Reti wireless: implementazione in sicurezza

- Termini e concetti.
- Principi di funzionamento.
- Struttura base della rete.
- Fattori ambientali e performance.
- Scelta delle apparecchiature.
- Configurazione delle apparecchiature.
- Problematiche sulla sicurezza.
- Sistemi di protezione.

Termini e concetti

Access point

Un Access Point è un dispositivo che permette all'utente mobile di collegarsi ad una rete wireless. L'access point, collegato fisicamente alla rete, riceve ed invia un segnale radio all'utente, permettendo così la connessione.

Client

Il Client è il dispositivo utilizzato dall'utente per connettersi ad una rete wireless. Può essere un computer, un palmare, un telefono voip o un apparecchio dedicato.

Termini e concetti

Ssid

L'Ssid (Service Set IDentifier) è il nome che viene stabilito come identificativo della rete. Esso è arbitrario, definibile dall'amministratore, e univoco all'interno della stessa rete.

Mac

L'indirizzo MAC (Media Access Control address) viene detto anche indirizzo fisico o indirizzo ethernet o indirizzo LAN, ed è un codice di 48 bit (6 byte) assegnato in modo univoco ad ogni scheda di rete ethernet prodotta al mondo.

Termini e concetti

Indirizzo ip

Un Indirizzo IP è un numero che identifica univocamente i dispositivi collegati con una rete informatica che utilizza lo standard IP (Internet Protocol). Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni,...) ha, quindi, il suo indirizzo.

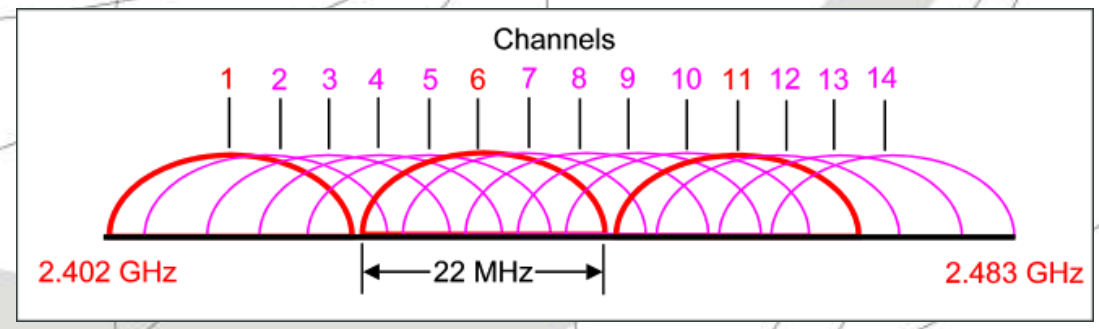
Canale

Lo spettro di frequenze utilizzate da un protocollo wireless viene a sua volta suddiviso in diversi canali, ognuno dei quali rappresenta un piccolo range di frequenze. Ad esempio, il protocollo 802.11b (e seguenti) prevede l'utilizzo di 14 canali da 2412 MHz a 2484 MHz.

