Bluetooth non permette di raggiungere velocità e copertura di trasmissione dati elevate. La sua ragione d'essere è quella di collegare in modo semplice ed affidabile piccoli dispositivi, con particolare attenzione alla durata delle batterie. La sua condizione di esercizio tipica è quella di un'area con estensione inferiore ai 15 metri. Del Bluetooth esistono diverse “revisioni” dello standard che si differenziano dalla velocità di trasmissione dati, come mostrato nella tabella seguente:

| Revisione | Velocità | Note |
|---|---|---|
| 1.1 | 723,2 Kbps | Modulazione FHSS (Frequency Hopping Spread Spectrum). |
| 1.2 | 723,2 Kbps | Modulazione AFH (Advanced Frequency Hopping), simile a FHSS ma con possibilità di evitare le frequenze più affollate. |
| 2.0 | 2,1 Mbps | Aumento della potenza assorbita. Vengono usati segnali più brevi, dimezzando così la potenza richiesta dalla 1.2 a parità di traffico inviato. |
| 2.1 | 3 Mbps | Minore richiesta energetica e migliore gestione del pairing. |

| Revisione | Velocità | Note |
|---|---|---|
| 3.0 | 400 Mbps | Futura evoluzione che implementerà lo streaming di contenuti video |

Un link Bluetooth può trasportare sia traffico dati che voce. Le trasmissioni voce utilizzano link di tipo SCO (Synchronous Connection Oriented), occupando 64 Kbps per direzione e possono essere al massimo tre per PAN. Le trasmissioni dati usano link di tipo ACL (Asynchronuos Connection Less), tipicamente asimmetrici, che nella revisione 1.x raggiungono una velocità massima di 723,2 Kbps in una direzione e 57,6 Kbps in quella opposta, ma sono possibili anche link simmetrici da 433,9 Kbps. Nel caso di link asimmetrici il master ottiene la velocità maggiore, ma è comunque possibile che ad un qualsiasi momento, master e slave possono scambiarsi di ruolo, raggiungendo in questo modo la velocità massima; questo tipo di link è estremamente vantaggioso. Una rete composta da un master ed uno o più slave, prende il nome di Piconet, tuttavia un master può essere slave di un master di un'altra Piconet: l'insieme delle Piconet prende il nome di Scatternet. Come si è potuto notare, il Bluetooth è estremamente flessibile ed è anche possibile creare link dati Ipv4 (link di tipo BNEP), link seriali (link di tipo RFCOMM) che possono inviare comandi interattivi come ad esempio il set di comandi AT, che vengono interpretati dai modem, fino ai protocolli studiati appositamente per trasferire file binari (link OBEX).
Di seguito è possibile vedere alcune foto di adattatori Bluetooth:

| USB to Bluetooth | LAN to Bluetooth | Compact Flash to Bluetooth |
|---|---|---|
|  |  |  |
| DBT-122 | DBT-900ap | DCF-650BT |

Giunti a questo punto vi starete sicuramente chiedendo perché parlare del Bluetooth in una guida che tratta le W-LAN con un occhio particolare alle reti Wi-Fi... Semplice, questo standard non sostituisce il Wi-Fi, ma è complementare poiché è possibile fornire connettività e condivisione dei servizi da/a dispositivi mobili, arricchendo la propria LAN di funzionalità particolari, oltre al fatto che usando la stessa frequenza, costituisce ulteriore spinta al modding ed all'hacking!!!

## 10.2 Modding

Modificare un adattatore non è un'operazione difficile e, in linea di principio, è come modificare un qualsiasi adattatore Wi-Fi, salvo tener presente che esistono differenze nei componenti presenti. Prima di cimentarsi nell'opera, occorre reperire il materiale che serve, oltre ad un saldatore con punta fine, anzi finissima, date le minuscole dimensioni dei particolari su cui si dovrà intervenire; una lente d'ingrandimento faciliterà alcune operazioni, nonché la verifica di quanto fatto. Nell'esempio successivo si modificherà una dongle USB della MSI, dotandola di presa MMCX a montaggio superficiale:

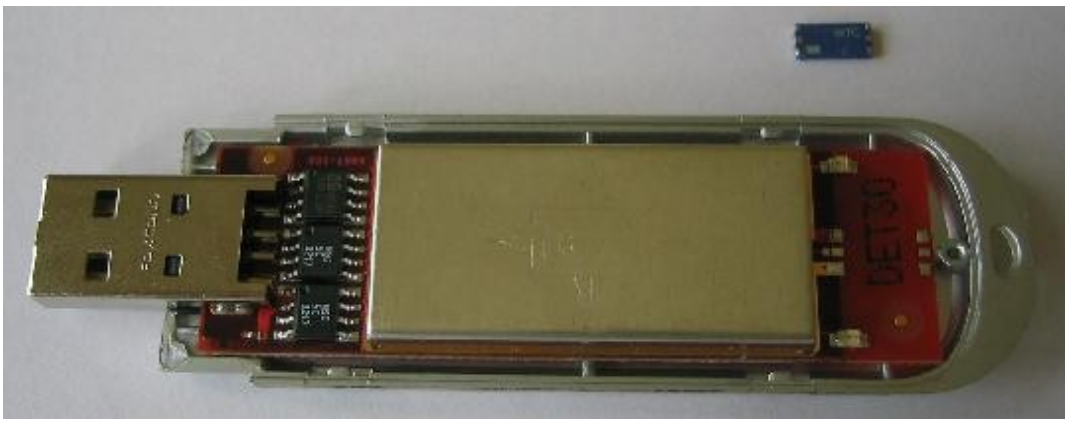
→ Apertura della Dongle:

Prendere un cacciavite piano a taglio fine ed inserirlo dolcemente nell'intersezione laterale tra i due gusci che costituiscono l'involucro... Ogni dongle ha le sue linguette di ancoraggio in punti diversi, perciò bisogna prestare attenzione, cercando di far scorrere lateralmente il cacciavite quanto più possibile. Eseguita l'apertura, si ottiene qualcosa del genere:

Dall'immagine è possibile osservare che, come avviene per gli adattatori Wi-Fi, tutta l'elettronica è racchiusa da una schermatura metallica... Ciò che più interessa è l'antenna, quel componente a montaggio superficiale di colore blu, perfettamente visibile sul lato destro. Sebbene sia dotata di 6 "piedini", gli adattatori Bluetooth non hanno due antenne ed il circuito del "diversity", facilitando notevolmente l'operazione di modding!

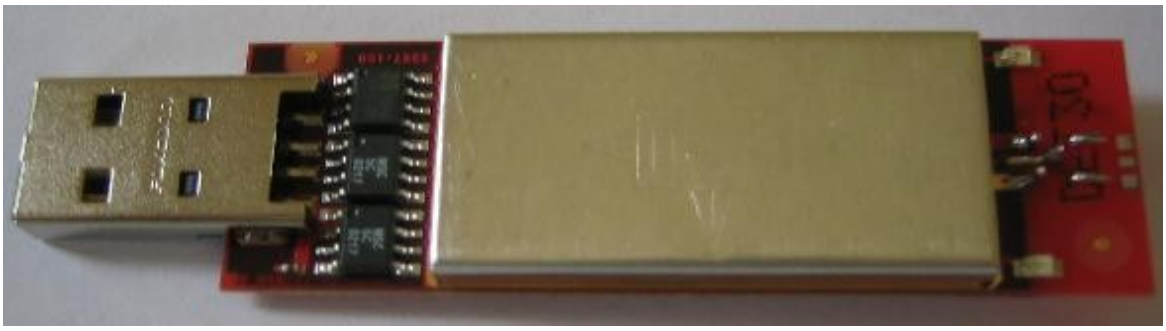
→ Rimozione dell'antenna SMD:

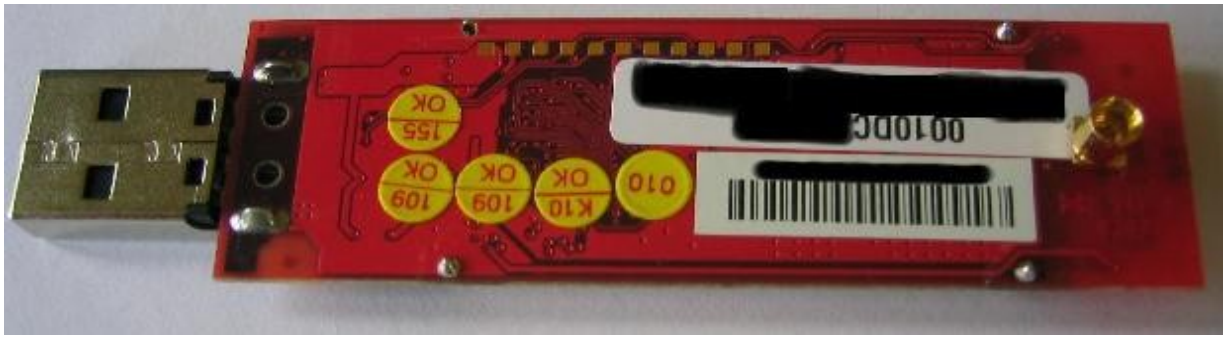
Rimuovere l'antenna utilizzando il saldatore ed il succhia-stagno; in alternativa anche un pezzetto di treccia dissaldante può fornire un buon risultato. Prestare la massima attenzione, le piste del circuito stampato coinvolte nell'operazione sono veramente sensibili. Se l'operazione ha avuto un buon esito, si otterrà quanto mostrato nella figura a seguire:



➔ Montaggio del connettore MMCX:

Come prima operazione occorre rimuovere lo stampato dal secondo guscio e praticare 5 piccoli fori sul PCB della scheda in modo tale che il connettore MMCX si posizioni con precisione al posto dell'antenna originale, ma sul lato opposto... Il connettore MMCX ha 4 “piedini” di massa collegati alla base che servono per “ancorarlo” al PCB. Al polo “caldo” si suggerisce di saldare un pezzo di filo di rame fine. Quest'ultimo andrà infilato nel quinto foro che andrà praticato nel centro dei quattro laterali. Piegare e tagliare i piedini di ancoraggio a sufficienza, in modo tale da saldarli alla massa dell'antenna, piazzole superiori ed inferiori a lato dell'antenna originale... Il polo caldo, quello che porta il segnale, andrà saldato alla piazzola centrale lato sinistro.
Siccome è più semplice a farsi che a dirsi, è utile prendere visione delle immagini che seguono che illustrano come dev'essere eseguito il lavoro:





→ Rifiniture e chiusura:

Utilizzando una punta da 4 mm, praticare un foro nel punto preciso dove il connettore uscirà dalla scocca. Riposizionare i gusci e imprimere una leggera pressione in modo che le linguette d'ancoraggio facciano presa tra loro. Ora l'adattatore Bluetooth ha una bella presa d'antenna esterna ed è possibile collegarci anche una parabola da 24dB...


si ricorda che in commercio esistono molti tipi di adattatori USB Bluetooth la cui elettronica, almeno nei pressi dell'antenna, difficilmente presenta sostanziali differenze. Non si hanno notizie riguardo le tecniche di apertura di altri adattatori, perciò conviene prestare la massima attenzione durante tale operazione, in modo d'evitare la rottura dei coperchi. Non usare per nessun motivo tecniche "a forza bruta", ma utilizzare forza quanto basta per capire come e dove sono disposti gli agganci.

### 10.3 Installazione e configurazione

Installare il driver di un adattatore Bluetooth su Windows 2000/XP non è un'operazione difficile. Le cose si complicano, invece, quando si ha a che fare con distribuzioni GNU/Linux. Fortunatamente le specifiche di questo protocollo sono libere ed ha portato a diverse implementazioni nel kernel. Tra tutte, si prenderà in considerazione solo BlueZ poiché è un progetto più maturo, inserito nel kernel a partire dalla serie 2.4 e di facile installazione. Prima di buttarsi a pesce nell'opera, conviene verificare se il proprio adattatore sia presente nella lista di compatibilità, disponibile al seguente link: http://www.holtmann.org/linux/bluetooth/features.html
La maggior parte degli adattatori USB sono supportati perfettamente dal modulo generico **hci_usb** poiché basati sul chipset **CSR** (Cambridge Silicon Radio) ma esistono alcune eccezioni:

- **AVM BlueFRITZ**: pur essendo un adattatore USB, si comporta come una seriale. E' necessario utilizzare un apposito modulo (**bfusb**), posizionando il file **bfubase.frm** all'interno di **/lib/firmware**;
- **Broadcom Bluetonium**: come sopra ma richiede i file **BCM2033-FW.bin** e **BCM2033-MD.hex** in **/lib/firmware** e che venga caricato il modulo **bcm203x**.

Occorre altresì verificare che il kernel in uso disponga del supporto al Bluetooth, provando a caricare con **modprobe** i moduli **l2cap, hci_usb, bluetooth, bnep** (opzionale)**, rfcomm** (opzionale). Se così non fosse, occorrerà ricompilare il kernel poiché è necessario aver abilitato le seguenti voci nel menù di configurazione **Networking/Bluetooth subsystem support**:

```
L2CAP protocol support
SCO links support
RFCOMM protocol support
RFCOMM TTY support
BNEP protocol support
Multicast filter support
Protocol filter support
HIDP protocol support
Bluetooth device driver -->
                            HCI USB driver
                            SCO (voice) support
                            HCI BCM203x USB driver
                            HCI BPA10x USB driver
                            HCI BlueFritz! USB driver
```

Essendo i dispositivi USB rimovibili, è meglio compilare quanto sopra come moduli. Se invece l'adattatore è integrato sulla scheda madre, come accade sui portatili di fascia alta, allora è meglio compilare quanto sopra come statici all'interno del kernel. Ricompilato ed installato, ricaricare i moduli come visto sopra (modprobe) e dare il comando **lsmod**, verificando che siano presenti:

```
l2cap          14752  5       (autoclean)
hci_usb        6816   1       (autoclean)
bluetooth      28032  3       (autoclean)   [rfcomm      l2cap   bnep   hci_usb]
```

ed opzionalmente

```
Bnep      9860      2      (autoclean)
rfcomm 27744        0      (autoclean)
```

si consiglia di ricavare ulteriori informazioni di verifica dando il comando **dmesg** che dovrebbe dare un output simile:

```
Bluetooth:    HCI USB driver ver 2.9
usbcore:      registered new driver hci_usb
Bluetooth:    BNEP (Ethernet Emulation) ver 1.2
Bluetooth:    BNEP filters: protocol multicast
```

OK, ora il kernel dispone del supporto Bluetooth e non resta che installare i programmi necessari che a seconda della distribuzione usata assume il seguente comando:

- **Red Hat/Fedora:** yum install bluez-utils bluez-libs bluez-hcidump
- **Debian/Ubuntu:** apt-get install bluez-utils libbluetooth1 bluez-hcidump bluez-pin
- **Mandriva:** rpmi bluez-utils bluez-hcidump libbluez2 bluez-pin
- **Suse:** yast --install bluez-utils bluez-libs bluez-hcidump
- **Gentoo:** emerge bluez-utils libbluetooth1 bluez-hcidump bluez-pin

cosa fanno i programmi installati? Una brave descrizione è utile per capire:

- **bluez-utils:** contiene i vari programmi indispensabili per configurare i dispositivi Bluetooth. In alcune distribuzioni questo pacchetto è suddiviso in bluez-pan e bleuz-sdp;
- **bluez-libs o libbluetooth:** contiene le librerie richieste;
- **bluez-pin:** permette di specificare il PIN segreto durante l'associazione di un dispositivo;
- **bluez-hcidump:** permette di sniffare il traffico Bluetooth.

All'interno di bluez-utils si trovano questi programmi:

- **hcid:** è il Bluetooth Host Controller Interface Deamon che stabilisce le connessioni con gli altri dispositivi ed effettua se necessario il pairing, cioè l'autenticazione;
- **sdpd:** è il Service Discovery Protocol Deamon che annuncia agli altri dispositivi i servizi che sono messi a disposizione;
- **rfcomm:** permette di emulare delle connessioni seriali RS232 su un link Bluetooth.

La configurazione del sistema avviene tipicamente mediante i file **hcid.conf** e **rfcomm.conf** presenti nella directory **/etc/bluetooth**.
Procedendo con ordine, vediamo com'è strutturato il file **hcid.conf**:

```
device {
        name "Linux-BlueZ";
        class 0x120104;
        iscan enable;
        pscan enable;
        lm accept;
        lp rswitch, hold, sniff, park;
        auth enable;
        encrypt enable;
}

options {
        autoinit yes;
        security auto;
        passkey "1234";
        pairing multi;
}
```

Nella sezione **device** si trovano le seguenti impostazioni:

- **name:** definisce il nome con il quale si presenterà agli altri dispositivi la Linux-Box;
- **class:** definisce con un codice esadecimale la tipologia di dispositivo sul quale il chip Bluetooth è stato installato (computer, stampante, telefono, fotocamera, ecc...) e l'utilizzo a cui è destinato il collegamento (stampa, riproduzione audio, ecc...). Trattandosi di una Linux-Box, questo valore può essere tenuto come da default, poiché sarà il nostro sistema a connettersi ad altri e non viceversa;
- **iscan:** se impostato su **enable** permetterà ad altri dispositivi nelle vicinanze di rilevare la Linux-Box;
- **pscan:** se impostato su **enable** permette agli altri dispositivi di tentare una connessione;
- **auth:** abilita i meccanismi di sicurezza a layer 1, il pairing. In questa modalità quando viene effettuata una connessione, verrà richiesto l'inserimento del PIN su entrambe le unità e se vengono forniti numeri diversi, la connessione sarà negata. Dal PIN viene generata la chiave che sarà usata per criptare il traffico;
- **encrypt:** permette di criptare il traffico con la chiave generata;
- **lm (link mode):** come detto in precedenza, due dispositivi possono scambiarsi di ruolo massimizzando l'utilizzo della banda su link asimmetrici. Impostandolo su **master**, la Linux-Box cercherà sempre di prendere la fetta di banda maggiore;
- **lp (link policy):** definisce il comportamento del dispositivo all'interno della Piconet. Con **rswitch** si consente lo scambio di ruolo dei dispositivi; **sniff** permette di effettuare altre operazioni anche quando il dispositivo è parte di una Piconet; **park** permette al dispositivo di andare in stand-by nei periodi di inattività; **hold** permette di mettere in pausa le comunicazioni audio su link SCO;
- **pairing:** se impostato su **multi** permette la connessione tra dispositivi già associati ad altri dispositivi; se impostato su **once**, l'associazione è esclusiva; se impostato su **none**, non permette associazioni;

- **security:** se si utilizza la keyword "**none**", il sistema di autenticazione viene disabilitato; se si utilizza "**user**" verrà richiesto il PIN ad ogni connessione; se si utilizza "**auto**" viene usato il parametro contenuto in passkey per le connessioni in ingresso e richiesto manualmente il PIN per quelle in uscita;
- **passkey:** specifica il PIN da utilizzare per le connessioni in ingresso quando "security" è impostato su "auto".

Si ricorda che ad ogni modifica al file di configurazione, bisogna ricordarsi di far rileggere la configurazione dando da shell il comando:

**$killall -HUP hcid** [invio]

## 10.4 Controllare l'hardware

Se tutto è stato eseguito bene, il sistema è pronto al funzionamento e non resta altro che fare il pairing per utilizzare i dispositivi. Utilizzando il comando **hciconfig**, una specie di *ifconfig*, si possono rilevare alcune informazioni riguardanti i dispositivi Bluetooth collegati al sistema; dal suo output, è possibile rilevare:

- il Bluetooth Device address, molto simile al MAC address ed assegnato in modo univoco ad ogni dispositivo Bluetooth;
- lo stato dell'interfaccia (UP, RUNNING);
- Il traffico generato;
- i pacchetti trasferiti e ricevuti su link ACL e SCO.

