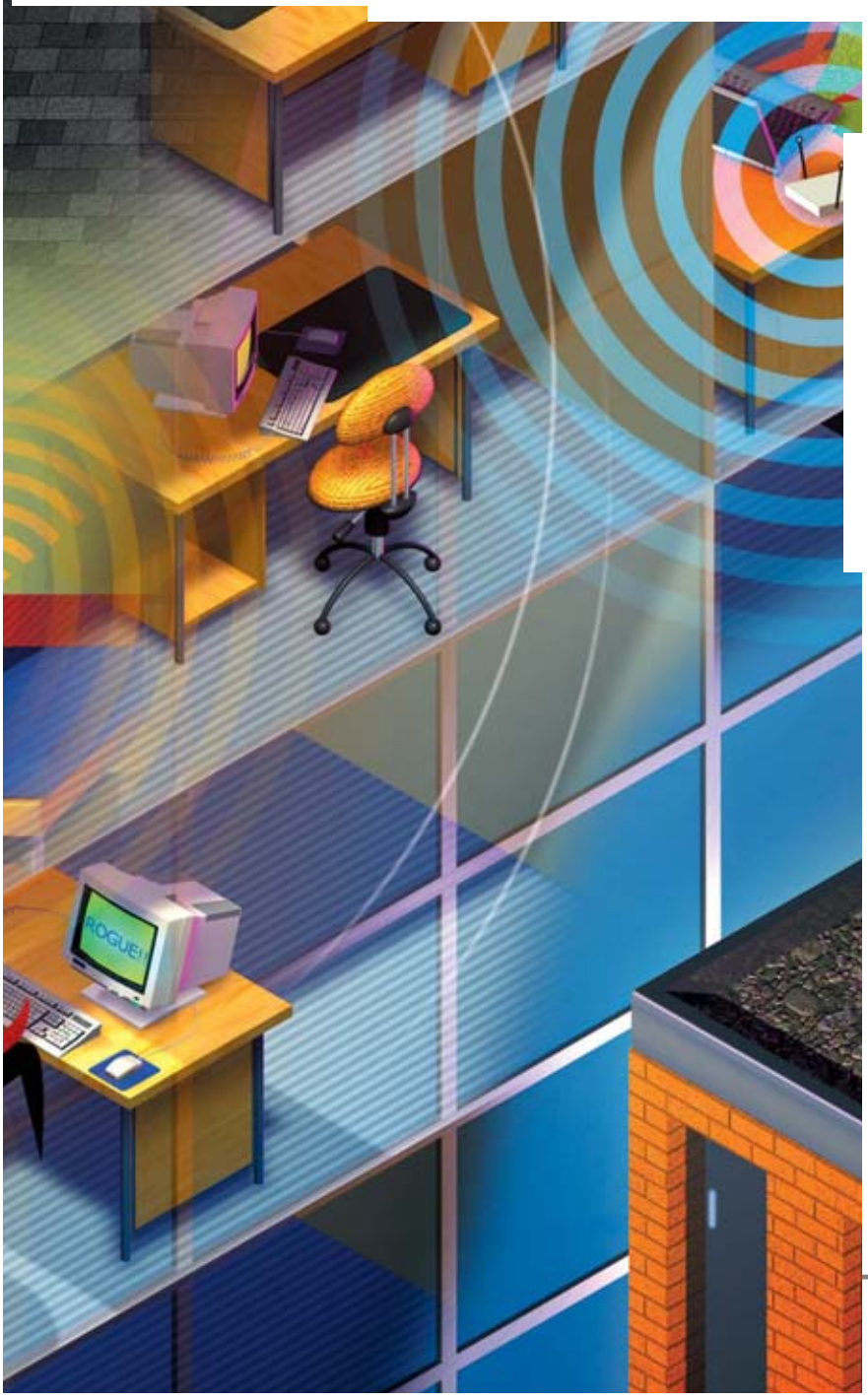
Reti locali senza fili: la guida essenziale



Le reti locali wireless hanno raggiunto il mercato di massa e continuano a crescere in prestazioni e sicurezza. Panoramica sulla tecnologia che ha sconvolto il concetto di connessione mobile.

A cura di Simone Zanardi

Le reti Wlan (*Wireless Local Area Network*, reti locali senza fili) non sono certo una novità di questi ultimi anni: il primo standard, l'IEEE 802.11, risale al 1997 e non fu accolto con eccessivi entusiasmi dal grande mercato. Lo scenario è cambiato radicalmente nel 2000, anno in cui la *Wireless Ethernet Compatibility Alliance* (Weca) ha lanciato il programma di certificazione Wi-Fi, atto a garantire l'interoperabilità dei dispositivi di produttori diversi. Questo passaggio, al pari del calo dei prezzi e dell'introduzione di standard più performanti, si è rivelato fondamentale per la diffusione su larga scala delle Wlan, che nel giro di pochi mesi hanno letteralmente rivoluzionato il concetto di connettività nei contesti domestici, aziendali e pubblici.

Una Wlan non raggiunge e probabilmente non raggiungerà mai le performance di un network cablato (attualmente la velocità su cavo in rame sfiora il Gigabit, contro picchi massimi teorici di 108 Mbps per le reti senza fili), ma il wireless ha ben altro da offrire: mobilità innanzitutto, ma anche costi di installazione ridotti e integrazione (tra personal computer, palmari, console da gioco). Tutto questo si traduce in una tecnologia vincente in ambito sia privato (la libertà dai cavi è irresistibile per gli utenti domestici) sia aziendale (la produttività può crescere considerevolmente grazie alla tecnologia Wlan).

Ecco quindi una panoramica su quello che il network wireless può fare per la vostra casa e il vostro ufficio, con una carrellata di prodotti per ogni esigenza e un occhio di riguardo a legislazione e problematiche di sicurezza.

Il wireless in casa

Spesso le esigenze di connettività domestica sono semplici: condividere un accesso Internet a banda larga tra un numero ridotto di Pc, accedere a un'unica stampante da ogni postazione, condividere file di piccole dimensioni e, per gli utenti più avanzati, distribuire contenuti multimediali da un server centrale.
La tecnologia wireless si sposa alla perfezione con queste applicazioni, portando in dote un valore aggiunto eccezionale: la mobilità. Inoltre, non richiede troppo tempo e denaro per l'installazione e la configurazione del sistema, evita l'annoso problema dei cablaggi di rete ed è la medesima utilizzata dai servizi di Hot Spot disponibili anche in Italia.
Il problema principale può paradossalmente risultare la quantità di prodotti wireless disponibili sul mercato e la conseguente difficoltà nell'operare delle scelte oculate. La ricompensa però può essere superiore alle aspettative: il wireless mostra il vero significato della parola portabilità, con i vantaggi e le comodità che ne derivano.
Al di là del fatto di essere relativamente facile da configurare, le reti wireless evitano di dover posare cavi tra le stanze di casa (una procedura spesso costosa e logisticamente complicata), estendono la copertura della rete a zone domestiche spesso sottovalutate, come la cucina, la lavanderia o il cortile, e permettono la connessione tra personal computer e dispositivi di elettronica di consumo e di intrattenimento. Molti nuovi prodotti consentono di connettere senza fili il sistema stereo e le console da gioco al Pc o a Internet, in modo da poter distribuire contenuti multimediali dal computer all'impianto audio/video.
La diffusione delle reti wireless domestiche è una evoluzione naturale dell'*home networking* in generale: l'installazione di reti nelle case dell'utenza privata è in continua crescita, con una forte percentuale di sistemi wireless, anche perché le realtà domestiche dove convivono due o più personal computer sono in costante aumento.
Mentre la tecnologia Ethernet è sulla breccia da ormai 30 anni, le reti wireless rimangono tutt'oggi una novità nel panorama del networking: il primo standard senza fili adottato su larga scala è in effetti l'802.11b, che è stato approvato dall'*Institute of Electrical and Electroincs Engineers* solo quattro anni

Gli standard di connessione per wireless Lan: presente e futuro

Standard	802.11b	802.11a	802.11g	802.11a/g	802.11n*
Primi prodotti distribuiti	Tardo 1999	Tardo 2001	Metà 2003**	Metà 2003	Inizio 2006
Attuale costo di un Access Point o router (euro Iva inclusa)	55-160	100-130	130-200	300	n.d.
Attuale costo di una PC Card (euro Iva inclusa)	30-90	100	80-130	100	n.d.
Frequenza (GHz)	2,4	5	2,4	2,4-5	n.d.
Throughput massimo teorico (Mbps)	11	54	54	54	320
Throughput effettivo da 6 a 18 metri (Mbps)***	4-6	15-20	15-20	15-20	n.d.
Portata massima in ambiente chiuso (metri)	45	23	45	45	n.d.
Tecnica di modulazione	Dsss	Ofdm	Ofdm	Ofdm	n.d.
Compatibilità	Con lo standard "g" se utilizzato in "mixed mode"	N.d. se non con chipset a doppio standard	Con lo standard "b" se utilizzato in "mixed mode"	I tre standard "a", "b" e "g" possono coesistere	n.d.
Numero massimo di utenti per AP (circa)	32	64	64	128	n.d.
Numero di canali radio non sovrapposti	3	12	3	16	
Utilizzo principale	Ambienti Soho e uffici, standard collaudato ed economico	Adottato soprattutto in ambiente aziendale: costi maggiori ma numero di canali disponibili più elevato e velocità superiore al "b"	Relativamente giovane ma in rapida diffusione sia nelle case che negli uffici e nelle aziende. Throughput elevato e retro compatibilità con le soluzioni "b"	Utile soprattutto in ambienti che privilegiano l'interoperabilità, anche se soprattutto qui in Europa, lo standard "a" risulta poco diffuso	Standard di prossima generazione in via di sviluppo per incrementare ulteriormente la velocità delle Wlan
Diffusione negli Hot Spot	Standard maggiormente diffuso	Non diffuso, soprattutto qui in Europa	Non ancora diffuso perché relativamente giovane	Non ancora diffuso	n.d.

* previsioni - ** prodotti aderenti al draft non definitivo - *** da test di laboratorio

Timeline delle wireless Lan

1942
Il pianista e compositore George Antheil e l'attrice Hedy Lamarr brevettano una tecnica di cifratura basata sul frequency hopping (salto di frequenze), in seguito chiamata tecnologia a spettro espanso. La donano quindi alla marina statunitense, che la classifica come di esclusivo uso militare ma la reputa inaffidabile per un utilizzo durante la Seconda guerra mondiale.

1958
La marina statunitense sviluppa il primo chip per le comunicazioni radio basato sulla tecnologia a spettro espanso.

1985
La marina statunitense declassa la tecnologia a spettro espanso, rendendola disponibile per gli utilizzi commerciali.

1989
La Ffc (Federal Communications Commission) autorizza l'utilizzo della tecnologia a spettro espanso su tre bande radio non licenziate.

1990
L'IEEE inizia a sviluppare standard per le connessioni senza fili nello spettro radio Ism (Industrial, Scientific and Medical) a 2,4 GHz.

1997
L'IEEE ratifica lo standard 802.11 come interfaccia su onde radio per la trasmissione tra client wireless e stazioni base. Non garantisce alcuna interoperabilità.

La Ffc aggiunge una quarta banda (5 GHz) al gruppo non licenziato per trasmissioni a spettro espanso.

1999
Settembre
L'IEEE ratifica gli standard 802.11b e 802.11a.

La Weca si organizza per certificare l'interoperabilità tra dispositivi IEEE 802.11, aprendo di fatto la porta a un'adozione globale di queste tecnologie.

Autunno
Sono distribuiti i primi prodotti IEEE 802.11b.

2000
Febbraio
Microsoft distribuisce Windows 2000, con supporto per le reti Wlan.

Marzo
La Weca lancia il programma di certificazione Wi-Fi per i prodotti che integrano la tecnologia IEEE 802.11b.

Dicembre
La Carlson Hotels Worldwide (proprietaria delle catene di hotel Country Inn & Suits, Radisson, Regent e International) annuncia i primi servizi wireless.

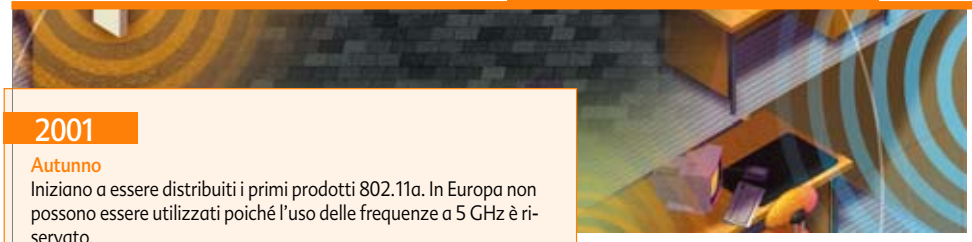
2001
Gennaio
Starbucks (nota catena alimentare americana) lancia gli hot spot wireless nei propri coffee shop.