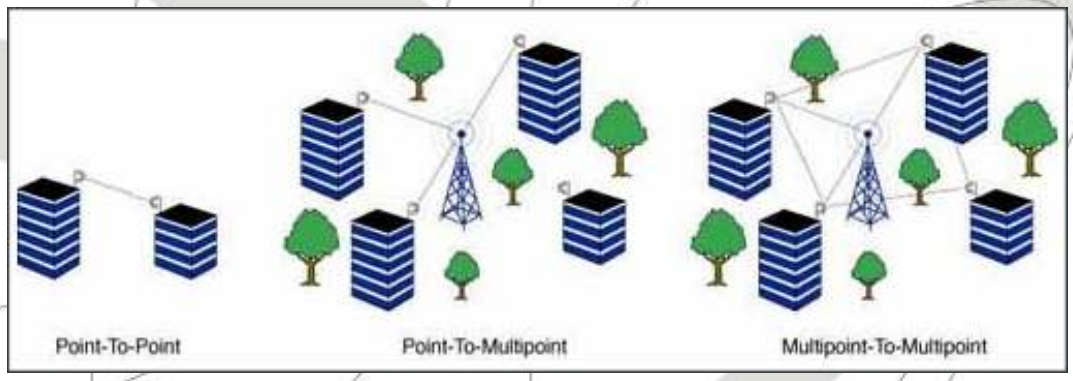
Principi di funzionamento

Canale e Ssid

Affinchè un client possa associarsi ad una rete wireless è sufficiente che entrambi utilizzino lo stesso canale e lo stesso ssid. Una volta associato, qualora sia presente un server DHCP, il client riceverà il suo indirizzo ip.
Se invece ci sono sistemi di sicurezza implementati nella rete (WEP, WPA, ...) il client dovrà conoscere anche le chiavi necessarie per autenticarsi sulla stessa.



Principi di funzionamento



Principi di funzionamento

Reti Mesh

Una rete mesh è un cluster di Wireless AP che formano un sistema reticolato. Questo cluster consente di estendere la copertura di un hotspot WLAN grazie a:

- Rilevamento e configurazione automatica di Wireless AP.
- Raccolta del traffico tramite hop multipli su link radio (bande non licenziate) fino al punto di connessione con la rete tradizionale (su cavo) a banda larga.
- Applicazione di funzioni evolute di sicurezza per il controllo e la protezione del traffico transitante sui collegamenti wireless (link radio).
- Applicazione di funzioni evolute di sicurezza per l'autenticazione e l'autorizzazione degli accessi alla rete mobile.

