Reti Wireless

1 Wireless LAN (WLAN) - IEEE 802.11

Gli standard per rete locale wireless sono emanati dal comitato IEEE 802.11. Le reti locali wireless sono dette anche WLAN (Wireless Local Area Network) o, usando il nome commerciale di un consorzio di produttori di apparecchiature, "Wi-Fi" (per analogia con Hi-Fi, alta fedeltà (audio!)).
Le reti wireless funzionano nelle banda "ISM" (Industrial, Scientifical, Medical), che sono di utilizzazione libera e per le quali non si deve pagare la concessione governativa che è richiesta per le altre bande utilizzate per le telecomunicazioni (radio, TV, ponti radio di telefonia fissa, telefonia mobile, militari, emergenza, satelliti, ..).
Negli USA le bande ISM sono incentrate sulle frequenze di: 900 MHz, 2 GHz e 5 GHz.
Dato che in Europa la banda dei 900 MHz è usata per i telefoni GSM, gli standard 802.11 sono stati sviluppati solo per le frequenze di 2 GHz e 5 GHz[1].
Per limitare i disturbi che le apparecchiature di questo tipo potrebbero causare ad altre dispositivi vicini che lavorano nella stessa banda dello spettro elettromagnetico[2], le leggi e le normative prevedono che:

1. i trasmettitori abbiano bassa potenza
2. la tecnica di modulazione distribuisca la potenza su tutta la banda disponibile (modulazioni "spread spectrum"). Viste le modalità di codifica dei numeri usate nelle modulazioni spread spectrum (vedi oltre), ciò che viene trasmesso dal mittente potrà essere decodificato dal destinatario, che conosce la chiave di decodifica, mentre per tutti gli altri possibili riceventi, diversi dal destinatario e che non posseggono la chiave di decodifica, il segnale trasmesso verrà visto solo come un piccolo aumento del rumore ambientale. I riceventi che non posseggano la chiave di decodifica non potranno estrarre il segnale originario da questo "rumore".

Data la limitatezza della potenza che si può erogare, il massimo raggio di copertura di una rete wireless non può superare i 2 km, con reti al limite della "legalità". Le distanze più comuni sono dell'ordine delle poche centinaia di metri. Gli standard prevedono che all'aumentare della distanza, quando il rapporto segnale/rumore si fa piccolo, venga diminuita la velocità di comunicazione, per cui per ottenere la massima velocità bisogna che le antenne dei vari apparati di rete siano abbastanza vicine. Per garantire alte velocità in tutto il raggio di interesse della rete è necessario usare più dispositivi di rete ("Access Point") di quanto strettamente indispensabili, in modo che ogni stazione, in qualsiasi punto si trovi, sia abbastanza vicina ad un Access Point da funzionare alla massima velocità.

1.1 Modalità di funzionamento delle reti WLAN

In una rete 802.11 le stazioni possono essere logicamente collegate in modo diverso ed i messaggi possono essere fisicamente indirizzati a stazioni diverse, anche se devono raggiungere la stessa destinazione. Ciò dipende dalla modalità di funzionamento della rete, che può richiedere o meno la presenza di uno o più nodi "speciali" detti "Access Point ".

BSS

Il più semplice tipo di rete WLAN è il **BSS** (Basic Service Set), che comprende al massimo un "Access Point ".
Una rete BSS può essere di due tipi:

- "**ad hoc**" (o peer to peer), è la rete wireless più semplice, che non comprende alcun Access Point . In modo "ad hoc" tutte le schede di rete comunicano direttamente una con l'altra. Dunque in questa modalità ogni scheda, per potere comunicare con una qualsiasi altra, deve poterla raggiungere con la sua antenna. Questa modalità viene anche detta "IBSS" (Independent Basic Service Set).
- "**ad infrastruttura**" (infrastructure network, con Access Point) è la topologia di rete wireless nella quale esiste un singolo nodo della rete che gestisce le comunicazioni e la sicurezza ed attraverso il quale passa tutto il traffico della rete. Questo particolare nodo viene detto "**Access Point** ". In una rete ad infrastruttura i pacchetti che partono da una scheda "normale" (che chiameremo scheda "mobile") raggiungono le altre schede "mobili" solo passando attraverso l'Access Point.

La rete wireless ad infrastruttura è la "BSS", in senso proprio. Dunque, se non si specifica nient'altro, una BSS sarà una rete ad infrastruttura.
In questo modo il raggio di copertura della rete può aumentare dato che due schede "mobili", per poter comunicare, basta che riescano a raggiungere entrambe l'Access Point, senza la necessità di raggiungersi direttamente. Oltre a questo vantaggio c'è anche il fatto che l'Access Point riesce a collegarsi con schede più lontane perché, non avendo bisogno di essere facilmente trasportabile, di solito ha antenne migliori, usate con segnali più potenti e non viene alimentato a batteria ma con la rete elettrica.
Ogni stazione mobile che vuole scambiare informazioni in una rete ad infrastruttura deve prima "associarsi" al suo Access Point. In seguito, per trasmettere dati ad ogni altro nodo della rete, dovrà passare comunque per l'Access Point.

1 per l'esattezza: da 2,4000 a 2,4835 GHz. Le bande a 5 GHz possono essere due: da 5,150 a 5,350 GHz e da 5,470 a 5,725 GHz.
2 le bande ISM vengono comunemente dette "garbage bands"!

Dato che tutto il traffico di una BSS passa attraverso l'Access Point, esso è il dispositivo ideale anche per fare da bridge fra la rete wireless e quella cablata, infatti tutti gli Access Point hanno anche almeno una porta RJ-45, attraverso la quale fanno da bridge trasparente verso la rete in rame.
Ogni Access Point può gestire fino ad un massimo di 127 stazioni mobili.
Ogni dispositivo WLAN in una BSS può essere in ogni istante o nella condizione di collegamento "ad hoc" oppure "ad infrastruttura", non può essere contemporaneamente in entrambe le condizioni.
Ogni BSS ha un nome univoco[3] detto SSID (**S**ervice **S**et **Id**entificator). Per poter collegarsi ad una rete tutte le stazioni devono usare lo stesso SSID. L'Access Point spedisce a tutti il suo SSID con un segnale detto "beacon[4]".
Una stazione mobile che non faccia parte di una rete wireless può ascoltare tutti segnali di beacon e conoscere l'SSID di tutte le reti cui si può collegare. In seguito l'utente, tramite il software che la controlla, può decidere, in base al nome, a quale BSS aggregarsi.
Naturalmente si può configurare l'Access Point in modo che non trasmetta il segnale di beacon ("hidden[5] SSID"). In questo modo la presenza della rete non è rilevata facilmente e per accedervi è indispensabile conoscerne il nome (SSID). Dunque il nascondere l'SSID è un'operazione che, sia pur di poco, aumenta la sicurezza della rete.
La banda ISM a disposizione viene suddivisa in "canali". I canali possono essere: 11, nella normativa USA, 13 in quella europea, 14 nella giapponese.
Ogni BSS trasmette in un solo canale, che viene predederminato sugli Access Point al momento della loro configurazione, mentre può essere "variabile" nelle schede di rete (durante la scansione, per il riconoscimento delle reti raggiungibili, la scheda di rete prova in tutti i canali).
Se diverse reti coesistono nella stessa zona, è meglio scegliere per esse canali di "numero lontano" (p.es., se abbiamo tre reti potremmo scegliere i canali 1, 7 e 13).
Range Extender