Agosto
I ricercatori Scott Fluhrer, Itsik Mantin e Adi Shamir annunciano di aver rilevato fondamentali debolezze nel sistema di sicurezza Wep, utilizzato dai prodotti IEEE 802.11.

fa, nel 1999. A quell'epoca i dispositivi hardware per le connessioni wireless erano molto costosi e solo per le grandi aziende con budget adeguato ed esigenze impellenti poteva dirsi giustificato il passaggio alle wireless Lan. Un Access Point, o base station, che agisce da ponte tra le sezioni cablate e senza fili della Rete, costava quasi 1.000 euro, mentre le schede wireless per notebook si avvicinavano ai 300 euro. Confrontando i prezzi odierni (sotto i 75 euro per un Access Point basilare e circa 40 euro per una scheda IEEE 802.11b), è facile capire perché il wireless si stia diffondendo in questo ultimo biennio. Vi è poi da considerare che molti Pc portatili, anche modelli entry-level, possiedono già capacità wireless integrate (grazie alla tecnologia Intel Centrino ma non solo) e quindi non vi è necessità di acquistare un'ulteriore scheda Pc Card.

> La tecnologia: 802.11b, "a" e "g"

Al momento di scegliere i prodotti wireless da acquistare, è facile confondersi tra la miriade di sigle, lettere e numeri che identificano i vari protocolli della tecnologia; cerchiamo quindi di fare chiarezza sul panorama odierno.
Oggi esistono tre standard per reti locali senza fili approvati dall'IEEE; essi sono, in ordine cronologico, l'802.11b, l'802.11a e l'802.11g. Il primo, l'802.11b, è al momento il più diffuso e popolare: i dispositivi distribuiti dal 1999 nel mondo sono all'incirca 40 milioni. Le reti "b" operano nello spettro di frequenze a 2,4 GHz, che è condiviso da altre tecnologie senza licenza come i telefoni cordless e i forni a microonde (potenzialmente fonti di interferenze).
La portata effettiva dei prodotti "b" ammonta a circa 30-50 metri in un ambiente chiuso, mentre la velocità massima teorica è di 11 Megabit al secondo. In realtà il throughput massimo si attesta tra i 4 e i 6 Mbps, dal momento che la banda rimanente è generalmente occupata dall'overhead per l'elaborazione dei segnali radio e per i protocolli di rete impiegati. Benché si tratti di velocità sensibilmente superiori a quelle raggiunte da una connessione Adsl, e in ogni caso adeguate per la diffusione in streaming di tracce audio, lo standard 802.11b non è sufficiente per la trasmissione di video ad alta definizione e per le connessioni Internet su fibra ottica. Il suo principale vantaggio rimane quindi il basso costo dei dispositivi.
Nel tardo 2001, negli Stati Uniti iniziarono a essere distribuiti i prodotti basati su di un nuovo standard, l'802.11a. A differenza dei dispositivi di precedente generazione, i modelli 802.11a operano nello spettro dei 5 GHz (contro i 2,4 GHz delle bande Ism). La velocità teorica massima sale a 54 Mbps, e quella reale a circa 22 Mbps, mentre risulta ridotto il raggio di copertura (che scende a un massimo di 25 metri circa). Un vantaggio significativo dello standard "a" è il maggior numero di canali non sovrapposti disponibili, che permettono di implementare un numero più alto di Access Point in una data area per incrementare la capacità di connessione in contesti ad alta densità. Il limite principale è individuabile invece nell'utilizzo della banda a 5 GHz che, oltre a rendere i nuovi dispositivi incompatibili con quelli 802.11b, ne ha in passato bloccato la diffusione qui in Europa a causa di specifiche restrizioni sull'utilizzo di tale banda da parte di soggetti privati e commerciali.
L'802.11g è lo standard più recente, approvato dall'IEEE nel giugno del 2003. Opera nel medesimo spettro delle specifiche 802.11b (2,4 GHz) e risulta per questo pienamente compatibile con i prodotti di precedente generazione; la velocità massima teorica si attesta sui 54 Mbps, identica quindi a quella dello standard 802.11a, mentre il throguhput reale è generalmente compreso tra i 15 e i 20 Mbps. Il raggio di copertura è di 30-50 in un ambiente chiuso.
Nonostante la teorica incompatibilità, la diffusione di prodotti wireless che abbinano nel proprio chi-



2001

Autunno
Iniziano a essere distribuiti i primi prodotti 802.11a. In Europa non possono essere utilizzati poiché l'uso delle frequenze a 5 GHz è riservato.

2002

Maggio
La Ffc modifica alcune regole intenre aprendo la strada allo sviluppo dei dispositivi IEEE 802.11g.

Settembre
Lucent Technologies dimostra un handoff trasparente tra una rete Wi-Fi e una cellulari di terza generazione, permettendo agli utenti di passare tra le due senza interrompere le sessioni di collegamento Internet.

Ottobre
Weca diviene Wi-Fi Alliance, inizia il programma di certificazione per prodotti IEEE 802.11a e pubblica le specifiche Wpa per il rimpiazzo del vecchio Wep.

Sono distribuiti i primi prodotti 802.11a/b.

2003

Gennaio
La Wi-Fi Alliance lancia il programma Wi-Fi ZONE per certificare e marchiare gli hot spot di pubblico accesso, in modo analogo a quanto già fatto per i prodotti Wi-Fi.

Marzo
Intel introduce la tecnologia mobile Centrino

McDonald's introduce dieci hot spot nei suoi locali di Manhattan e promette di portare il numero a 300 entro la fine dell'anno.

Sono distribuiti i primi prodotti basati sulle specifiche provvisiorie IEEE 802.11g.

Aprile
La Wi-Fi Alliance certifica i primi prodotti Wpa, tra cui i chipset di Atheros, Broadcom, Cisco, Intel e altri.

Oltre 40 milioni di dipsositivi basati su standard IEEE 802.11 sono distribuiti a livello mondiale.

Compaiono i primi prodotti IEEE 802.11a/g (basati sul draft provvisorio g).

Maggio
Verizon Communications annuncia 150 cabine telefoniche Wi-Fi nell'area di Manhattan e ne promette 1.000 entro fine anno.

Giugno
L'IEEE approva in via definitiva lo standard 802.11g

Luglio
I prodotti IEEE 802.11g ricevono le prime certificazioni Wi-Fi.

Sono 865 i prodotti certificati Wi-Fi dal 2000, da 112 aziende.

Settembre
Lo standard di sicurezza Wpa diventa obbligatorio per la certificazione Wi-Fi.

2005

Stime conservative indicano che, al ritmo di adozione corrente, quasi mezzo miliardo di dispositivi IEEE 802.11 saranno venduti in un solo anno (tra cui access point, telefoni cellulari, desktop, lettori Dvd, lettori Mp3, schede di Rete, notebook, Pda, televisori e altri).

pset le capacità di trasmissione sia secondo lo standard 802.11g/b sia secondo quello 802.11a permette l'installazione di reti wireless a triplo standard.
In ogni caso, se si desidera ricorrere a una sola tecnologia, è indubbio che quella più indicata oggi sia la IEEE 802.11g: spesso i prodotti che la integrano costano poco più che quelli 802.11b e, grazie alla completa interoperabilità, la diffusione dello standard si sta rivelando rapida e indolore.

Per cominciare

Una rete wireless connessa a Internet richiede le seguenti componenti: un servizio di collegamento alla Rete (preferibilmente a banda larga), un modem, un router, un firewall, un Access Point wireless e un adattatore wireless per i propri Pc portatili (sia esso integrato nella macchina o in formato Pc Card) e desktop (in formato di scheda Pci o di adattatore esterno Usb). Alcune di queste funzioni possono essere integrate in un unico dispositivo.
Chi dispone di un contratto di accesso alla Rete è sicuramente già munito di modem, o acquistato o concesso in comodato d'uso dal proprio Internet Service Provider. Il problema può sorgere se si accede alla Rete con un unico personal computer: in questi casi infatti la tendenza è quella di utilizzare un modem con interfaccia Usb per il collegamento al Pc. Questo standard, che presenta indubbi vantaggi dal punto di vista della facilità di installazione e configurazione, mal si adatta alla condivisione dell'accesso su di una rete locale, sia essa wireless o cablata. Al contrario sono adatti i modem con interfaccia Ethernet, che si collegano al Pc o alla Rete utilizzando lo standard Lan più diffuso. Nell'ottica di creare una struttura wireless è indispensabile che il modem sia dotato di interfaccia Ethernet, e quindi se si dispone di un'unità Usb è purtroppo necessario procedere alla sostituzione.
Praticamente tutti i prodotti disponibili sul mercato supportano ormai gli standard di collegamento Adsl più diffusi. È comunque buona norma verificare al momento dell'acquisto la compatibilità con i protocolli utilizzati dal proprio contratto di connessione, tipicamente PPPoA, PPPoE o, più raramente, IPaA.

Gateway

Come accennato, esistono dispositivi che integrano in un'unica soluzione le funzioni necessarie a una rete locale wireless: si tratta dei cosiddetti residential gateway, unità che includono il modem, un router per la distribuzione dei pacchetti sulla rete locale, un punto di accesso wireless per il collegamento di terminali in modalità senza fili e persino dei servizi di firewall per la gestione della sicurezza sulla Lan.
Il vantaggio principale di questi apparecchi per le utenze domestiche è la necessità di configurare un unico dispositivo senza doversi preoccupare dell'interazione tra più unità. In questo modo la procedura di installazione risulta di gran lunga semplificata e più rapida, e si riducono i potenziali problemi di conflitto in fase di configurazione. D'altro canto l'integrazione in un unico dispositivo lega una tecnologia all'altra, obbligando in caso di upgrade verso un nuovo standard alla sostituzione dell'intero pacchetto.

Wireless Router

Se si dispone già di un modem Ethernet collegato a un unico Pc e si desidera installare una rete wireless, la soluzione ideale è quella di un router wireless. Essenzialmente si tratta di un dispositivo analogo al residential gateway appena trattato ma senza le funzioni di modem, che vengono demandate a un modulo esterno. In questo modo il router risulta indipendente dalla tecnologia di accesso adottata, e nel caso di un cambio di quest'ultima non è necessario sostituirlo. Spesso i router wireless integrano anche switch a 4 o più porte che consentono di colle-

Glossario

3g
Terza generazione di telefonia mobile. Succede, qui in Europa, alle generazioni Gsm e Gprs promettendo di incrementare la velocità di trasmissione fino alla soglia dei 2 Mbps e offrendo di conseguenza servizi evoluti. Il sistema adottato dal mercato europeo è l'Umts.

54g
Chipset di produzione Broadcom. I dispositivi che lo integrano sono compatibili con lo standard IEEE 802.11g o possono essere aggiornati in modo da diventarlo.

802.11a
Specifiche di trasmissione per wireless Lan standardizzate dall'IEEE. Lo standard "a" opera nell'intorno delle frequenze a 5 GHz e per questo non è compatibile con i dispositivi "b" e "g". Dotato di una velocità massima teorica di 54 Mbps, non si è diffuso in Europa a causa delle limitazioni legislative che impedivano l'utilizzo di tale banda.

802.11b
Seconda generazione delle specifiche per comunicazioni locali senza fili. Questo standard IEEE ha segnato la diffusione di massa della tecnologia Wlan, rendendo disponibili prodotti in grado di comunicare a buona velocità (11 Mbps massimi teorici) nello spettro dei 2,4 GHz.

802.11e
Standard proposto dall'IEEE per la definizione di meccanismi di Quality Of Service in ambito wireless.

802.11g
Evoluzione dello standard 802.11b, porta il throughput massimo teorico a 54 Mbps, pur mantenendo piena compatibilità con i prodotti di precedente generazione (opera a 2,4 GHz). Incompatibile con lo standard 802.11a.

802.11i
Standard proposto dall'IEEE per il rafforzamento dei meccanismi di sicurezza nelle wireless Lan. Tra le componenti di maggior rilievo vi sono Tkip, autenticazione 802.11x e Aes. L'approvazione definitiva dello standard è prevista per la metà del 2004.