Per scoprire le funzionalità supportate dal dispositivo in uso (role switch, power control, ecc...) basta dare il comando:

**$hciconfig hci0 features** [invio]

Ogni singola interfaccia, nel caso di più dispositivi collegati alla stessa macchina, (hci0, hci1, ecc...) può essere disattivata o attivata attraverso semplici comandi:

**$hciconfig hci0 down** [invio]
**$hciconfig hci0 up** [invio]

Per rendere invece invisibile il computer agli altri dispositivi, basta dare in qualsiasi momento il comando:

**$hciconfig hci0 iscan disable** [invio]

Avendo tra le mani un sistema pronto, come fare per scovare i dispositivi Bluetooth nelle vicinanze? Basta semplicemente dare da shell il comando:

**$hcitool scan** [invio]

Il risultato ottenuto sarà la lista di tutto ciò che è a portata, visualizzandone il MAC. Come fare a sapere se ciò che ci interessa è giusto, è cosa quasi semplice se trattasi ad esempio di cellulari Nokia, dove basta inserire il cheat code *#2820# e verificare che il MAC combaci... Per altri dispositivi, basta fare una ricerca in internet...
Ulteriori informazioni possono essere reperite attraverso i comandi **hcitool name** e **hcitool info** che danno un output simile a quanto riportato di seguito:

**$hcitool name xx:xx:xx:xx:xx:xx** [invio]
**BlueZ (hci@morticia.localnet)**

**$hcitool info xx:xx:xx:xx:xx:xx** [invio]
**Requesting information ...**
**BD Address: xx:xx:xx:xx:xx:xx**
**Device Name: BlueZ (hci@morticia.localnet)**
**LMP Version: 1.1 (0x1) LMP Subversion: 0x8a**
**Manufacturer: Cisco, Inc.**
**Features: 0xff 0xff 0x3d 0x00**
**<3-slot packets> <5-slot packets> <encryption> <slot offset> <timing accuracy> <role switch>**
**<hold mode> <sniff mode> <park mode> <RSSI> <channel quality> <SCO link>**
**<HV2 packets> <HV3 pakets> <u-law log> <A-law log> <power control> <transparent SCO>**

## 10.5 L'autenticazione (pairing)

L'autenticazione, cioè il pairing, avviene prima che i dispositivi si scambino i dati. A riga di comando, sotto GNU/Linux, esistono i comandi **cc** (Create Connection) e **auth**. Gli esempi potrebbero essere:

**$hcitool cc 00:13:FD:DF:3A:EF** [invio]
**$hcitool auth 00:13:FD:DF:3A:EF** [invio]

Se dopo aver eseguito questi comandi si accetta la connessione sul dispositivo che ha il MAC indicato e si inserisce il PIN corretto, i dispositivi effettuano il pairing. La verifica può essere fatta attraverso:

**#$hcitool conn** [invio]
**Connection:  ACL 00:13:FD:DF:3A:EF handle 1 state 1 lm MASTER**

Si può altresì rilevare l'affidabilità della connessione al dispositivo associato tramite il comando **l2ping** che invia degli echo request al MAC address del dispositivo Bluetooth specifico e misura il ritardo con cui vengono ricevuti gli echo replay. Un esempio potrebbe essere:

```
$l2ping -c 3 00:13:FD:DF:3A:EF [invio]
Ping 00:13:FD:DF:3A:EF from 00:E0:98:87:25:3C (data size 20) [...]
20 byte from 00:13:FD:DF:3A:EF id 200 time 31.02ms
20 byte from 00:13:FD:DF:3A:EF id 200 time 29.89ms
20 byte from 00:13:FD:DF:3A:EF id 200 time 30.43ms
3 sent, 3 recevied, 0% loss
```

La connessione fornita da hcitool non risulta essere utile perché solitamente si vogliono utilizzare i servizi offerti dal dispositivo connesso. Il comando utile per vedere quali servizi sono offerti è:

```
$sdptool browse 00:13:FD:DF:3A:EF [invio]
```

per ogni servizio si otterranno le seguenti informazioni:

- **Service Name:** il nome per esteso del dispositivo;
- **Service Description:** breve descrizione;
- **Protocol Descriptor List/Channel:** il canale sul quale viene reso disponibile il servizio;

La richiesta di pairing può essere fatta direttamente da applet grafici, generalmente inseriti negli ambienti grafici KDE e GNOME. E' da tener presente che ogni applicazione che si andrà a configurare per sfruttare un servizio offerto, necessita di specificare il canale da utilizzare; la Protocol Descriptor List/Channel risulta essere di particolare aiuto.

### 10.6 Connessione GSM

**Rfcomm** è il protocollo che emula un link seriale RS232. BlueZ mette a disposizione due interfacce per accedere a questo tipo di link, una emulata tramite TTY ed una basata su socket. L'interfaccia TTY consente di utilizzare tutti quei software che erano stati pensati per comunicare su seriale senza effettuare nessuna modifica al codice. Quando viene creata una connessione di questo tipo, è possibile comunicare con il dispositivo attraverso un device opportuno (come per esempio /dev/rfcomm0), in modo altamente trasparente, senza preoccuparsi di come viene gestito il link; sarà perciò possibile utilizzare un emulatore di terminale, oppure stabilire un collegamento TCP/IP tra i dispositivi, sfruttando PPP. Per poter usare RFCOMM bisogna per prima cosa verificare che il device (ad esempio /dev/rfcomm0) sia presente, altrimenti occorrerà crearlo con il seguente comando dato dalla shell:

**$mknod /dev/rfcomm0 p** [invio]

Si darà per scontato che si sia già verificata la corretta disponibilità del dispositivo attraverso il comando “l2ping” e si sia già a conoscenza dell'opportuno indirizzo MAC con “hcitool scan”. Si esegua perciò:

**$rfcomm bind 0 00:13:FD:DF:3A:EF 1** [invio]

sostituendo naturalmente il MAC con uno opportuno, il comando dato ordina a RFCOMM di creare un'associazione (bind) tra il primo device (con il parametro 0, cioè /dev/rfcomm0) ed il secondo, avente per MAC quello specificato, utilizzando il canale 1. La scelta del canale è stata effettuata basandosi sull'output di “sdptool browse”, creando il canale relativo al servizio “Dial-Up Networking”. E' altresì possibile ottimizzare la procedura attraverso la modifica del file **/etc/bluetooth/rfcomm.conf** come nell'esempio di seguito:

```
rfcomm0 {
        bind yes;
        device 00:13:FD:DF:3A:EF;
        channel 1;
        comment “Dial-Up cellulare”;
}
```

E' possibile verificare lo stato delle connessioni dando il comando:

$**rfcomm** [invio]
**rfcomm0: 00:13:FD:DF:3A:EF channel 1 clean**

E' opportuno notare che il collegamento viene aperto su quel canale solo quando devono effettivamente transitare dei dati attraverso il dispositivo, in questo modo viene risparmiata energia, incrementando la durata delle batterie.
Verificando che l'utente abbia accesso in scrittura a /dev/rfcomm0, dare il comando:

**$minicom -s** [invio]

scegliere “serial port setup” e selezionare le voci da modificare, inserendo i valori:

**Serial device: /dev/rfcomm0**
**Bps/Par/Bits: 115200 8N1**

salvare le modifiche come default od in alternativa, per tenerle attive solo per questa sessione, con EXIT. Nel momento in cui minicom cercherà di aprire /dev/rfcomm0 sarà richiesto l'inserimento del PIN.
Se tutto ciò sarà andato a buon fine, si potranno impiegare i comandi AT da inviare al modem... Utilizzando ad esempio un cellulare, dando il comando

**$ATD123456** [invio]

si cercherà di stabilire una connessione dati GSM (perciò a 9600 bps) al numero 123456.

### 10.7 Connessione GPRS - EDGE - UMTS

La connessione dati via GSM è a circuito, cioè tiene occupato il canale per tutto il tempo di attività della connessione, pertanto è soggetta a tariffazione a tempo. Le connessioni via GPRS, EDGE, UMTS sono invece a pacchetto, dove il canale viene occupato solo quando devono transitare dati, pertanto la tariffazione è a traffico. Ciò rende l'utilizzo di questo tipo di connessioni estremamente vantaggioso. Prendendo in considerazione l'uso di un telefono cellulare, utilizzandolo come modem, bisognerà districarsi tra le innumerevoli cifre sulla classe GPRS di appartenenza, che differenziano i vari apparati, per capire quale tra tutti può essere quello che più si presta a soddisfare le proprie esigenze. Esistono variegati modi che descrivono la classe d'appartenenza, come singolo numero, somma di due numeri, oppure attraverso lette dell'alfabeto. Per capire questo dato occorre per prima cosa capire come funzionano il GSM ed il GPRS.
Nel GSM, più dispositivi possono trasmettere su una sola frequenza a turno e, nel caso di una telefonata, viene usato uno slot per trasmettere ed uno per ricevere, mentre quelli lasciati liberi possono essere impiegati per il trasferimento di dati.

- La capacità di un telefono di mantenere attivi sia una comunicazione GSM sia una GPRS, appartengono ai dispositivi di ***Capability Class A***.
- La capacità di un telefono di mettere in pausa la sessione dati per ricevere una telefonata e

riprenderla nel momento in cui la telefonata viene terminata, sono dispositivi di ***Capability Class B***.

- Quei dispositivi che invece non prevedono la commutazione automatica da GPRS a GSM e viceversa, come i modem, sono dispositivi di ***Capability Class C***.

C'è da sottolineare che sono pochissimi i dispositivi GPRS in grado di gestire completamente i 6 timeslot non riservati alle comunicazioni GSM. Nella tabella a seguire è possibile vedere le corrispondenze tra le classi multislot ed il numero di slot disponibili per l'upstream ed il downstream, con il numero massimo di timeslot utilizzabili simultaneamente:

| Classe Multislot | Timeslot Down - Up | Slot attivi |
|---|---|---|
| 1 | 1+1 | 2 |
| 2 | 2+1 | 3 |
| 3 | 2+2 | 3 |
| 4 | 3+1 | 4 |
| 5 | 2+2 | 4 |
| 6 | 3+2 | 4 |
| 7 | 3+3 | 4 |
| 8 | 4+1 | 5 |
| 9 | 3+2 | 5 |
| 10 | 4+2 | 5 |
| 11 | 4+3 | 5 |
| 12 | 4+4 | 5 |
| ... | ... | ... |
| 32 | 5+3 | 6 |

Il GPRS permette 4 codifiche che vanno da una velocità minima di circa 9 Kbps utilizzando il ***Coding Scheme 1*** (CS1), codifica molto robusta ed utilizzata quando il segnale è debole, fino a circa 21 Kbps utilizzando il ***Coding Scheme 4*** (CS4), solo nel caso di segnale molto forte.
A questo punto, per ottenere la massima velocità ottenibile, basta moltiplicare il numero di timeslot disponibili per la velocità di ognuno, considerando che essa varia a seconda della qualità del segnale e dal numero di utenti presenti nella stessa cella, anche collegati simultaneamente...
A seguire è possibile notare le variazioni di velocità in base al tipo di segnale, di quattro dispositivi GPRS presi come esempio:

| Classe | Segnale | Velocità Slot (Kbps) | Slot Downstream | Slot Upstream | Velocità max Downstream | Velocità max Upstream |
|---|---|---|---|---|---|---|
| GPRS 32 | ottimo | 20 | 5 | 3 | 100 Kbps | 60 Kbps |
| GPRS 32 | scarso | 8 | 5 | 3 | 40 Kbps | 24 Kbps |
| GPRS 10 | ottimo | 20 | 4 | 2 | 80 Kbps | 40 Kbps |
| GPRS 10 | scarso | 8 | 4 | 2 | 32 Kbps | 16 Kbps |
| GPRS 8 | ottimo | 20 | 4 | 1 | 80 Kbps | 20 Kbps |
| GPRS 8 | scarso | 8 | 4 | 1 | 32 Kbps | 8 Kbps |
| GPRS 6 | ottimo | 20 | 3 | 2 | 60 Kbps | 40 Kbps |
| GPRS 6 | scarso | 8 | 3 | 2 | 24 Kbps | 16 Kbps |

Per quanto riguarda la tecnologia EDGE la velocità si aggira intorno ai 240 Kbps in downstream mentre per la tecnologia UMTS arriva a 384 Kbps in downstream e 64 Kbps in upstream. La tecnologia HSDPA supporta fino a 3,6 Mbps in downstream e 384 Kbps in upstream, più o meno allineato con molte offerte utilizzanti tecnologia xDSL.
Per quanto riguarda il collegamento, l'attivazione della connessione non cambia utilizzando le tecnologie GPRS, EDGE, UMTS e la sua evoluzione HSDPA. Gli unici fattori che determinano l'uso di una tecnologia piuttosto di un'altra, sono il tipo di cellulare o dispositivo utilizzato, il piano telefonico scelto e la copertura dell'operatore. L'operazione di "base" per aprire una connessione, basta inviare i seguenti comandi:

**$AT+CGDCONT=1,"IP","*apn-name*","0.0.0.0",0,0** [invio]
**$ADT*99***1#** [invio]

Queste istruzioni si applicano non solo ai cellulari tramite bluetooth, ma anche se ad esso ci si collega tramite cavo USB; in quest'ultimo caso occorrerà verificare che nel kernel sia caricato il modulo **cdc-acm** ed utilizzare il device **/dev/ttyACM0** in luogo di **/dev/rfcomm0**.

Il comando CGDCONT permette di creare un nuovo profilo per la connessione GPRS il cui primo parametro (1) corrisponde al CID (Context Identifier) e permette di identificare univocamente il profilo utilizzato.
Il secondo parametro indica il protocollo utilizzato, in questo caso IP.
Il terzo parametro prende il nome di **apn-name** ed è fornito dall'operatore scelto. Lo **APN** è detto anche Access Point Name, un record sul DNS interno dell'operatore telefonico che restituisce l'indirizzo IP del GCSN (GPRS Gateway Support Node) che è il nodo di connessione tra internet e lo SGSN (Serving GPRS Support Node), il nodo che mantiene la comunicazione diretta all'utente mobile. Perché la connessione abbia successo, occorre conoscere il proprio apn-name di appartenenza, che in Italia assume i seguenti valori:

**Vodafone:** web.omnitel.it
**Tre:** tre.it
**TIM:** ibox.tim.it
**Wind:** internet.wind

Il quarto parametro è impostato su 0.0.0.0 per indicare che si vuole ottenere un indirizzo IP dinamico dal proprio gestore.
Il quinto parametro indica se attivare (1) o disattivare (0) la compressione dei dati.
Il sesto parametro indica se attivare (1) o disattivare (0) la compressione dell'header.

Se viene utilizzato un dispositivo GPRS e la SIM è protetta dal PIN, bisognerà istruire il sistema affinché fornisca il codice prima dei comandi precedenti, inserendo la riga:

**$AT+CPIN="1234"** [invio]

naturalmente 1234 indica il codice PIN della SIM. Per facilitare le cose, se la SIM è utilizzata solo per la connessione dati, si consiglia di disabilitare temporaneamente la richiesta del PIN.
Altri comandi interessanti, utili per avere una connessione migliore sono:

**AT+CSQ** fornisce un numero indicante l'intensità del segnale;
**AT+COPS** forza la ricerca dell'operatore migliore a cui connettersi.
Per non dare ogni volta i comandi sopraelencati nella shell, conviene approntare uno script che faccia per noi il lavoro, automatizzando la connessione PPP. Creare un file chiamato **gprs** in **/etc/ppp/peers/** con all'interno quanto segue:

```
115200
noauth
connect "usr/sbin/chat -v -f /etc/chatscripts/gprs"
debug
/dev/rfcomm0
defaultroute
noipdefault
-crtscts
local
lcp-echo-interval 0
```

Siccome tipicamente le connessioni GPRS non sono propriamente affidabili, se si notano instabilità di connessione, sarebbe quantomai opportuno inserire anche l'opzione **"persist"** che forza il demone pppd a ripristinare il collegamento ogni volta cade, fino a quando non sarà l'utente a decidere di terminarlo. Dal listato sopra si evince quanto segue:

**-crtscts** disabilita l'hardware flow control, poiché non disponibile in queste connessioni;
**lcp-echo-interval 0** disabilita l'invio degli LCP, non usati in ambiente GPRS. Normalmente una sessione PPP invia degli LCP periodici e se non riceve una risposta per un certo numero di volte, il link viene interrotto. Per questo motivo viene impostato a zero.

Si crei ora il file **gprs** in **/etc/chatscript/** con all'interno quanto segue:

```
ABORT BUSY
ABORT 'NO CARRIER'
ABORT VOICE
ABORT 'NO DIALTONE'
ABORT 'NO ANSWER'
ABORT DELAYED
'' “AT&F”
OK-AT-OK “ATE1”
OK-AT-OK AT+CGDCONT=1,”IP”,”apn-name”,”0.0.0.0”,0,0
OK-AT-OK “ATD*99***1#”
CONNECT c
```

Fatto ciò, è ora possibile stabilire una connessione PPP invocando il comando:

**$pppd call gprs** [invio]

dopo alcuni istanti dovrebbe essere creato un nuovo dispositivo ppp e dovrebbero essere presenti degli output in /var/log/message o in /var/log/ppp.log. Analizzandoli è possibile verificare che tutto funzioni. L'unico tipo di errore che si può presentare è il timeout degli LCP, se non sono stati disabilitati:

```
sent [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xc0e617bf>]rcvd [LCP ConfReq id=0x1 <asyncmap 0x0> <magic 0xc0e617bf>]sent [LCP ConfNak id=0x1]
```

Una volta stabilita la connessione, dovrebbe essere possibile la navigazione. Se ciò non dovesse accadere, risulta utile verificare che la tabella di routing sia corretta. Se ci sono altre interfacce di rete attive, come quella Wi-Fi, verificare che la route di default sia impostata verso il gateway della connessione GPRS, prendendo in considerazione quanto contenuto nell'output precedente visto e che dovrebbe contenere un'unica entry 0.0.0.0. Quindi per la colonna ***Destination*** dovremmo avere un'unica entry 0.0.0.0 ed assomigliare a quanto segue:

```
$ /sbin/route -n

Destination     Gateway         Genmask         Flags Metric         Ref    Use    Iface
    [...]
0.0.0.0         10.6.6.1        0.0.0.0         0     0              0      0      ppp0
```

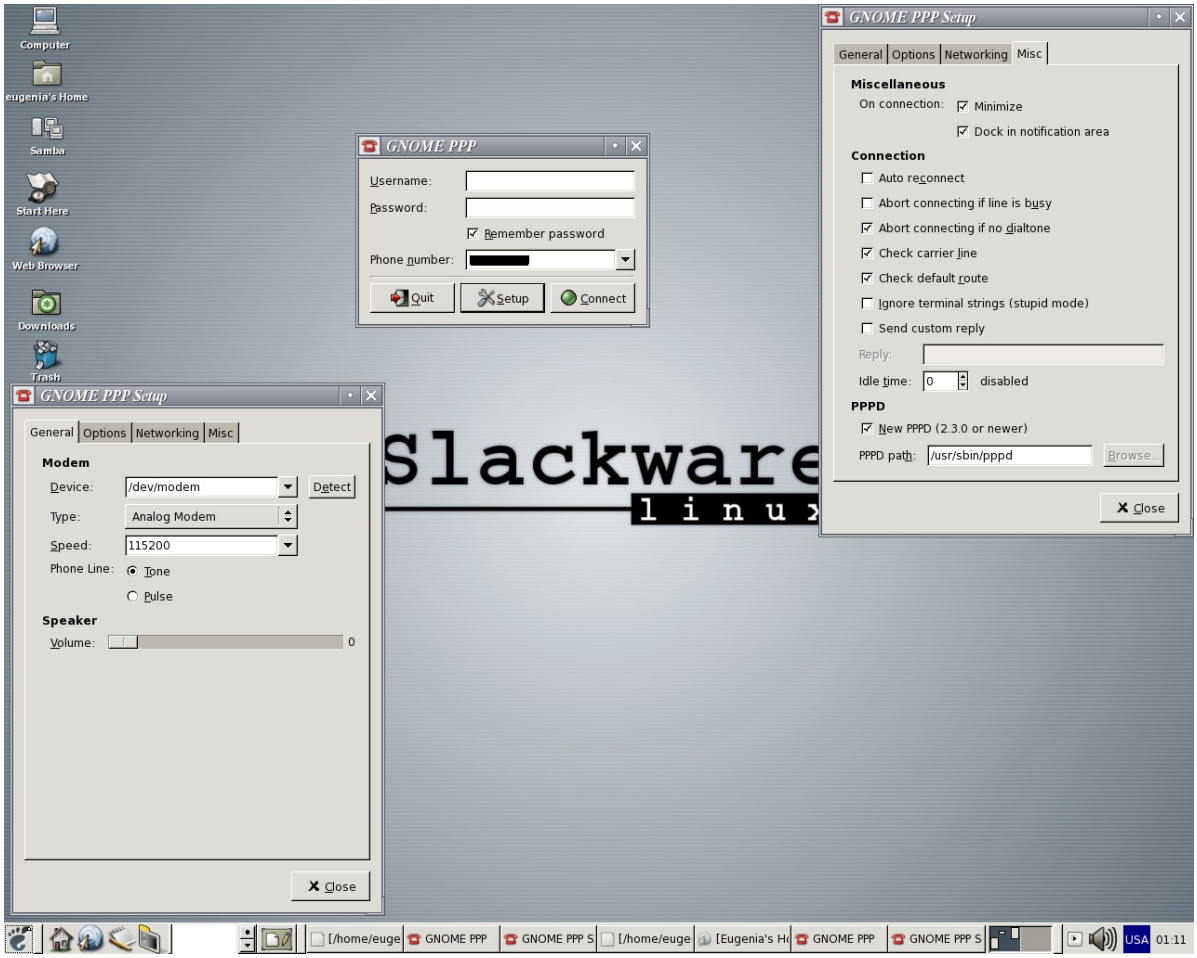
In caso di problemi derivanti dal DNS, è utile verificare pingando un sito a piacimento con un altro tipo di connessione, verificandone la risposta; riavviare la connessione GPRS e ripetere la prova di ping. E' utile sapere che le risposte del ping attraverso connessioni GPRS presentano RTT piuttosto elevati se paragonati a quelli delle connessioni xDSL e PSTN.