ESS

Un "**range extender**" è un dispositivo che amplifica i segnali ricevuti da un Access Point e li ritrasmette ai nodi mobili che gli stanno intorno, permettendo a questi nodi di raggiungere l'Access Point. Si potrebbe ottenere un risultato analogo usando due access point, ma con un range extender non sarà necessario colleganre in due A.P. in wireless, né utilizzare A.P. più costosi, in grado di connettersi come ESS (vedi in seguito).

Le reti WLAN di tipo BSS non permettono ai dispositivi mobili di "migrare" senza soluzione di continuità dall'area di copertura di un Access Point a quella di un altro vicino. Per questo scopo c'è la modalità di funzionamento **ESS** (Extended Service Set).
Una rete ESS è costituita da più di una infrastruttura BSS ("**cella**"), ciascuna con il suo Access Point, ma con aree di copertura parzialmente sovrapposte. In una rete ESS due schede mobili nell'area di copertura di due Access Point diversi sono in grado di comunicare fra loro. Gli Access Point provvederanno a fare da bridge fra le due celle.
E' inoltre possibile il "**roaming**" fra gli Access Point . Quando una scheda mobile, muovendosi, si porta nel raggio di copertura di un Access Point diverso, i due Access Point sono in grado di negoziare il passaggio del controllo della scheda da un Access Point all'altro (fenomeno che viene detto "**handover**" del terminale mobile).
In questo modo di funzionamento le reti 802.11 somigliano alle reti di telefonia cellulare. Di diverso c'è il fatto che, operando in bande di frequenza "libere" possono usare potenze molto più basse e raggiungere distanze molto più brevi fra antenna ed antenna.
Per identificare tutta una rete ESS, nella quale è possibile fare il roaming delle stazioni remote, è definito un nome unico, detto ESSID (**E**xtended **S**ervice **S**et **Id**entificator).
E' buona norma, per minimizzare le mutue interferenze, che due Access Point contigui che appartengano alla stessa ESS vengano configurati in modo da lavorare su canali diversi. In questo caso, dato che ogni BSS funziona su un unico canale è ovvio che durante l'handover la stazione mobile dovrà anche cambiare canale.
Gli Access Point possono aggregarsi e costituire una rete ESS se rispettano il protocollo **IAPP** (**I**nter **Access Point P**rotocol). Il protocollo IAPP, che è stato ratificato dalla IEEE, non è ancora usato universalmente, per cui gli Access Point di marche diverse potrebbero non essere interoperabili. Verificare prima dell'acquisto!

La negoziazione delle modalità di funzionamento è prevista dai protocolli ed è effettuata dalle schede di rete WLAN in modo largamente automatico. Per l'utente finale non c'è alcuna differenza fra collegarsi in modalità peer to peer, ad infrastruttura o ESS.
E' possibile uscire da una ESS ed entrare in un'altra, ma questo non può avvenire in modo trasparente all'utente, che dovrà:
1. disconnettersi dalla prima ESS
2. scegliere l'ESSID della nuova ESS cui collegarsi
3. effettuare la richiesta di collegamento

Anche se c'è un Access Point a portata d'antenna, non è escluso che due schede mobili non possano comunicare direttamente in modalità peer to peer. Ciò può accadere, per esempio, se le due schede avevano già in corso una comunicazio-

3 Si tratta di una semplice stringa, di tipo "case sensitive": l'SSID "Rete" è diverso da "rete".
4 Segnalazione con fuoco che avverte dell'avvicinarsi di un nemico o, più in generale, ciò che dà notizia di un pericolo (tradotto da Wiktionary)
5 nascosto

ne quando sono entrate nel campo dell'Access Point . In questo caso però non saranno in grado di comunicare con l'Access Point se non dopo aver chiuso la loro comunicazione diretta.

MAC 802.11

Il MAC 802.11 viene detto CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance).
L'utilizzazione anche nelle WLAN di uno schema MAC identico a quello Ethernet (CSMA/CD), avrebbe richiesto costosi ricetrasmettitori full duplex per poter rilevare la collisione. Per questo si è preferito utilizzare uno schema diverso, semplice da realizzare come quello Ethernet, ma senza rilevazione della collisione.
A dispetto del significato della parola "Avoidance[6]", il MAC CSMA/CA non rende matematicamente impossibili le collisioni, ma le rende "solo" molto improbabili. Dunque, dato che le collisioni sono improbabili, esse non vengono nemmeno rilevate. Nei rari casi in cui accadono, esse genereranno errori nei dati e verranno gestite dagli strati superiori dello stack di rete, così come avviene per le collisioni in ritardo nelle reti Ethernet.
Il MAC CSMA/CA prevede che ogni stazione, prima di trasmettere un segnale:

1. "ascolti" se qualcuno sta già trasmettendo ("Carrier Sense")
2. se qualcuno sta trasmettendo, non trasmetta ed attenda, prima di un prossimo tentativo, "un certo tempo".
   Se nessuno sta trasmettendo, incominci a trasmettere.

E' chiaro che sino a qui tutto funziona come nella normale Ethernet (d'altronde entrambe sono CSMA!); la differenza concerne il "certo tempo" di attesa, che nel CSMA è calcolato in modo deterministico, non casuale come in Ethernet.
Quando una stazione trasmette, essa comunica, all'inizio del frame, un'informazione importante detta NAV (**N**etwork **A**llocation **V**ector) che indica alle altre stazioni per quanto tempo essa prevede di impegnare il mezzo di trasmissione. Le altre stazioni leggono questo valore e lo usano per regolare il tempo di attesa prima di ritentare di nuovo la trasmissione, quando, dovendo trasmettere, trovano la rete già occupata. Dunque in questo caso il tempo di attesa non è completamente casuale, come in Ethernet, ma è legato al NAV comunicato dal dispositivo che sta correntemente trasmettendo.
Questo spiega a grandi linee come si riesce a rendere molto improbabile la collisione[7], e perchè non c'è bisogno di rilevarla.