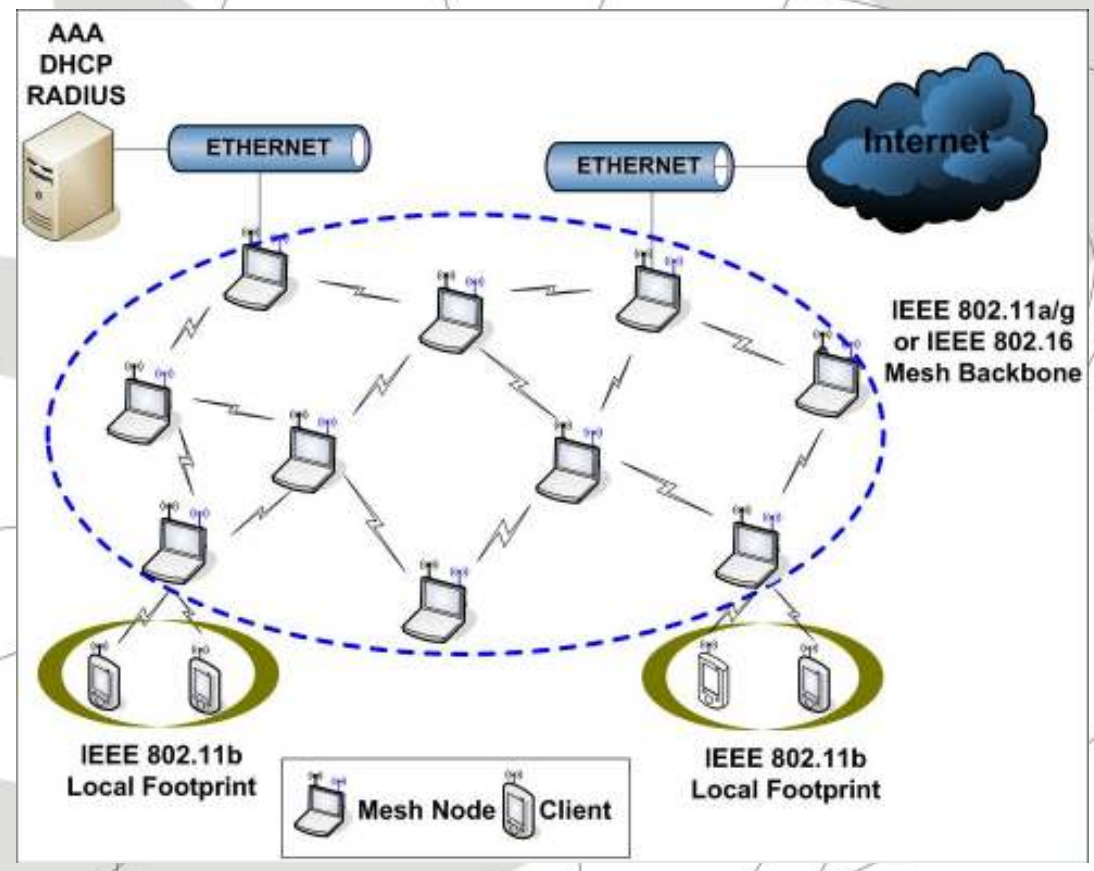
Principi di funzionamento

Reti Mesh

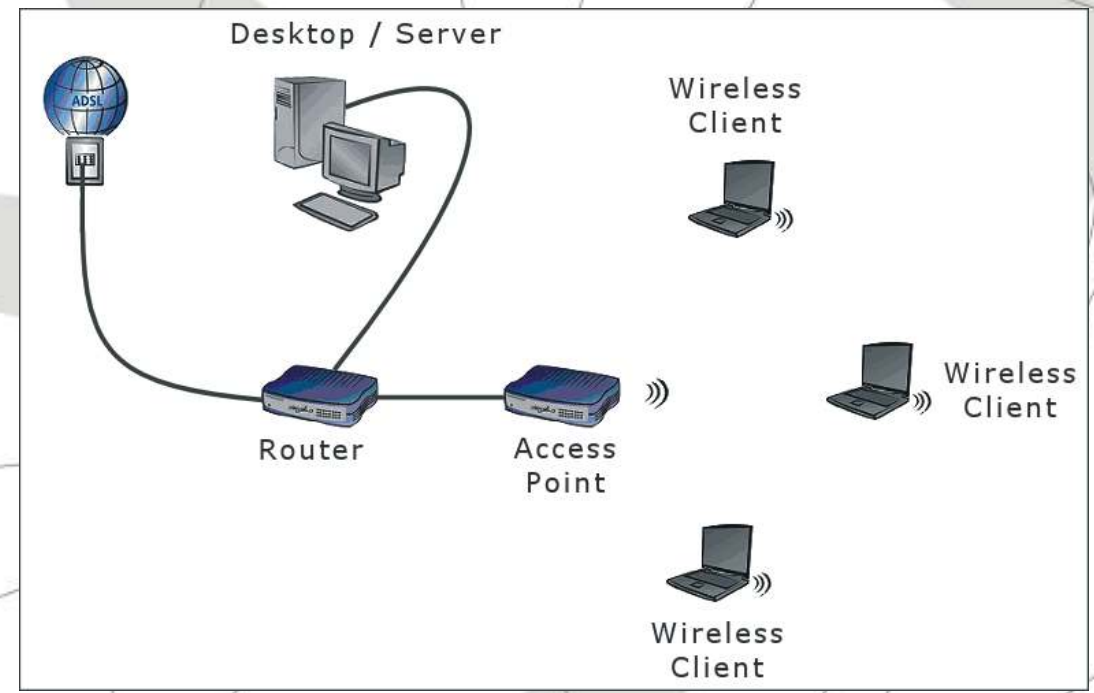
La Wireless Mesh Network consente di estendere la portata della rete WLAN:

- impedendo le interruzioni di servizio grazie al routing intelligente che impiega algoritmi di "auto-discovery" e "self-healing"
- impiegando interfacce standard 802.11b/g, che consentono di sfruttare l'immensa gamma, in continua crescita, di dispositivi compatibili con la tecnologia WLAN
- offrendo la possibilità di realizzare reti CAN (Community Area Network) in cui riunire tutti gli "hotspot" per garantire maggiore mobilità e una copertura omogenea.

Principi di funzionamento



Struttura base della rete



Fattori ambientali e performance

dB

Decibel: unità per la misura di rapporti di potenza in termini di guadagno o di perdita. Le unità sono espresse in termini di logaritmo in base 10 di un rapporto e sono generalmente espresse in watt.

dBi

Rapporto, misurato in decibel, dell'effettivo guadagno di un'antenna paragonato ad un'antenna isotropica. Più alto è il valore di dBi, maggiore sarà il guadagno e, quindi, più acuto sarà l'angolo di copertura.

dBm

Decibel riferiti ad un milliwatt - utilizzato per misurare determinati livelli, come quelli di trasmissione.