802.11n
Standard proposto (approvazione definitiva prevista per il 2005 o 2006) per le reti Lan wireless di prossima generazione. Dovrebbe portare le velocità massime teoriche alla soglia dei 320 Mbps.

Access Point (Ap)
È il dispositivo che agisce da ponte tra una rete cablata e la sezione wireless. I prodotti presenti oggi sul mercato possono integrare le funzioni di punto di accesso con quelle di router.

Ad Hoc mode
Metodo di comunicazione peer-to-peer tramite cui i client wireless (Pc Card o adattatori per desktop) possono comunicare direttamente senza la necessità di un Access Point.

Aes (Advanced Encryption Standard)
Standard di codifica delle informazioni che utilizza chiavi di cifratura a 128, 192 e 256 bit. Rientra nelle specifiche IEEE 802.11i per la sicurezza delle comunicazioni senza fili.

Bluetooth
Tecnologia di trasmissione senza fili che opera nell'interno della frequenza 2,4 GHz. In grado di raggiungere tipicamente un throughput teorico di 720 Kbps e una copertura di 10 metri circa, si caratterizza per il basso consumo energetico che lo rende adatto alla comunicazione tra periferiche portatili.

Centrino
La nuova tecnologia mobile di Intel, che integra il processore Pentium M, il relativo chipset 855 e la sezione Intel PRO/Wireless 2100, dedicata alla trasmissione wireless secondo lo standard IEEE 802.11b. Solo i sistemi che includono tutti e tre questi componenti possono fregiarsi del logo Centrino.

Chiave condivisa
Una chiave di cifratura conosciuta solamente dal mittente e dal destinatario dei dati codificati.

Cifratura
Processo di codifica dei dati finalizzato a renderli inintelligibili se non dagli utenti autorizzati. Generalmente si utilizzano una o più chiavi di cifra per la codifica e decodifica dei dati.

Dhcp (Dynamic Host Configuration Protocol)
Protocollo utilizzato da router, gateway, o altri dispositivi di rete per assegnare in modo automatico e dinamico i parametri di connessione Tcp/Ip (tipicamente gli indirizzi di rete dei dispositivi).

Dsss (Direct Sequence Spread Spectrum)
Tecnologia di trasmissione a spettro espanso utilizzata per trasmettere dati tramite onde radio. Utilizzata dallo standard IEEE 802.11b, divide lo spettro a disposizione in più canali sovrapposti, in modo da ridurre i fenomeni di interferenza. Incompatibile con la trasmissione Fhss.

Eap (Extensible Authentication Protocol)
Un insieme di specifiche che permette agli adattatori wireless di comunicare con server di autenticazione come nel caso dei sistemi Radius. Le versioni più diffuse sono le Eap-Tls (*Eap-Transport Layer Security*), Eap-Ttls (*Eap-Tunnel Transport Layer Security*) e Peap (*Proteceted Eap*).

Essid (Extended Service Set Identifier)
Identificatore di una rete wireless. Si applica sia agli access point sia alle schede wireless ed è allegato a ogni pacchetto trasmesso sulla Wlan. In questo modo il punto di accesso può riconoscere e organizzare il traffico.

Fhss (Frequency Hopping Spread Spectrum)
Tecnologia di trasmissione a spettro espanso utilizzata per trasmettere dati tramite onde radio.
La trasmissione sfrutta delle frequenze adiacenti saltando da un canale all'altro secondo uno schema predefinito. È utilizzata dal protocollo Bluetooth, dai telefoni cordless e dai dispositivi IEEE 802.11 di prima generazione.

Gateway
In questo contesto, un dispositivo all-in-one che connette la rete locale wireless al mondo esterno attraverso Internet. Include perciò un modem, un router, un access point e, tipicamente, un firewall.

<segue>

Hot Spot
Un area pubblica o commerciale all'interno della quale è offerto un servizio wireless di accesso a Internet, sia in modo gratuito sia con tariffe orarie o giornaliere.

IEEE (Institute of Electrical and Electronical Engineers)
Organizzazione che studia, elabora e definisce standard informatici e di comunicazione, come nel caso della famiglia 802.11 dedicata alle wireless Lan.

Infrarosso (IR)
Una tecnologia wireless a corto raggio con una portata di circa 3 metri e una velocità di trasmissione teorica massima di 4 Mbps. Utilizzata principalmente per la sincronizzazione tra dispositivi palmari o telefoni cellulari, e personal computer.

Indirizzo IP
Un identificatore numerico per un dispositivo all'interno di una rete Tcp/Ip. Generalmente espresso da una stringa di quattro numeri decimali (ciascuno variabile da 0 a 255) divisi da punti.

Infrastructure mode
Metodo di connessione nel quale i client Pc Card comunicano con un punto di accesso.

Mac (Media Access Control)
Indirizzo fisico di un dispositivo hardware, applicato dal produttore. Identifica in modo univoco un dispositivo, come un adattatore wireless o un router, su di una rete locale, globale o wireless.

Nat (Network Address Translation)
Meccanismo di traduzione degli indirizzi che permette a una intera sezione di una rete di condividere un unico indirizzo Ip.

Ofdm (Orthogonal Frequency Division Multiplexing)
Tecnica di modulazione in cui il segnale radio è diviso in sottobande d frequenza multiple per trasmettere un numero superiore di dati. Gli standard 802.11a e 802.11 la utilizzano.

Preambolo
Un segnale preliminare che un dispositivo di rete trasmette per controllare la segnalazione sul network e la sincronizzazione tra gli elementi della Rete.

Prism Nitro
Tecnologia sviluppata da Intersil e basata sugli standard 802.11. I prodotti che la adottano mostrano un incremento di banda soprattutto se utilizzati in mixed mode (coabitazione con prodotti standard).

Radius (Remote Authentication Dial-In User Service)
Sistema di autenticazione e accounting che verifica le credenziali degli utenti e garantisce l'accesso alle risorse richieste.

Rc4
Algoritmo di cifratura sviluppato dai laboratori RSA. È costituito da un codice di flusso di byte pseudo-casuali ed è utilizzato da Wep e da altre forme di cifratura.

Roaming
In questo contesto, la capacità di spostarsi da un access point a un altro all'interno di una Wlan senza interruzioni di trasmissione.

Router
Dispositivo che unisce due reti distinte e inoltra i pacchetti dall'una all'altra. Un router utilizza protocolli di rete come l'Ip per indirizzare il flusso di informazioni proveniente e indirizzato alla rete di appartenenza. Molti router per la casa o il piccolo ufficio includono uno switch a più porte Ethernet, per la trasmissione dei dati tra elementi interni alla rete locale.

Spi (Stateful Packet Inspection)
Meccanismo di filtraggio utilizzato dai firewall per decidere quali dati lasciare circolare e quali bloccare. Analizza il contenuto dei pacchetti oltre che il loro header e, tenendo traccia dello stato della trasmissione possono individuare pacchetti non autorizzati con maggior efficacia.

Tkip (Temprary Key Integrity Protocol)
Protocollo di sicurezza facente parte delle specifiche IEEE 802.11i. Fornisce una ricombinazione di chiave per ogni pacchetto, un controllo sull'integrità dei messaggi, e un meccanismo di riassegnazione delle chiavi. Come componente dello standard Wpa, Tkip è progettato per superare i limiti di sicurezza del Wep.

UPnP (Universal Plug aNd Play)
Architettura che facilita le connessioni tra personal computer e altri dispositivi che utilizzano il protocollo Tcp/Ip e un derivato dell'Http. Permette ad ogni apparecchio di acquisire automaticamente un indirizzo di rete e di annunciare la propria presenza al network.

Weca
Vedi Wi-Fi Alliance.

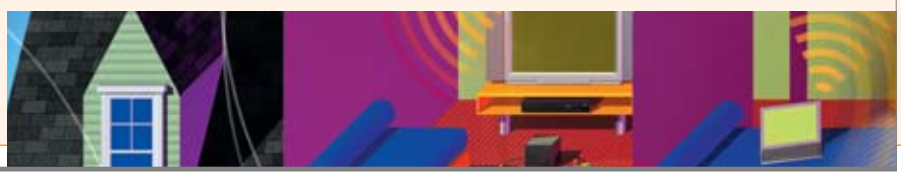
Wep (Wireless Equivalent Privacy)
Standard di sicurezza per le reti wireless. Ha mostrato nel corso degli anni delle pesanti debolezze, dovute in gran parte alla natura statica delle chiavi di cifra utilizzate.

Wi-Fi (Wireless Fidelity)
Programma di certificazione creato dalla Wi-Fi Alliance per assicurare l'interoperabilità tra prodotti IEEE 802.11. Solo i prodotti certificati possono adottare il logo Wi-Fi.

Wi-Fi Alliance
Associazione internazionale no-profit formata nel 1999 per certificare l'interoperabilità dei prodotti Wlan. Precedentemente conosciuta con il nome di Weca (*Wireless Ethernet Compatibility Alliance*), include ora 180 aziende aderenti.

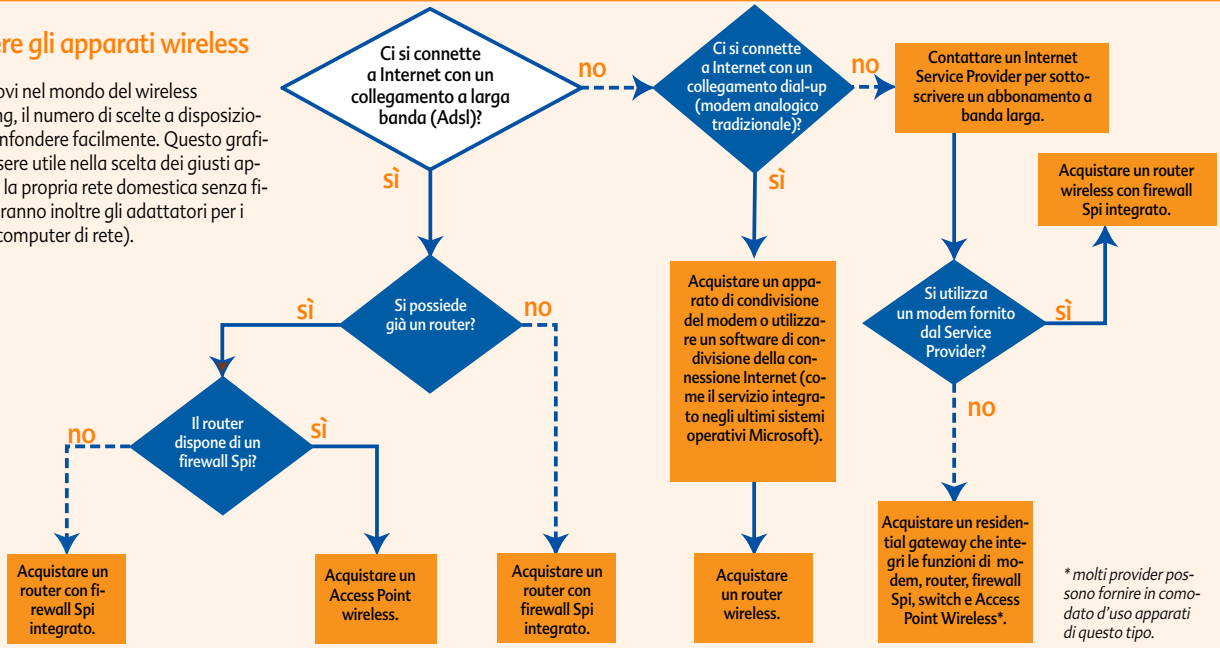
Wpa (Wireless Proteced Access)
Un sottoinsieme delle prossime specifiche IEEE 802.11i supportato dal mercato, che utilizza tra l'altro l'autenticazione 802.11x e il protocollo Tkip. Molti dispositivi hardware presenti sul mercato potranno essere aggiornati al Wpa tramite aggiornamento del firmware o del software di utilizzo.

Xpress
Una tecnologia sviluppata da Broadcom e basata sugli standard di mercato che si fonda sulle specifiche Wireless Multimedia Enhancements (Wme). Parte fondamentale delle specifiche provvisorie IEEE 802.11e. I prodotti che sfruttano questa tecnologia mostrano incrementi di throughput, soprattutto in modalità mixed mode (coabitazione con prodotti standard).



Scegliere gli apparati wireless

Se si è nuovi nel mondo del wireless networking, il numero di scelte a disposizione può confondere facilmente. Questo grafico può essere utile nella scelta dei giusti apparati per la propria rete domestica senza fili (occorreranno inoltre gli adattatori per i personal computer di rete).