Strato DLL, il frame 802.11

Esistono tre tipi di frame 802.11, diversi in base alle funzioni che debbono essere svolte (frame di tipo "data", frame di tipo "control", frame di tipo "management").
Nel frame 802.11 sono presenti 3 o 4 indirizzi, il cui significato è diverso in base alla topologia della rete (peer to peer o ad infrastruttura).
Gli indirizzi usati sono identici a quelli di Ethernet.
Il frame 802.11, che ha lunghezza massima di 2304 Byte di dati, ha la possibilità (opzionale) di essere frammentato, quando sia necessario trasportare messaggi più lunghi del massimo ammesso.

Modalità di trasmissione del segnale nelle reti wireless

Come già accennato, nelle reti locali wireless devono usati schemi di modulazione a spettro diffuso (spread spectrum).
In 802.11 si usano modulazioni digitali di tipo DSS (Direct Sequence Spread Spectrum), frequency hopping od OFDM.
Norme
Le prime specifiche 802.11 delineavano reti da 1 o 2 Mbit/s, poi (Dicembre 1999) vennero ratificati gli standard 802.11a e 802.11b, che funzionano rispettivamente a 54 Mbit/s e 11 Mbit/s ed utilizzano le bande di 5,8 GHz e 2,4 GHz. La frequenza superiore e la maggiore velocità hanno reso molto più lenta la realizzazione di reti 802.11a, per cui le reti 802.11b si sono molto affermate sul mercato prima dell'arrivo delle 802.11a. Dato che l'uso di diverse banda rende del tutto incompatibili le apparecchiature 802.11a e 802.11b, 802.11a ha avuto difficoltà ad affermarsi, tanto che è stato emesso successivamente un nuovo standard 802.11g, che funziona a 54 Mbit/s nella banda dei 2,4 GHz, mantenendo compatibilità con le apparecchiature 802.11b.

1.2 802.11b

La frequenza della portante è nella banda dei 2.4 GHz. E' il primo degli standard 802.11 ad aver avuto implementazioni commerciali.
La sua velocità massima è di 11 Mbit/s (teorici), naturalmente non si raggiunge mai il massimo e di solito la velocità è intorno ai 4 o 5 Mbit/s.
La distanza massima di collegamento è di 150 m, all'interno di edifici, 500 in esterni.
Lo standard prevede diverse velocità di trasmissione, negoziate automaticamente dai dispositivi, che cambiano la velocità quando le condizioni lo richiedono.
La velocità diminuisce all'aumentare della distanza ed agli estremi del campo si va solo a 1 Mbit/s. La velocità cala se e quando ci si trova in un ambiente con una presenza significativa di rumore elettrico. Di solito in questi casi le schede garantiscono comunque il funzionamento, anche se a velocità degradata.

6 to avoid = evitare, avoidance = ciò che ci permette di evitare
7 in realtà il meccanismo è più complesso

Per avere la massima velocità non si devono superare i 50 m in interni ed i 250 m in esterni.
Esiste un modo "enhanced" non standard, che permette di operare alla velocità di 22 Mbit/s, disponibile solo con dispositivi che usano circuiti integrati di un particolare produttore.

1.3 802.11a

La frequenza della portante è nella banda dei 5 GHz. La sua velocità massima teorica è di 54 Mbit/s, comunemente si ottengono velocità fra 20 e 25 Mbit/s.
In cambio della maggiore velocità bisogna accettare distanze minori; 802.11a può raggiungere al massimo i 100 m in interni, 350 in esterni. Alla massima distanza la velocità è di 6 Mbit/s.
Per avere la massima velocità non si devono superare i 18 m, 30 m in esterni.
Data la maggiore frequenza del segnale, è più difficile per le reti 802.11a penetrare gli ostacoli e più facile che le sue riflessioni lo danneggino.
Anche per questi dispositivi sono stati sviluppati miglioramenti non standard che possono portare a 72 o 108 Mbit/s teorici.
Come già detto, 802.11a e 802.11b sono incompatibili, a meno di non ricorrere ad apparecchiature "dual band", che esistono sul mercato e che fanno da bridge fra i due tipi di rete.

1.4 802.11g

E' completamente compatibile verso il basso con 802.11b, per cui è in grado di usare gli stessi tipi di modulazione di 802.11b; peraltro funziona anche a velocità superiori agli 11 Mbit/s, fino a 54 Mbit/s, utilizzando in questo caso la modulazione OFDM.

1.5 Enhaced wireless: 802.11n

Un nuovo standard per reti WLAN ad alta velocità della serie 802.11 dovrebbe apparire dal 2007. Esso permetterà di raggiungere velocità di 600 Mbit/s. Per aumentare la velocità 802.11.n farà ampio uso della modalità MIMO.

MIMO

Multiple In Multiple Out è una modalità di comunicazione nella quale, per raggiungere un'alta velocità, si usano simultaneamente più antenne e più canali di trasmissione su ogni antenna. La proposta per 802.11n è di utilizzare 4 antenne in ricezione e 4 in trasmissione.

1.6 Modulazioni spread spectrum

Modulazione DSS (Direct Sequence Spread Spectrum)

Modulazione frequency hopping

In questa modalità di trasmissione la banda a disposizione viene divisa in molte "sottobande" (canali). All'interno dei canali la modulazione è "normale" (es. FSK). Lo "sparpagliamento" dello spettro avviene cambiando molto velocemente i canali in cui si trasmette, secondo una sequenza pseudocasuale nota a tutti i nodi che devono comunicare. Il cambio di banda viene detto "frequency hop" ed avviene migliaia di volte al secondo.