Fattori ambientali e performance

Watt

Il watt (simbolo: W) è l'unità di misura della potenza del Sistema Internazionale.
Un watt equivale a 1 voltampere (1 V · A).
Il watt prende il nome da James Watt per il suo contributo nello sviluppo della macchina a vapore.

Normativa

La normativa tecnica ETS 300-328 impone di non irradiare con una potenza E.I.R.P. superiore ai 100 mW (equivalente a 20 dBm).

Fattori ambientali e performance

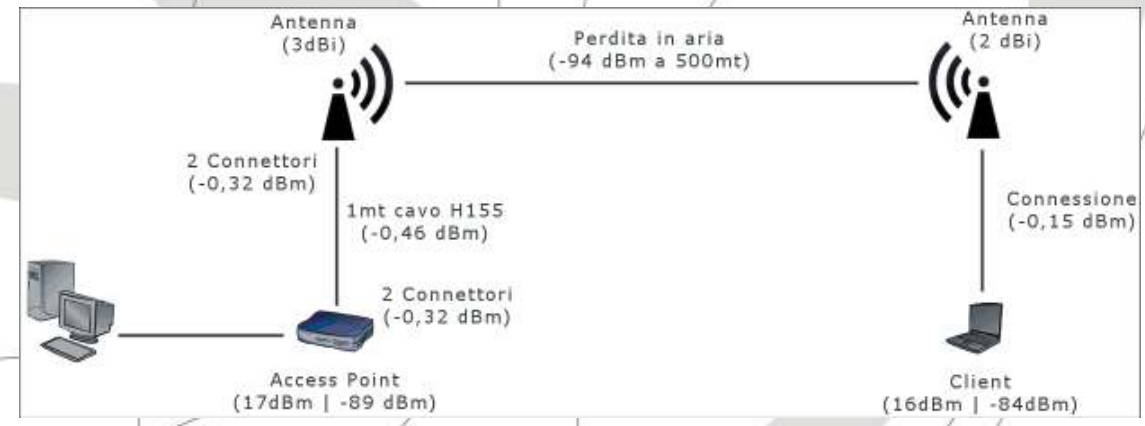
Potenza

In elettrotecnica la potenza è definita come il lavoro svolto da una carica elettrica in un campo elettrico nell'unità di tempo, ovvero la velocità di trasformazione dell'energia.

Sensibilità

La sensibilità è in generale l'attitudine a percepire qualcosa, uno stimolo, un sentimento ecc.
In fisica in particolare la sensibilità di uno strumento di misura o un sensore, è il rapporto tra la variazione del valore misurato R e la variazione del valore reale E della grandezza considerata

Fattori ambientali e performance



Fattori ambientali e performance

Calcoli

Adesso facciamo un po' di calcoli per capire se un determinato collegamento funzionerà o meno.
Dall'ap al client succede:

+17-0,32-0,46-0,32+3-94+2-0,15=-73,25

Essendo -73,25 > -84 il segnale viene ricevuto.
Al contrario invece:

+16-0,15+2-94+3-0,32-0,46-0,32=-74,25
Essendo -74,25 > -89 il segnale viene ricevuto.

Per un link ottimale, il segnale dovrebbe giungere con un'intensità superiore di 10dBm a quella minima dell'apparecchio.