** molti provider possono fornire in comodato d'uso apparati di questo tipo.*

gare altrettanti dispositivi cablati, oltre ai personal computer dotati di interfaccia wireless.
I router permettono di condividere il singolo indirizzo Ip fornito dall'Isp tra diversi computer sulla rete utilizzando un meccanismo chiamato Nat (*Network Address Translation*). Il Nat fornisce anche un primo strumento di sicurezza su Internet poiché è il router che assume l'indirizzo pubblico, assegnando esso stesso ai terminali locali degli indirizzi privati (statici o dinamici, nel caso sia supportato il servizio di Dhcp). Questi indirizzi privati non sono visibili su Internet. Per accrescere ulteriormente la sicurezza, è comunque bene assicurarsi che il router integri le funzioni di firewall, meglio se con tecnologia Spi (*Stateful Packet Inspection*).
Un firewall Spi analizza il contenuto di ogni pacchetto transitante, assicurandosi che corrisponda a specifiche richieste del sistema. Ai pacchetti indesiderati è quindi inibito l'accesso alla rete locale.

Access Point

Nel caso in cui si disponga già di una rete domestica perfettamente funzionante (comprensiva di modem, router e firewall), l'unico elemento aggiuntivo necessario per dotare la Lan di funzionalità wireless è un Access Point. Un Ap è poco più di una ricetrasmittente radio compatibile con lo standard wireless desiderato; il suo unico scopo è di agire da ponte tra il segmento di rete cablato e quello senza fili. Un punto di accesso deve essere collegato a una qualsiasi porta Rj-45 disponibile sul proprio router o switch, dopo di che è sufficiente completarne la configurazione con le impostazioni di sicurezza e di identificazione sulla Wlan e il gioco è fatto.

Equipaggiamento per desktop

Per collegare un personal computer desktop a una rete wireless sono disponibili due opzioni: la prima è una scheda Pci, ma per installarne una è necessario agire all'interno del telaio del Pc, operazione non complessa ma al di fuori dell'esperienza di una grande fetta di utenti. Inoltre, un adattatore di questo tipo obbliga generalmente l'antenna in una posizione (il retro del Pc) che spesso limita la capacità di ricezione e trasmissione, soprattutto se il telaio è posizionato sotto la scrivania o incassato in un mobile predisposto. Alcuni produttori offrono un'antenna esterna da posizionare sulla scrivania o comunque sopra il telaio: tale soluzione è sicuramente consigliabile, dal momento che ottimizza le capacità radio del dispositivo.
La seconda opzione è un adattatore Usb: l'installazione in questo caso richiede il semplice collegamento fisico a una porta disponibile sul Pc, mentre l'alimentazione è fornita direttamente dal bus. Grazie al supporto plug'n'play il dispositivo è riconosciuto automaticamente e si procede all'installazione dei driver forniti; l'intera procedura non dura che qualche minuto.
Oltre alla facilità d'installazione, uno dei più ovvi vantaggi di un adattatore Usb è la semplicità di posizionamento dell'unità e quindi dell'antenna, che è limitata solo

dalla lunghezza del cavo Usb (al massimo 5 metri per le specifiche dello standard). Inoltre lo stesso adattatore può essere utilizzato sia su di un computer desktop sia su di un portatile.
La grande maggioranza di adattatori Usb presenti sul mercato utilizzano la versione 1.1 dello standard, che fornisce una velocità di connessione paragonabili a quella dello standard IEEE 802.11b. Per questo motivo nel caso si opti per una rete wireless a 54 Mbps gli adattatori esterni da implementare sono di tipo Usb 2.0 (capaci di un massimo di 480 Mbps circa), in caso contrario il bus seriale costituirebbe un collo di bottiglia per la trasmissione dei dati.

Equipaggiamento per notebook

Molti notebook di ultima generazione (anche i modelli relativamente economici), si presentano equipaggiati con una scheda wireless mini Pci integrata. In particolare la tecnologia Intel Centrino ha di fatto reso la connettività wireless un elemento basilare per ogni Pc portatile. Prima di procedere all'acquisto è comunque bene tener presente che un notebook Centrino include il processore Pentium M, il chipset 855 e la scheda Intel PRO/Wireless 2100. Quest'ultima adotta lo standard 802.11b e non il più performante "g", sebbene Intel abbia promesso

Come installare una rete wireless domestica

Si possono distinguere diversi scenari per l'installazione di una rete wireless domestica, in base alla presenza o meno di altri dispositivi di rete come modem o router. In questa breve guida passo-passo prenderemo in considerazione il caso in cui sia già disponibile un accesso a banda larga (con un modem Adsl ad esempio) ma non un router, e per questo il personal computer collegato a Internet è agganciato direttamente al modem. Un'ulteriore ipotesi è che il modem sia di tipo Ethernet, ovvero collegato al Pc attraverso un normale cavo di rete; nel caso si disponga di un dispositivo Usb sarà invece necessario procedere all'acquisto di un nuovo modem o di un dispositivo che integri le funzioni di quest'ultimo al router.
Presupporremo inoltre che si voglia mantenere un desktop collegato al modem in modo cablato e installare un secondo Pc (desktop o notebook) con un collegamento senza fili. È sempre una buona idea mantenere un personal computer con connessione cablata alla rete, dal momento che in caso di problemi durante la fase di configurazione (ad esempio se si smarriscono le chiavi di cifratura wireless) è più semplice ripristinare i valori di default. Date queste premesse i dispositivi che sarà necessario acquistare sono un router wireless e una scheda client wireless (Pci o Usb per un desktop e Pc Card per un notebook).

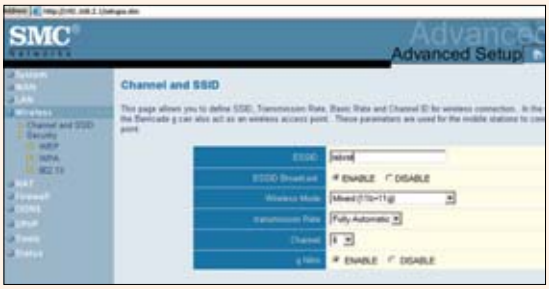
1 Connettere il router wireless

a. Spegnere il modem Adsl e il personal compuer già collegato.

b. Sganciare il cavo Ethernet dal modem e agganciarlo a una delle prese di rete Lan del router wireless. L'altro estremo del cavo deve rimanere collegato al personal computer.

c. Collegare un secondo cavo di rete (generalmente fornito con il router) tra il modem Ethernet e la porta Wan del router.

d. Accendere modem, router e Pc.



2 Configurare il router

a. Accedere al router tramite interfaccia Web, indicando nel browser del pc l'indirizzo del router e facendo comunque riferimento alla guida rapida inclusa nella confezione del router.

b. Per prima cosa cambiare la password di accesso al router: lasciare il valore di default può costituire una falla di sicurezza fondamentale.

c. Inserire i parametri del proprio accesso a Internet, forniti dal provider, nell'apposita sezione dell'interfaccia.

d. Abilitare le funzioni di sicurezza del punto di accesso. Le opzioni possono essere Wep e Wpa; in ogni caso sarà richiesto l'inserimento di una chiave di codifica. A seconda del tipo di interfaccia potrebbe essere necessario procedere nella sezione di impostazioni avanzate dell'interfaccia.

e. Cambiare l'Ssid, l'identificativo della rete wireless: in questo modo si rafforza la sicurezza di rete, dal momento che gli hackers spesso conoscono i valori di default assegnati dal produttore.

f. Se disponibile, abilitare e configurare il filtro sugli indirizzi fisici (Mac) dei client che si collegheranno al punto di accesso. In questo modo l'Access Point consentirà la trasmissione solo alle schede che si presentano con i giusti Mac.

<segue>

3 Installare una scheda Pci wireless in un Pc desktop

a. Fare riferimento alla guida rapida inclusa nella scheda. Se necessario, eseguire il programma software di installazione.

b. Spegnere il Pc.

c. Rimuovere le paratie del telaio.

d. Individuare uno slot Pci disponibile e rimuovere la corrispondente staffa sul pannello posteriore del telaio.

e. Indirizzare con cautela l'antenna attraverso lo slot aperto e inserire la scheda nello slot, assicurandola con una vite. Riapplicare le paratie.

f. Accendere il Pc. Il nuovo hardware dovrebbe essere riconosciuto e abilitato.

g. Accedere al pannello di controllo, quindi alla sezione rete e selezionare la connessione di rete wireless. Selezionando proprietà, selezionare il Ssid e impostare le chiavi di sicurezza in accordo con quanto fatto al punto 2.

4 Installare una scheda Pc Card wireless in un notebook

a. Seguire i passi "a" e "b" del punto 3.

b. Inserire la scheda wireless in uno slot disponibile sul notebook.

c. Seguire i passi "f" e "g" del punto 3.

un'evoluzione in questo senso per i prossimi mesi.
Per questo è possibile acquistare un personal computer portatile magari dotato del medesimo processore Pentium M ma con una card wireless più veloce, soluzione proposta da più di un produttore.
Per una disamina approfondita sui notebook Centrino vi rimandiamo alla comparativa comparsa sul numero 152 di Novembre di *PC Professionale*.
Se si desidera invece aggiornare il proprio notebook in modo da abilitarlo alle connessioni wireless, è possibile utilizzare, come già detto, un adattatore Usb; un dispositivo di questo tipo può però rivelarsi scomodo da trasportare in viaggio e una soluzione spesso più comoda è rappresentata da una scheda Pc Card che si può inserire nello slot Pcmcia sul lato del notebook.

> Il marchio Wi-Fi

Qualunque sia il dispositivo scelto, se si vuole essere sicuri che esso funzioni con modelli di produttori differenti è bene accertarsi che sia marchiato con il logo Wi-Fi.
Wi-Fi è l'acronimo di WIreless Fidelity: benché spesso questo termine sia utilizzato intendendo il wireless per reti locali in generale, in realtà Wi-Fi è un marchio registro dalla Wi-Fi Alliance (*www.wi-fi.org*), un'associazione no profit costituita nel 1999 per certificare l'interoperabilità di prodotti Wlan basati sulle specifiche 802.11.
La Wi-Fi Alliance utilizza una serie di test che ogni prodotto deve superare per ottenere la certificazione e il logo Wi-Fi. Esistono test per ogni standard wireless disponibile, così come per le specifiche di sicurezza Wpa. È consigliabile acquistare unicamente prodotti certificati Wi-Fi.

> Rendere il tutto operativo

Una volta che si dispone di tutto l'equipaggiamento necessario, è il momento di installare la rete wireless; sia che si utilizzi, in base alle proprie esigenze, un access point, un gateway o un router, la prima cosa da fare è individuare un punto strategico dove piazzare il dispositivo wireless in modo tale che l'antenna copra al meglio l'area interessata. Se l'appartamento è strutturato su due piani più un seminterrato e si desidera coprire tutti e tre i livelli, è consigliabile disporre il dispositivo al primo piano: per ragioni pratiche, la maggior parte degli utenti piazzano l'antenna nello stesso locale del modem Adsl. È inoltre opportuno assicurarsi che il dispositivo non sia nascosto da altri oggetti, e che l'antenna sia in posizione scoperta per un'efficienza ottimale.
Se nonostante questi accorgimenti non si riesce a ottenere la copertura voluta, può essere necessario installare un secondo Access Point per fornire connettività nelle zone più ostiche da raggiungere (come ad esempio un cortile) o per migliorare le performance in locali in cui il primo segnale risulti debole.

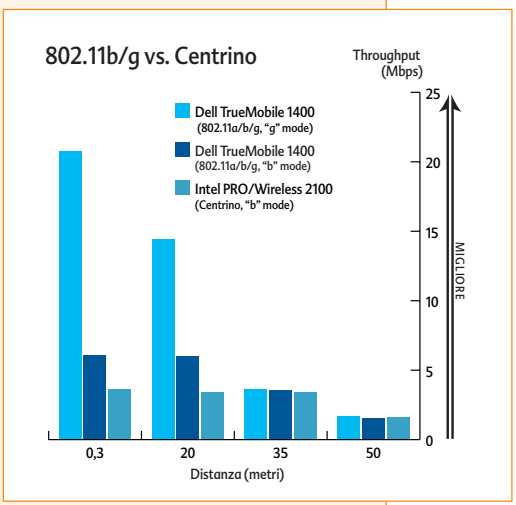
Per la grande maggioranza delle utenze domestiche può comunque essere sufficiente un unico AP.
Se la rete wireless è utilizzata per scopi tradizionali come la condivisione di accesso Internet e di una stampante, la tecnologia 802.11b può essere adeguata. Nei prossimi anni comunque le esigenze di banda per una rete domestica cresceranno fino a includere applicazioni come la diffusione di audio e video ad alta risoluzione. Per i fruitori di questi servizi è bene orientarsi fin d'ora verso le specifiche a 54 Mbps.