**NOTE:** Non tutti i cellulari utilizzano lo stesso specifico numero per la connessione GPRS. Affidarsi alla tabella seguente per reperire quello adatto:

| Marca del cellulare | Numero da comporre |
|---|---|
| | |
| Sony Ericsson | *99***9# |
| Nokia e Motorola | *99# |
| Samsung | *99**1*1# |
| LG | *99***1# |

### 10.8 Semplificarsi la vita con Gnome-PPP e GPRS Easy Connect

Iniziamo l'esposizione di questi programmi utilizzando per primo il semplice tool di rete **Gnome-PPP** con cui è molto facile accedere ad internet tramite il telefono cellulare. In pratica esso è il front-end grafico del software dial-up wvDial per modem. Nell'immagine a seguire si può vedere il programma girare sulla distribuzione Slackware Linux, tenendo presente che anche con le altre distribuzioni il risultato è simile:



All'avvio del programma apparirà una finestra dove s'inserirà il nome utente e la password (normalmente non necessari), il numero da chiamare. Cliccando sul pulsante configura, nella sezione “modem”, alla voce dispositivo, si indicherà il dispositivo **/dev/rfcomm0** che dovrebbe corrispondere al telefono e creato col comando **rfcomm**. Già che siamo in questa finestra, aumentare i tentativi di connessione ad almeno 3. Appena sotto si trova il pulsante “Stringhe di configurazione” dove, cliccandoci sopra, andranno inserite nella prima linea (la numero 2) le stringhe di configurazione al gestore utilizzato come si è visto in precedenza (10.7).
Ok, la configurazione è ultimata e non resta che chiudere le finestre di configurazione e cliccare sul pulsante “**Connetti**”.
Questo tool è specificatamente pensato per l'utilizzo con l'ambiente desktop Gnome. Se si usa invece KDE, esiste **KDEBluetooth**, che permette anche la semplice gestione dello scambio file.
Ma esiste un modo ancora più semplice per fare tutto ciò? Certamente, ed è il programma di gestione inserito normalmente nel cd fornito a corredo dei nuovi telefoni cellulari. Tutto questo sarebbe una bella cosa se solo il cd d'installazione fosse pensato non solo per sistemi operativi Windows... Che fare? Sebbene non presente nei cd ufficiali, basta affidarsi ad una versione (che supporta più telefoni) alternativa dello stesso per sistemi operativi GNU/Linux!!!

**GPRS Easy Connect** è un programma scritto in perl e fa tutto quello che serve in modo più o meno intuitivo e veloce. La lista dei telefoni attualmente supportati è enorme e il fatto che un telefono non sia nella lista non significa affatto che non funzioni, molto facilmente lo sarà totalmente nelle prossime revisioni. Per prima cosa bisogna procurarsi il pacchetto, disponibile al link al sito del progetto:

**http://easyconnect.linuxuser.hu**

E' importante verificare le dipendenze, poiché questo software usa moduli perl non molto comuni e spesso non inclusi nelle distribuzioni linux, FreeBSD compreso.
Il programma è in formato tar.gz ed operando dalla shell eseguire il comando per scompattare:

```
$tar xvzf GPRS_Easy_Connect_XXX_Install.tar.gz [invio]
```

come indicato dal file README eseguire sempre dalla shell il comando:

```
$./INSTALL [invio]
```

se il responso della shell è simile a questo:

```
GPRS Easy Connect Installer
Checking depedencies...

perl [OK]
pppd [OK]
perl Tk [Error]

Can't find the Perl Tk modul.
The program needs the Tk (800.023) modul!
For more informations see the http://easyconnect.linuxuser.hu site.
```

non risulta installato il modulo Perl che fornisce la libreria grafica Tk.
Per il test del programma, ho usato le distribuzioni Mandrake 10.0 e Fedora Core 4, grazie alla compatibilità dei pacchetti rpm. Utilizzando il gestore di pacchetti rpmdrake, ho inviato la ricerca di tutto ciò che riguarda il Perl. Individuato il pacchetto perl-Tk-800.024-1mdk si scoprirà che necessita di alcune dipendenze individuate automaticamente (perl-PerllO-gzip-xxx-2mdk.i586.rpm e perl-base.xxxmdk.i586rpm). Installare tutto il necessario e procedere ridando dalla shell il comando:

**$./INSTALL** [invio]

Se il responso della shell è simile a ciò che segue, significa che l'installazione ha avuto successo:

**...**
**perl [OK]**
**pppd [OK]**
**perl Tk [OK]**
**...**

Come da istruzioni sul programma eseguire il comando:

**$gprsec** [invio]

a questo punto deve partire l'interfaccia grafica.
La configurazione prevede la scelta del modello del telefonino, dell'operatore, della lingua da utilizzare e del DNS. Nell'ultima voce in fondo bisogna selezionare la porta o dispositivo di comunicazione col telefono (di tipo seriale: ttyS[x]; di tipo Bluetooth: rfcomm[x]), ma se non appare la lista, è possibile scriverlo manualmente poiché il programma lo consente. Il risultato ottenuto, se inserito manualmente (utilizzando la distribuzione Mandrake) e cliccando su connetti, apparirà una finestrella di errore: Port error.
Se ricontrollando la correttezza della configurazione, non si riscontrano errori, è il programma che presenta problemi sulla distribuzione citata... niente paura, il programma funziona sulla distribuzione ma solo in lingua inglese e solo con alcune revisioni di GPRS Easy Connect.

Utilizzando la distribuzione Fedora Core 4, eseguire tutte le operazioni già svolte su Mandrake. Ora, installandolo apparirà lo stesso errore sul perl. Sebbene il pacchetto Tk-perl risulta già installato ed è evidente che mancano ulteriori dipendenze. La compatibilità di pacchetti fra Mandrake e Fedora è d'aiuto. Prendendo i cd di Mandrake 10.0 "prelevare" l'rpm necessario:

**Perl-Tk-xxx-4mdk.i586.rpm**

il pacchetto richiede delle dipendenze e bisogna installare i pacchetti:

**perl-PerllO-gzip-xxx-2mdk.i586.rpm**
**perl-base.xxx.3mdk.i586rpm**

risolte le dipendenze, eseguire di nuovo il comando d'installazione del programma dalla shell:

**$./INSTALL** [invio]

se tutto è andato per il verso giusto, il programma GPRS Easy Connect è installato.
Sempre dalla shell e eseguire:

**$gprsec** [invio]

l'interfaccia grafica del programma dovrebbe a questo punto avviarsi e non resta che impostare la configurazione. Ora alla voce "porta" deve scorrere un indice di scelta. Impostare quanto necessario. Salvare le impostazioni e cliccare su connetti. Se tutto è ok, appare una finestrella che indica la connessione avvenuta, l'indirizzo IP ottenuto, l'IP del server remoto e l'IP del DNS.

per gli utenti dell'operatore Wind il punto di APN da impostare alla configurazione è da modificare da “internet.wind” a “internet.wind.biz”. Per lanciare il programma, il comando **gprsec** va eseguito aprendo la shell da interfaccia grafica. L'utilizzo su altre distribuzioni non è diverso, ma le dipendenze andranno risolte attraverso i repository ufficiali.

## 10.9 OBEX: trasferimento dati

Lo standard Bluetooth non serve solo per la connessione ad internet tramite cellulare o modem ma può essere molto utile per trasferire dati ad esempio con il cellulare stesso. Per fare ciò, il protocollo OBEX, usato inizialmente per lo scambio di file binari su IrDA e poi implementato per il Bluetooth, aiuta parecchio in questo scopo ed oltretutto funziona su qualsiasi collegamento come l'infrarosso, il Bluetooth, USB e TCP/IP. Esiste un'implementazione molto valida di OBEX rilasciata con licenza GPL ed è ***OpenOBEX.*** Il canale di trasmissione utilizzato tipicamente da OBEX è il 12 e per verificare che anche il cellulare utilizzi il medesimo è utile dare da shell il comando:

**$sdptool browse** 'mac-cellulare' [invio]

il canale utilizzato dal cellulare sarà visibile nella sezione relativa a “OBEX PC Suite Services”.
Il pacchetto OpenOBEX contiene due preziosi strumenti:

- **obex_test**: permette di controllare che il collegamento funzioni bene;
- **obexftp**: è un client simile all'ftp per trasferire i file attraverso OBEX.

Vediamone l'utilizzo ed il funzionamento di obex_test dando da shell il comando:

**$obex_test -b 00:13:FD:DF:3A:EF 12** [invio]

che restituirà quanto segue:

```
Using Bluetooth RFCOMM transport
OBEX Interactive test client/server.
>c
Connect OK!
Version: 0x10. Flags: 0x00
>d
Disconnect done!
```

Se abbiamo ottenuto quanto sopra, allora è possibile tentare d'ottenere la lista dei file contenuti nel cellulare, tenendo conto che normalmente i cellulari indicano con C: la memoria flash e con E: la memoria estraibile, tipicamente una scheda di memoria aggiuntiva. Per utilizzare obexftp si dovranno specificare le seguenti opzioni permesse:

**-b** il MAC address del cellulare;
**-B**: il canale utilizzato e identificato tramite sdptool;
**--get** oppure **--put** il nome del file da scaricare od inviare senza il percorso;
**-c** come sopra ma specificando il percorso completo.

Supponendo di voler visionare il contenuto della directory principale della flash si dovrà perciò dare il seguente comando:

**$obexftp -b 00:13:FD:DF:3A:EF -B 12 -c 'C:/' -l** [invio]

se invece si volesse scaricare la foto ***image001.jpg*** presente nella cartella **Photo** della memoria aggiuntiva, si dovrà dare il comando:

**$obexftp -b 00:13:FD:DF:3A:EF -B 12 -c 'E:/Photo/' -g image001.jpg** [invio]

se invece la si volesse inviare dal computer al cellulare, si dovrà dare il comando:

**$obexftp -b 00:13:FD:DF:3A:EF -B 12 -c 'E:/Photo/' -p image001.jpg** [invio]

Malgrado tutto, obexftp risulta essere poco pratico nel suo utilizzo e fortunatamente esiste un modo semplicissimo per gestire i file contenuti nel cellulare... trattare lo stesso come fosse un'estensione userspace del filesystem: ***Obexfs.*** In parole povere permette di navigare all'interno del cellulare come navighiamo nel filesystem del computer, utilizzando il file manager preferito.
Essendo basato su FUSE, occorrerà caricare il supporto per FUSE nel kernel. Dare prciò il comando:

**$modprobe fuse** [invio]

occorrerà altresì installare anche le **fuse-utils** e **libfuse2** per ottenere il supporto di un qualsiasi filesystem basato su FUSE; procurarsi il pacchetto **Obexfs** puntando il browser all'indirizzo:

**http://openobex.triq.net/obexfs**

installare come al solito dando il comando:

**$./configure && make install** [invio]

similmente a quanto visto per obexftp, anche obexfs richiede che vengano definiti il canale utilizzato con -B ed il MAC del dispositivo con -b, quindi:

**$obexfs -b  00:13:FD:DF:3A:EF -B 12 /mnt/phone** [invio]

Ora si potrà navigare direttamente nella memoria del cellulare semplicemente entrando nella directory **/mnt/phone**. Termite tutte le operazioni desiderate, occorre smontare il filesystem, dando il comando:

**$fusermount -u /mnt/phone** [invio]

### 10.10 L'audio

Uno tra gli utilizzi interessanti dello standard Bluetooth è quello della trasmissione dell'audio tramite link di tipo SCO. E' bene tener presente che non tutti gli adattatori Bluetooth supportano perfettamente link di questo tipo, i migliori attualmente sono quelli che adottano chipset CSR.
Per far funzionare le cuffie Bluetooth è necessario disporre del pacchetto **Bluetooth-alsa** e disponibile per il download sul sito:

**http://bluetooth-alsa.sourceforge.net/**
questo pacchetto consta di un modulo in kernelspace chiamato **snd_bt_sco** e di un tool in userspace chiamato **btsco**. Bisogna altresì considerare che è in fase di sviluppo una nuova versione di btsco che non necessiterà del modulo del kernel ma impiegherà un plug-in del driver alsa.
Verificare per prima cosa la presenza nel kernel del supporto ***CONFIG_BT_SCO*** come modulo oppure statico, in caso contrario, procedere alla sua compilazione.
Passiamo alle cuffie e scoprirne il MAC address dando il comando:

**$hcitool -i hci0 scan** [invio]

e poi predisporre il chipset Bluetooth per accettare un canale bidirezionale audio con il comando:

**$hciconfig hci0 voice 0x0060** [invio]

infine lanciare btsco con il comando:

**$btsco -r -f mac_cuffia** [invio]

a questo punto avviene il pairing e si dovrà digitare il PIN della cuffia, generalmente fornito nel manuale della stessa.
Le opzioni utilizzate in btsco assolvono alle seguenti funzioni:

- **-r**: obbliga btsco a riaprire la connessione ogni volta che viene persa;
- **-f**: manda in background btsco a connessione avvenuta.

A link attivo, si dovrà riconfigurare i programmi preferiti, come quelli di telefonia VoIP, per l'utilizzo del dispositivo appena creato.

# APPENDICI

# Accenni sulla normativa

Siccome l'attuale normativa italiana impone dei limiti all'uso delle W-LAN, è cosa giusta fornire almeno un'infarinatura del suo contenuto. Il testo integrale del decreto pubblicato sulla gazzetta ufficiale n.126 del 3 giugno 2003 è disponibile in formato pdf per il download sul sito del ministero delle comunicazioni (www.comunicazioni.it) e dice:

Art. 1 (Definizioni):

1. Ai fini dei presente decreto si intendono per:
   a) "Radio Local Area Network (di seguito denominate "Radio LAN` o "R-LAN"): un sistema di comunicazioni in rete locale mediante radiofrequenze che utilizza apparati a corto raggio secondo le caratteristiche di armonizzazione e tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze, nelle seguenti bande di frequenza: 2.400,0 -2.483,5 MHz (brevemente banda a 2.4 GHz), 5.150 - 5.350 MHz, 5.470 -5.725 MHz (brevemente bande a 5 Ghz);
   b) “Access Point”: strumento di accesso per un numero variabile di utenti tra la Radio-LAN e la struttura di rete di telecomunicazioni;
   c) "codici di abilitazione e identificazione": codici forniti dall'impresa autorizzata all’abbonato per identificarlo univocamente e verificarne l'abilitazione all'accesso alla rete tramite l'access point;
   d) "autorizzazione generale": un'autorizzazione che è ottenuta su semplice dichiarazione di inizio attività.

2. Ai fini del presente decreto si applicano le definizioni di cui all'articolo 1, comma 1, del decreto dei Presidente della Repubblica 19 settembre 1997, n. 319.

Art. 2 (Oggetto ed ambito di applicazione):

1. Il presente provvedimento fissa le condizioni per il conseguimento dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN nella banda 2,4 GHz o nelle bande 5 G1-17, dell'accesso dei pubblico alle reti e ai servizi di telecomunicazioni in modalità fissa e nomadica.
2. Ai fini della limitazione delle interferenze dannose ad altri servizi previsti dal Piano nazionale di ripartizione delle frequenze, gli access point operanti nella banda 5.150-5.350 MHz possono essere installati all'interno di edifici secondo le caratteristiche tecniche di cui alla nota 184 del Ministero nazionale di ripartizione delle frequenze come modificato dal decreto dei Ministro delle comunicazioni 20 febbraio 2003, pubblicato nella Gazzetta Ufficiale n. 50 del 1° marzo 2003.

Art. 3 (Procedura per il conseguimento dell' autorizzazione generale):

1. La fornitura del servizio di cui all'articolo 2 è subordinata ad un'autorizzazione generate secondo le condizioni di cui all'articolo 6.
2. Il soggetto che intende fornire il servizio di cui all'articolo 2, avente sede in ambito nazionale o in uno dei paesi dello Spazio economico europeo (SEE), in uno dei paesi appartenenti all'Organizzazione mondiale del commercio (ONIC), o in altri Patti con i quali vi siano accordi di reciprocità nel settore disciplinato dal presente provvedimento, fatta comunque salva ogni eventuale limitazione derivante da accordi internazionali, è tenuto a presentare al Ministero delle comunicazioni di seguito denominato "Ministero", una dichiarazione comprensiva di tutte le informazioni necessarie a verificare la conformità alle condizioni di cui all'articolo 6. La predetta dichiarazione, che deve attenersi a quanto indicato nell'allegato A al presente decreto, costituisce denuncia di inizio attività e dà titolo ad avviare il servizio contestualmente alla sua presentazione.
3. Il soggetto richiedente allega alla dichiarazione la documentazione di cui all'art6, comma 1, lett. a) e b) della delibera dell'Autorità n. 467/00/Cons. Il soggetto che abbia precedentemente ottenuto una o più autorizzazioni all'offerta al pubblico di servizi dì telecomunicazioni , può presentare la dichiarazione facendo riferimento alla documentazione già esibita, nei limiti della prevista validità.
4. I soggetti autorizzati sono obbligati all'iscrizione al registro degli operatori di comunicazione, previsto dall'articolo 1, comma 6, lett. a), n. 5), della legge 31 luglio 1997, n. 249, secondo le disposizioni della delibera dell'Autorità n. 236101/Cons e successive modificazioni.
5. I soggetti che hanno presentato la dichiarazione di cui al presente articolo, comunicano entro 30 giorni al Ministero ogni variazione delle informazioni contenute nella stessa e nella relativa documentazione allegata.

Art. 4 (Contributi):

1. I diritti amministrativi imposti al soggetti autorizzati ad offrire il servizio di cui all'articolo 2 coprono esclusivamente i costi amministrativi sostenuti per la gestione, il controllo e l'applicazione del regime di autorizzazione generale.
2. La misura di tali contributi sarà fissata con apposito provvedimento e resa pubblica ai sensi delle normative vigenti.

Art. 5 (Validità e cessione dell'autorizzazione generale):

1. L'autorizzazione generale di cui all'articolo 3 ha una durata non superiore a nove anni a decorrere dalla data di notifica della dichiarazione di cui al medesimo articolo ed è rinnovabile, previa nuova dichiarazione presentata con almeno trenta giorni di anticipo rispetto alla scadenza.
2. La scadenza coincide con il 31 dicembre dell'ultimo anno di validità dell'autorizzazione generale.
3. L'autorizzazione generale non può essere ceduta a terzi senza l'assenso dei Ministero volto a verificare la sussistenza dei requisiti in capo a111mpresa cessionaria, per il rispetto delle condizioni di cui all'autorizzazione medesima.