Modulazione OFDM (Orthogonal Frequency Division Multiplex)

Le basi di questo tipo di modulazione sono state poste negli ultimi anni '60. E' una tecnologia a spettro diffuso (spread – spectrum). I dati sono trasmessi in parallelo su migliaia di "sottocanali" a banda stretta. Questi canali hanno portanti a diverse frequenze, molto vicine. Esse non si sovrappongono, nè interferiscono, perchè sono "ortogonali", secondo una complicata definizione matematica che senz'altro omettiamo. Le frequenze delle portanti sono determinate, con calcoli aritmetici complessi, in modo da essere le più vicine possibili. I dati sono trasmessi dopo essere stati modificati con tecniche matematiche che permettono, a destinazione, di distinguere da quale dei diversi sottocanali essi provenivano. I questo modo può essere ricostruito il numero spedito inizialmente.
Uno dei problemi più grossi nelle comunicazioni digitali wireless ad alta velocità è la presenza di riflessioni multiple delle onde. Ogni volta che l'onda viene riflessa (p.es. da una superficie metallica) essa giunge lo stesso a destinazione ma con tempi diversi rispetto al segnale che percorre la linea retta. Dunque gli stessi numeri (simboli) si presentano a destinazione molte volte, con ritardi diversi, che variano in base a ciò che sta in mezzo fra il trasmittente ed il ricevente. Aumentando la frequenza di trasmissione dei simboli il problema delle riflessioni multiple diventa sempre più importante (interferenza intersimbolo).
La tecnica di modulazione OFDM permette di spedire ogni bit a velocità relativamente bassa e di ottenere l'alta velocità attraverso l'uso parallelo di molti canali. Spedendo lentamente ogni bit l'effetto delle riflessioni multiple (multipath reflections) è minimizzato, perchè si dà tempo al segnale di stabilizzarsi dopo l'arrivo di tutte le onde riflesse.

1.7 Dispositivi Wi-Fi

Schede di rete
In ogni computer che si vuole collegare ad una rete wireless deve avere una scheda di rete (NIC) 802.11. Esistono schede di tutti i tipi: PCI, da mettere nelle schede di espansione di un PC, PC Card (PCMCIA) usate nei PC portatili, USB, che possono essere collegate ovunque. Molti modelli di computer portatile hanno una NIC 802.11 inclusa.

Access Point
Da un punto di vista logico, un Access Point può essere considerato un hub per la rete wireless, ogni stazione mobile spedisce tutti i suoi pacchetti all'Access Point ed esso li smista agli altri nodi della rete; tutte le stazioni della rete sono in grado di leggere tutti i pacchetti che passano nell'Access Point, solo quella interessata ritiene l'informazione.
Un Access Point è anche è un bridge, di livello LLC, che può collegare in modo trasparente una rete Ethernet alla WLAN. Esso collega la rete wireless ad altre reti, cablate o wireless, come per esempio una Ethernet, Bluetooth, o ad Internet. Cattura tutti i pacchetti che vede nelle stazioni wireless e li inoltra nella rete cablata, e viceversa. Se lavora a livello MAC si comporta come un bridge, se lavora anche a livello Network si comporta come un router. Se è un router lavora con il protocollo IP (vedi oltre).
Per collegarsi a Internet un Access Point può contenere un modem ADSL od un altro dispositivo di accesso alla Rete. In altre configurazioni può avere una porta Ethernet "WAN" tramite la quale si collega al dispositivo che a sua volta si collega ad Internet (p.es. un modem ADSL collegabile con interfaccia Ethernet).
Gli Access Point che svolgono solo la funzione di bridge possono avere un leggero vantaggio di prestazioni rispetto ai router, perchè la loro CPU non è impegnata nelle elaborazioni relative al routing.

Antenne
!!!! TO BE COMPLETED !!!!

Hot spot wireless
Il sistema che mette a disposizione del pubblico un accesso wireless ad Internet viene detto "hot spot wireless". Gli hot spot wireless stanno cominciando a crescere in numero e possono essere presenti presso condomìni, in esercizi pubblici, ed anche in aeroporti, stazioni, ospedali o altri luogo ad alta intensità di frequentazione. In questi ultimi casi sono gestiti da grosse aziende, dette WISP (Wireless Internet Service Provider) che mettono in rete geografica i loro hot spot ed offrono un servizio in abbonamento. Il loro cliente può accedere ad Internet da uno qualunque degli hot spot "convenzionati" ed è disponibile la funzione di roaming, con la quale si può spostare da un hot spot all'altro, anche di altri WISP, senza perdere il collegamento.
La creazione delle reti wireless è stata deregolamentata dal Governo Italiano con Decreto del 28 Maggio 2003. Mentre precedentemente per installare una WLAN era necessario pagare un canone annuale forfettario (di basso importo), con la deregolamentazione non si deve più pagare nulla, né si deve chiedere un'autorizzazione, se la rete rimane in ambiti privati. Solo se la copertura della rete comprende suolo pubblico è necessario fare una richiesta di autorizzazione all'installazione, che viene concessa con silenzio-assenso se l'amministrazione non risponde entro 30 giorni.
Funzioni che possono essere fornite da un hot spot:
- accesso ad Internet
- telefonia IP (con eventuali gateway alle reti telefoniche tradizionali)
- collegamento con la telefonia cellulare e la videofonia (con eventuali gateway a GSM o UMTS)
- video on demand
- giochi interattivi

Il decreto citato obbliga i WISP a fornire servizio di roaming anche verso altri provider, per cui se si fa l'abbonamento con un provider dovrebbe essere garantita l'accessibilità, magari dietro pagamento di un sovrapprezzo, anche attraverso gli hot spot di altri WISP.

1.8 Sicurezza WLAN

I dati di una WLAN sono trasmessi senza fili in tutti i dintorni delle apparecchiature. Dato che è facile per una qualsiasi stazione mobile aggiungersi ad una WLAN e visto che la trasmissione avviene in broadcast, è chiaro che è piuttosto facile intercettare i dati e leggere tutto quanto venga scambiato nella rete.
Per ovviare all'intercettazione, è importante che tutti i dati trasmessi vengano crittati. Per questo le norme 802.11 nascono prevedendo la possibilità di crittografare ogni pacchetto scambiato in rete.
Si illustrano in seguito le contromisure da prendersi per ottenere maggiore sicurezza.

SSDI nascosto
Come già spiegato, nascondere l'SSID può essere una misura di sicurezza, perché chi non conosce l'SSID non sarà in grado di sapere che esiste una rete cui collegarsi, per cui non dovrebbe nemmeno provarci. Si noti peraltro che esistono software in grado di individuare la presenza di traffico di rete 802.11 anche se il segnale di beacon non viene trasmesso.

Filtraggio degli indirizzi MAC
Gli Access Point dispongono di una funzione di filtraggio degli indirizzi MAC. E' possibile fare in modo che l'A.P. Comunichi solo con schede mobili il cui indirizzo MAC è compreso in una "lista bianca".

Dato che non è molto difficile leggere l'indirizzo MAC delle stazioni che trasmettono in rete e modificare la stazione mobile in modo che utilizzi un indirizzo fra quelli della "lista bianca", questa contromisura di sicurezza non è molto efficace.