Installazione e sicurezza

Installare un sistema wireless poteva essere un'esperienza complicata fino a pochi anni fa, ma in questo ultimo periodo i produttori sono riusciti a semplificare le procedure in misura significativa. In effetti, molti dispositivi risultano perfettamente funzionanti subito dopo il collegamento hardware; la maggior parte dei modelli include inoltre un comodo wizard di configurazione che segue l'utente in tutti i passi necessari all'impostazione dei parametri di funzionamento necessari, a cui si aggiunge un supporto telefonico per qualsiasi problema.
Purtroppo però, per rendere l'installazione quanto più semplice possibile, molti produttori distribuiscono i propri dispositivi con le funzioni di sicurezza disattivate; in questo modo la rete risulta del tutto non protetta. Per evitare questi rischi i passaggi indispensabili sono perlomeno il cambio di Ssid (l'identificativo della rete) e della password di amministrazione, i cui valori di default sono ampiamente noti nelle comunità di hacker, oltre all'abilitazione del più alto livello di sicurezza previsto dai dispositivi. Il Wep (*Wireless Equivalent Privacy*) è al momento lo standard di sicurezza più diffuso, ma tutti i prodotti di prossima generazione implementeranno il più robusto Wpa.

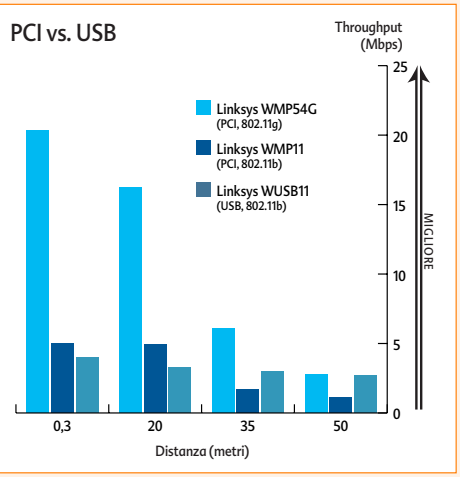
Centrino: le prestazioni wireless a confronto

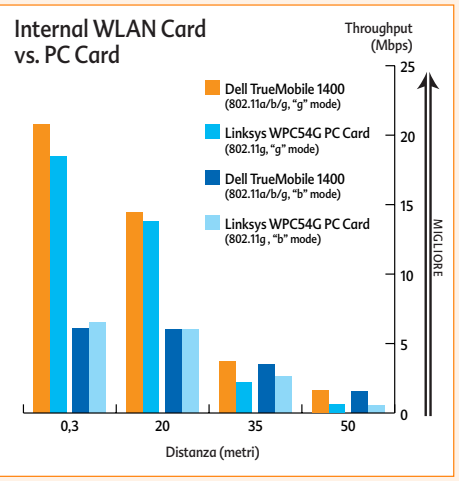
Quando Intel introdusse l'architettura Centrino in marzo, chiunque non fosse stato un addetto ai lavori o un appassionato di tecnologia avrebbe potuto pensare che questa tecnologia segnasse l'inizio della rivoluzione wireless. In realtà, benché Intel abbia fatto parecchio per promuovere il wireless nel mercato di massa, non si tratta certo del primo attore in questo segmento, e il suo prodotto non include l'ultima tecnologia disponibile, l'IEEE 802.11g, anche se l'azienda ha in programma di utilizzarla entro i prossimi mesi.
Per provare Centrino contro la concorrenza nel settore wireless, abbiamo utilizzato due notebook Dell Latitude X300, identici in tutto tranne che per la presenza delle due diverse schede mini Pci offerte da Dell: in un caso si tratta del modello Dell TrueMobile 1400 (una soluzione 802.11a/b/g che utilizza un chipset Broadcom), nell'altro dell'adattatore Intel PRO/Wireless 2100, il componente dell'attuale architettura Centrino che sfrutta lo standard IEEE 802.11b.
I test riguardanti il TrueMobile 1400 sono stati eseguiti in modalità sia "g" che "b": a distanze variabili dai 30 centimetri ai 20 metri il throughput misurato nella modalità "g" è risultato più del doppio di quello relativo alla modalità "b", mentre a circa 50 metri il segnale è sceso a livelli tali da livellare le prestazioni di tutte le configurazioni di prova.
Anche se Centrino ha ottenuto un segnale utilizzabile lungo tutto l'intervallo di distanze utilizzate per il test, la soluzione TrueMobile 1400 (anche in modalità "b") ha mostrato in ogni caso un throughput o eguale o maggiore, con una differenza più significativa nell'intervallo tra i 30 centimetri e i 20 metri.
La tecnologia Intel, comunque, è ancora nella sua prima generazione e come tutte le prime versioni necessita ancora di perfezionamenti.
Chi fosse interessato ad acquistare un notebook con capacità wireless integrate dovrebbe tenere in considerazione le performance delle comunicazioni senza fili, dal momento che in questo momento non esistono soluzioni comode per un aggiornamento interno successivo. Intel prevede di offrire supporto per la tecnologia 802.11g nelle versioni future di Centrino, ma per il momento le soluzioni concorrenti 802.11g a 54 Mbps sono indubbiamente più performanti e comunque retrocompatibili.
Tutti i test sono stati eseguiti in un area libera da interferenze radio e utilizzando un router Linksys WRT54G sia per le prove in modalità "b" che per quelle in modalità "g".
Per una disamina approfondita sui notebook Centrino vi rimandiamo alla comparativa comparsa sul numero 152 di Novembre di *PC Professionale*.

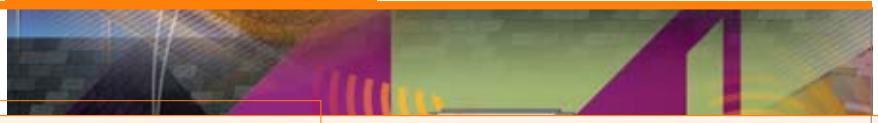


Client wireless: le opzioni

Per gli utenti di desktop che desiderino collegare il proprio personal computer alla Rete in modalità wireless esistono due opzioni: le schede Pci e gli adattatori Usb. Per quanto riguarda i notebook le alternative principali sono una scheda interna o una PC Card.
Il principale vantaggio degli adattatori Usb è che possono essere installati con facilità su qualsiasi desktop o notebook con una porta Usb disponibile. Il posizionamento dell'adattatore è inoltre più flessibile che nel caso di una scheda Pci, potendo piazzare l'antenna sopra il telaio o la scrivania in modo da evitare le interferenze e i blocchi di segnale provocati dal metallo del case. Durante i test di laboratorio l'adattatore Linksys WUSB11 ha surclassato la scheda Pci in modalità "b" a distanza tra i 35 e i 50 metri.
Nel caso di utilizzo dello standard IEEE 802.11g è indispensabile che l'adattatore utilizzi la versione 2.0 delle specifiche Usb, dal momento che solo con l'incremento di velocità da esse apportate al bus (480 Mbps teorici contro gli 11 della versione 1.1) è possibile evitare dei colli di bottiglia per la trasmissione wireless. Da notare inoltre che se l'adattatore wireless è agganciato ad un hub, le prestazioni possono risultare inferiori poiché tutti i dispositivi sul replicatore di porte condividono la medesima banda
Se si è abituati ad aprire il telaio del proprio personal computer, una scheda wireless Pci può essere un'alternativa. Una soluzione di questo tipo è in ogni caso consigliabile solo se l'Access Point è relativamente vicino, come si evince anche dai risultati dei test, nei quali la scheda interna ha mostrato performance migliori dell'apparato Usb (in modalità sia "b" che "g") nell'intervallo dai 30 centimetri ai 20 metri). Lo svantaggio principale delle schede Pci rimane comunque la maggior difficoltà dell'installazione.
Per quanto riguarda i notebook, tutto dipende se al momento dell'acquisto si decide per un modello che integra le funzionalità wireless o si preferisce attendere per un upgrade futuro. Anche in questo caso esistono pro e contro. Aggiornare un dispositivo wireless interno può essere complicato, così se si opta per la soluzione integrata é meglio fin d'ora indirizzarsi verso lo standard "g". D'altro canto, una scheda Pc Card può essere acquistata a prezzi ormai ragionevoli, e l'installazione è sicuramente più semplice.
La maggior parte delle schede PC Card dispongono di sezioni che rimangono all'esterno del profilo del notebook, e alcune utilizzano antenne esterne per migliorare la ricezione. Dal momento che una scheda PC Card è generalmente dotata di una sola antenna, è spesso soggetta a fluttuazioni di segnale quando si allontana il portatile dall'Access Point. Come mostrato dai risultati dei test, la soluzione interna (la Dell TrueMobile 1400) ha superato in prestazioni la scheda Pc Card in quasi tutto l'intervallo di distanze. Questo è in parte dovuto allo sviluppo dell'antenna interna portaato a termine dal produttore del notebook, che ha potuto così ottimizzarne la trasmissione e ricezione, e in parte al fatto che si tratta di apparati doppi contro le singole antenne delle schede Pc Card.







Access Point e router wireless per il Soho

Di seguito riportiamo alcuni esempi di router e Access Point conformi alle specifiche IEEE 802.11b e 802.11g. Alcuni prodotti "g" sono stati introdotti sul mercato prima della ratifica delle specifiche definitive nel giugno del 2003 e sono quindi stati definiti come compatibili con lo standard draft provvisorio. Ognuno di questi dispositivi supporta comunque oggi le specifiche definitive.
Vi rimandiamo inoltre alla sezione *First Looks* di *PC Professionale* per la prova dei primi prodotti in grado di raggiungere velocità massime teoriche di 100 Mbps.

D-Link AirPlus Xtreme G DI-624

Euro 220,00 Iva inclusa
Voto: 3/5: ●●●○○
www.dlink.com

Il router wireless è semplice da installare e configurare e dispone di una buona serie di funzioni per le applicazioni domestiche e del piccolo ufficio. La gestione da remoto e le statistiche sul traffico vanno oltre le consuete caratteristiche di questo genere di prodotti. D-Link ha aggiunto una modalità "g" pura per ottimizzare le prestazioni in ambiti con alte densità di client.

Prestazioni in modalità 802.11g (Mbps)
0,3 metri: 16.0
20 metri: 10.2
35 metri: 0
50 metri: 0

Linksys Wireless-G WRT54G

Euro 160,00 Iva inclusa
Voto: 4/5 ●●●●○
www.linksys.com

Il Linksys WRT54G fornisce un buonissimo throughput a 0,3 e 20 metri in modalità "g" pura. La sua interfaccia rimane pressoché la stessa dei precedenti modelli e l'utility di setup inclusa rende l'installazione e la configurazione molto semplici.

Prestazioni in modalità 802.11g (Mbps)
0,3 metri: 21.0
20 metri: 15.5
35 metri: 1.3
50 metri: 0

Netgear WG602

Euro 167,00 Iva inclusa
Voto: 4/5 ●●●●○
www.netgear.com

Se si approccia per la prima volta il mercato del wireless e si è alla ricerca di un semplice Access Point, il modello Netgear può essere la soluzione ideale. Il prezzo è molto competitivo e il dispositivo offre notevoli funzionalità di sicurezza, anche se con prestazioni solo nella media. Da sottolineare in modo particolare l'intuitivo software di installazione e configurazione.

Prestazioni in modalità 802.11g (Mbps)
0,3 metri: 15.3
20 metri: 13.7
35 metri: 0
50 metri: 0

SMC Barricade g SMC2804WBR

Euro 138,00 Iva inclusa
Voto: 4/5 ●●●●○
www.smc.com

Questo router wireless include molte caratteristiche appropriate per il piccolo e medio ufficio pur presentandosi come un dispositivo per gli ambienti domestici. La sicurezza può essere gestita attraverso il protocollo di autenticazione IEEE 802.11x con un server esterno Radius.
Per espandere l'area di copertura, è possibile amplificare la potenza del segnale trasmesso grazie a un'antenna ad alto guadagno venduta separatamente.