Art. 6 (Condizioni dell'autorizzazione generale):

1. Il soggetto titolare dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio LAN, dell'accesso del pubblico alle reti e al servizi di telecomunicazioni, è tenuto e soddisfare le seguenti condizioni :
   a) l'utilizzazione di apparecchiature conformi a quanto previsto del decreto legislativo 9 maggio 2001, n. 268, di recepimento della direttiva 199915/CE;
   b) la sicurezza della rete contro l'accesso non autorizzato conformemente alla normativa in materia, il mantenimento dell'integrità della rete, l'interoperabilità dei servizi nonché la protezione dei dati ed in particolare le prestazioni ai fini di giustizia sin dall'inizio dell'attività; a tal fine è ammesso il collegamento tra gli access point appartenenti al medesimo operatore nonché ad operatori distinti nel rispetto delle caratteristiche tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze;
   c) la fornitura delle informazioni necessarie per verificare il rispetto delle condizioni stabilite ed a fini statistici;
   d) il rispetto della normativa vigente in materia di tutela della salute pubblica e dell'ambiente, ivi incluso il rispetto dei tetti previsti per le emissioni elettromagnetiche;
   e) l'utilizzazione delle frequenze di cui all'articolo 1, comma 1, lett. a) esclusivamente secondo le caratteristiche di armonizzazione e tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze, con l'esclusione dì utilizzo delle medesime per scopi di interconnessione;
   f) l'assenza di interferenze dannose alle altre utilizzazioni previste dal vigente Piano nazionale di ripartizione delle frequenze nelle bande di cui all'articolo 1, comma 1, lettera a), senza alcun diritto a protezione dalle medesime utilizzazioni in particolare secondo quanto previsto dalle raccomandazioni CEPT ERC/REC 70/03 e successive modifiche;
   g) la pubblicizzazione delle condizioni di offerta dei servizio, incluse quelle attinenti alle condizioni economiche, alla qualità e alla disponibilità del servizio nonché le relative variazioni delle condizioni stesse;
   h) l'istituzione di una procedura per la trattazione dei reclami;
   i) il pagamento dei contributi, ove previsti;
   j) la fornitura di fatture dettagliate e documentate, ove applicabile in funzione della tipologia del servizio offerto;
   k) l'adozione di opportuni codici di abilitazione e identificazione per identificare univocamente l'abbonato e verificarne l'abilitazione all'accesso alla rete tramite l'access point ;
   l) il rispetto delle disposizioni vigenti in materia di pubblica sicurezza e tempestiva collaborazione con l'Autorità giudiziaria, ai sensi dell'articolo 7, comma 13 dei decreto dei Presidente della Repubblica n. 318 del 1997;
   m) il rispetto di ogni ragionevole misura tecnica di mitigazione, come previsto dalle rilevanti raccomandazioni e decisioni dell'ECC;
   n) il rispetto delle eventuali disposizioni emanate dall'Autorità in materia di accesso, condivisione degli apparati e delle strutture, garanzie in materia di tutela della effettiva concorrenza.

2. In particolare il soggetto di cui al comma 1 è tenuto al rispetto degli obblighi di cui agli articoli 4 e 5 della direttiva 97166/CE ed alle successive modificazioni di cui alla direttiva 2002/58/CE, quando recepita nell'ordinamento nazionale, che disciplinano gli aspetti legati alla sicurezza ed alla riservatezza delle reti e dei servizi

Art. 7 (Controlli e verifiche - Disposizioni sanzionatorie - Conciliazione e risoluzione delle controversie):

1. Il Ministero e l'Autorità, nell'ambito delle rispettive competente, possono procedere all'attuazione di controlli periodici per la verifica del rispetto delle condizioni di cui al presente decreto.
2. In caso di inosservanza delle condizioni previste per le autorizzazioni generali di cui al presente decreto si applicano le disposizioni di cui all'articolo 6, comma 4, del decreto del Presidente della Repubblica 19 settembre 1997, n. 318 e all'articolo 25 della legge 24 aprile 1998, n. 128, come modificato dall'articolo 13 della legge 21 dicembre 1999, n. 526
3. Le procedure dì conciliazione e risoluzione delle controversie sono disciplinate dall'articolo 18 del decreto del Presidente della Repubblica 19 settembre 1997, n. 318.

Art. 8 (Disposizioni transitorie e finali):

1. Le imprese già autorizzate all'esercizio sperimentale dei servizio di fornitura, attraverso le applicazioni Radio LAN, dell'accesso dei pubblico alle reti e ai servizi dì telecomunicazioni mediante l'impiego delle frequenze 2.400 2.483,5 MHz. cessano la sperimentazione entro sessanta giorni della entrata in vigore del presente decreto.
2. I titoli abilitativi di cui al presente decreto verranno adeguati alla normativa comunitaria di recepimento di cui alle premesse, in materia di comunicazioni elettroniche.

Modifiche successive:

Art. 2:

1. In relazione a quanto disposto dalla delibera dell'Autorità per le Garanzie nelle Comunicazioni 183/03/CONS, i soggetti autorizzati all'offerta al pubblico, attraverso reti ed applicazioni Radio LAN nella banda 2,4 GHz o nelle bande 5 GHz, di reti e servizi di comunicazione elettronica, ai sensi dell'art. 3 del decreto ministeriale del 28 maggio 2003, come modificato dal presente decreto acconsentono in maniera non discriminatoria ad ogni ragionevole richiesta di accesso indipendentemente dalla tecnologia utilizzata, ai sensi del decreto legislativo 1° agosto 2003, n. 259.
2. I titolari di diritti concessori o di esclusiva, a qualsiasi titolo, che operano in locali aperti al pubblico o in aree confinate a frequentazione pubblica, quali a titolo esemplificativo aeroporti, stazioni ferroviarie e marittime e centri commerciali, devono consentire alla più ampia pluralità di soggetti l'installazione e l'esercizio di infrastrutture Radio LAN a condizioni eque, trasparenti e non discriminatorie, indipendentemente dalla tecnologia utilizzata, e senza alcuna limitazione che non sia oggettivamente dovuta ad insuperabili ragioni legate alla sicurezza delle reti o all'esercizio di servizi di pubblica utilità che siano state accertate da parte del Ministero delle comunicazioni. Eventuali dinieghi motivatamente opposti a richieste di installazione ed esercizio dovranno essere comunicati, al Ministero delle comunicazioni - Direzione generale per i servizi di comunicazione elettronica e di radiodiffusione.

Art. 3:

1. Le imprese già autorizzate all'esercizio sperimentale del servizio negli ambiti consentiti dal presente provvedimento, cessano la sperimentazione di cui in premessa entro sessanta giorni dall'entrata in vigore del presente decreto.

Art. 4:

1. Si applicano ai titoli abilitativi di cui al decreto ministeriale 28 maggio 2003, secondo quanto già disposto dall'art. 8 comma 2 dello stesso, le definizioni e le disposizioni del decreto legislativo 1° agosto 2003 n. 259 citato nelle premesse.

Il presente decreto è pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana.
In parole "povere", la normativa prevede che al massimo venga usata per l'irradiazione una potenza massima non superiore ai 20dB EIRP, comprensiva di guadagni e perdite. Si deve perciò conteggiare la potenza del trasmettitore, il guadagno dell'antenna, le perdite di cavi, connettori e fare il totale che, non deve superare i 20dB.
Per i radioamatori, la cosa è diversa perché la normativa, che ha uniformato la patente A e la B in una sola patente, prevede che possano essere usate potenze di trasmissione fino a 500W. In questo caso però, ci si riferisce alla potenza RF reale emessa dagli apparati di trasmissione, non contando le antenne ecc ecc.

# Risoluzione dei problemi comuni

Nelle varie realizzazioni, di tanto in tanto, si verifica l'insorgere di problemi iniziali piuttosto strani ed incomprensibili che complicano di fatto la vita a chi deve creare la W-LAN. Molte delle volte, questi problemi sono di facile risoluzione e causati per lo più da distrazioni e sviste involontarie...

1) **I connettori d'antenna:** sembra strano ma il loro riconoscimento è da parte dei neofiti piuttosto ostico ed oltre a questo, si deve aggiungere che non tutti i produttori di hardware utilizzano lo stesso tipo, ma si affidano a soluzioni più diverse. I più usati, sono i seguenti:

Maschio

Femmina

Immagini ingrandite di connettori di tipo SMA. Di rado accade di trovarli su access point e adattatori Wi-Fi di tipo PCI.

Maschio da pannello


Femmina da pannello

Maschio

Femmina

Facilmente confondibili con lo SMA, questi connettori presentano una polarità invertita. Il loro nome è **RP-SMA** e sono largamente impiegati in tutti gli apparati.

Maschio da pannello

Maschio

Femmina da pannello

I connettori di tipo **MMCX** sono utilizzati frequentemente su apparati di dimensioni ridotte come le schede mini-PCI e PCMCIA.

Maschio

Femmina

I connettori di tipo **MCX** sono utilizzati di frequente su apparati di dimensioni ridotte come le schede mini-PCI e PCMCIA.

Maschio

Femmina

I connettori di tipo **N** sono spesso usati per le connessioni all'antenna esterna, dove garantiscono bassa perdita e resistenza a condizioni ambientali avverse.

Maschio da pannello

Femmina da pannello

Maschio

Femmina

I connettori di tipo **BNC**, sebbene non siano indicati per l'uso in applicazioni Wi-Fi a causa delle perdite d'inserzione elevate, sono spesso usati durante i test con schede moddate, grazie alla facilità e velocità di connessione di cui godono.

Femmina da pannello

Femmina da pannello

I connettori d’antenna sopra esposti non esistono per un solo tipo di cavo. Ciò comporta che ad ogni tipo di cavo corrisponde un diverso tipo di connettore. Oltre ai diversi connettori d’antenna esistono tutta una serie di adattatori, alcuni dei quali particolari che permettono la connessione tra due diversi tipi di connettori. E’ utile ricordare che ogni connettore ed adattatore, introduce una attenuazione di circa 1-1,5dB. Per questo motivo, è utile limitarne l’impiego e quando non si può farne a meno, occorre compensare con una antenna di guadagno maggiore.

Adattatori

BNC (F) to SMA (M)

BNC (M) to SMA (M)

SMA (F) to SMA (F)

SMA (M) to SMA (M)

RP-SMA (F) to N (M)

RP-SMA (M) to N (F)

MCX (F) to SMA (F)

MCX (F) to SMA (M)

MCX (M) to N (M)

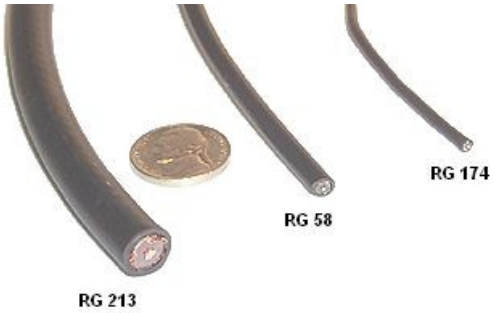
MMCX (M) to N (F)

MMCX (M) to N (M)

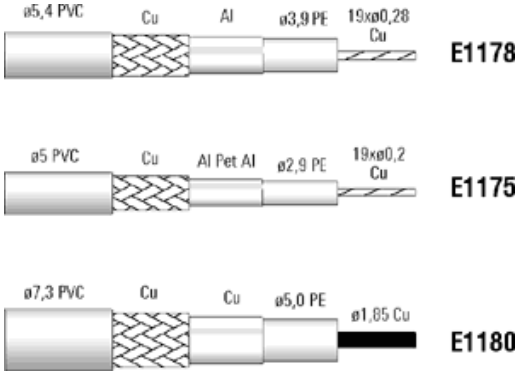
SMA (F) to N (F)

2) **Cavi RF:** i cavi per radiofrequenza (RF) non sono tutti uguali e le caratteristiche che più li distinguono sono l'impedenza e l'attenuazione che aumenta con l'aumentare della frequenza utilizzata. Da ciò, si deduce che non tutti hanno le caratteristiche opportune per l'impiego nelle W-LAN ma in alcuni casi particolari, come test e prove "on the road" dove è richiesta flessibilità con poco ingombro, l'uso di un cavo RF non adatto in impianti "fissi" è tollerato. A seguire sono elencate le principali caratteristiche dei cavi più comunemente impiegati:

| Tipo | Diametro esterno (mm) | Impedenza tipica (Ohm) | Attenuazione a 1GHz (dB) su 100m | Attenuazione a 2,4 GHz (dB) su 100m |
|---|---|---|---|---|
| | | | | |
| RG 58 U | 5 | 50 +/- 2 | 49.6 | 78,9 |
| RG 174 A/U | 2.8 | 50 +/- 2 | 95 (max freq) | ---- |
| RG 213 U | 10.3 | 50 +/- 2 | 22.1 | 53.7 |
| H 155 (E1178) | 5.4 | 50 +/- 2 | 30.9 | 49.6 |
| H 2000 Flex | 10.3 | 50 +/- 2 | 13.5 | 21.8 (2.3GHz) |
| LMR 400 | 10.29 | 50 +/- 2 | 12.8 (900MHz) | 22.2 (2.5GHz) |
| Aircell 7 | 7.3 | 50 +/- 2 | 22.52 | 35.6 |
| Aircom Plus | 10.3 | 50 +/- 2 | 13.4 | 22.5 |
| Ecoflex 10 | 10.2 | 50 +/- 2 | 14.2 | 23.6 |
| Ecoflex 15 | 14.6 | 50 +/- 2 | 9.8 | 16.3 |
| Heliax ½" | 15.7 | 50 +/- 2 | 7.28 | 12.09 (2.5GHz) |
| Cellflex ½"-50 | 16.2 | 50+/- 1 | 7.2 | 11.6 |




RG Type




H 155 Type

H 2000 Flex

LMR 400

Aircell 7

Aircom Plus

Ecoflex 10


Ecoflex 15

Heliax ½”

Heliax Type

Cellflex ½”

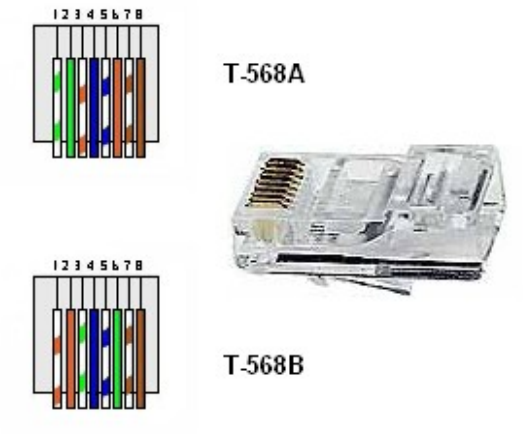
Come già accennato in precedenza, il cavo d'antenna dev'essere il più corto possibile, specialmente se vengono impiegati cavi con attenuazioni rilevanti come nel caso di RG 58. Per prove tecniche di link, l'uso di RG58 è consigliato per la flessibilità che gli conferisce ottima maneggevolezza, spesso richiesta quando si opera in condizioni non proprio favorevoli. Generalmente le antenne vengono fornite di un "codino" di RG213. l'uso di questo tipo di cavo costituisce un buon compromesso tra attenuazione e costo d'acquisto. L'uso di H155 costituisce ottima alternativa all' RG213 ma presenta difficoltà di reperibilità, ancora più accentuata con l' Aircell, Aircom, LMR400, Ecoflex, Heliax e Cellflex. Questi ultimi, oltre ad essere ottimi, sono preferiti in ambito professionale. Il "difetto" principale è un costo d'acquisto piuttosto alto e necessitano di appositi connettori, cosa che ne scoraggia l'uso da parte dell'utente medio, in ambito amatoriale. Non vorrei scadere in ripetizioni ma occorre ricordare sempre la linea generale, che impone, a causa della bassa potenza erogata dagli access point, il cavo d'antenna sempre il più corto possibile e quando non praticabile, occorre compensare con antenna/e di maggior guadagno, unito da un ottimo puntamento.

3) **Link lento a causa di altre reti wireless:** quando sono presenti altre reti wireless, particolare attenzione va data ai canali usati, evitando quanto più possibile l'utilizzo di uno già occupato e se non possibile, usare un livello di potenza sufficiente per garantire il link, cercando altresì di direzionare il segnale solo nel punto voluto. Questa semplice norma, è stata mutuata dal "principio del buon vicinato", permettendo di far convivere più reti senza recare (o almeno limitare) disturbo ad altri. Sebbene gli standard 802.11b e 802.11g permettano l'uso di più canali (13 in Italia), solamente 3 sono quelli non sovrapposti (detti in gergo tecnico "non overlapped") e come deducibile dalla tabella che ne illustra le frequenze (paragrafo 1.2), sono: 1, 6, 11. Per meglio capire il perché, si può fare riferimento alla rappresentazione grafica.
   Utilizzando invece gli standard 802.11a/h, questo problema è piuttosto raro poiché i canali disponibili sono 8 e non sono sovrapposti ma, il "principio del buon vicinato" è sempre bene rispettarlo.

4) **L'AP è raggiungile da w-lan ma non dalla lan:** è un problema non raro quando si stendono e si cablano cavi di rete ethernet. Sebbene tutto questo possa sembrare un gioco da ragazzi, i difetti di un cavo, autocostruito o no, possono essere diversi e precisamente:

   - Una piega troppo angolata lungo il cavo, può indurre all'interruzione di qualche conduttore interno.
   - Un montaggio poco accurato dei connettori rj45 od uno strappo dato durante la stesura, possono creare cortocircuiti.
   - Lo scambio di una coppia di conduttori rende impraticabile il link ed è la causa più subdola e frequente non solo nei cavi autocostruiti, ma anche in quelli commerciali.

   Da quanto esposto finora, in linea generale, il mancato funzionamento è da ricercare nella sequenza dei colori utilizzata durante la crimpatura dei plug rj45 utilizzati nella rete lan. Si fa presente che un cavo ethernet va spelato per un massimo di 1,5 centimetri ed usare la giusta sequenza dei colori, definita attraverso gli standard **T-568A** e **T-568B**.
   I due tipi di presa e connettore, differiscono per la codifica di cablaggio dei morsetti, mentre le prestazioni sono uguali. Ogni morsetto viene identificato con un colore, che deve corrispondere al colore del cavo collegato. In Italia viene tipicamente utilizzato il cablaggio tipo **T-568B**.




Nelle realizzazioni pratiche, utilizzando reti ethernet 10/100 Mbps, l'utilizzo di uno standard piuttosto di un altro, non è strettamente vincolante. Si fa però presente che per una connessione diretta tra pc ed hub o tra access point ed hub, bisogna utilizzare cavi ethernet dritti, perciò andrà usato un solo standard (T-568A oppure T-568B).
Utilizzando entrambi gli standard (una presa utilizza T-568A e l'altra T568B), si realizza un cavo **"incrociato"** (chiamato anche **"cross"**) che premette la connessione diretta tra due pc o tra pc e access point che non usano l'auto-sense (o **auto DMI**).
I cavi usati per le connessioni ethernet, si suddividono in categorie, secondo le prestazioni:

| | | |
|---|---|---|
| Categoria 1 | Nessun criterio di prestazioni | Cavetto telefonico, non usato per trasferimento dati tra computer |
| Categoria 2 | 1 MHz (cavi telefonici) | 4Mbps |
| Categoria 3 | 16 MHz (Ethernet 10Base-T) | 10Mbps |
| Categoria 4 | 20 MHz (Token-Ring e Ethernet 10Base-T) | 16Mbps |
| Categoria 5 | 100 MHz (Ethernet 100Base-T e 10Base-T) | 100Mbps |
| Categoria 6 | 1 GHz (Ethernet 1000Base-T, 100Base-T e 10Base-T) | 1000Mbps |

5) **Perdita di connessione tra AP e client PCI o PCMCIA:** è un problema che affligge le reti Wi-Fi e Windows XP service pack 1. Il problema è la perdita di connessione che si verifica ciclicamente ad intervalli da 4 a 10 minuti. Alla base di questo malfunzionamento vi è una errata implementazione dei protocolli da parte di Microsoft, risolto con il service pack 2 che oltretutto utilizza strumenti di gestione migliorati. Si manifesta quando, utilizzando l'utility interna di Windows XP per la gestione delle reti Wi-Fi chiamata "*Wireless Zero Configuration Service*", e si disabilita il parametro "*Broadcast SSID*": il client sembra associarsi correttamente ma, ad intervalli regolari, si disconnette. Lasciando invece il parametro "Broadcast SSID" abilitato, il bug non si presenta ma tale impostazione non è consigliabile poiché rivela ai potenziali "sniffer" l'esistenza di una w-lan ed il corretto SSID per l'accesso. Da fonti Microsoft si apprende che tale malfunzionamento si dovrebbe

verificare solo in presenza di 2 access point in cui il parametro SSID Broadcast è abilitato solo su uno di essi, in una nota si specifica inoltre che non si tratta di un malfunzionamento ma proprio del modo in cui è stato deciso di implementare la funzione SSID Broadcast.
Dai messaggi scambiati nei forum si apprende che il problema non è relativo solo alla presenza di due AP, ma anche in presenza di uno solo. In alcuni casi avendo modificato i parametri di default, non è più stato possibile associarsi correttamente all' AP, unica soluzione il reset dei parametri.