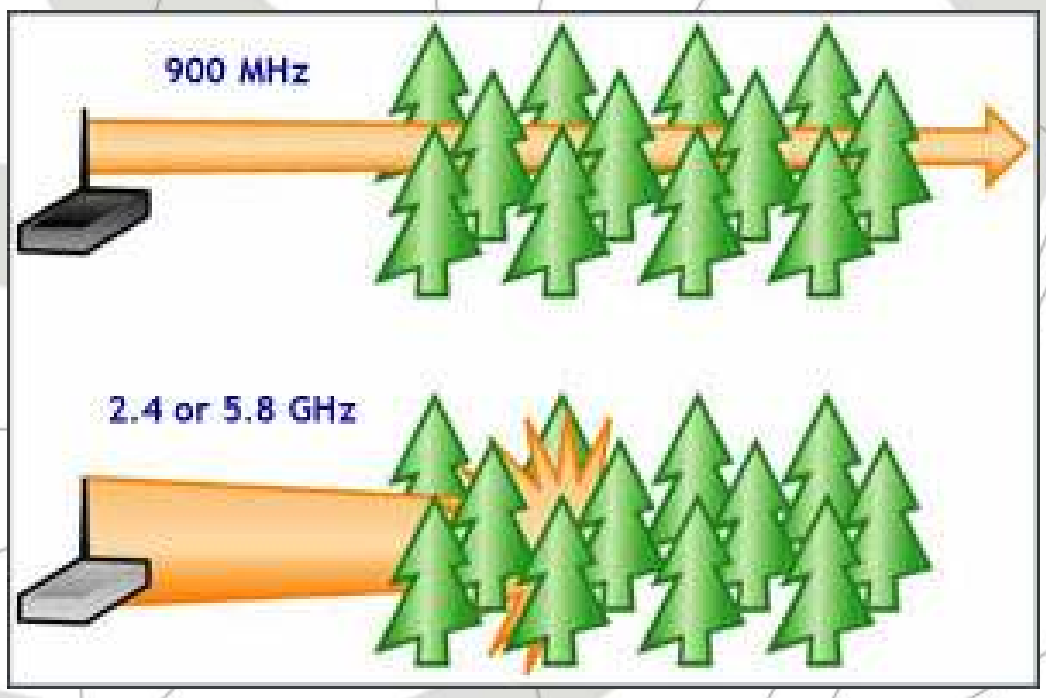
Fattori ambientali e performance

Perdite in aria

Il valore di perdita in aria (free space loss) viene riportato come assoluto. Come ben sappiamo, però, le condizioni sono mutevoli ed i fattori che più influiscono sul collegamento sono:
- umidità dell'aria (afa, nebbia, ...);
- pioggia;
- neve.

Le microonde (2,4GHz è proprio la frequenza dei forni) vengono assorbite da tutto ciò che contiene acqua... e dall'acqua stessa, ovviamente.
Per cui i valori di perdita in aria sono sempre soggetti alle condizioni ambientali.