WEP (Wireless Equivalent "Privacy")

Lo standard di sicurezza iniziale di 802.11 è WEP. WEP viene gestito dall'Access Point, nel quale sono concentrati tutti i dati scambiati. L'Access Point crittografa tutti i dati, con un algoritmo di tipo RC4, con chiavi simmetriche di lunghezze diverse, in base al livello di sicurezza voluto.
Inizialmente 802.11b usava una chiave di 40 bit, oggi troppo piccola e considerata insicura. Oggi si usano chiavi di 64 o 128 bit, 802.11a usa chiavi da 152 o 256 bit.
Naturalmente, i calcoli richiesti dalla cifratura possono avere un forte impatto sulla velocità di comunicazione; più è lunga la chiave, più lente sono le operazioni di cifratura e decifratura.
La crittografia WEP assicura sia la confidenzialità delle trasmissioni, mediante la cifratura, sia la loro integrità, con una forma di checksum.
WEP utilizza in ogni sessione una fra alcune chiavi definite dall'utente. Tutti i terminali mobili e gli A.P. devono usare la stessa chiave, che deve essere impostata manualmente con il software di configurazione del dispositivo.
La chiave di cifratura in WEP è statica, cioè sempre la stessa durante un collegamento e può essere cambiata solo manualmente, riconfigurando i dispositivi e con un certo sforzo di amministrazione.
Questo è il maggior problema di WEP; infatti, se la chiave non cambia mai durante la comunicazione, è possibile ottenere un campione statistico sufficiente scoprire la chiave WEP. Esistono infatti programmi che, catturando dalla rete un numero sufficiente di pacchetti ed utilizzando tecniche statistiche di criptoanalisi scoprono la chiave e permettono l'ingresso nella rete.
E' importante far notare che l'attaccante, una volta ottenuto l'ingresso "abusivo" nella WLAN, è in grado di comunicare senza autorizzazione, e di leggere tutto ciò che passa per la rete.
Maggiore è il traffico di rete, più veloce è la scoperta della chiave, per cui la tecnologia WEP è adatta alle reti piccole, che non scambiano molti dati.
WEP non autentica gli utenti e critta solo i dati del frame, non l'header. Questo significa che gli indirizzi di mittente e destinatario del pacchetti sono sempre visibili e possono essere informazioni interessanti, per un "attacker", per provare ad "impersonare" un nodo legittimo della rete.
Normalmente l'Access Point si fa sempre vedere in broadcast a tutte le stazioni che transitano nel suo raggio di azione e garantisce accesso ad ogni scheda di rete che ne faccia richiesta. Per questo è piuttosto debole dal punto di vista della sicurezza.
Come già accennato, a mitigare queste caratteristiche, è possibile effettuare il "MAC filtering" e nascondere l'ESSID.
Per reti complesse che debbano usare WEP, è meglio ricorrere a meccanismi di crittazione a livello più alto, come per esempio nelle VPN con dati crittografati, trasportati da IP (livello 3, network. Vedi oltre per i dettagli su queste tecniche).

WPA (Wi-Fi Protected Access)

Per ovviare alle debolezze di WEP è stato sviluppato WPA, che, come WEP, fa parte dell'insieme delle norme 802.11.
Le prime apparecchiature che usano questo standard sono del 2003. WPA è una soluzione "transitoria" in attesa dell'estensione finale, data dalla norma IEEE 802.11i.
WPA richiede obbligatoriamente un'autenticazione alla stazione che entra in rete. L'autenticazione può essere fatta in due modi:

1. Basata sull'Access Point locale
   L'amministratore dell'A.P. deve dare una chiave iniziale (master key), che deve essere digitata nell'A.P. ed in tutte le stazioni mobili. Essa però è solo un punto d'inizio per calcolare chiavi dinamiche, che vengono cambiate durante le comunicazioni e non vengono mai riusate (per la generazione della nuova chiave si usa il protocollo **TKIP**, Temporal Key Integrity Protocol). La master key è usata anche come password per autenticare la scheda di rete nel momento della sua associazione alla rete. Se l'Access Point è configurato per usare WPA tutte le schede e gli Access Point che si aggiungono alla rete ad infrastruttura devono essere in grado di usare WPA. Questa tecnica di autenticazione non necessita di server di autenticazione.
2. Basata su di un server di autenticazione
   Il server di autenticazione è un programma che gira su uno dei nodi della rete e che contiene il database delle password delle stazioni di rete. Tramite un preciso protocollo è possibile verificare la congruenza della password con l'utente che richiede di associarsi alla rete.
   Questa modalità di autenticazione è utile per la gestione centralizzata delle reti complesse, perché non c'è bisogno di configurare manualmente gli Access Point e le stazioni mobili.
   Il tipo di server usato solitamente negli A.P. wireless è "RADIUS".

In genere gli Access Point che supportano WPA possono anche funzionare in modo WEP, per compatibilità con il passato.
Esiste una versione aggiornata di WPA (WPA2).

RADIUS

Remote **A**uthentication **D**ial-**I**n **U**ser **S**ervice (RADIUS) è un protocollo Internet, normalizzato dalla RFC2138, ed è uno dei protocolli conformi allo standard 802.11i sui server di autenticazione per le reti wireless. 802.11i precede anche altri metodi di autenticazione.
Permette la centralizzazione dell'amministrazione degli utenti, facilitando la gestione delle reti con moltissimi utenti. A differenza di altri protocolli per server di autenticazione, come p.es. LDAP, è protetto specificamente contro lo sniffing, cosa che, come abbiamo visto, nelle reti wireless è molto importante.
Utilizza UDP, sulle porte 1812, per l'autenticazione e 1813, per l'accounting.
Il client RADIUS è a sua volta un "access server" ed è esso che comunica direttamente con l'utente (scheda di rete mobile):

- un Access Point wireless
- un server dial-up, che collega agli utenti i modem di un provider Internet
- un firewall, che filtra i pacchetti in una internet
- un router VPN (Virtual Private Network), che realizza con la crittografia una rete "privata" usando l'infrastruttura di una rete pubblica (vedi nel seguito).

Il client RADIUS ("access server") riceve richieste di autorizzazione da parte delle stazioni di rete e le inoltra al server RADIUS.
Il server autentica ed autorizza le richieste, essendo collegato ad un database di utenti e di politiche di accesso.
Le versioni server di Windows sono in grado di funzionare come server RADIUS, utilizzando il programma IAS (Internet Authentication Service), che si può configurare fra le funzioni di RRAS (**R**outing and **R**emote **A**ccess **S**ervices).
In alternativa si potrebbe usare con 802.11i il protocollo Kerberos.
Anche Linux è in grado di essere usato come server RADIUS.

War-Driving

!! TODO !!