Le soluzioni sono 2: l'abilitazione della funzione "SSID Broadcast", abbassando però il livello di sicurezza della rete wireless, oppure non utilizzare l'utility Wireless Zero Configuration, optando per i sobri tools che vengono forniti a corredo dei vari client.

6) **DWL900AP+ bloccato alla pagina di aggiornamento firmware:** è un difetto che saltuariamente si presenta nelle revisioni "C" e risultano praticamente vani i tentativi di ripristino utilizzando revisioni di firmware precedenti o successive a quella installata. Sebbene l'ap risulta bloccato alla pagina d'aggiornamento del firmware senza dare nessun segno di funzionamento, è comunque possibile il recupero, utilizzando una particolare revisione del firmware 3.07 denominata "3.07 fw recovery" e disponibile in rete.
La procedura per riprendersi da questo letargo, si compone di questi semplici passi:

**A)** Spegnere l'unità scollegando il cavo d'alimentazione;

**B)** Inserire una clip nel foro del reset e tenere premuto il pulsante;

**C)** Accendere il dispositivo inserendo lo spinotto d'alimentazione, tenendo sempre premuto il pulsante di reset;

**D)** Dopo 5 secondi, rilasciare il reset e puntare il proprio browser all'indirizzo IP 192.168.0.50 che, presenterà la pagina di "Firmware Upgrade". Ricercare il nuovo file del firmware ed eseguire l'aggiornamento, poi l'apparato si riavvierà automaticamente. Tornare all'indirizzo indicato in precedenza dove sarà ora possibile effettuare le normali impostazioni.
La tecnica di risveglio non è sempre di facile attuazione e spesso bisogna ripeterla più volte affinché sortisca l'effetto desiderato.

7) **DSL-G604T/G624T bloccato ed irraggiungibile:** questa procedura è stata descritta nel forum di dlinkpedia (www.dlinkpedia.net) e funziona per i router D-Link DSL-G604T e DSL-G624T, che presentano un hardware molto molto simile, fermo restando una diversa gestione dello switch di cui sono dotati. I sintomi che decretano il blocco dell'apparato sono:

- Il sistema operativo segnala cavo di rete collegato regolarmente o connettività limitata od assente e non riuscite a "uscire" su Internet, ovvero non riuscite a navigare né ad usare qualsiasi applicazione che necessiti della connessione ad Internet o LAN.
- Il led WLAN spento, ma potrebbe non esserlo.
- Impossibile accedere alla pagina di amministrazione del router. Utilizzando il browser preferito e tentando di collegarsi all'IP del router si ottiene "Impossibile visualizzare la pagina" dopo un certo timeout.
- Nessun tipo di risposta al ping sulll'IP del router.

- Anche cambiando il vostro IP o cambiando proprio PC ottenete gli stessi sintomi.
- Provando a fare il reset manuale premendo il pulsante dietro al router per 30 secondi, la situazione non cambia.

Tali sintomi si possono presentare dopo un tentativo di aggiornamento non andato a buon fine, caricando file di configurazione di firmware diversi od errori di configurazione ed anche dopo diverso tempo di corretto funzionamento, in seguito alla modifica di regole di port-forwarding. In questi modelli purtroppo il firmware può anche venire corrotto in seguito ad un utilizzo prolungato... Per ottenere il recupero dell'apparato, occorre cambiare il firmware attualmente corrotto con un firmware straniero di recovery, operando in un modo particolare, così da tornare ad avere un router operativo e successivamente installare firmware originale ed appropriato per il nostro modello posseduto. Ma vediamo come effettuare questa procedura, che è possibile ripetere se non funziona al primo tentativo:

- Assicurarsi per prima cosa che il router sia alimentato e correttamente collegato tramite cavo ethernet al PC. NON tentare l'aggiornamento tramite connessione Wi-Fi, se disponibile, perché pericoloso e comunque mai farlo su apparati wireless!!!
- Procurarsi il firmware australiano del DSL-G604T in formato .EXE. Ne esiste anche uno specifico per il DSL-G624T, ma su quest'ultimo funziona anche quello del 604T che, sebbene sconsigliato, nel 98% dei casi assolve a questo compito. Il download alla pagina: http://www.dlink.com.au/tech/Download/download.aspx?product=DSL-G604T&revision=REV_A&filetype=Firmware
- Impostare i parametri dell' adattatore ethernet del PC come segue:

    IP: 10.1.1.99
    SubnetMask: 255.0.0.0
    Default gateway: 10.1.1.1
    DNS server preferito: 10.1.1.1
    DNS server alternativo: 4.2.2.2

Assicurarsi di aver applicato correttamente tali impostazioni

- Disattivare o disabilitare temporaneamente, se presenti, il firewall e l'antivirus.
- Lanciate il firmware upgrade tool australiano scaricato precedentemente. Nella prima schermata attivare la casella "Corrupted-image mode" e premete il pulsante Next.
- Come viene richiesto dal tool, nella seconda schermata, staccare l'alimentazione del router ed attendere almeno 10 secondi.
- Trascorsi i 10 secondi, PRIMA ricollegare l'alimentazione del router e POI premere sul pulsante Next.
- Se le operazioni richieste sono state eseguite correttamente, dopo qualche secondo si vedrà la scritta Upgrading New firmare ed una progress bar che si riempie pian piano. Se si verifica ciò, siete messi bene perché significa che il tool è riuscito a trovare il router e sta eseguendo la sovrascrittura del firmware con il firmware australiano del G604T il quale vi consentirà di raggiungere ed usare la pagina di amministrazione!. Finito l'upgrade cliccare sul pulsante Finish.

**ATTENZIONE!!** Se dopo aver ridato l'alimentazione al router compare un messaggio tipo:

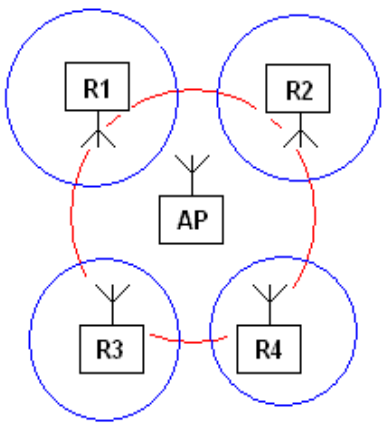
**FTP Timeout**
**Device's IP address is x.x.x.x**
**...**

Allora uscire dal tool chiudendo l'applicazione e staccare l'alimentazione del router. Cambiare l'indirizzo IP del PC in x.x.x.x+1 e come default gateway mettere x.x.x.x. La subnet mask verrà assegnata automaticamente, i DNS lasciarli come prima. Ricollegare l'alimentazione del router e ripetere il procedimento.

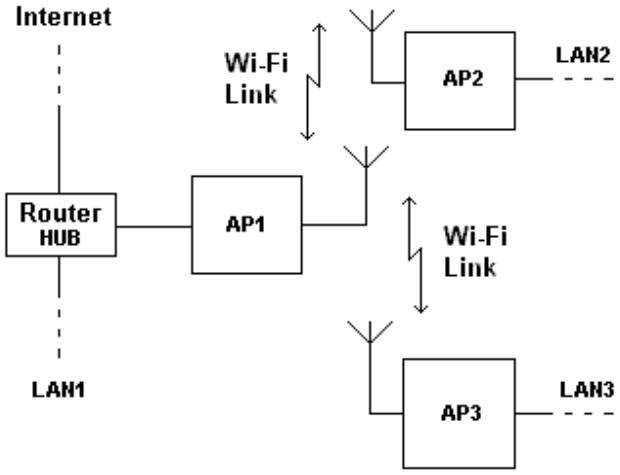
- Se con l'ip 10.1.1.1 o con l'ip uscito nel messaggio di errore, l'upgrade del firmware va a buon fine, allora potete usare quell'IP per accedere alla pagina di amministrazione del router. Se tutto è andato correttamente a buon fine, dovreste vedere di nuovo il led WLAN acceso, segno che il firmware è stato sostituito perfettamente. Aprire con il browser preferito l'indirizzo 10.1.1.1 oppure x.x.x.x, che risponderà con la richiesta delle credenziali di default per l'amministrazione. Bene, si proceda ora all'aggiornamento con il software nativo del proprio apparato.
- Dalla pagina di amministrazione del router dovrebbe comparirvi che adesso avete un modello G604T (anche se in realtà avete il G624T). Entrare nel menù Tools -> Firmware ed aggiornare il firmware del router col firmware corretto, ovvero l'ultimo firmware originale per il modello posseduto ed offerto dal sito del produttore (italiano o straniero non fa differenza).

**ATTENZIONE!!** Se non è possibile accedere alla pagina di amministrazione del router anche dopo averlo aggiornato col firmware australiano, ma vedete il led WLAN acceso, è bene ricordarsi che adesso il router è perfettamente funzionante e quindi risulta possibile fare il reset manuale e riprovare ad accedere col browser provando l'IP dell'aggiornamento, ovvero 10.1.1.1. E' bene far presente che i firmware AU e NZ sono accessibili ad un indirizzo diverso dal default europeo (bisogna prestare attenzione soprattutto se si è newbie). Lo stesso problema si presenta se viene eseguito un "reset to default" dei parametri. Ipotizzando di essere su 192.168.1.1, effettuando un "reset to default", l'apparato non sarà più accessibile allo stesso indirizzo IP.

8) **Utilizzo di più repeater su un singolo AP:** è la condizione d'esercizio degli apparati più critica, poiché, molte volte, si pensa che la ripetizione del segnale di un ap sia possibile innumerevoli volte ma ciò non corrisponde alla realtà, risultando pressoché impossibile realizzare un link del genere. Da questa considerazione si evince che è possibile utilizzare più repeater, purché ad ognuno di essi giunga il segnale originale dell'access point. Nella seguente figura, viene illustrata la giusta sequenza o disposizione dei vari apparati:



9) **Multi-link in una rete mista con router ed accesso internet:** Da quanto spiegato nel capitolo 7 (PC in rete: la creazione), è possibile realizzare una connessione wireless unendo diverse LAN, condividendone la connessione ad internet. Lo schema riportato di seguito è la situazione classica in cui ci si può trovare:




Sebbene questa configurazione sia sempre valida, può accadere che, utilizzando alcuni dispositivi, le risorse delle reti LAN siano perfettamente accessibili mentre la connessione ad internet no. Il difetto si presenta quando il link Wi-Fi utilizza apparati in modalità AP e Client. Sebbene con questa modalità la compatibilità tra i dispositivi è sempre garantita, si consiglia di utilizzare apparati identici e di posizionare l'apparato in modalità AP collegato al router. Questa disposizione è quella corretta e che si dovrebbe usare anche nelle configurazioni più complesse, dov'è richiesta anche la condivisione della connessione ad internet. Se si desidera permettere la connessione anche ai computer portatili, è bene utilizzare apparati che consentano la modalità WDS che, dovrà essere impostata a tutti gli apparati. In questo modo si avrà un "bridge" tra i diversi apparati che permetteranno anche la connessione ai client, rendendo oltretutto la rete più sicura.

10) **Impostazioni approfondite degli AP:** Esistono molte voci nella configurazione degli access point e non di rado vengono usati termini criptici. Il significato di questi termini, aiutano a modificare il comportamento della rete wireless, migliorandone le prestazioni. I parametri più significativi sono:

***Beacon Interval:*** i Beacon sono i pacchetti che gli access point inviano per sincronizzarsi con una rete. Il range di valori ammessi va da 20 a 1000 ma normalmente non occorre superare i 100 pacchetti.

***DTIM:*** il Delivery Traffic Indication Message è il conto alla rovescia per informare i client sulla successiva finestra d'ascolto dei messaggi di Broadcast e Multicast. Il suo range di valori ammessi va da 1 a 255. Un valore di 1 o 3 è sufficiente.

***Fragmentation Threshold:*** il livello di frammentazione con il relativo valore in byte, determina quanto i dati saranno frammentati. I pacchetti che eccederanno al valore settato, saranno frammentati prima dell'invio. Valori bassi determinano un rallentamento della rete wireless. Il suo range di valori ammessi va da 256 a 2346. Normalmente questo valore

dev'essere di 2346 Byte, ma può variare secondo il tipo di apparato e standard di trasmissione dati utilizzato.

***RTS Threshold:*** il Request To Send è la negoziazione della richiesta per inviare blocchi di dati tra il client e l'access point. il valore è compreso tra 256 e 2346. Generalmente non conviene intervenire su questo parametro, ma sono permesse comunque piccolissime variazioni.

***Preamble Type:*** di tipo ***Short*** o ***Long***, determina la lunghezza del blocco ***CRC*** (Cyclic Redundancy Check, il controllo ridondante ciclico) degli errori. Conviene settarlo su ***Short*** quando nella rete si ha elevato traffico di dati, garantendo in questo modo un aumento della velocità di trasferimento. Alcune volte, il suo valore può garantire una maggiore efficienza del link wireless su lunghe distanze.

***Authentication:*** determina il modo con cui gli apparati si autenticano tra loro. Assume generalmente tre diverse modalità di funzionamento:

***Open System:*** comunica attraverso la rete le chiavi di autenticazione.
***Shared Key:*** l'autenticazione avviene solo con apparati aventi stesso WEP.
***Auto:*** determina il settaggio automatico all'autenticazione dei client.

11) **Quali materiali attenuano il segnale di una W-LAN: T**utti i materiali sono in grado di attenuare il segnale Wi-Fi. Nella tabella a seguire è possibile capire quale materiale può provocare maggiori problemi in termini di segnale:

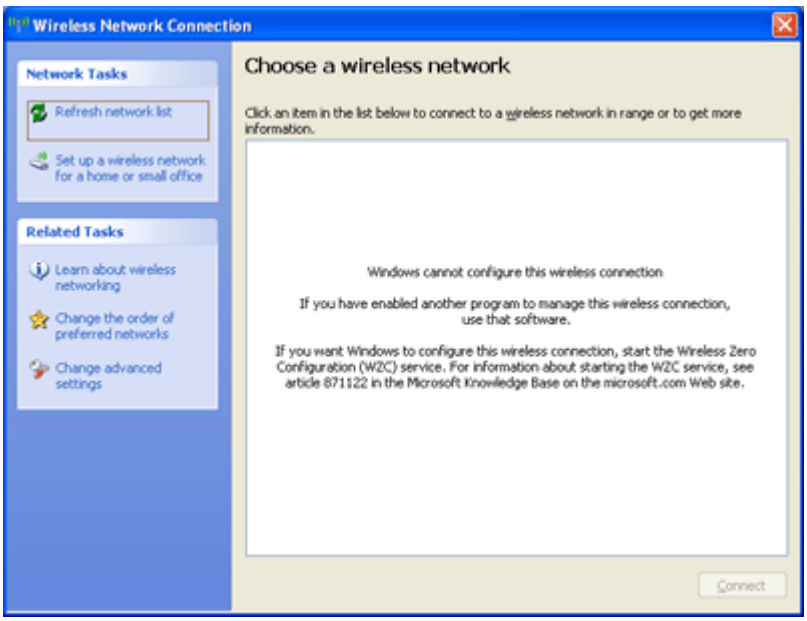
| Barriera RF | Degrado del segnale | Esempio |
|---|---|---|
| Legno | Basso | Tramezzo d'ufficio |
| Plastica | Basso | Rifiniture d'interno |
| Materiali sintetici | Basso | Tramezzo d'ufficio |
| Vetro | Basso | Finestre |
| Acqua | Medio | Legno umido |
| Mattoni | Medio | Muri interni / esterni |
| Marmo | Medio | Muri interni / esterni |
| Carta | Alto | Carta parati / giornali |
| Cemento armato | Alto | Pavimenti / muri esterni |
| Vetro antiproiettile | Alto | Separé di sicurezza |
| Metalli | Altissimo | Armature cemento armato |

12) **Abilitare lo WZC in NetStumbler:** Come si è visto nel capitolo riguardante l'attacco alla (propria) rete, Network Stumbler è un tool che rileva le reti wireless attraverso una scansione attiva utilizzando delle richieste di "probe". Il programma, quando lanciato, forza delle restrizioni che sono state volutamente inserite in modo da impedire l'utilizzo in Windows del servizio **Wireless Zero Configuration**, impedendo di fatto l'uso simultaneo con i tool di gestione del sistema operativo che permettono di associarsi ad un AP. Esiste tuttavia un hack creato da "appassionati" che permette di ripristinare il tutto semplicemente apportando una modifica con un editor esadecimale. I passi da seguire sono questi:

- utilizzare la versione 0.4.0 di Network Stumbler;
- controllare che il **checksum** sia **86E7586E4E45444F23EF2B71E2A93BFB**;
- installare il programma;
- nella directory del programma verificare il checksum del file NetStumbler.exe sia **5EF079E5D178CB4CA7F2C904465EDF36**;
- utilizzando un editor esadecimale (consigliato UltraEdit 32 o WinHex), cercare l'indirizzo **000387b0h**;
- mantenendo invariato il primo valore (76), cambiare il secondo da 63 a **61;**
- salvare la modifica;
- verificare che il checksum sia **2F753FD1D69B5C4138AEDB572F2D58FD.**