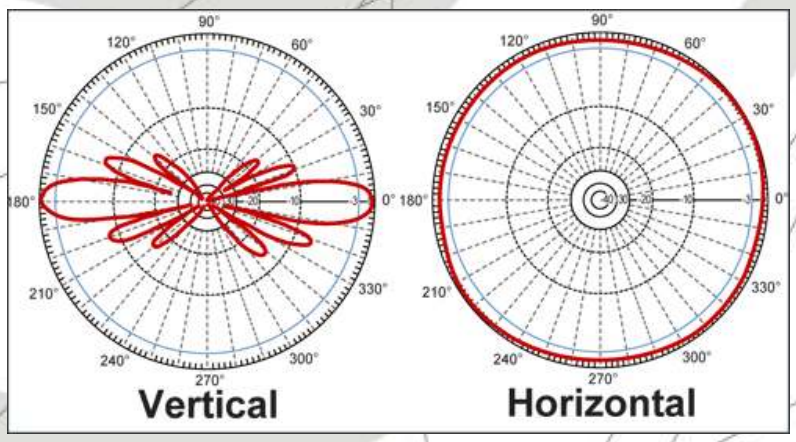
Fattori ambientali e performance



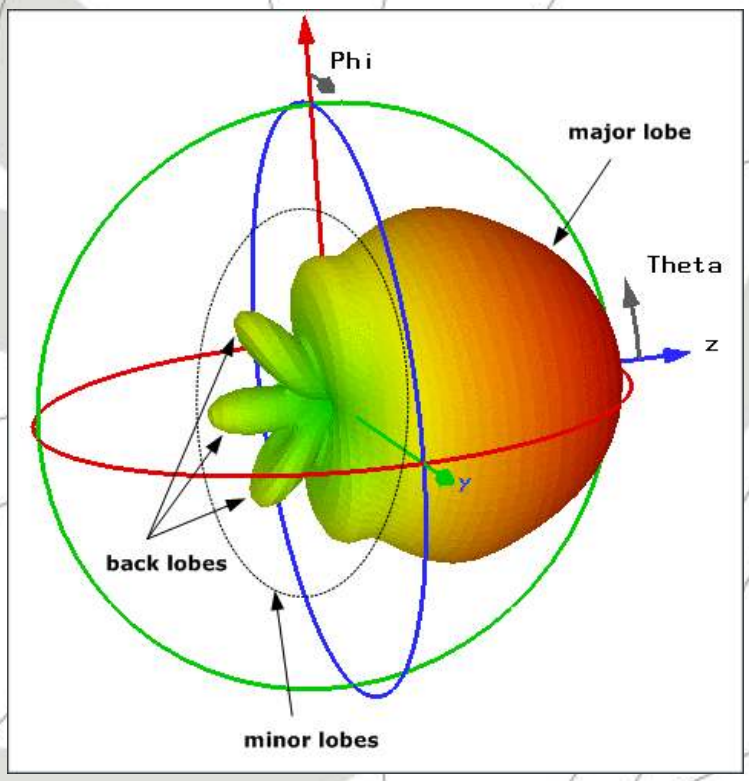
Fattori ambientali e performance

Rifrazione

L'emissione delle microonde non è lineare, ma si sviluppa lungo i tre assi. Questo significa che una parte delle onde emesse possono riflettere contro gli ostacoli diventando "dannose" in quanto portatrici di disturbo.



Fattori ambientali e performance

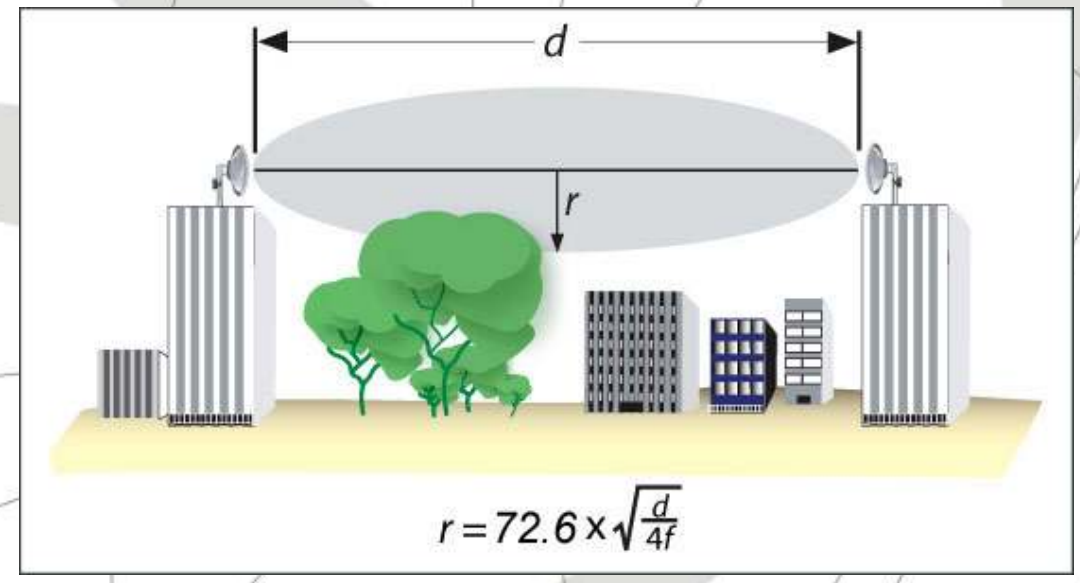


Fattori ambientali e performance

Zona Fresnel

L'effetto Fresnel è un insieme di fenomeni di interferenza sempre presente in una trasmissione radio. Le trasmissioni radio ad alta frequenza richiedono che il percorso tra due antenne sia libero da ostacoli: questo percorso viene comunemente detto line of sight (LOS), letteralmente "linea di visibilità". Ma in un collegamento radio non basta considerare la LOS: parte dell'energia di un'onda radio è infatti confinata nello spazio attorno alla LOS. Si può pensare a questo spazio come una specie di pallone da football americano il cui asse è la LOS stessa: tale spazio viene detto Zona di Fresnel. Nella pratica è sufficiente che il 60% di questa zona sia libero da ostacoli.