Prestazioni in modalità 802.11g (Mbps)
0,3 metri: 20.0
20 metri: 13.6
35 metri: 2.8
50 metri: 0.5

Linksys WAP11

Euro 105,00 Iva inclusa
Voto: 3/5 ●●●○○
www.linksys.com

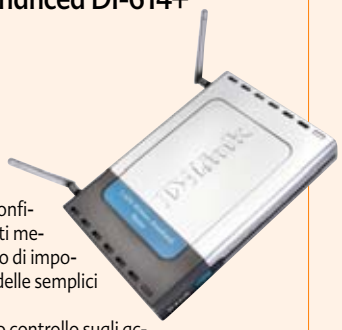
Il termine venerabile può essere giustamente accostato al Linksys WAP11, dal momento che quella odierna è ormai la terza versione di questo popolare Access Point. È indicato in particolar modo ai novizi del networking wireless che necessitano solo di un punto di accesso da collegare a un router preesistente. L'installazione è semplice e intuitiva, così come l'interfaccia di navigazione basata su pagine Web.

Prestazioni in modalità 802.11b (Mbps)
0,3 metri: 4.9
20 metri: 4.7
35 metri: 2.1
50 metri: 0

<segue>

D-Link AIrPlus Enhanced DI-614+

Euro 161,00 Iva inclusa
Voto: 4/5 ●●●●○
www.dlink.com



Il broadband router con funzionalità wireless Airplus DI-614+ è fornito con un'intuitiva interfaccia di configurazione adatta agli utenti meno esperti e un gran numero di impostazioni che vanno al di là delle semplici funzioni di base.
Offre inoltre il più avanzato controllo sugli accessi di tutti i prodotti Soho provati, inclusi i filtri sugli indirizzi Mac, su quelli Ip, oltre al blocco degli Url in base a parole chiave o dominio.

Prestazioni in modalità 802.11b (Mbps)
0,3 metri: 5.8
20 metri: 6.4
35 metri: 3.7
50 metri: 1.5

Netgear ME102

Euro 119,00 Iva inclusa
Voto: 3/5 ●●●○○
www.netgear.com

Prestazioni in modalità 802.11b (Mbps)
0,3 metri: 4.5
20 metri: 4.2
35 metri: 1.8
50 metri: 0.4

Il Netgear ME102 è un altro Acces Point senza fronzoli per la casa e il piccolo ufficio, ma può anche essere utilizzato come ponte wireless per collegare una rete cablata con una zona senza fili. L'unità non dispone di un'interfaccia basata su pagine Web, ma il software di gestione attraverso porta Usb permette di configurare l'unità direttamente da Pc.

Zyxel ZyAIR B-2000

Euro 349,00 Iva inclusa
Voto: 4/5 ●●●●○
www.zyxel.com

Prestazioni in modalità 802.11b (Mbps)
0,3 metri: 4.6
20 metri: 4.5
35 metri: 2.0
50 metri: 0

Lo ZyXel ZyAIR B-2000 offre il miglior pacchetto di sicurezza di tutti i dispositivi Soho provati. Un server di autenticazione IEEE 802.11x per 32 utenti, installazione semplificata, buon throughput e un prezzo ragionevole fanno di questo prodotto una soluzione difficile da battere.

L'ufficio senza fili

Le aziende e gli uffici di qualunque settore possono trovare ragioni impellenti per installare una rete wireless come parte della propria struttura IT. Il beneficio maggiore è indubbiamente l'accresciuta produttività dei dipendenti: con un accesso senza fili alle informazioni aziendali, oltre che all'e-mail, Instant Messaging e Internet, i lavoratori possono rimanere produttivi e disponibili anche quando sono occupati in meeting e lontani dalla propria scrivania. Questa maggior accessibilità alle informazioni è anche sinonimo di migliori e più numerose collaborazioni.
Inoltre vi è un fattore di riduzione dei costi: la maggior parte dei notebook di classe corporate di ultima generazione dispone di adattatori wireless integrati, e le schede wireless per portatili più vecchi sono ormai disponibili a cifre inferiori ai 40 euro. In un nuovo spazio di lavoro si possono risparmiare migliaia di euro collegando in rete i client con la teconologia senza fili piuttosto che cablare ogni ufficio e scrivania.
I dipendenti che hanno già sperimentato i benefici del wireless networking a casa sono i primi a sentire il bisogno degli stessi vantaggi sul lavoro; se l'azienda non li accontenta, qualcuno potrebbe addirittura provvedere a installare a proprie spese un piccolo access point nella rete aziendale, creando così una rete senza fili dipartimentale. Questa soluzione, a prima vista innocua, può però creare gravi brecce nel sistema di sicurezza informatica aziendale. In quest'ottica è molto meglio rispondere alle esigenze con una struttura wireless aziendale controllata.
Gli amministratori di rete e i manager IT che devono installare una rete wireless si trovano spesso di fronte a problematiche molto diverse da quelle associate alle reti cablate, o anche alle strutture senza fili domestiche: sicuramente il problema principale è relativo alla sicurezza di rete, ma bisogna anche badare a quali standard tecnologici adottare, a come pianificare la copertura del segnale radio, a come monitorare le prestazioni della rete. Infine, la rete wireless deve essere affidabile, scalabile e totalmente gestibile.

802a, b, g

Uno degli aspetti più delicati in fase di progettazione di una rete wireless aziendale è indubbiamente la scelta della tecnologia migliore. Con la ratifica (a giugno di quest'anno) delle specifiche IEEE 802.11g definitive, si aggiunge una concreta alternativa a quelle già disponibili.
Come si è accennato in precedenza, i dispositivi 802.11g operano nel medesimo campo di frequenza di quelli di precedente generazione (2,4 GHz come l'802.11b), ma a una velocità significativamente superiore, 54 Mbps contro 11 Mbps. Inoltre, lo standard "g" fornisce la garanzia di compatibilità con i dispositivi 802.11b, e dispone di una comunicazione nel cosiddetto "mixed mode" che permette la creazione di reti ibride.
Quest'ultima caratteristica costituisce un aspetto molto allettante per le organizzazioni che hanno già investito risorse e denaro in una rete Wi-Fi 802.11b, poiché esse possono gradualmente aggiungere apparati a 54 Mbps alla struttura già presente. In ogni caso, le aziende che combinano i due standard devono ricordare che quando si opera nel "mixed

Tablet: il massimo dei wireless Pc

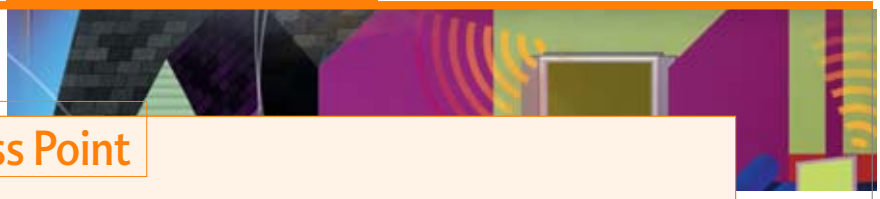
Per oltre tre decenni, la visione della "tavoletta digitale", in grado di riconoscere e registrare la scrittura a mano e (più recentemente) la voce umana, è sempre apparsa in anticipo di 5 o 10 anni sui tempi. Ma forse questo è il momento buono. I produttori hanno imparato che per assicurare un'accoglienza su vasta scala la connettività wireless (sia locale che su area estesa) è cruciale, così come l'impiego di Cpu più potenti ed efficienti dal punto di vista dell'autonomia.
Due generi di tablet Pc sono oggi disponibili sul mercato: i tablet puri (sotto 1,5 kg), privi di tastiera e utilizzati soprattutto in mercati verticali e come aggiunta a un Pc standard, e i dispositivi convertibili. Questi ultimi hanno in configurazione standard la stessa struttura di un comune notebook, ma grazie alla capacità di rotazione il display può adattarsi in modo da nascondere la tastiera rimanendo accessibile anche quando ripiegato. In ogni caso la dotazione di connettività wireless rimane l'elemento chiave per l'efficienza di questi dispositivi. In Italia sono disponibili modelli di Tablet Pc prodotti da Acer, Fujitsu Siemens, Nec, Hp, Toshiba, ViewSonic, con caratteristiche diverse ma tutti dotati di connessioni wireless.

mode", le performance degli apparecchi 802.11g possono ridursi fino a tornare a livelli paragonabili a quelle delle specifiche "b". Nuove tecnologie introdotte recentemente sul mercato all'interno dei prodotti 802.11g, e basate sui chipset wireless di Broadcom e Intersil, possono ridurre questo problema (si vedano a tal proposito le definizioni di *Prism Nitro* e *Xpress* nel glossario). In aggiunta, sono disponibili aggiornamenti firmware per i prodotti distribuiti sul mercato in precedenza.

In effetti i test di laboratorio hanno evidenziato un raddoppio di prestazioni nel "mixed mode" da parte di dispositivi con queste tecnologie, anche se non si raggiungono i dati nominali dichiarati dai produttori.
La terza opzione, IEEE 802.11a, raggiunge velocità massime teoriche di 54 Mbps, proprio come l'802.11g. Anche se i dispositivi 802.11b/g hanno generalmente un raggio di copertura maggiore rispetto a quelli aderenti allo standard "a", il numero di canali non sovrapposti disponibili depone a favore di quest'ultimo standard: operando in un intorno di frequenze più ampie (centrato a circa 5 GHz), le specifiche "a" possono contare su almeno 12 canali indipendenti (il numero esatto dipende dalle tecniche di modulazione e dalla divisione di spettro adottata dai singoli produttori), contro i soli 3 dello spettro a 2,4 GHz utilizzato dagli standard "b" e "g".
Tutto ciò implica un grande vantaggio per i contesti ad alta densità dove è necessario piazzare un numero

Wireless Lan: il punto sulla legislazione

Le comunicazioni tramite onde radio sono da sempre caratterizzate da problematiche peculiari quali l'assegnazione del piano di frequenza per la trasmissione e la regolarizzazione, dal punto di vista legislativo, delle norme da rispettare in termini di potenze emesse e regolarità degli impianti.
Le reti locali senza fili non sono da meno, e lo sviluppo e la diffusione della tecnologia Wlan sono stati fortemente condizionati negli anni passati dalla legislazione italiana.
Va premesso che quanto segue si riferisce alle comunicazioni wireless o per la fornitura di servizi pubblici (Hot Spot e Internet Service) o comunque in un ambito che coinvolga strutture pubbliche (come nel caso di due uffici che vogliano essere posti in collegamento wireless attraversando una strada), mentre l'impiego in contesti strettamente privati è del tutto consentito.
Fino al 31 dicembre 2001 la normativa italiana riguardante la costituzione e la manutenzione di una rete locale funzionante tramite onde radio consentiva la creazione di un network unicamente all'interno di un fondo (edificio, cortile, giardino) di proprietà. Le cose si complicavano nel caso si volesse realizzare una connessione tra due fondi divisi da una porzione di suolo pubblico o comunque non di proprietà: in questi casi era necessario richiedere la concessione della frequenza (richiesta che spesso veniva respinta). Era infine vietato l'allacciamento alla rete pubblica e questo in pratica impediva l'utilizzo della tecnologia wireless per la fornitura di accesso a Internet o alla linea telefonica. Anche l'installazione della rete era riservata ad aziende in possesso di certificazioni ministeriali.
La normativa è cambiata con il decreto del Presidente della Repubblica 5 ottobre 2001 n. 447 (in vigore dall'1 gennaio 2002) che opera delle modifiche sostanziali in direzione di una liberalizzazione del settore.
In primo luogo l'installazione e l'utilizzo di reti locali basate su tecnologie wireless, radio o ponti ottici è totalmente di libero uso all'interno del proprio fondo: non è necessario quindi richiedere alcuna autorizzazione e non sono previste imposte.
Per quanto riguarda gli impianti che esulano dal fondo di proprietà, bisogna richiedere la cosiddetta Autorizzazione Generale: il soggetto richiedente deve allegare alla domanda il progetto tecnico dell'impianto che intende costituire oltre che alcune dichiarazioni e attestati formali.
Esistono infine restrizioni per la gestione di sistemi di Voice Over Ip: l'utilizzo di strutture wireless limita queste trasmissioni all'ambito privato, ovvero è impedita la vendita di traffico VoIP veicolato tramite collegamenti senza fili. Questo per garantire un regime di corretta concorrenza nei confronti dei fornitori di servizi di telefonia mobile di terza generazione.
Il quadro si è ulteriormente evoluto il 28 maggio 2003 con l'approvazione, da parte del ministero delle Comunicazioni, del regolamento atto a disciplinare l'utilizzo delle cosiddette Radio Lan in contesti pubblici. Il risultato normativo più evidente è il riassetto del *Piano nazionale di ripartizione delle frequenze*, che libera di fatto le bande a 2,4 e 5 GHz utilizzate dagli standard 802.11b, a e g.
Il regolamento impone una procedura di richiesta dell'autorizzazione generale da parte di quei soggetti che intendano fornire connettività wireless locale in aree pubbliche come locali aperti, stazioni ferroviarie, aeroporti, centri commerciali e località turistiche. Ottenuta l'autorizzazione, i soggetti sono tenuti ad iscriversi al *Registro degli operatori di comunicazione*.
Sebbene rimangano alcuni dubbi su particolari aspetti del regolamento, come quello che impone all'operatore di "rispettare la sicurezza delle operazioni di rete e la protezione dei dati", nel complesso si tratta di una normativa che può fornire un impulso decisivo alla diffusione degli Hot Spot, ormai una realtà affermata negli Stati Uniti, anche nel territorio italiano.