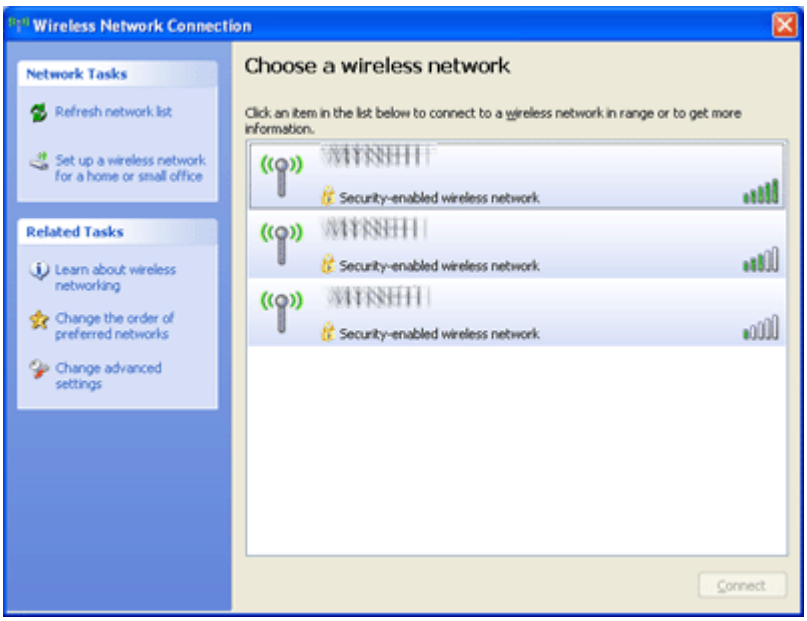
A seguire è possibile vedere gli screenshot di NetStumbler attraverso l'editor esadecimale e dell'utility di gestione delle reti wireless di Windows prima della modifica:

```
00038680h: 72 75 6E 6E 69 6E 67 20 61 74 20 61 6C 6C 00 00 ; running at all..
00038690h: 4E 65 74 77 6F 72 6B 20 53 74 75 6D 62 6C 65 72 ; Network Stumbler
000386a0h: 20 4F 70 74 69 6F 6E 73 00 00 00 00 00 00 00 00 ;  Options........
000386b0h: 53 74 6F 70 70 69 6E 67 20 74 68 65 20 57 69 72 ; Stopping the Wir
000386c0h: 65 6C 65 73 73 20 5A 65 72 6F 20 43 6F 6E 66 69 ; eless Zero Confi
000386d0h: 67 75 72 61 74 69 6F 6E 20 53 65 72 76 69 63 65 ; guration Service
000386e0h: 2E 20 54 68 69 73 20 6D 61 79 20 74 61 6B 65 20 ; . This may take
000386f0h: 61 20 77 68 69 6C 65 2E 00 00 00 00 1C EF 42 00 ; a while......ïB.
00038700h: A0 62 40 00 00 14 40 00 80 5A 40 00 00 14 40 00 ;  b@...@.€Z@...@.
00038710h: 6F 70 65 6E 00 00 00 00 62 C6 A1 E8 44 01 FB 3F ; open....bÆ¡èD.û?
00038720h: 25 73 20 20 28 42 75 69 6C 64 20 25 75 29 0D 0A ; %s  (Build %u)..
00038730h: 0D 0A 25 73 0D 0A 25 73 25 73 00 00 50 6C 65 61 ; ..%s..%s%s..Plea
00038740h: 73 65 20 73 65 65 20 48 65 6C 70 20 6D 65 6E 75 ; se see Help menu
00038750h: 20 66 6F 72 20 6C 69 63 65 6E 73 65 20 69 6E 66 ;  for license inf
00038760h: 6F 72 6D 61 74 69 6F 6E 2E 0D 0A 0D 0A 00 00 00 ; ormation........
00038770h: FE EB 42 00 B0 3F 41 00 F0 55 41 00 80 5A 40 00 ; þëB.°?A.ðUA.€Z@.
00038780h: 00 14 40 00 D0 56 41 00 FE EB 42 00 E0 3F 41 00 ; ..@.ÐVA.þëB.à?A.
00038790h: 00 14 40 00 80 5A 40 00 00 00 14 40 00 2E 63 68 6D ; ..@.€Z@...@..chm
000387a0h: 00 00 00 00 2E 68 6C 70 00 00 00 00 77 7A 63 73 ; .....hlp....wzcs
000387b0h: 76 63 00 00 4D 53 20 53 61 6E 73 20 53 65 72 69 ; vc..MS Sans Seri
000387c0h: 66 00 00 00 57 45 00 00 53 4E 00 00 54 68 65 20 ; f...WE..SN..The
000387d0h: 63 6F 6E 66 69 67 75 72 61 74 69 6F 6E 20 69 6E ; configuration in
000387e0h: 66 6F 72 6D 61 74 69 6F 6E 20 63 6F 75 6C 64 20 ; formation could
000387f0h: 6E 6F 74 20 62 65 20 73 65 6E 74 2E 00 00 00 00 ; not be sent.....
00038800h: 54 68 65 20 73 65 72 76 65 72 20 72 65 74 75 72 ; The server retur
00038810h: 6E 65 64 20 74 68 65 20 66 6F 6C 6C 6F 77 69 6E ; ned the followin
00038820h: 67 20 6D 65 73 73 61 67 65 3A 0D 0A 0D 0A 00 00 ; g message:......
00038830h: 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 ; Content-Type: ap
00038840h: 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D ; plication/x-www-
00038850h: 66 6F 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D ; form-urlencoded.
00038860h: 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A ; .Content-Length:
00038870h: 20 25 64 00 50 4F 53 54 00 00 00 00 2F 63 6F 6D ;  %d.POST..../com
00038880h: 70 61 74 2F 6E 73 30 34 30 2E 70 68 70 00 00 00 ; pat/ns040.php...
00038890h: 77 77 77 2E 73 74 75 6D 62 6C 65 72 2E 6E 65 74 ; www.stumbler.net
000388a0h: 00 00 00 00 74 65 78 74 2F 70 6C 61 69 6E 00 00 ; ....text/plain..
CHRONICLESOFAWARDRIVER.ORG  25 75 00 00 ; NetStumbler/%u..
```




Di seguito è possibile vedere gli screenshot di NetStumbler attraverso l'editor esadecimale e dell'utility di gestione delle reti wireless di Windows ad hack ultimato:

```
00038680h: 72 75 6E 6E 69 6E 67 20 61 74 20 61 6C 6C 00 00 ; running at all..
00038690h: 4E 65 74 77 6F 72 6B 20 53 74 75 6D 62 6C 65 72 ; Network Stumbler
000386a0h: 20 4F 70 74 69 6F 6E 73 00 00 00 00 00 00 00 00 ;  Options........
000386b0h: 53 74 6F 70 70 69 6E 67 20 74 68 65 20 57 69 72 ; Stopping the Wir
000386c0h: 65 6C 65 73 73 20 5A 65 72 6F 20 43 6F 6E 66 69 ; eless Zero Confi
000386d0h: 67 75 72 61 74 69 6F 6E 20 53 65 72 76 69 63 65 ; guration Service
000386e0h: 2E 20 54 68 69 73 20 6D 61 79 20 74 61 6B 65 20 ; . This may take
000386f0h: 61 20 77 68 69 6C 65 2E 00 00 00 00 1C EF 42 00 ; a while......ïB.
00038700h: A0 62 40 00 00 14 40 00 80 5A 40 00 00 14 40 00 ;  b@...@.€Z@...@.
00038710h: 6F 70 65 6E 00 00 00 00 62 C6 A1 E8 44 01 FB 3F ; open....bÆ¡èD.û?
00038720h: 25 73 20 20 28 42 75 69 6C 64 20 25 75 29 0D 0A ; %s  (Build %u)..
00038730h: 0D 0A 25 73 0D 0A 25 73 25 73 00 00 50 6C 65 61 ; ..%s..%s%s..Plea
00038740h: 73 65 20 73 65 65 20 48 65 6C 70 20 6D 65 6E 75 ; se see Help menu
00038750h: 20 66 6F 72 20 6C 69 63 65 6E 73 65 20 69 6E 66 ;  for license inf
00038760h: 6F 72 6D 61 74 69 6F 6E 2E 0D 0A 0D 0A 00 00 00 ; ormation........
00038770h: FE EB 42 00 B0 3F 41 00 F0 55 41 00 80 5A 40 00 ; þëB.°?A.ðUA.€Z@.
00038780h: 00 14 40 00 D0 56 41 00 FE EB 42 00 E0 3F 41 00 ; ..@.ÐVA.þëB.à?A.
00038790h: 00 14 40 00 80 5A 40 00 00 14 40 00 2E 63 68 6D ; ..@.€Z@...@..chm
000387a0h: 00 00 00 00 2E 68 6C 70 00 00 00 00 77 7A 63 73 ; .....hlp....wzcs
000387b0h: 76 61 00 00 4D 53 20 53 61 6E 73 20 53 65 72 69 ; va..MS Sans Seri
000387c0h: 66 00 00 00 57 45 00 00 53 4E 00 00 54 68 65 20 ; f...WE..SN..The
000387d0h: 63 6F 6E 66 69 67 75 72 61 74 69 6F 6E 20 69 6E ; configuration in
000387e0h: 66 6F 72 6D 61 74 69 6F 6E 20 63 6F 75 6C 64 20 ; formation could
000387f0h: 6E 6F 74 20 62 65 20 73 65 6E 74 2E 00 00 00 00 ; not be sent.....
00038800h: 54 68 65 20 73 65 72 76 65 72 20 72 65 74 75 72 ; The server retur
00038810h: 6E 65 64 20 74 68 65 20 66 6F 6C 6C 6F 77 69 6E ; ned the followin
00038820h: 67 20 6D 65 73 73 61 67 65 3A 0D 0A 0D 0A 00 00 ; g message:......
00038830h: 43 6F 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 ; Content-Type: ap
00038840h: 70 6C 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D ; plication/x-www-
00038850h: 66 6F 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D ; form-urlencoded.
00038860h: 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A ; .Content-Length:
00038870h: 20 25 64 00 50 4F 53 54 00 00 00 00 2F 63 6F 6D ;  %d.POST..../com
00038880h: 70 61 74 2F 6E 73 30 34 30 2E 70 68 70 00 00 00 ; pat/ns040.php...
00038890h: 77 77 77 2E 73 74 75 6D 62 6C 65 72 2E 6E 65 74 ; www.stumbler.net
000388a0h: 00 00 00 00 74 65 78 74 2F 70 6C 61 69 6E 00 00 ; ....text/plain..
CHRONICLESOFAWARDRIVER.ORG                  25 75 00 00 ; NetStumbler/%u..
```




Questo hack è stato tradotto dalla versione originale in lingua inglese e disponibile al link: http://www.chroniclesofawardriver.org/How-To_Hack_NSv4.4.0_Enable_WZC.html

13) **Router abilitati per DynDNS e NO-IP:** I servizi per DynDNS e NO-IP inseriti nel firmware di alcuni router, permettono di creare un sito direttamente nel proprio pc senza la necessità d'avere un indirizzo IP statico fisso dal provider che ci fornisce la connettività. Da ciò si capisce che anche da una linea xDSL per uso casalingo può fornire quanto voluto, basta dotarsi del giusto router che permetta l'inserimento dei dati relativi alla mail ed alla password. Di seguito sono elencati quegli apparati che gestiscono i servizi DynDNS e NO-IP, correlati da una breve descrizione:

**D-Link DSL-G624T** (Modem Router ADSL, ADSL2/2+, AP 802.11g 54Mbps, switch 4 porte, firewall SPI, QoS, filtri su IP autorizzati per LAN e W-LAN)

Servizi per il solo DynDNS:

**Linksys WRT54GS con dd-wrt**
**Linksys WGT624**
**Linksys WGT634W**
**Netgear DGT834GT** (Modem Router ADSL, ADSL2/2+ - AP 802.11g 108Mbps - switch 4 porte - Firewall SPI)

14) **Problemi di allineamento dei router xDSL:** molte volte ci si chiede perché un router faccia fatica ad allinearsi con la portante della linea xDSL. Se il vostro apparato contempla tra i menù quello relativo allo status dettagliato della connessione (Status – Phisical Layer), è bene prestare attenzione ai valori di attenuazione della linea:

Rapporto segnale rumore (SNR)

| | | |
|---|---|---|
| < 5dB | = | problemi di linea, estrema difficoltà di sincronizzazione |
| 5db-7db | = | problemi alla linea, possibili allineamenti intermittenti od assenti |
| 8db-13db | = | valori nella media, nessun problema di allineamento |

14db-22db = molto buono
23db-28db = eccellente
29db-35db = raro, quando la centrale è sotto casa

Attenuazione in Download ed Upload:

< 20 = raro, linea molto buona o quando la centrale è sotto casa
20-30 = eccellente
30-40 = molto buono
40-60 = nella media
60-65 = scadente
>= 65 = possibili problemi

La velocità di connessione dipende non solo dalla qualità della linea, ma anche dal tipo di modulazione e tecnologia implementata:

ADSL_G.dmt = Discrete Modulation Tone a velocità adattativa, tipica della ADSL che permettono fino a 8 Mbit in downstream ed 1 Mbit in upstream; la distanza massima di copertura è di 3-4 Km. I principali standard appartenenti sono: ITU-T G.992 Annex-A, ITU-T G.992.1 (G.dmt), ITU-T G.992.1 (G.lite), ITU-T G.994.1 (G.hs, Multimode).

ADSL_G.cap = Sviluppata nei laboratori di AT&T, la modulazione CAP (Carrierless Amplitude/Phase Modulation) è una variante della modulazione QAM che modula la fase e l'ampiezza di una portante in 64 modi diversi.

In entrambe le modulazioni, per migliorare il rapporto segnale-rumore si utilizza la codifica Trellis e Viterbi.

Esistono diverse "versioni" di tecnologia xDSL, esattamente:

- VDSL: Very High speed DSL, con link asimmetrico. Downstream da 13 a 52 Mbps ed upstream da 1,5 a 6 Mbps. Massima distanza di 1500 metri, doppino telefonico ritorto con l'utente e collegamento della centrale in fibra ottica.
- HDSL: High data-rate DSL garantisce un link simmetrico, uguale per il downstream ed upstream, ad alta velocità. La velocità massima è di 2,048 Mbps. Il limite è quello che deve utilizzare due o tre linee telefoniche per funzionare. Utilizzata prevalentemente per collegamenti dedicati come intranet aziendali. Copertura massima 3,3 Km.
- SHDSL: detta anche SDSL è Single line HDSL. Versione semplificata della HDSL, dove viene utilizzata solo una linea, con link simmetrico di 768 Kbps. Utilizzata per estendere LAN o server remoti.
- ADSL: DSL di tipo asimmetrico, dove il downstream e superiore all'upstream. Utilizza una parte della banda della linea telefonica e non si sovrappone alla linea voce. La velocità massima è 8 Mbps per il downstream e 640 Kbps per l'upstream. La massima distanza di copertura è di 3-4 Km.
- ADSL2: ADSL2 utilizza la stessa tecnologia di ADSL ma incrementa la velocità di downstream fino a 12 Mbps contro gli 8 Mbps di ADSL, e quella in upstream fino ad 1 Mbps contro i 640 Kbps. Viene inoltre esteso il raggio di copertura.
- ADSL2+: Con essa il flusso dati arriva a 25 Mbps in downstream ed 1 Mbps in upstream su cavo telefonico la cui lunghezza non supera i 1520 metri.

In conclusione, la massima velocità dipende da una serie di fattori, di cui i più rilevanti sono

il tipo di cavo utilizzato per la linea telefonica, la distanza tra modem ed il tipo di modulazione impiegata. Nella tabella a seguire, è possibile notare le variazioni di velocità di una linea ADSL in funzione della distanza e del tipo di cavo utilizzato:

| 24 AWG (Km) | 26 AWG (Km) | Downstream (Mbps) | Upstream (Kbps) |
|---|---|---|---|
| 5,5 | 4,6 | 1,544 | 160 |
| 4,9 | 4 | 2,048 | 160 |
| 5,6 | 3,9 | 3,088 | 240 |
| 5,4 | 3,8 | 4,096 | 320 |
| 4,3 | 3,7 | 4,632 | 320 |
| 3,7 | 2,8 | 6,312 | 640 |
| 2,8 | 2,4 | 8,448 | 640 |

La dimostrazione matematica di quanto esposto implica calcoli particolari ed una conoscenza approfondita di tale tecnologia. Per questo motivo direi di non dilungarsi oltre, accettando quando esposto come informazione aggiuntiva ed eventualmente approfondile attraverso ricerche in internet.

15) **Link irrealizzabile causa interferenze CB:** saltuariamente si presenta l'inspiegabile problema di link irrealizzabile, malgrado le condizioni siano estremamente favorevoli. Questa problematica appare più evidente quando nelle vicinanze è presente un'antenna CB (Citizen Band). E' stato dimostrato che, sebbene la banda dei 27 MHz sia notevolmente distante dai 2,4 Ghz utilizzati dal Wi-Fi, gli apparati utilizzati hanno la pessima “abitudine” di emettere spurie ed armoniche di ogni genere, andando ad “oscurare” o “disturbare” altri apparati. Questo difetto è particolarmente accentuato quando vengono impiegati amplificatori lineari per i CB. Se si rientra in questo caso, per sopperire parzialmente ai problemi, occorre innanzitutto evitare di posizionare l'AP sullo stesso palo dell'antenna del CB, evitando oltretutto che allo stesso vengano accoppiati amplificatori lineari.

16)

# Glossario

- **10Base2 (Thin Ethernet)**: uno standard per il cablaggio di computer in rete, con velocità di trasferimento di 10Mbps. Utilizza cavi coassiali con impedenza di 50 Ohm, esteticamente simili a quelli della televisione, come l' RG58. La connessione alla scheda di rete avviene attraverso deviatori a "T" e la terminazione (o chiusura) degli estremi avviene attraverso resistenze da 50 Ohm. La lunghezza del cavo dev'essere compresa tra 0,5 e 185 metri. Questo tecnica di cablaggio è ormai considerata obsoleta.
- **10Base5 (thick Ethernet)**: come la 10Base2, ma utilizza un cavo semirigido a doppia schermatura, sempre terminato agli estremi. I computer sono collegati alla rete tramite trasmettitore/ricevitore con interfaccia a 15 poli. Il trasmettitore/ricevitore è a sua volta collegato al cavo di rete mediante connettori speciali. La lunghezza massima ammessa è di 500 metri. Come il 10Base2, anche questa tecnica di cablaggio è considerata obsoleta.
- **10BaseT**: standard moderno per i cablaggi delle reti di computer, dove si utilizzano coppie di conduttori intrecciati (twisted pair) e connettori Western RJ45. Velocità di trasferimento dei dati di 10Mbps e lunghezza massima del cavo di rete massimo 100 metri.
- **100BaseT**: caratteristiche simili a 10BaseT ma quando vengono impiegati schede, distributori e cavi adatti, si raggiunge una velocità di 100Mbps.
- **Access point + bridge**: particolare modalità di funzionamento di un access point che ingloba sia le funzionalità di access point classico sia quelle di bridge wireless.
- **Access point (classico)**: questa configurazione consente all'access point di funzionare solo ed esclusivamente come punto d'accesso per i soli client.
- **Accesso remoto**: funzione che serve per collegare un computer ad un'altro. L'accesso remoto viene di regola utilizzato anche per la connessione di un computer a internet.
- **Anello (Token Ring)**: particolare tipologia di rete che prevede la possibilità che ogni apparato connesso possa ciclicamente avere il diritto di utilizzare la rete per inviare dati ad un altro dispositivo connesso alla stessa rete.
- **Attenuazione**: in radiotecnica, l'attenuazione è quella caratteristica che determina la perdita di segnale, tipica dei cavi RF. L'unità di misura è sempre in dB negativi.
- **BIOS**: acronimo di Basic Input Output System, è il primo codice che viene eseguito da un computer dopo l'accensione. Ha principalmente tre funzioni:
  Eseguire una serie di test diagnostici per controllare lo stato di funzionamento dell'hardware e segnalare eventuali guasti rilevati tramite un codice sonoro (beep code); localizzare il sistema operativo e caricarlo nella RAM; fornire una interfaccia software per l'accesso alle periferiche e all'hardware del PC. Nei primi PC il BIOS supportava tutte le periferiche e il DOS faceva completo affidamento su di esso per le operazioni a basso livello, ma con l'evoluzione tecnologica, le capacità offerte dalle routine di gestione del BIOS (all'epoca non aggiornabili, perché scritte in ROM) divennero rapidamente insufficienti. I moderni sistemi operativi non usano più il BIOS per le loro operazioni di I/O ma accedono direttamente all'hardware. Il BIOS è scritto di solito nel linguaggio assembler nativo della famiglia di processori utilizzata. Oggigiorno il BIOS è scritto su memorie EEPROM riscrivibili, quindi può essere modificato e aggiornato: generalmente i costruttori mettono a disposizione nuove versioni di BIOS, correggendone difetti oppure per aggiungere supporto a periferiche hardware non previste inizialmente. Non è consigliabile aggiornare il BIOS di un PC senza un motivo ben preciso, poiché l'operazione di aggiornamento, se non va a buon fine, può rendere il PC inutilizzabile. Data l'alta difficoltà di scrittura del codice, si sta migrando dal BIOS classico ad EFI.
- **Bluetooth**: sistema di trasmissione wireless su aree molto limitate, tipicamente non oltre i 10 metri per la classe 2. E' molto utilizzato per la connessione tra telefoni cellulari e altri dispositivi come auricolari, palmari, navigatori GPS, notebook, ecc..
- **Bridge Point to Multipoint (multipunto)**: particolare configurazione di un access point che consente la contemporanea connessione tra più access point, permettendo l'unione di più LAN. Non è permesso ai comuni appartati wireless (client) la connessione.
- **Bridge Point to Point**: Particolare configurazione di un access point che permette di

connettere due access point, unendo di conseguenza due reti LAN. Come per la precedente, non sono ammesse le connessioni dei comuni apparati wireless (client).