Fattori ambientali e performance



Scelta delle apparecchiature

Sensibilità

Più importante della potenza è la sensibilità. Essendo la legge molto restrittiva, con il suo limite di 100 mW di emissione all'altenna, è meglio lavorare con apparecchiature molto sensibili, capaci di captare segnali molto deboli, piuttosto che apparecchiature potenti, che andrebbero poi limitate.

Sicurezza

Il wep è ormai superato: la sicurezza che offere può essere superata in pochi minuti, per cui... abbandoniamolo! Esiste il wpa, o ancora meglio il wpa2, soluzioni capaci di offrire una reale sicurezza... per ora. Purtroppo le apparecchiature più obsolete non li supportano!

Potenza

Meglio scegliere apparecchiature che offrano la possibilità di modulare la potenza, così da evitare di "sforare" i limiti di legge... e da rendersi vulnerabili per i passanti.

Configurazione delle apparecchiature

Driver e moduli

E' il classico problema dell'amministratore del sistema: far riconoscere al PC il proprio hardware.

Se il driver della tua scheda non é presente nel Kernel, dovrai scaricarlo, installarlo e ricompilarlo in una nuova directory.

Una volta che conosci il nome del driver é il momento di caricarlo: nel caso di Pcmcia ci penserà il demone relativo (attivabile tramite /etc/rc.d/init.d/pcmcia start per le distribuzioni RedHat), mentre per le altre schede basterà dare "modprobe module_name options". Tra le opzioni vi sono ioport, irq e i settaggi data-link relativi al driver Wireless.

Configurazione delle apparecchiature

Ad ogni modo ci sono una serie di strumenti molto comodi per controllare il riconoscimento a basso livello del driver:

1. "tail /var/log/messages" che mostra le ultime informazioni scritte sul log di sistema (syslog)
2. "dmesg" for ulteriori info sul log
3. /proc directory: files ioports, devices, irq e sottodirectories specifiche per il driver.

Configurazione delle apparecchiature

Wireless tools

Managed Mode

 # Stabiliamo la modalità di funzionamento
iwconfig wlan0 mode managed
 # Specifichiamo su quale rete wireless (fra quelle intercettate) connetterci
iwconfig wlan0 ESSID MY_ACCESS_POINT_NAME
 # Utilizziamo sistemi di protezione attraverso il WEP
iwconfig wlan0 key open XXXXXXXX
 # Configurazione TCP/IP (i valori sono di esempio)
ifconfig wlan0 192.168.0.10 netmask 255.255.255.0 up
 # Eventualmente specifichiamo il nostro Default Gateway e DNS
route add default gw 192.168.0.1
echo "name server 123.123.123.1" > /etc/resolv.conf

Configurazione delle apparecchiature

Wireless tools

Ad-hoc Mode

 # Stabiliamo la modalità di funzionamento
iwconfig wlan0 mode ad-hoc
 # Specifichiamo quale rete wireless stiamo costituendo
iwconfig wlan0 ESSID MY_AD_HOC_TEST
 # Non utilizziamo (per il momento...) sistemi di protezione attraverso il WEP
iwconfig wlan0 enc off
 # Configurazione TCP/IP (i valori sono di esempio)
ifconfig wlan0 192.168.0.2 netmask 255.255.255.0 up
 # Eventualmente specifichiamo il nostro Default Gateway e DNS
route add default gw 192.168.0.1
echo "name server 123.123.123.1" > /etc/resolv.conf

Configurazione delle apparecchiature

Ndiswrapper

Ndiswrapper è un adattatore open source per i driver delle schede wireless scritti per windows. Mediante Ndiswrapper è possibile utilizzare interfaccie wireless in linux che non sono supportate direttamente dal kernel o dal produttore.
Per fare ciò ndiswrapper utilizza una parziale riscrittura del kernel di windows e della api NDIS (Network Driver Interface Specification) e convertendo a runtime le chiamate di sistema windows in chiamate di sistema linux. Non tutte le schede (o meglio i chipset) sono compatibili con ndiswrapper, ma una buona parte delle schede pci e pcmcia lo è.

Configurazione delle apparecchiature

Madwifi

MadWifi è un acronimo per Multiband Atheros Driver for Wireless Fidelty. In altre parole: questo progetto fornisce un driver per il kernel linux per interfacce di rete wireless basate su chipset prodotti da Atheros. Il driver lavora in modo da far apparire la scheda WLAN come una normale interfaccia di rete. Inoltre implementa il supporto per le api wireless. Questo consente di configurare l'interfaccia mediante gli usali wireless tools (ifconfig, iwconfig ecc).

Problematiche sulla sicurezza

Minacce alle reti wireless

- Rilevamento e furto di informazioni confidenziali.
- Accesso non autorizzato ai dati (intercettazioni e modifiche).
- Impersonificazione di un client autorizzato (spoofing, vengono utilizzati strumenti per "captare" SSID di rete e validi MAC dei client).
- Interruzione del servizio wireless (attacchi DoS agli access point).
- Accesso non autorizzato a Internet (usare le reti wireless circostanti per collegarsi a Internet in maniera fraudolenta).
- Minacce accidentali (chi non ha intenzione di collegarsi a rete wireless, ma il suo pc lo fa involontariamente captando il segnale wireless).

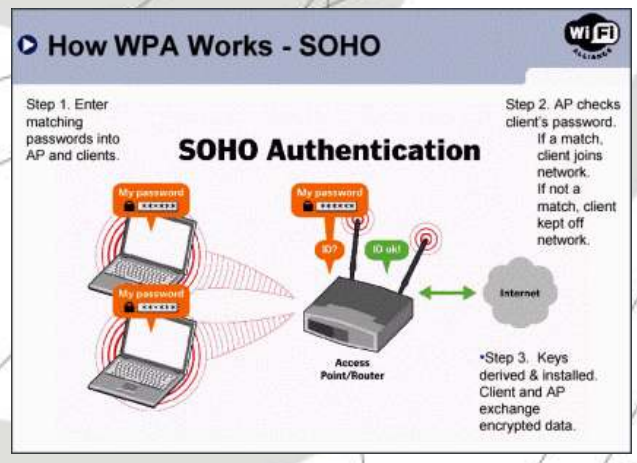
Sistemi di protezione

Soluzione wireless	Ambiente tipico	Componenti di infrastruttura addizionali richiesti?	Certificati usati per l'autenticazione dei client	Password usate per l'autenticazione dei client	Metodo tipico di crittazione dei dati
Wi-Fi Protected Access con Pre-Shared Keys (WPA-PSK)	Small Office Home Office (SOHO)	Nessuno	NO	SI Usa la chiave di crittazione WPA per l'autenticazione alla rete	WPA
PEAP + password (PEAP-MS-CHAPv2)	Piccole/medie aziende	RADIUS Certificato richiesto per il server RADIUS	NO (ma almeno un certificato deve essere rilasciato per validare il server RADIUS)	SI	WPA o chiave WEP dinamica
Certificati (EAP-TLS)	Aziende medio/grandi	RADIUS Servizi Certificati	SI	NO (possibilita' di modifica, inserendo la richiesta di password)	WPA o chiave WEP dinamica

Problematiche sulla sicurezza

Wep e Wpa

Come abbiamo visto, per configurare la chiave wep è sufficiente passare il parametro key attraverso iwconfig. Per il wpa invece le cose sono un po' più contorte, ed abbiamo bisogno dell'aiuto di wpa_supplicant, un piccolo tool che permette di effettuare l'autenticazione wpa. Per maggiori informazioni leggete l'ottima guida all'indirizzo http://www.archlinux.it/wpa-supplicant



Fonti

http://it.wikipedia.org/
http://www.hyperlinktech.com/
http://www.rfprop.com/
http://drmuey.com/
http://www.avalanwireless.com/
http://www.harpax.com/
http://www.microsoft.com/
http://kunz-pc.sce.carleton.ca/
http://www.shorecliffcommunications.com/
http://www.bertolinux.com/wireless/italiano/Wireless-HOWTO.html
http://www.mobydik.it/services/wireless_linux_script.aspx
http://www.archlinux.it/wpa-supplicant
http://www.tomshardware.pl/

Per approfondire:
http://security.fi.infn.it/TRIP/802.1x-wireless/index.html