Streaming di dati multimediali in tempo reale

Se si vuole trasmettere in wireless dati in tempo reale, si possono usare apparecchiature che supportino lo standard IEEE 802.11e ("Wireless Multimedia Enhancements"), che è stato sviluppato a questo proposito. Esso permette di ottenere QoS garantite ed assegnare ai dispositivi i parametri di QoS voluti.

1.9 IEEE 802.15 - Bluetooth

Le **WPAN** (**W**ireless **P**ersonal **A**rea **N**etwork) sono reti sviluppate per collegare dispositivi che risiedono sulla persona o nei suoi immediati dintorni. Le caratteristiche delle WPAN sono:

- campo d'azione ristretto
- bassa potenza
- basso costo
- reti con pochi nodi
- dispositivi piccoli

I protocolli WPAN sono sviluppati dal sottocomitato 15 del comitato 802 di IEEE.
Protocolli 802.15:

- 802.15.1 Bluetooth
- 802.15.2 Specifiche per la coesistenza "pacifica" fra reti 802.15 e 802.11
- 802.15.3 WPAN ad alta velocità
- 802.15.2 WPAN a bassa velocità

Bluetooth – 802.15.1

Bluetooth è un insieme di protocolli sviluppato inizialmente dalla azienda svedese Ericcson ed adottato successivamente da molte altre aziende, che hanno partecipato alla "Bluetooth Foundation", infine ratificato come standard internazionale come IEEE 802.15.1 (prima versione anno 2002).
Bluetooth prevede comunicazioni wireless a corta distanza (max 10 m), a velocità relativamente alta, almeno considerando i protocolli che esistevano in quel momento.
Dal livello fisico fino a LLC, Bluetooth e 802.15.1 sono praticamente identici.
Il protocollo, pubblicato come "Bluetooth Foundation Specifications" nel Luglio 1999, suscitò subito molto interesse per la sua flessibilità e semplicità d'uso, la velocità ottenibile e per la miniaturizzazione ed il basso costo della componentistica elettronica (l'obiettivo era la realizzazione di circuiti integrati che integrassero l'intero stack di protocolli Bluetooth al prezzo di 5 $).
La velocità di trasmissione lorda massima dei dispositivi Bluetooth è 1 Mbit/s, la velocità "netta" massima è di 721 kbit/s, con in più un canale "voce" da 64 kbit/s; pur non essendo velocità impressionanti, per i parametri di oggi, sono circa dieci volte la velocità di un collegamento ISDN.
Dunque un collegamento Bluetooth può supportare la trasmissione contemporanea di voce non compressa a 64 kbit/s e di dati, nella banda che resta.

La trasmissione avviene con portanti nella banda dei 2,4 GHz, che in Europa è "libera" e non richiede la concessione di licenze.
Con Bluetooth possono comunicare, senza necessità di aggiungere fili, i dispositivi della "casa automatica" (domotica) o i dispositivi di I/O con l'unità centrale di un computer (p.es. la stampante, il mouse od una fotocamera digitale).
Naturalmente chi ne beneficia di più sono i dispositivi mobili, come i notebook (computer portatili) od i PDA (**P**ersonal **D**igital **A**ssistant, detti anche "palmtop" o computer palmari, perchè stanno nel palmo di una mano).
Per esempio un PDA può trasmettere i file aggiornati quando si trova nelle vicinanze del computer che lo richiede, o collegarsi ad Internet o alla LAN tramite il computer "più vicino".
Bluetooth può consentire di integrare al meglio anche i computer ed i telefoni cellulari, che sempre più divengono terminali digitali portatili. Infatti i dispositivi nei quale Bluetooth è più usato sono i telefoni cellulari. Tipico è l'auricolare senza fili Bluetooth.
Altri dispositivi a basso costo ed a basso consumo adatti a Bluetooth possono essere: tessere di riconoscimento, identificazione biometrica (lettori di impronte digitali) giocattoli, sensori, telecomandi, "penne scanner", "borsellini elettronici".
E' in corso di sviluppo (2006) una nuova tecnologia per più alta velocità per 802.15.1 (20 Mbit/s o più) focalizzata sulla trasmissione di immagini e multimedia.

Struttura di una rete Bluetooth

Il MAC Bluetooth non è propriamente da rete locale, infatti esso è di tipo master – slave, con un nodo diverso dagli altri, a differenza dell'approccio peer to peer tenuto dalle altre LAN.
Piconet
Due o più dispositivi Bluetooth connessi formano una piccola rete wireless, chiamata "**piconet**". Una piconet viene controllata da uno suoi nodi, che assume la funzione di "master". Il master controlla gli altri nodi ("slave") ed il traffico della piconet. In una piconet possono essere attivi al massimo 7 slave contemporanei e possono essere gestiti più di 200 slave "dormienti".
Ogni piconet condivide la banda massima di 1 Mbit/s.
Scatternet
L'insieme di più piconet che abbiano raggio di copertura sovrapposto viene detto "**scatternet**". Tutti i nodi di una scatternet possono scambiarsi dati, passando per i relativi master. Ci possono essere fino a 10 piconet in una scatternet. Una radio (nodo della rete) può stare su più di una piconet.
Un dispositivo può fare da slave in più di una piconet di una scatternet ma può fare da master solo in una.

Livello fisico Bluetooth

La trasmissione è spread spectrum, di tipo frequency hopping, sono usati 79 canali di 1 MHz nella banda ISM da 2,402 GHz a 2,480 GHz, si effettuano 1600 cambi di frequenza (hop) al secondo, la modulazione è di tipo GFSK.
Ogni dispositivo in una singola piconet condivide la stessa sequenza di salti di frequenze. La sequenza viene decisa dal master della piconet e comunicata agli slave al momento della loro connessione.
Ogni piconet all'interno di una scatternet ha una sequenza diversa di salti di frequenze; in questo modo si distingue dalla altre.

Frame

In Bluetooth esistono molti formati di frame, distinti in base al fatto che trasportino i dati od informazioni di servizio, ed in base alla scelta di un collegamento connection oriented o connectionless. La massima lunghezza di un frame è 341 Byte.
E' possibile trasportare informazioni ridondanti per la rilevazione dell'errore. Gli algoritmi di rilevazione sono diversi in base al tipo di frame (CRC o "Forward error correction").

Collegamento con gli strati più alti degli stack di protocolli

"Host Controller Interface" (HCI) è uno strato di rete che permette agli strati superiori di trattare un dispositivo Bluetooth in modo analogo ad altri dispositivi semplici preesistenti. L'interfaccia di HCI è compatibile con USB, UART o RS-232. In pratica il dispositivo Bluetooth emula il comportamento di una UART o di una porta USB, in modo che si possano facilmente adattare i software preesistenti che lavorano su dispositivi USB o seriali.

Livello LLC e tipi di traffico

Sopra HCI c'è lo strato Logical Link Control and Adaptation Protocol (L2CAP), che fornisce i servizi tipici del livello di LLC, come il multiplexing dei collegamenti, la segmentazione e riassemblaggio dei pacchetti. I protocolli sopra ad L2CAP possono essere del tutto agnostici sulla conoscenza degli strati sottostanti.
Tramite L2CAP è possibile formare canali di trasmissione "end to end" fra dispositivi, infatti sono possibili trasferimenti di tipo connection oriented.
Questo livello di Bluetooth supporta la QoS, distinguendo fra i seguenti tipi di traffico, che devono essere specificati al momento del collegamento:

- polling based
  trasferimento di pacchetti su base regolare, con un periodo garantito di 0,625 ms
- Syncronous Connection Oriented (SCO)
  trasferimento a 64 kbit/s full duplex con latenza garantita, collegamento da nodo a nodo

- Asyncronous Connectionless Link (ACL)
  trasferimento best effort non affidabile, in broadcast a tutti i nodi appartenenti ad un gruppo, senza QoS, con pacchetti di dimensione variabile e velocità simmetrica o asimmetrica:
  - simmetrico: velocità max da 108,8 a 432,6 kbit/s
  - asimmetrico: velocità max 721 kbit/s downstream, 57,6 kbit/s upstream

Un master di una piconet può stabilire con uno slave fino a 3 collegamenti SCO e uno ACL.
Uno slave può fare tre collegamenti con lo stesso master, ma anche uno per uno con due master diversi, situandosi in questo modo su due diverse piconet contemporaneamente.
Un device Bluetooth può essere contemporaneamente un master in una piconet ed uno slave in un'altra.
Gli slave non possono comunicare fra loro, ma solo con i loro master.

Scoperta dei servizi (service discovery)
Un dispositivo che entri in rete può usare una funzione di scoperta dei servizi, realizzata tramite il protocollo SDP (Service Discovery Protocol). Dietro sua richiesta i nodi già connessi alla piconet dichiareranno quali servizi implementano ed il nodo "entrante" potrà sapere cosa potrà ottenere dagli altri nodi. Ogni servizio ha un codice univoco assegnato dallo standard (Universally Unique Identifier, UUID) ed esiste un metodo per creare UUID univoci.

Profili
Gli standard Bluetooth non riguardano solo il lato fisico o di trasporto, ma includono anche specifiche fino al livello applicazione. Infatti essi prevedono l'esistenza di "profili" che definiscono le caratteristiche del device.
Ogni profilo fa riferimento a protocolli di alto livello che rendono completo lo scambio di informazioni fra i due device.
Ogni device Bluetooth deve dichiarare di appartenere almeno ad un profilo.
Seguono alcuni esempi di profili esistenti.
Profilo di sincronizzazione
Usato per sincronizzare le modifiche fatte su un telefono od un PDA con il file di un computer. Gli strati più alti fanno uso dei protocolli di più alto livello di IrDA (vedi).
Profilo "cuffie"
Definisce un modo per scambiare un "audio stream", per esempio fra un telefono ed un auricolare. Si comanda con opportuni "comandi AT", come se si trattasse di un modem acustico.
Profilo "LAN access"
Fornisce al protocollo PPP gli strati "bassi", per collegare il dispositivo Bluetooth ad una LAN. Per un collegamento Internet od in rete locale, al disopra di PPP stanno i normali strati TCP/IP (vedi oltre).
Altri profili esistenti sono "Fax", "telefono cordless" ed altri ne vengono sviluppati quando servono.

Sicurezza Bluetooth
I nodi devono essere autenticati per entrare in una piconet, presentando una chiave di 128 bit. L'autenticazione è di tipo challenge – response.
I dati di tutti i payload sono crittati.
Ogni dispositivo deve essere inizializzato con un PIN unico la prima volta che entra in una piconet. Dal PIN viene generata la chiave a 128 bit da usare ogni volta che si entra nella rete (i dispositivi se la ricordano e la mandano in automatico!).
Il fatto che il campo d'azione di una rete Bluetooth sia di soli 10 m non è solo uno svantaggio; dato che stiamo trattando di PAN questa può essere considerata una caratteristica di sicurezza, dato che per entrare in una di queste reti bisogna esserle fisicamente vicini.
La sicurezza a basso livello di Bluetooth non è molto alta, sono stati riportati episodi di "rottura" delle reti. Per questo se si trasmettono dati confidenziali è raccomandato l'uso anche di altri schemi di sicurezza, da applicare a più alto livello.

1.10 802.15.3

Standard in corso di sviluppo (2005) che si propone di realizzare reti WPAN veloci, con gli obiettivi di:
- 100 Mbit/s entro 10 m
- 400 Mbit/s entro 5 m

Lo scopo è realizzare WPAN che trasmettano dati multimediali in tempo reale (audio, TV ..).

1.11 802.15.4

Le WPAN a bassa velocità puntano alla semplicità, al basso costo ed al basso consumo, le velocità vanno da 20 a 250 kbit/s. Come esempio si possono prendere le reti di sensori "intelligenti" wireless, bottoni della luce in camere d'albergo.
Il livello LLC è 802.2.
I nodi di questa rete sono di tipo "Full Functional Device", che si possono collegare fra loro con qualsiasi topologia, o di tipo "Reduced Functional Device", che possono costare meno e si possono solo collegare a stella ad un Full Functional Device.
E' impostabile una QoS, con tre tipi di traffico:
- Dati periodici: generati regolarmente con latenza non critica, es. polling di un sensore di temperatura
- Dati intermittenti: generati ogni tanto, con latenza non critica, es. bottoni della luce

- Dati ripetitivi a bassa latenza: generati regolarmente con necessità di bassa latenza, es. auricolari, mouse

1.12 Wireless MAN - WiMAX - IEEE 802.16

Questo standard è stato sviluppato come alternativa wireless alle tecnologie cablate di tipo XDSL, per il collegamento a larga banda su reti cittadine (MAN). La velocità massima è di 40 Mbit/s. E' pensato per funzionare con dispositivi fissi, portabili (che si spostano lentamente) ed eventualmente anche mobili (che si spostano velocemente). Con WiMax non c'è la necessità che le antenne siano in vista.
Come WiFi, la sigla WiMAX (**W**orldwide **I**nteroperability for **M**icroware **A**ccess) non sta ad indicare lo standard, ma piuttosto un consorzio[8] formato da Aziende interessate allo standard IEEE 802.16, che ha sviluppato un insieme di test che, se superato dalle apparecchiature di rete, ne garantiscono l'interoperabilità con altre apparecchiature a standard 802.16.
802.16 rispetto alle reti 802.11 ha il vantaggio di un campo di copertura molto più vasto, da 3 a 10 km, il che fa pensare che alcuni operatori potranno realizzare reti ad ampia copertura, metropolitana (MAN) o nazionale.

Livello fisico

Le frequenze di trasmissione di 802.16 sono nella banda da 10 a 66 GHz, mentre 802.16a ha aggiunto una banda da 2 a 11 GHz. Il metodo di modulazione di WiMAX si chiama OFDMA (**O**rthogonal **F**requency **D**ivision **M**ultiplexing **A**ccess).

MAC

Il livello MAC di 802.16 supporta livelli fisici diversi, si può quindi adattare più velocemente ai rapidi cambiamenti delle teconologie di rete.
Si tratta di un MAC in cui la "base station" (Access Point) distribuisce ai nodi di rete che si "abbonano" ("subscribers") un "time slot" ciascuno. Durante il "time slot" di un nodo, solo esso può trasmettere e gli altri devono stare ad aspettare il proprio turno. Il time slot delle stazioni può aumentare o diminuire in base alla "volontà" della base station, che è in grado in questo modo di gestire la qualità del servizio (QoS).

Livello LLC
IEEE 802.16 usa lo stesso livello LLC delle altre LAN, dato che impiega 802.2.

Sicurezza
La crittazione di 802.16 usa algoritmi di "strong encription" reputati più sicuri rispetto a quelli di 802.11.

2 Installazione di reti wireless

Il cablaggio degli Access Point è un normale cablaggio Ethernet, si deve eventualemente mettere in conto un collegamento POE, per evitare di portare l'alimentazione all'A.P. La localizzazione dell'A.P. È la cosa più critica della sua installazione. E' opportuno mettere l'Access Point in posizione baricentrica rispetto alle stazioni che deve servire, non necessariemento nel centro geometrico; se il grosso delle stazioni da servire sono vicine fra loro, sarà opportuno mettere l' A.P. più vicino a dov'è la maggior parte del nodi mobili. In questo modo la maggior parte delle stazioni potrà funzionare a velocità massima. Se in questo modo alcune stazioni saranno troppo lontane, si potrà aggiungere un range extender od in secondo A.P..
Inoltre bisogna fare in modo che in cui il percorso verso i NIC dei computer non sia ostruito, specie da materiali metallici (armadi metallici, armature nei muri di cemento armato). Essi infatti riflettono le onde elettromagnetiche e generano dei percorsi di ritorno del segnale (multipath signal) che causano interferenza. Più l'access point, od eventualmente solo la sua antenna, è in alto, meglio è: le ostruzioni saranno più improbabili.
Meglio tenere l'Access Point lontano da sorgenti di rumore elettrico o da alti campi elettrici o magnetici (case, alimentatore o monitor CRT di un computer, motori elettrici, "reattore" di lampade a fluorescenza). Trovare un buon posto anche per le antenne (se si possono staccare dalla scatola dell'Access Point) ed orientarle per ottenere il massimo campo nei punti ove necessita. Tenerle "lontano" dalla scatola dell'access point dovrebbe aiutare.
I muri di cemento e gli altri materiali densi tendono ad assorbire le onde radio più fortemente che non il legno, il cartongesso od i materiali sintetici. Tenere presente che alla massima velocità non si possono superare più di tre o quattro muri. Posizionare l'Access Point in modo che il percorso più breve verso le stazioni mobili passi perpendicolarmente attraverso i muri. Infatti se l'onda giunge al muro con un angolo molto diverso da 90°, esso può avere una larghezza "apparente", per l'onda, di decine di volte la sua larghezza reale.
Per coprire lunghe distanze si possono sostituire le antenne in dotazione all'Access Point con altre più direzionali (le antenne normali sono in genere omnidirezionali, mandano la loro radiazione in quantità uguale in ogni direzione e perciò possono raggiungere distanze inferiori, quando interessa raggiungere punti specifici).
Per queste cose è richiesta un po' di sperimentazione "sul campo". Si potrà ispezionare il sito d'interesse con un computer portatile. Il software di una scheda wireless installata nel portatile ci potrà dare un'indicazione sulla potenza del se-

8 WiMAX Forum

gnale ricevuto nei vari punti di interesse del nostro ambiente; potremo trovare punti in cui il segnale è debole o assente. In questo caso, se si può, cambieremo la posizione dell'Access Point o l'orientamento della sua antenna; se ciò non basterà potremo cambiare antenna od aggiungere un altro Access Point .
Su Internet si possono trovare "trucchi" sul posizionamento delle antenne e sulla loro autocostruzione con scatole di patatine o lattine di birra usate.
Nel caso dell'installazione di un Wireless Router con modem ADSL, nella sua localizzazione bisognerà tener conto che dovrà essere vicino alla presa telefonica.

2.1 IrDA

Raggi infarossi.
Non esiste un unico standard, link punto - punto.

2.2 DECT

Digital **E**nhanced **C**ordless **T**elecommunications (DECT) è uno standard che è stato sviluppato per i telefoni senza filo moderni (telefoni "cordless"). Questo sistema permette di avere più apparecchi in rete a condividere la stessa linea telefonica ed a parlare fra loro, in un uso da "interfono". E' inoltre possibile trasportare l'apparecchiatura anche in giro per la città ed ottenere la possibilità di telefonare anche da fuori di casa con lo stesso cordless.
Quest'ultima idea non ha però avuto sviluppi commerciali significativi, per l'alto costo dell'infrastruttura, che avrebbe richiesto l'installazione di migliaia di antenne nella città. Tali costi non sarebbero stati giustificabili, considerando che con la rete cellulare GSM era già esistente e forniva funzioni alnaloghe.

2.3 "HomeRF"

E' uno standard non molto usato, sviluppato per la casa ed il piccolo ufficio, che si basa su modulazioni "classiche" a divisione di tempo (TDMA) e la possibilità di riservare la banda ai flussi voce. Per la trasmissione della voce usa il protocollo di DECT. Lavora nelle stesse frequenze di Bluetooth e 802.11 (banda ISM).

Curiosità
Il nome Bluetooth deriva dal nomignolo di un famoso condottiero vichingo, Harald Blaatand re di Danimarca, evidentemente famoso anche per la sua scarsa igiene orale :-)