- **Browser Web**: applicazione specifica che permette la navigazione e la visualizzazione delle pagine internet.
- **Bruteforcing**: attacco tipico a "forza bruta", che usa programmi studiati per violare l'accesso ai sistemi informatici, sfruttando dizionari che raccolgono tutte le password e gli ID "standard" usati dai produttori di hardware per configurare i dispositivi.
- **BSSID**: Basic Service Set Identifier, praticamente lo SSID in una rete "Ad-hoc".
- **Buffer Overflow**: è una vulnerabilità di sicurezza che può affliggere un programma software. Consiste nel fatto che tale programma non controlla in anticipo la lunghezza dei dati in arrivo, ma si limita a scrivere il loro valore in un buffer di lunghezza prestabilita, confidando che l'utente non immetta più dati di quanti esso ne possa contenere: questo può accadere se il programma è stato scritto usando funzioni di libreria di input/output che non fanno controlli sulle dimensioni dei dati trasferiti. Quando per errore o per malizia vengono inviati più dati della capienza del buffer che deve contenerli, i dati extra vanno a sovrascrivere le variabili interne del programma; come conseguenza, a seconda di cosa è stato sovrascritto e con quali valori, il programma può dare risultati errati o imprevedibili, bloccarsi, o (se è un driver di sistema o lo stesso sistema operativo) bloccare il computer. Conoscendo molto bene il programma in questione, il sistema operativo e il tipo di computer su cui gira, si può confezionare una serie di dati malevoli, che inviata per provocare un buffer overflow, consente ad un malintenzionato di prendere il controllo del programma e, a volte, dell'intero computer. Questo tipo di debolezza dei programmi è noto da molto tempo, ma solo di recente la sua conoscenza si è diffusa tanto da permettere anche a dei cracker dilettanti di sfruttarla per bloccare o prendere il controllo di altri computer collegati in rete. Non tutti i programmi sono vulnerabili a questo tipo di inconveniente: perché un dato programma sia a rischio è necessario:
  - che il programma preveda l'input di dati di lunghezza variabile e non nota a priori;
  - che li immagazzini entro buffer allocati nel suo spazio di memoria dati vicini ad altre strutture dati vitali per il programma stesso;
  - che il programmatore non abbia implementato alcun mezzo di controllo della correttezza dell'input in corso.
- **Bug**: il termine, dall'inglese "insetto", identifica un errore nella scrittura di un software e che causa un suo funzionamento errato o comunque diverso da quello che l'autore ha previsto ed in alcuni casi anche il suo blocco totale; meno comunemente, il termine può indicare un difetto di progettazione in un componente hardware che ne causa un comportamento imprevisto o comunque diverso da quello specificato dal produttore. Se presenti in un programma, possono essere talvolta particolarmente gravi a tal punto da rendere vulnerabile ad attacchi informatici anche il computer che ospita il software.
- **Bus**: modello di rete locale basato sulla presenza di un unico cavo che collega in parallelo tutti gli apparati.
- **Cavo coassiale**: è un conduttore con anima centrale, che porta il segnale, e schermatura esterna. Le sue caratteristiche sono l'impedenza e la perdita in dB per metro di lunghezza.
- **Cavo incrociato**: cavo twisted pair nel quale le coppie di doppini utilizzati per la trasmissione dei segnali di rete sono invertite in una delle due estremità. Permette il collegamento diretto di due computer senza perciò far uso di HUB o Switch. Sono utilizzati anche per la connessione in cascata di HUB o Switch privi di una porta specifica per l'interconnessione.
- **Client**: termine generico con il quale vengono indicati i computer o dispositivi connessi ad una rete. Altre volte definisce l'utente di una particolare applicazione che gira su un server.
- **CSMA**: acronimo di Carrier Sensing Multiple Access cioè il sistema di accesso alla trasmissione concorrenziale che permette il controllo preventivo delle eventuali trasmissioni già in corso. E' stato rivisitato e migliorato, correggendone i difetti.

- **CSMA/CA**: evoluzione di CSMA dove è stato inserito il Collision Avoidance. Questo sistema di accesso è utilizzato solo in ambito wireless, basandosi sul rilevamento della portante, evita che due o più client tentino di inviare dati contemporaneamente.
- **CSMA/CD**: evoluzione di CSMA dove è stato inserito il Collision Detection. Questo sistema è simile al CSMA/CA ma viene utilizzato in ambito wired.
- **DHCP**: acronimo di Dynamic Host Configuration Protocol che consente tra le altre cose di assegnare in modo dinamico ed automatico l'indirizzo IP ad un client di rete. Consente anche la gestione delle informazioni relative ai gateway, subnet mask e DNS.
- **Dial-UP**: con questo termine viene indicata la connessione tra due o più computer mediante l'uso di un modem analogico, con delle normali linee telefoniche.
- **DNS**: acronimo di Dynamic Name System, il servizio di directory alla quale è demandato il compito di tradurre in formato numerico IP il nome "semplice" o logico di un dominio internet, ma può essere altresì implementato anche in regime locale per la risoluzione dei nomi dei client di un a LAN.
- **ESSID**: Extended Service Set Identifier, praticamente è lo SSID in una WLAN in modalità "infrastruttura".
- **EDGE**: acronimo di Enhanced Data rates for GSM Evolution, è la versione più veloce dello standard GPRS per il trasferimento dati sulla rete cellulare GSM. Talvolta è definita come 2.75G
- **EFI**: acronimo di Extensible Firmware Interface, rappresenta l'evoluzione del BIOS e faciliterà ai produttori l'integrazione nel firmware del computer di applicazioni e nuove funzionalità, fra cui tool per la diagnostica e il ripristino dei dati, servizi di crittografia dei dati, estensioni per la gestione dei consumi e dotati di alcune utility di rete ed eventualmente, anche di un browser web. Altra miglioria promessa da EFI è la capacità di ridurre anche drasticamente i tempi di caricamento del sistema operativo e quello di supportare, similmente a quanto succede con i computer palmari, forme di avvio istantaneo. L'EFI ha anche il compito di dotare il firmware del PC di un'interfaccia grafica più amichevole, facile da usare e in grado di supportare le risoluzioni video permesse dalle moderne schede grafiche. In un certo senso, EFI si può considerare un piccolo sistema operativo dedicato a presiedere tutte quelle operazioni che intercorrono fra l'accensione fisica della macchina e l'avvio del sistema operativo vero e proprio, superando però tutte le problematiche emerse negli anni con gli attuali BIOS. Come tale infatti, sarà in grado di far girare applicazioni di alto livello scritte attraverso tool di programmazione standard. Tutto questo verrà reso possibile dal fatto che le interfacce di EFI saranno totalmente scritte in linguaggio C++, mettendo così definitivamente al bando l'ostico codice assembler degli attuali BIOS.
- **Ethernet**: protocollo di rete che consente la trasmissione dei dati tra più computer. La lavorazione a questo standard iniziò nel 1972 ad opera di Xerox ed approdò nel 1980 alla prima versione utilizzabile. Nel 1983 uscì lo standard 802.3 con una velocità di 10 Mbit/s su cavo coassiale. Nel 1985 iniziò il perfezionamento con l'aggiunta di versioni capaci di funzionare su cavi di tipo diverso con velocità di 1 Mbit/s, poi 10 Mbit/s, 100 Mbit/s (802.3u fast ethernet) e 1Gbit/s. Ethernet è il tipo di rete locale più diffuso al mondo.
- **FHSS**: acronimo di Frequency Hopping Spread Spectrum ed è la tecnica di trasmissione wireless attraverso il cambio rapido e pseudocasuale del canale di trasmissione. Consente di migliorare la larghezza di banda, riducendo i disturbi e garantendo un buon livello di sicurezza.
- **File Inclusion**: tipo di attacco che si manifesta quando i parametri passati ad uno script web-based vulnerabile non sono opportunamente verificati prima di essere usati. Ne esistono di due categorie: Local File Inclusion e Remote File Inclusion. Nel primo caso, chi attacca può usare solo file residenti nel sistema come parametri da inserire in uno script vulnerabile; nel secondo invece possono essere usati file residenti in altri web server.
- **Firewall**: può essere di tipo software o hardware e serve per proteggere un computer o una

rete da attacchi provenienti dall'esterno o da internet. Nel tipo **Stateful Inspection**, non si blocca solo l'accesso a porte specifiche ma, si controlla l'intero traffico della rete, verificando attività non consentite.

- **Firmware:** software che risiede in una memoria interna non volatile in ogni dispositivo avanzato. Frequentemente viene data la possibilità di aggiornarlo, aggiungendo funzionalità e correggendone i bug.
- **Gateway:** viene così definito un dispositivo attraverso il quale è possibile instradare dati di una rete locale verso il mondo esterno.
- **Geek:** è un utilizzatore sfrenato di computer; colui che va fiero ed entusista della tecnologia o di dispositivi tecnologici, talvolta a livello complulsivo ed eccessivo.
- **Generazioni della telefonia mobile**: dalla sua comparsa, il telefono cellulare ha usato diversi sistemi di funzionamento principali (ed alcuni "intermedi"), chiamati generazioni, basati su differenti tecnologie e standard di comunicazione e cioè:
    - **0G**: Radiotelefoni usati prima dell'avvento dei telefoni cellulari.
    - **1G** (I° generazione): standard TACS (Total Access Communication System), ETACS (Extended TACS, TACS Esteso con l'aggiunta di nuove frequenze), AMPS (Advanced Mobile Phone System) e NMT (Nordic Mobile Telephone system). Utilizzato dai telefoni cellulari analogici.
    - **2G** (II° generazione): standard GSM (Global System for Mobile Communications), CDMA IS-95 e D-AMPS IS-136. Utilizzato dai primi cellulari digitali.
    - **2.5G**: standard GPRS (General Packet Radio System), utilizzato dai cellulari digitali ad alta velocità di trasmissione dati.
    - **2.75G**: standard EDGE (Enhanced Data rates for GSM Evolution), è la versione più veloce dello standard GPRS per il trasferimento dati sulla rete cellulare GSM.
    - **3G**: **(**III° generazione): standard UMTS (Universal Mobile Telephone System), Wideband CDMA (W-CDMA), CDMA 2000. Usato dai videocellulari o cellulari 3GPP (3rd Generation Partnership Project).
    - **4G**: **(**IV° generazione): standard VSF-Spread OFDM (Variable-Spreading-Factor Spread Orthogonal Frequency Division Multiplexing).
- **GPRS**: è il precursore dei sistemi 3G e l'oramai diffusissimo sistema di telefonia mobile GSM, spesso denominato sistema 2G (cioè di seconda generazione). Sistema evolutosi dal 2G, è conosciuto anche come 2.5G. Il GPRS supporta un transfer-rate nettamente più alto del GSM (fino ad un massimo di 140,8 kbit/s), e può essere talvolta utilizzato insieme al GSM.
- **GPS**: acronimo di Global Positioning System, un sistema di localizzazione geografica satellitare basato sul tracciamento di satelliti geostazionari.
- **GNU**: è l'acronimo di GNU is Not Unix, ovvero "GNU non è Unix". Il Progetto GNU, nasce nel 1983 da Richard Stallman e si basa su una gestione particolare dei diritti d'autore del software, secondo la definizione di software libero, in contrapposizione al software proprietario. Lo scopo ultimo del Progetto GNU è la creazione di un sistema operativo completamente libero; per arrivare a questo risultato, all'interno del progetto vengono creati programmi per coprire ogni necessità informatica: compilatori, lettori multimediali, programmi di crittografia... Nel 2005 il sistema operativo non è ancora stato sviluppato completamente (il kernel HURD non è ancora pronto per poter essere utilizzato), ma grazie al lavoro di Linus Torvalds è possibile usare il sistema GNU con il kernel Linux, ovvero il sistema GNU/Linux. Fulcro di tutta l'attività del Progetto GNU è la licenza chiamata GNU GPL, ovvero GNU General Public License, che sancisce e protegge le libertà fondamentali che, secondo Stallman, permettono l'uso e lo sviluppo collettivo e naturale del software.
- **Hacker, Cracker e Lamer**: c'è molta confusione nel riconoscerli e spesso si pensa siano sinonimi ma, in realtà, sono tre figure diverse.
    - L'**Hacker** è colui che studia i sistemi informatici e le reti alla ricerca di caratteristiche e di vulnerabilità. La conoscenza è il suo motto e possiede una

propria etica: non approfitta delle situazioni che trova o che crea, non trae guadagno economico e non causa mai danni ai sistemi in cui scopre debolezze anzi, la sua conoscenza è resa pubblica e sprona sé stesso e gli altri al miglioramento.
    - Il **Cracker** è colui che viola i sistemi con l'obbiettivo di creare danni. Molto spesso il suo comportamento è motivato dal vantaggio economico, sfrutta i sistemi violati per sferrare altri attacchi o ne sfrutta l'ampiezza di banda come un parassita.
    - Il **Lamer** è un aspirante Cracker con rudimentali conoscenze informatiche che, copiando ed utilizzando tecniche di altri, crea danni con l'intento di danneggiare o distruggere informazioni. Molto spesso usa i computer violati per sferrare attacchi a siti internet.
- **Hot Spot**: con questo termine si indica un'area pubblica all'interno della quale è possibile navigare in internet mediante una connessione wireless Wi-Fi.
- **HTML**: è l'acronimo di Hyper Text Mark-Up Language, un linguaggio usato per descrivere i documenti ipertestuali disponibili nel Web. Non è un linguaggio di programmazione ma un linguaggio di markup, ovvero descrive il contenuto, testuale e non, di una pagina web. I file con estensione .html o .htm, è comune dei documenti HTML.
- **HTTP**: è l'acronimo di Hyper Text Transfer Protocol (protocollo di trasferimento di un ipertesto), usato come principale sistema per la trasmissione di informazioni sul web.
- **HUB**: è in pratica una sorta di distributore in una rete locale. I pacchetti di dati vengono vengono semplicemente inviati a tutte le porte dei computer collegati, ma solo il destinatario li accetterà. Ne consegue un traffico di rete inutilmente elevato, percui anche nelle piccole reti viene spesso sostituito dagli Switch.
- **Hyper LAN**: è il nome di una tecnologia sviluppata in Europa e recentemente liberalizzata per trasmissioni wireless LAN a 54Mbps sui 5GHz.
- **IP (indirizzo)**: acronimo di Internet Protocol, standard utilizzato per l'assegnazione di indirizzi numerici univoci a tutti i computer ed altri dispositivi connessi ad una rete.
- **Ipx/Spx**: acronimo di Internetwork Packet Exchange/Sequenced Packet Exchange. Protocollo di rete creato da Novell per le reti che utilizzano server NetWare. Oggi è sempre più spesso sostituito dal TCP/IP.
- **JTAG**: acronimo di **J**oint **T**est **A**ction **G**roup, è un protocollo standard per i test funzionali di apparati, sempre più complessi e difficili da controllare, rendendo impossibile il tradizionale metodo manuale.
- **Kbps**: indica i kilo bit per secondo, la velocità con cui vengono trasferiti i dati in una rete. 1Kbps è pari a circa 0,1Kbyte per secondo.
- **Kernel**: è il nucleo di un sistema operativo, un software che ha il compito di fornire ai processi in esecuzione sul computer un accesso sicuro e controllato dell'hardware. Siccome possono essere eseguiti simultaneamente più programmi, il kernel ha anche la responsabilità di assegnare una porzione di tempo-macchina e di accesso all'hardware a ciascun programma. L'accesso diretto all'hardware può essere anche molto complesso, quindi i kernel usualmente implementano uno o più tipi di astrazione dell'hardware. Queste astrazioni servono a "nascondere" la complessità e a fornire un'interfaccia pulita ed uniforme all'hardware sottostante, in modo da semplificare il lavoro degli sviluppatori. I kernel si possono classificare, in base al grado di questa astrazione dell'hardware, in quattro categorie:
    - ***Kernel monolitici***, che implementano direttamente una completa astrazione dell'hardware sottostante. Fanno ad esempio parte di questa categoria i kernel derivati da Unix e Linux;
    - ***Microkernel***, che forniscono un insieme ristretto e semplice di astrazione dell'hardware e usano software, chiamati device driver o server, per fornire maggiori funzionalità. Fanno ad esempio parte di questa categoria i kernel di

Minix, AIX, BeOS, RadiOS, MorphOS;
    - ***Kernel ibridi*** (o *microkernel modificati*), che si differenziano dai microkernel puri per l'implementazione di alcune funzioni aggiuntive al fine di incrementare le prestazioni. Fanno ad esempio parte di questa categoria i kernel di Mac OSX, DragonFly BSD, Windows NT e suoi derivati (Win 2000, XP, Vista), ReactOS, MorphOS;
    - ***Esokernel***, che rimuovono tutte le limitazioni legate all'astrazione dell'hardware e si limitano a garantire l'accesso concorrente allo stesso, permettendo alle singole applicazioni di implementare autonomamente le tradizionali astrazioni del sistema operativo per mezzo di speciali librerie. Al momento gli esokernel sono più che altro dei progetti di ricerca e non sono usati in sistemi operativi commerciali od open.
- **LAN**: acronimo di Local Area Network. Con questo termine si identificano le reti di comunicazione tra computer di dimensioni ridotte.
- **Linux**: è il nome del kernel originariamente sviluppato da Linus Torvads. Il nome Linux a dispetto dell'assonanza tra il nome dell'ideatore e quello del sistema (Linus - Linux) è da attribuire a Ari Lemke, l'amministratore che rese disponibile Linux su internet via FTP. In particolare Linux era il nome della directory dove i file del nuovo sistema operativo erano disponibili. Con il termine "Linux" spesso si indica erroneamente il sistema operativo libero basato sul kernel Linux e sul sistema GNU, che secondo una parte della comunità informatica dovrebbe per questo chiamarsi “GNU/Linux”.
- **MAC (indirizzo)**: indirizzo numerico univoco proprio di ogni scheda di rete. E' composto da sei coppie di valori esadecimali e viene attribuito dal produttore ed assolutamente immodificabile, se non temporaneamente via software e comunque solamente in alcuni casi. Il Media Access Control è indipendente dall'indirizzo IP di qualsiasi dispositivo di rete (wired o wireless) e dal nome di rete poiché “lavora” ad uno strato inferiore, quello hardware. Come già detto prima, esso si compone di 48 bit (6 byte) di cui i primi 24 (3 byte) identificano univocamente il produttore e vengono anche detti in gergo OUI (Organizationally Unique Identifier), assegnati ai singoli produttori dal IEEE; i restanti 3 byte sono liberamente assegnabili dal produttore che, solitamente, li usa per il seriale, potendo contare sulla disponibilità di oltre 16 milioni di numeri univoci. Un esempio di indirizzo MAC potrebbe essere 00-11-95-08-c8-de, dove le prime tre coppie (00-11-95) indicano il produttore D-Link, mentre le altre tre coppie (08-c8-de) indicano il numero seriale.
- **Mbps**: acronimo di Mega Bit Per Secondo, unità di misura utilizzata per indicare la quantità di dati che transita in una rete nell'unità di tempo. 1Mb = 1024 Kb ovvero 1048576 bit.
- **MIMO**: acronimo di Multiple Input Multiple Output, tecnologia alla base del protocollo 802.11n che prevede l'impiego di più antenne al fine di trasmettere più volte il segnale in modo indipendente, permettendo una larghezza di banda e copertura maggiore.
- **NAT**: acronimo di Network Address Translation. E' la tecnologia che permette di modificare in modo fittizio l'indirizzo IP di un computer in un processo di trasmissione dati al fine di mascherarne la vera origine o il destinatario della trasmissione.
- **NetBios**: speciale interfaccia di programma che mette a disposizione alcuni comandi di rete. Veniva usato in passato per le comunicazioni di applicazioni o giochi, per essere indipendenti dai protocolli di rete.
- **OFDM**: acronimo di Orthogonal Frequency Division Multiplexing, una tecnica utilizzata nelle telecomunicazioni, che consente d'avere una maggiore banda per la trasmissione dati rispetto a quella usata tradizionalmente.
- **Open Source**: detto anche “a sorgente aperto”, identifica quelle applicazioni o software in generale realizzato secondo standard aperti, dove il codice sorgente è liberamente visionabile. Il fatto che un software sia disponibile come Open Source, non significa che sia gratuito, come si è portati a pensare. Si contrappone al “closed source”, dove il software è

proprietario ed il sorgente non è visionabile.