Le prestazioni degli Access Point

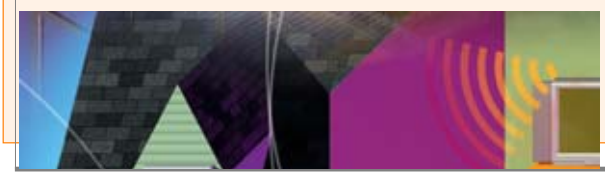
Le prestazioni dei prodotti portati ad esempio in queste pagine sono state misurate in termini di throughput al variare della distanza. Durante i test si è disposto un notebook su di un tavolo girevole di 70 centimetri di diametro, facendolo roteare a un ritmo di circa 20 giri al minuto mentre erano misurate le prestazioni di ogni combinazione Access Point e PC Card. È stata utilizzata la suite Chariot di NetIQ (*www.netiq.com*), un software che valuta le performance di dispositivi e applicazioni di rete. Il tavolino girevole era predisposto su di un carrello piazzato prima a 33 cm, quindi a 20, 35 e 50 metri dall'Access Point. Ciascun test è stato ripetuto almeno due volte per assicurare l'affidabilità dei risultati.

> I Test

Ogni client wireless è stato collegato a un Dell Ispiron 600m, un notebook funzionante con Microsoft Windows XP Professional come sistema operativo, e utilizzando gli ultimi driver disponibili per la scheda. Il terminale statico era invece un Dell Dimension 4100 con Windows 2000. Per ogni Access Point sono state conservate le impostazioni di fine-tuning del produttore ed è stato configurato un network aperto con velocità di trasmissione in grado di adeguarsi automaticamente alle condizioni di collegamento. I test sono stati eseguiti in due modi differenti: in un primo momento si sono configurati i dispositivi in modalità "g" pura, garantendo quindi il throughput massimo disponibile ai client 802.11g ed escludendo di conseguenza i dispositivi a 11 Mbps. In seguito il test è stato ripetuto in *mixed mode*, nel quale i client "b" e "g" coesistono sulla rete ed il traffico è inviato a entrambe le categorie. Per quest'ultima configurazione alla topologia è stato aggiunto un terminale statico costituito da un laptop munito di scheda 802.11b Cisco Aironet 350.

> I risultati

Molte speranze erano riposte nelle nuove tecnologie "g" atte a migliorare le prestazioni nel *mixed mode*: le specifiche Prism Nitro di Intersil e Xpress di Broadcom. La prima sostiene un incremento pari a un fattore 3 nel throughput di sistema, la seconda di un fattore 6. Sviluppate e registrate dai produttori dei chipset, queste tecnologie utilizzano i processi di *frame bursting* o *packet bursting* e sono state incluse in molti dei prodotti provati, tra cui i modelli D-Link e Smc. I risultati evidenziano al più un raddoppio effettivo delle prestazioni durante il test in *mixed mode*.
Come da previsioni, tutti i dispositivi IEEE 802.11g hanno ottenuto i risultati migliori operando in modalità "g" pura: nel complesso il prodotto Netgear si è rivelato il più performante e stabile in questa modalità, mentre in *mixed mode* è stato surclassato dal modello Netgear a brevi distanze. Nel segmento dei prodotti a 11 Mbps il modello D-Link ha invece superato gli altri a tutte le distanze.
Per quanto riguarda i prodotti aziendali, il SonicWall Soho TZW si è dimostrato un ottimo dispositivo 802.11b, specialmente considerando il carico di lavoro aggiuntivo necessario alle funzioni di tunnel Vpn e Firewall. È interessante notare che la scheda Pc Card di SoniWall opera a una tensione di 200 milliwatt, contro i 100 milliwatt delle altre schede provate, e di conseguenza ha un impatto maggiore sull'autonomia del dispositivo portatile con il quale è utilizzato.



Prestazioni degli Access Point

Valori maggiori corrispondono a prestazioni migliori. Il grassetto evidenzia i risultati migliori. Risultati espressi in Mbps.

	Distanza dall'Access Point (metri)			
	0,33	20	35	50
DISPOSITIVI SOHO				
Access Point IEEE 802.11g				
"Modalità" "g" "pura"				
D-Link AirPlus Xtreme G DI-624	16,0	10,2	0,0	0,0
Linksys Wireless-G WRT54G	21,0	15,5	1,3	0,0
Netgear FWAG114	19,8	15,7	4,7	1,6
Netgear WG602	15,3	13,7	0,0	0,0
SMC Barricade g SMC2803WBR	20,0	13,6	2,8	0,5
Mixed mode con client 802.11b attivo				
D-Link AirPlus Xtreme G DI-624	4,6	3,1	0,0	0,0
Linksys Wireless-G WRT54G	6,9	7,4	1,4	0,0
Netgear FWAG114	4,5	3,7	1,8	0,8
Netgear WG602	4,8	2,8	1,2	0,0
SMC Barricade g SMC2803WBR	4,5	3,3	1,8	0,0
Access Point IEEE 802.11b				
D-Link AirPlus Enhanced DI-614+	5,8	6,4	3,7	1,5
Linksys WAP11	4,9	4,7	2,1	0,0
Netgear ME102	4,5	4,2	1,8	0,4
Zyxel ZyAIR B-2000	4,6	4,5	2,0	0,0
DISPOSITIVI AZIENDALI				
Access Point IEEE 802.11g				
"Modalità" "g""pura"				
3Com Office Connect Wireless 11g	19,9	14,5	1,8	0,4
Mixed mode con client 802.11b attivo				
3Com Office Connect Wireless 11g	9,0	6,1	0,9	0,0
Access Point IEEE 802.11b				
SonicWall Soho TZW	3,1	3,1	3,1	3,0

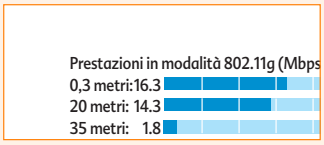
Access Point Aziendali

Di seguito riportiamo un esempio di due Access Point di classe business, tutti provati nei nostri laboratori. Il 3Com OfficeConnect Wireless 11g è uno dei primi prodotti di questo tipo compatibile con lo standard IEEE 802.11g. Il SonicWall Soho TZW utilizza le specifiche IEEE 802.11b ed è indirizzato agli uffici di piccole e medie dimensioni.

3Com OfficeConnect Wireless 11g

Euro **147,00** Iva inclusa
Voto: 4/5 ●●●●○
www.3com.com

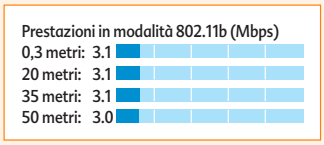
Questo dispositivo di 3Com è un dispositivo a doppia antenna senza fronzoli: il telaio in metallo garantisce una robustezza sopra la media, l'Access Point supporta il Wpa ed è in grado di salvare la propria configurazione che può poi essere esportata per l'installazione delle schede clilent. È inclusa un'applicazione che ricerca altri Access Point 3Com sulla rete e dà accesso alla configurazione dei parametri basilari di funzionamento.



SonicWall Soho TZW (802.11b)

Euro **942,00** Iva inclusa
Voto: 4/5 ●●●●○
www.sonicwall.com

Il SonicWall Soho TZW integra un firewall Spi ed è una completa appliance per la sicurezza di rete, sia essa wireless o cablata. Benché sia un dispositivo 802.11b e non "g", rimane un robusto sistema per i piccoli e medi uffici. Il TZW offre più funzioni di sicurezza e management della maggior parte dei prodotti 802.11b presenti sul mercato: protegge l'azienda ponendo la rete wireless su una Vlan separata, i client senza fili accedono alla rete attraverso un client Vpn e, a discrezione dell'amministratore, possono collegarsi o meno a Internet.



elevato di Access Point per garantire la copertura e le prestazioni richieste, senza il rischio di interferenze reciproche e cancellazioni di segnale. D'altro canto la frequenza più elevata utilizzata significa non solo un inferiore raggio di copertura, ma anche una maggiore sensibilità del segnale nei confronti di muri e altri ostacoli, spesso determinanti nella definizione della topologia di rete wireless per un ufficio.
La tendenza di mercato è comunque quella di rendere disponibili Access Point che combinino i tre standard; gli analisti sostengono inoltre che entro la metà del prossimo anno la maggior parte dei dispositivi wireless integrati nei notebook corporate saranno in grado di operare sia a 2,4 sia a 5 GHz. In definitiva, se non si hanno esigenze particolari in termini di densità di connessioni e se si desidera operare con un occhio di riguardo al budget, è più che sufficiente una rete 802.11g; al contrario se si vuole privilegiare l'interoperabilità, sono consigliabili dispositivi ibridi "a/b/g".

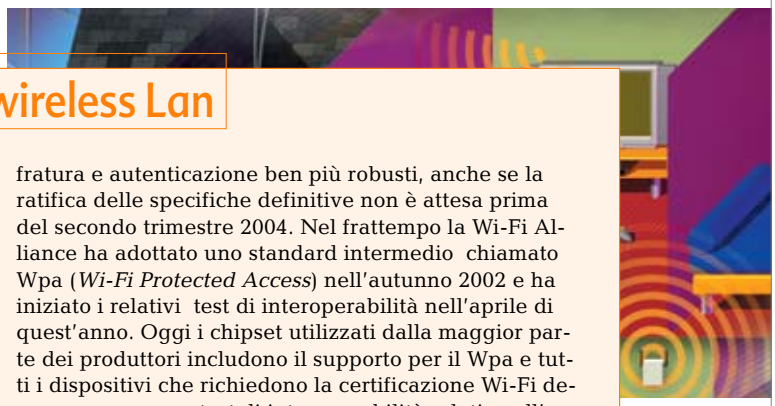
Lo studio del sito da coprire

La prima fase di progettazione della rete wireless presuppone lo studio della pianta e un sopralluogo sull'area che si desidera coprire con il segnale wireless. Si tratta di un passo fondamentale per pianificare i punti in cui piazzare gli Access Point, tenendo in considerazione il fatto che nella maggior parte dei casi ogni stazione base deve disporre di una connessione alla rete cablata e una per l'alimentazione. In realtà molti AP possono operare in modalità *bridge*, ovvero come semplici replicatori di segnale senza la necessità di essere collegati al network cablato; in ogni caso questo tipo di soluzione è generalmente utilizzato per collegamenti a lunga distanza e mal si adatta a un ufficio con area contigua. Parecchi produttori di Access Point per il mercato aziendale supportano la tecnologia *Power Over Ethernet* (PoE), che permette di trasmettere l'alimentazione su una coppia supplementare di fili all'interno di un cavo Ethernet di categoria 5 o superiore. Tutto ciò permette di risparmiare sull'estensione della rete elettrica, ma richiede switch compatibili con la tecnologia PoE.
Un altro aspetto da tenere in considerazione è la sicurezza fisica degli Access Point: la maggior parte dei modelli è così compatta da essere un facile obiettivo per un furto di materiale se non assicurata a una parete o a una struttura tramite un apposito lucchetto. Si può anche considerare l'ipotesi di installare l'Access Point in un punto non in vista (come in particolari posizioni sul soffitto), badando in ogni caso alle norme anti-incendio.
L'ispezione del sito dovrebbe includere in aggiunta un'analisi delle onde radio: utilizzando un notebook e un programma shareware come Network Slumber (*www.netslumber.com*) o commerciale come AiroPeek di WildPackets (*www.wildpackets.com*) e AirMagnet

(*www.airmagnet.com*) è possibile determinare se delle reti o dei segnali radio preesistenti possono interferire con il progetto della Wlan. Se si scoprono altre reti senza fili, è bene annotare le rispettive zone di copertura, nonché le frequenze e i canali utilizzati. In questo modo si identificano i parametri per la progettazione del cosiddetto *channel plan*, essenzialmente una mappa sovrapposta alla planimetria con le indicazioni sui canali radio che si intendono utilizzare per gli Access Point. Questo problema è logicamente più rilevante per le reti 802.11b/g, che come detto dispongono di meno canali non sovrapposti rispetto a quelle 802.11a.
Di default, la maggioranza degli Access Point sono configurati per utilizzare tutti lo stesso canale: è quindi necessario modificare i parametri di trasmissione in modo da servirsi di tutti i canali disponibili, poiché due AP adiacenti con la medesima frequenza operativa possono causare cancellazioni di segnale e conseguenti zone morte nella copertura radio.

Problematiche di capacità

Mentre si pianifica la disposizione di ogni Access Point, è fondamentale tenere in considerazione il carico di traffico che la rete wireless deve essere in grado di sostenere; in base alla capacità richiesta, può difatti variare in modo sensibile il numero di Access Point richiesti dall'infrastruttura.
Ciascun AP copre un'area circolare a meno che non si predispongano antenne direzionali per concentrare l'amplificazione di segnale in una precisa direzione; muri, mobili, divisori e altri ostacoli assorbono inoltre l'energia delle onde radio e distorcono in modo a volte imprevedibile la copertura circolare. In aggiunta, è importante comprendere che la potenza di segnale è inversamente proporzionale al quadrato della distanza: ad esempio, in campo aperto, la potenza a 30 metri dall'antenna sarà un quarto rispetto a quelle misurabile a 15 metri; con il diminuire di potenza del segnale cala anche il throughput veicolabile dalla rete, così che mentre i client 802.11g collocati nei pressi dell'Access Point possono connettersi a velocità tra i 15 e i 20 Mbps, i terminali posti ai margini dell'area di copertura possono scendere a 1 o 2 Mbps. In questi casi un'unica connessione può non essere sufficiente, e si necessita di segnali abbastanza forti da veicolare un throughput adeguato alle applicazioni di rete che si



Il punto sulla sicurezza di una wireless Lan

Essendo le reti wireless si basate su segnali a radio frequenza, tutto quello che serve per infiltrarsi in un sistema non protetto è un notebook o un Pda abilitato alle trasmissioni senza fili e un software liberamente scaricabile da Internet. È per questo che in qualsiasi wireless Lan, sia essa domestica o per un'azienda con migliaia di dipendenti, si deve seriamente tenere in considerazione la sicurezza di rete. Sorprendentemente, spesso non è così: in un recente sondaggio condotto da *Jupiter Research*, su 500 intervistati meno della metà implementa sulla propria struttura wireless degli accorgimenti di sicurezza.
Nel 1997 l'IEEE ha adottato il Wep (*Wireless Equivalent Privacy*) come mezzo per garantire la sicurezza sulla rete wireless; è tutt'oggi fortemente consigliabile che reti domestiche e Soho attivino il Wep, specialmente se si tratta dell'unica opzione di sicurezza disponibile (alcuni prodotti datati non sono compatibili con le più recenti tecnologie). Pur fornendo un algoritmo di sicurezza basilare, il Wep si è dimostrato essenzialmente inefficace contro gli hacker più smaliziati, principalmente a causa dell'utilizzo di chiavi di cifra statiche che, come dimostrato nel 2001 da un gruppo di ricercatori, consentono di accedere alle informazioni riservate dopo poche ore di "ascolto" delle comunicazioni.
Fortunatamente il gruppo di lavoro 802.11i dell'IEEE è al lavoro su di un nuovo standard di sicurezza per le reti locali wireless in grado di fornire meccanismi di cifratura e autenticazione ben più robusti, anche se la ratifica delle specifiche definitive non è attesa prima del secondo trimestre 2004. Nel frattempo la Wi-Fi Alliance ha adottato uno standard intermedio chiamato Wpa (*Wi-Fi Protected Access*) nell'autunno 2002 e ha iniziato i relativi test di interoperabilità nell'aprile di quest'anno. Oggi i chipset utilizzati dalla maggior parte dei produttori includono il supporto per il Wpa e tutti i dispositivi che richiedono la certificazione Wi-Fi devono superare un test di interoperabilità relativa all'accesso protetto.
Il Wpa è una parte del futuro standard IEEE 802.11i e dovrebbe essere compatibile con le specifiche definitive; è stato progettato affinché l'hardware attuale possa essere aggiornato con firmware e driver nel momento in cui i produttori rilascino versioni Wpa. Solo i dispositivi più recenti al momento sul mercato sono già compatibili con il Wpa, ma la richiesta dei test per la certificazione Wi-Fi è destinata a cambiare lo scenario in pochi mesi.
Il Wpa è pensato per rimediare alle debolezze del Wep: utilizza il protocollo Tkip per la cifratura e un altro standard IEEE, l'802.11x, per l'autenticazione e la distribuzione delle chiavi di cifra. Inoltre il *Message Integrity Check* (Mic) garantisce protezione contro gli attacchi che minano la struttura delle informazioni trasmesse.
Il Wpa supporta due modalità operative: il *Preshared key mode* è appropriato per i piccoli uffici e gli am-

<segue>

bienti domestici che non dispongono di un'infrastruttura di autenticazione preesistente. Un segreto condiviso è impostabile sia nell'Access Point sia nei client, e le chiavi di cifratura vengono rinnovate dinamicamente a intervalli prestabiliti in modo da scongiurare la possibilità che vengano ricavate in tempi utili dagli hacker in ascolto.
La seconda modalità, l'*enterprise mode*, necessita di un server di autenticazione basato sullo standard Radius. Occorre quindi impostare il protocollo Eap (*Extensible Authentication Protocol*) e l'IEEE 802.11x per tutte le stazioni wireless. Può sembrare una grande mole di lavoro, ma si tratta di tempo ben speso, dal momento che l'infrastruttura di distribuzione delle chiavi e di autenticazione dovrebbe in futuro integrarsi senza sforzo con il prossimo standard IEEE 802.11i.

Consigli per rafforzare la sicurezza di rete sulla Wlan

Cambiare il Ssid di default sul router/Access Point. L'identificativo di rete wireless preimpostato dai principali produttori è facilmente reperibile dagli hacker; il Ssid non dovrebbe contenere informazioni relative al nome o alla locazione dell'azienda.

Se il router o l'Access Point la supporta, disabilitare la funzione di broadcast del Ssid. In questo modo i visitatori occasionali non potranno rilevare la rete wireless.

Cambiare la password di amministrazione del router/AP. Gli hacker conoscono la password di default per tutti i principali marchi presenti sul mercato e in questo modo possono facilmente riconfigurare tutti i parametri di sicurezza.

Attivare il più elevato livello di scurezza che l'hardware supporta. Anche se si dispone di apparecchiature datate compatibili solo con il Wep, essere sicuri di averlo abilitato: anche se si tratta di un metodo non robusto, può comunque bloccare la maggior parte degli hacker.

Controllare periodicamente il sito Web del produttore dei propri dispositivi per verificare la disponibilità di firmware e driver aggiornati. Molti forniscono upgrade in grado di aggiungere le funzionalità Wpa.

Considerare l'attivazione dei filtri di controllo sugli indirizzi Mac. In questo modo è possibile specificare quali schede wireless possono accedere alla rete ed escludere le altre.

Se il router/Access Point supporta il protocollo Snmp, cambiare i nomi di comunità in modo da non fornire scelte ovvie. Questo impedisce agli hacker di gestire i dispositivi di rete utilizzando software Snmp standard.

Considerare con attenzione la posizione degli Access Point. Se non si necessita di un accesso wireless al di fuori dell'edificio, piazzare gli AP al centro della struttura per minimizzare la copertura di segnale all'esterno.

Eseguire in proprio delle prove di sicurezza. Utilizzando Windows 2000 o XP, o software come Network Stumbler (*www.networkstumbler.com*) su di un notebook o Pda, percorrere il perimetro dell'edificio alla ricerca di potenziali falle del sistema.

Se si utilizza un numero limitato di client wireless, fornire loro degli indirizzi Ip statici e disabilitare le funzionalità Dhcp dei router/Access Point. Questo renderà più difficile una eventuale intrusione sulla rete.

In un'azienda, piazzare la rete wireless su di una diversa Lan virtuale, e implementare dei tunnel Vpn verso i client wireless. Questa soluzione è particolarmente efficace se l'hardware non supporta il Wpa e non possono essere aggiornati a tal fine. Le Vpn forniscono uno standard di sicurezza a livello 3 comprovato. Prodotti per il piccolo e medio ufficio come il Netgear FVM318 o il SonicWall Soho TZW permettono di isolare la rete wireless dalla rete cablata e di utilizzare le Vpn per connessioni sicure tra i due segmenti di rete.>

debbono utilizzare per ciascun terminale.
Un altro aspetto da considerare è che un Access Point irradia anche in direzioni non complanari rispetto alla propria posizione, fornendo quindi una copertura anche ai piani superiori e inferiori, sebbene soffitti e pavimenti possano ridurre sensibilmente la copertura di segnale. In alcuni casi è comunque indispensabile mantenere una "dorsale verticale" cablata, o perlomeno piazzare un Access Point per ogni piano.
Le reti wireless, a differenza di quelle commutate su cavo, si basano su un mezzo di trasporto condiviso: come regola generale è bene non associare più di 25 client a ciascun Access Point e di conseguenza installare più AP sovrapposti in aree ad alto carico di lavoro. Se si rivela indispensabile l'utilizzo di canali sovrapposti da parte di più di un AP, è indispensabile verificare che questi siano posti a distanza sufficiente da evitare eventuali interferenze distruttive che ne limitino le prestazioni.

Un piano di sicurezza aziendale

Molti amministratori di rete installano i propri Access Point verso il centro dell'ufficio, in modo da limitare il rischio di connessioni non autorizzate all'esterno del perimetro aziendale. Benché questa strategia possa

essere una componente del piano di sicurezza aziendale, è molto più importante dotarsi di una politica che includa meccanismi di autenticazione e forte cifratura dei dati trasmessi. Tale politica può limitarsi a non consentire l'accesso ai dispositivi non approvati o forniti dall'azienda, ma può essere necessario rinforzarla o con un controllo sugli accessi relativo alle porte di comunicazione o servendosi di una delle suite di sicurezza commerciali.

Scegliere l'equipaggiamento

Una volta terminato il sopralluogo e definito un piano di sicurezza, è tempo di passare all'acquisto degli apparati di rete wireless, scegliendo ad esempio se puntare su Access Point di fascia aziendale o limitarsi a dispositivi indirizzati al Soho; questi ultimi possono all'inizio attrarre a causa dei prezzi sensibilmente inferiori, ma in caso di una rete complessa spesso non dispongono delle caratteristiche di gestione che un amministratore di rete può desiderare.
Gli AP di ispirazione aziendale, come la serie AP1200 di Cisco, o gli 8700 di 3Com, offrono meccanismi di management centralizzato, modalità di funzionamento a doppia banda, autenticazione sugli indirizzi Mac e supporto per il Power Over Ethernet; inoltre, tali dispositivi forniscono tipicamente diverse funzioni relative alla sicurezza, ad esempio il supporto ai protocolli Wep e Wpa. Questo facilita l'upgrade delle caratteristiche di rete anche dal punto di vista degli utenti, come nel caso in cui si aggiornino le schede client ai nuovi meccanismi Wpa o IEEE 802.11i.
È comunque importante tenere in considerazione che le schede wireless più datate possono non supportare l'upgrade verso il protocollo Wpa; utilizzando una struttura mista, ad esempio con AP 802.11b insieme a più moderni prodotti 802.11g (retrocompatibli) può comunque fornire la necessaria flessibilità per fornire ai vecchi client perlomeno il Wep in attesa di futuri aggiornamenti hardware.

La pianificazione è la chiave

Progettare e installare una rete wireless è un compito complesso, che richiede una piena comprensione del layout del proprio ufficio, delle esigenze dei dipendenti, e degli obbiettivi futuri dell'azienda.
Il segreto è quindi quello di tenere in considerazione tutti questi aspetti prima di procedere all'acquisto delle apparecchiature, assicurandosi che il network abbia caratteristiche ottimali per il contesto presente, ma sia al contempo scalabile per adattarsi alla potenziale espansione dell'azienda e delle sue esigenze. Infine, è fondamentale porre le problematiche di gestione e sicurezza in primo piano. ■