- **P2P**: detto anche Peer To Peer o Punto a Punto, è il sistema per lo scambio di dati diretto tra due PC in rete aventi più o meno gli stessi diritti di accesso, che condividono risorse.
- **PCB**: acronimo di Printed Circuit Booard, ovvero la scheda a circuiti stampati, è in pratica il supporto contenente tutte le connessioni per componenti elettronici. Può essere a singola/doppia faccia o a multi strato.
- **PCI, PCMCIA, USB**: sono interfacce d'interconnessione per dispositivi aggiuntivi interni (PCI ), per i portatili (PCMCIA) e periferiche esterne con bus seriale universale (USB).
- **Plug-in**: piccola applicazione accessoria ad un programma che permette l'aggiunta di comandi e di funzionalità.
- **PPP**: acronimo di Point-to-Point Protocol, protocollo di comunicazione che consente la comunicazione diretta tra due dispositivi all'interno della stessa rete.
- **PPPoA**: acronimo di PPP over Asynchronous Transfer Mode (ATM), un protocollo di comunicazione appositamente studiato per consentire ad un client remoto la connessione ad internet su ADSL.
- **PPPoE**: acronimo di PPP over Ethernet, un protocollo di comunicazione utilizzato per stabilire una connessione di tipo punto-punto tra computer connessi ad internet. Utilizzato in numerosi collegamento ADSL.
- **POST**: acronimo di Power On Self Test. E' un test, eseguito all'accensione in un computer, di verifica automatica di tutte le periferiche installate.
- **Privilege Escalation**: una hacker, o peggio ancora un cracker, per compiere attività illecite nel sistema violato, deve possedere privilegi da amministratore. Per ottenerli, solitamente, chi attacca sfrutta i bachi delle applicazioni residenti sulla macchina attaccata, tramite la tecnica di Buffer Overflow.
- **Protocollo**: nell'informatica descrive in generale una raccolta di regole per i formati dei dati ed il loro trasferimento. In termini semplici si può descrivere come una sorta di linguaggio comune tra i computer collegati.
- **PSK**: acronimo di Pre Shared Key, è la chiave di codifica nota e condivisa tra i client wireless. E' utilizzata nei protocolli WEP e WPA.
- **QoS**: acronimo di Quality Of Service ed è utilizzato per indicare i parametri qualitativi positivi e negativi di un servizio.
- **RAS**: acronimo di Remote Access Server. Computer al quale ci si può collegare a distanza, tramite linea telefonica od altro sistema. Questa funzione è presente, con diverse possibilità di configurazione ed utilizzo, in tutte le versioni di Windows a partire dalla 3.11.
- **Rete**: termine con il quale si indica una qualsiasi rete di computer o di altri dispositivi connessi tra loro.
- **Ripetitore (o repeater)**: configurazione particolare di un access point che, permette la ripetizione del segnale wireless di un access point principale, estendendone la copertura e diventando completamente trasparente nella rete.
- **Router**: Un router è un dispositivo che regola il collegamento di due o più LAN per costituire una WAN. Si occupa della conversione dei formati dei dati, protocolli e dei corretti indirizzamenti. Spesso vengono integrati con dei firewall che proteggono dagli accessi indesiderati o non autorizzati a una LAN.
- **RPM**: acronimo di RedHat Package Manager, il sistema di pacchettizzazione e gestione delle dipendenze dei pacchetti sviluppato da Red Hat.
- **Server**: qualsiasi computer che archivia informazioni e gestisca risorse che devono essere usate dagli altri computer di una LAN. Un server si può ad esempio usare per condividere una stampante tra decine di computer, ospitare siti web, ecc...
- **SIM**: acronimo di Subscriber Identity Module è il modulo d'identità del sottoscrittore di un contratto di fonia/dati nelle comunicazioni cellulari. Si presenta con la forma di una piccola scheda elettronica.
- **SMD**: in elettronica è l'acronimo Surface Mounted Device, quei componenti elettronici

miniaturizzati a montaggio superficiale.

- **Sniffing**: tecnica che consente d'individuare ed intercettare i dati veicolati in una rete.
- **SSID Broadcast**: tecnica che consente la visualizzazione dello SSID di una rete wireless ad opera di tutti i client presenti entro il raggio di copertura di una LAN wireless.
- **SSID**: acronimo di Service Set Identifier e consiste nell'identificativo univoco di una LAN wireless.
- **Stella**: particolare configurazione di una rete LAN, dove il computer centrale, usato come server, si occupa di ricevere e smistare tutte le comunicazioni tra i vari computer client.
- **STP**: acronimo di Shielded Twisted Pair. Trattasi di particolari cavi dove sono presenti 8 conduttori ritorti a coppie. Ogni coppia ritorta è schermata dalle altre e ritorta sulle altre. Una ulteriore schermatura protegge le quattro coppie da possibili interferenze ambientali esterne.
- **Switch**: particolare dispositivo di rete che permette l'accentramento e lo smistamento dei dati provenienti da ogni computer o altro dispositivo. E' chiamato volgarmente HUB intelligente poiché la banda a disposizione su ogni ramo è sempre quella massima permessa e ogni dato viene veicolato verso il destinatario, senza essere ripetuto su tutti i rami.
- **TCP**: acronimo di Trasmission Control Protocol, cioè un protocollo che garantisce il trasporto corretto dei dati all'interno di una rete.
- **Throughput**: termine con il quale si definisce la capacità effettiva, cioè le prestazioni, di comunicazione di una rete. Un esempio potrebbe essere lo standard 802.11b che a fronte di una capacità nominale di 11Mbps, presenta un throughput reale di 5-6 Mbps.
- **Token passing**: architettura di rete con accesso deterministico; prevede che per poter iniziare una trasmissione dati, il computer debba essere in possesso di un segnale particolare che viene passato circolarmente da una stazione all'altra. In questo modo, non si può mai verificare che due stazioni tentino di effettuare contemporaneamente una trasmissione (come invece succede su rete Ethernet).
- **Topologia**: nel senso originario del termine, è la scienza per l'ordinamento di oggetti in un ambiente. Nell'ambito delle reti, s'intende il tipo di cablaggi dei singoli computer, per esempio a forma di anello o di stella attorno a un computer centrale, oppure anche a forma di bus.
- **Tunnel VPN**: con la Virtual Private Network si crea una rete virtuale sicura in una rete di natura insicura. Esistono molti protocolli VPN ma il più noto è Ipsec.
- **Twisted Pair**: termine col quale vengono nominati tutti i cavi che presentano al proprio interno delle coppie ritorte intrecciate su sé stesse. Ciò permette di ridurre le interferenze ambientali.
- **UDP**: acronimo di Universal Datagram Protocol ed è un protocollo di rete utilizzato per la trasmissione di dati a pacchetto. Molto simile al TCP, ma si differenzia per la non ritrasmissione dei dati eventualmente persi né la riorganizzazione.
- **UMTS**: acronimo di Universal Mobile Telecommunications System è la tecnologia alla base della telefonia mobile di terza generazione, detta anche 3G e successore del GSM. Tale tecnologia impiega lo standard base WCDMA come interfaccia di trasmissione ed è compatibile con lo standard 3GPP e rappresenta la risposta europea al sistema ITU di telefonia cellulare 3G. Il sistema UMTS supporta un transfer-rate massimo di 1920 Kbps. Le applicazioni tipiche attualmente implementate dalle reti UMTS in Italia, sono: voce, videoconferenza e trasmissione dati a pacchetto. Ad ognuno di questi tre servizi è assegnato uno specifico transfer-rate, per la voce 12,2 Kbps, 64 Kbps per la videoconferenza e 384 Kbps per trasmissioni di tipo dati. Tuttavia da misurazioni effettuate sul campo ed in mobilità su reti scariche si sono raggiunti 300 Kbps. In ogni caso questo valore è decisamente superiore ai 14,4 Kbps di un singolo canale GSM con correzione di errore ed anche al transfer-rate di un sistema a canali multipli in HSCSD. Le attuali reti UMTS potranno essere potenziate mediante il sistema di accesso denominato HSDPA (*High Speed Downlink Packet Access*), con una velocità massima teorica di download dati di 10 Mbit/s.

- **URL**: acronimo di Uniform Resource Locator, è uno dei vari modi con cui viene indicato un indirizzo di una pagina web.
- **UTP**: acronimo di Unshielded Twisted Pair e trattasi di particolari cavi dove sono presenti 8 conduttori ritorti a coppie. Ogni coppia ritorta è ritorta sulle altre. Non è presente una ulteriore schermatura che protegge le quattro coppie da possibili interferenze ambientali esterne.
- **UWB**: acronimo di Ultra Wide Band, si posiziona fra Bluetooth, che rimarrà la tecnologia preferita per i dispositivi portatili con poca autonomia, ed il Wi-Fi che, sebbene meno veloce di UWB, ha un raggio d'azione assai superiore. Opera su uno spettro di frequenza compreso fra 3,1 e 10,6 GHz ed è in grado di supportare una velocità massima di trasferimento dati di 480 Mbit al secondo, dunque simile a quella di USB 2.0 e sono proprio queste caratteristiche ad indicare come uno dei primi campi di applicazione di UWB sia destinato ad essere quello dei **dispositivi USB senza fili**, per i quali è stata creata la specifica Wireless USB. Quest'ultima promette di raggiungere velocità di 480 Mbit/s entro distanze di 3 metri e di 110 Mbps fino a 10 metri. UWB è stato recentemente legalizzato nel Regno Unito e presto dovrebbero esserlo in tutta Europa.
- **VoIP**: acronimo di Voice Over IP ed indica la trasmissione di comunicazioni vocali attraverso un rete IP internet. Comunemente viene usato come sinonimo della telefonia via internet.
- **VPN**: acronimo di Virtual Private Network e s'intende di regola l'utilizzo di internet come "trasportatore" di dati tra due pc o tra due LAN. Tramite il cosiddetto tunneling protocol i dati destinati al "partner" vengono suddivisi e codificati in pacchetti TCP/IP. I due pc o LAN possono utilizzare anche un protocollo di rete diverso, come per esempio l'IPx, che viene incapsulato in un "guscio" TCP/IP.
- **WAN**: acronimo di Wide Area Network che sta ad indicare una rete di computer di dimensioni molto estese, come un paese.
- **Wardriving**: particolare attività che consiste nello spostarsi all'interno di aree urbane in macchina o a piedi (dove prende il nome di Warwalking), alla ricerca di reti wireless.
- **WDS**: acronimo di Wireless Distribution System, un sistema che abilita le interconnessioni tra access point permettendo in questo modo d'espandere la copertura della rete. La modalità WDS non è compatibile con apparati diversi e non è certificata dal Wi-Fi Alliance.
- **WEB**: il World Wide Web, detto comunemente Web, è una rete di risorse di informazioni basata sull'infrastruttura di internet e, per rendere queste risorse disponibili agli utenti, utilizza: un sistema di denominazione uniforme per localizzare le risorse sul Web (ergo, URL); dei Protocolli, per accedere alle risorse del Web (ergo HTTP); l'Ipertesto, per una facile navigazione tra le risorse (ergo, HTML).
- **WEP**: acronimo di Wired Equivalent Privacy. E' il primo protocollo di crittografia integrato in uno standard Wi-Fi.
- **Wi-Fi**: abbreviazione di Wireless Fidelity e vengono così indicate tutte quelle reti wireless basate sugli standard IEEE802.11x.
- **WINS**: acronimo di Windows Internet Naming Service, cioè il protocollo proprietario Microsoft che consente la risoluzione del nome logico di un computer nel suo equivalente indirizzo numerico IP.
- **Wired**: termine con il quale vengono definite tutte le reti di comunicazione basate su cavo.
- **Wireless**: contrariamente al Wired, vengono indicate tutte le reti di comunicazione dove non è richiesto un cavo di connessione.
- **W-Lan**: acronimo di Wireless Local Area Network che definisce una rete locale, o una porzione di essa, senza fili e basata sui protocolli Wi-Fi.
- **WPA – WPA 2**: acronimo di Wi-Fi Protected Access. Il WPA è l'evoluzione del WEP, un metodo di protezione integrato al fine di garantire la sicurezza di una W-Lan. A differenza del WEP, è considerato molto efficace. La sua ulteriore evoluzione prende il nome di WPA2.

Per alcuni termini, si sono date volutamente informazioni generiche poiché non necessarie per lo studio e lo sviluppo delle reti wireless. E' comunque possibile estendere la propria conoscenza attraverso la lettura di manuali ad essi correlati o tramite ricerche in internet.

# Note Finali

Sono doverose alcune note riguardanti l'utilizzo di questa guida che servono più che altro come disclaimer:

- L'autore non si assume nessun tipo di responsabilità legale e morale per eventuali danni diretti od indiretti derivanti dall'uso improprio delle nozioni e/o dei programmi contenuti e descritti in questa guida; siate sempre rispettosi della legge e delle norme in vigore!
- Il presente documento è ad uso di semplice scopo divulgativo-informativo;
- Il presente documento è frutto di sperimentazioni personali, integrate da approfondimenti letti e studiati nel corso degli anni su riviste specializzate e documentazioni amatoriali, rilasciate con licenza GPL e trovate in internet con l'ausilio di motori di ricerca;
- I marchi e i modelli citati sono di proprietà dei rispettivi proprietari e sono stati usati per scopo didattico e divulgativo;
- L'uso o il riutilizzo di questa guida è liberamente consentito per scopi didattici od informativi, previa citazione della fonte;
- Sono possibili errori e/o imprecisioni. Se ne trovate, segnalateli nell'apposito thread aperto sul forum di Nabuk.org (www.nabuk.org), nella sezione “Progetti in corso – Guida alle W-Lan”;
- Chi volesse integrare il documento può scrivere nell'apposito thread aperto sul forum di Nabuk.org nella sezione “Progetti in corso – Guida alle W-Lan”.
- Non finirò mai di ripetere d'usare una potenza di poco superiore allo stretto necessario, in modo di dare la possibilità anche al “vicino” di crearsi una propria rete wireless.
- Ove richiesto, ovvero per link che attraversano il suolo pubblico, si deve fare una richiesta al Ministero delle Comunicazioni. Siate rispettosi delle leggi.

# Bibliografia

| Titolo | Lingua | Autore/Indirizzo | Editore | Note |
|---|---|---|---|---|
| | | | | |
| Linux & C. | Ita | www.oltrelinux.com | Piscopo s.r.l. | Rivista mensile |
| Linux PRO | Ita | www.linuxpro.it | Future Media | Rivista mensile |
| GNU Linux Magazine | Ita | www.linux-magazine.it | Edizioni Master | Rivista mensile |
| Hackers magazine | Ita | vari | Sprea Editori | Rivista mensile; tutti i software indispensabili spiegati passo - passo |
| Hacker Journal | Ita | www.hackerjournal.it | Sprea Editori | Rivista quindicinale, tutta dedicata all'hacking |
| Linux server – per l'amministratore di rete | Ita | Silvio Umberto Zanzi | Apogeo | Guida completa |
| Linux Fedora – guida professionale | Ita | Vari | Apogeo | Guida esaustiva su Fedora Linux |
| Linux e le reti | Ita | Roberto Butti | J.Group | Linux Book N.1 |
| Usare Linux al 101% | Ita | Giorgio Zarrelli | J.Group | Linux Book N.3 |
| Tutto sul wireless | Ita | Leo Sorge | Apogeo | Standard e tecnologie varie |
| Usare Linux – guida avanzata | Ita | Brian Ward | Mondadori | Approfondimenti essenziali |
| L'arte dell'hacking | Ita | Jon Erickson | Apogeo | Idee, strumenti e tecniche degli hacker |
| Hacker 5.0 – guida completa | Ita | McClure, Scambray, Kurtz | Apogeo | Per utenti avanzati, non esiste di meglio |
| Webopedia | Ita | www.webopedia.com | --- | Dizionario free online |
| Wikipedia | Ita | www.wikipedia.it | --- | Enciclopedia free online |
| Appunti di informatica libera | Ita | a2.pluto.it | --- | Introduzione a GNU/Linux ed al software open source |
| Reti wireless domestiche | Ita | Marco Colombo | Hoepli | Costruire una rete wireless |
| Server Linux sicuri | Ita | Michael D. Bauer | Hops | Guida per costruire server sicuri con GNU/Linux |
| Open source & Linux | Ita | --- | IDG | Le guide di PC World |
| Tutto software gratis | Ita | Silvia Ponzio | Mondadori | Ottima descrizione di molti software gratuiti |
| Configurare e aggiornare il PC | Ita | Alessandro Valli | FAG | Elementi di base per aggiornare e configurare un computer |
| Chip – computer & communications | Ita | Vari | Vogel Burda Communications | Rivista mensile dedicata alle novità IT |
| PC World | Ita | Vari / www.pcworld.it | | Rivista mensile dedicata alle novità IT |
| Nuova Elettronica | Ita | www.nuovaelettronica.it | | La rivista dedicata con kit di montaggio |
| Fare elettronica | Ita | www.farelettronica.com | Inware | Elettronica applicata |

| | | | | |
|---|---|---|---|---|
| Ministero delle comunicazioni | Ita | www.comunicazioni.it | --- | Normative e leggi |
| Hardware Upgrade | Ita | www.hwupgrade.it | --- | Novità e recensioni HW |
| Nabuk | Ita | www.nabuk.org | --- | Sperimentazioni wireless |
| OpenWTR | UK | http://wiki.openwrt.org/TableOfHardware | --- | Qui si sta lavorando al porting di OpenWRT su diversi apparati |
| DD-WRT | UK | | --- | Alternativa a OpenWRT |
| Google | multi | www.google.com | --- | Motore di ricerca |
| D-LinkPedia | Ita | www.dlinkpedia.net | --- | Tutto sugli apparati D-Link |
| Fedora Core | Ita | fedora.redhat.com | --- | La distribuzione Fedora Linux |
| Ubuntu | Ita | www.ubuntu-it.org | --- | La distribuzione Ubuntu Linux per desktop / server |
| MCNLive Linux | UK | www.mcnlive.org | --- | La distribuzione GNU/Linux portatile, su chiavetta USB |
| Simple Machine Forum | UK | http://www.simplemachines.org/download/ | --- | Un'ottima piattaforma per forum |
| Alnath Web Space | Ita | http://alnath.supereva.it http://srvalnath.no-ip.org | --- | Antenne, firmware per apparati D-Link e Linksys (DD-WRT), test... |
| WiFi Radar | UK | http://wifi-radar.systemimager.org | --- | Sito di riferimento e sviluppo di WiFi-Radar |
| WPA Supplicant | UK | http://hostap.epitest.fi/wpa_supplicant | --- | Sito di riferimento e sviluppo di WPA Supplicant |
| Ndis Wrapper | UK | http://ndiswrapper.sourceforge.net | --- | Sito di riferimento e sviluppo di NdisWrapper |
| BlueZ | UK | http://www.bluez.org | --- | Sito di riferimento e sviluppo di BlueZ |
| GPRS easy connect | UK | http://easyconnect.linuxuser.hu | --- | Connessioni GPRS semplici e veloci |
| D-Link Mediterraneo | Ita | http://www.dlink.it | --- | Il sito italiano della D-Link |
| Linksys | multi | http://www.linksys.com | --- | Il sito della Linksys |
| Open Office | multi | http://it.openoffice.org | --- | La suite open-source per l'ufficio |
| Anti Digital Divide | Ita | http://www.antidigitaldivide.org | --- | Associazione per la banda larga per tutti |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |