WIRELESS LAN: STATO DELL'ARTE E PROSPETTIVE

Carlo Alberto Marchi
Francesco Vatalaro

Le WLAN sono reti radio d'area locale, operanti oggi secondo lo standard IEEE 802.11b, che offrono una copertura in zone ad alta densità di traffico per trasmissione dati e accesso veloce a Internet e alle reti Intranet aziendali. Si attende sul mercato la diffusione dei sistemi che rispondono a versioni più recenti dello standard e che offriranno una banda, e una capacità di traffico, più ampia. Obiettivo dell'articolo è approfondire le nuove opportunità di servizio offerte dal Wi-Fi a partire dagli aspetti tecnologici, regolamentari e di mercato.

3·4

1. INTRODUZIONE

Una WLAN (*Wireless Local Area Network*) è una rete radio d'area locale in grado di offrire copertura in zone ad alta densità di traffico con tipica estensione fino al centinaio di metri per trasmissione dati e per l'accesso veloce a Internet e alle Intranet aziendali. Si sta affermando in tutto il mondo lo standard *IEEE 802.11*, che è uno standard per *wireless LAN* di strato fisico (*OSI layer 1*) e strato di collegamento (*OSI layer 2*) per connessioni Ethernet negli uffici e per applicazioni domestiche. Sulla base dello standard operano i prodotti Wi-Fi (*Wireless Fidelity*) certificati dalla *Wi-Fi Alliance*. Wi-Fi è, dunque, un marchio commerciale che assicura la compatibilità tra prodotti basati sullo standard *IEEE 802.11b*, che è la versione attualmente operativa in Italia.

A seguito del successo delle *Wireless LAN* in ambito privato (uffici, abitazioni), si sta procedendo all'estensione del Wi-Fi anche ad aree pubbliche caratterizzate da un'alta densità di traffico (dette *hotspot*) per l'accesso a Internet a banda larga che, da un lato promette di essere la principale opportunità di mercato per il futuro sviluppo delle WLAN e dall'altro potrà assicurare una piattaforma per l'accesso ubiquo alle reti di telecomunicazione, affiancando altre soluzioni in via di introduzione, dall'UMTS (*Universal Mobile Telecommunications System*) al DVB (*Digital Video Broadcasting*) interattivo.

Wi-Fi, non più realizzato soltanto attraverso schede esterne PCMCIA, è ora disponibile come funzionalità integrata in molti terminali d'utente: infatti, più di 10 milioni di PC (*Personal Computer*) portatili (10%) sono già dotati di *hardware* IEEE 802.11b (fine 2002); inoltre, è previsto che il 31% dei PC portatili nel 2004 e il 68% nel 2007 sarà dotato di funzionalità Wi-Fi integrata [10].

Una delle principali ragioni alla base della diffusione del Wi-Fi consiste nella scelta della banda di frequenza. Infatti, lo standard IEEE 802.11b opera in una banda di frequenza allocata per utilizzazioni industriali, scientifiche e mediche (da cui la denominazione di banda ISM). Le bande ISM (*Instrument Scientific Medical*) sono state originariamente

concepite per la messa in opera di sistemi atti a utilizzare in uno spazio ridotto (da pochi metri a qualche centinaio di metri) le radioonde a fini industriali, scientifici, medici, domestici o analoghi, con esclusione, quindi, dell'impiego per servizi di telecomunicazioni a grande distanza [2, 3].
Alle bande ISM si attribuisce lo *status* normativo di bande "esenti da licenza", definizione che non deve essere, tuttavia, considerata sinonimo di "non regolamentate". In effetti, l'uso delle bande ISM, di norma concesso in condizioni di limitazione sulla potenza massima emessa, in moltissimi Paesi non richiede una licenza governativa per un'assegnata classe di applicazioni; l'uso da parte di ogni altra applicazione, di norma, richiede la licenza o, quantomeno, l'autorizzazione. Lo status normativo delle bande ISM ha incoraggiato, dunque, significativi investimenti in applicazioni che non richiedono di accedere a procedure di acquisizione di licenza complesse, costose e dall'esito spesso incerto.
Nella figura 1 sono illustrate le bande ISM impiegate negli Stati Uniti d'America e in Europa dai sistemi a standard IEEE 802.11 e la banda allocata in Europa per lo standard *HiperLAN/2* definito per applicazioni simili; in particolare, in ambito europeo, la decisione CEPT ERC/DEC/(01)07 ha destinato la banda di frequenze 2400,0 – 2483,5 MHz per un impiego con dispositivi della categoria SRD (*Short Range Device*), tra cui gli apparati usati per applicazioni WLAN, e ha ratificato la decisione di esonerare tali apparati dalla necessità di licenza individuale.
In ambito italiano, l'utilizzo delle frequenze della banda esente da licenza 2400,0 – 2483,5 MHz è disciplinato dal *Piano Nazionale di Ripartizione delle Frequenze* (PNRF) che alla nota n. 158, aggiornata dal Decreto 20 febbraio 2003, stabilisce che esse "*possono essere impiegate ad uso collettivo per usi civili da reti locali mediante apparati a corto raggio per la trasmissione di dati a larga banda con tecniche a dispersione di spettro (R-LAN) aventi le caratteristiche tecniche della raccomandazione della CEPT ERC/REC 70-03 (annesso 3). Tali utilizzazioni non debbono causare interferenze alle utilizzazioni dei servizi presenti in tabella, ne' possono pretendere protezione da tali utilizzazioni. (...). Per quanto riguarda l'uso pubblico, lo stesso sarà disciplinato con un'apposita regolamentazione.*"

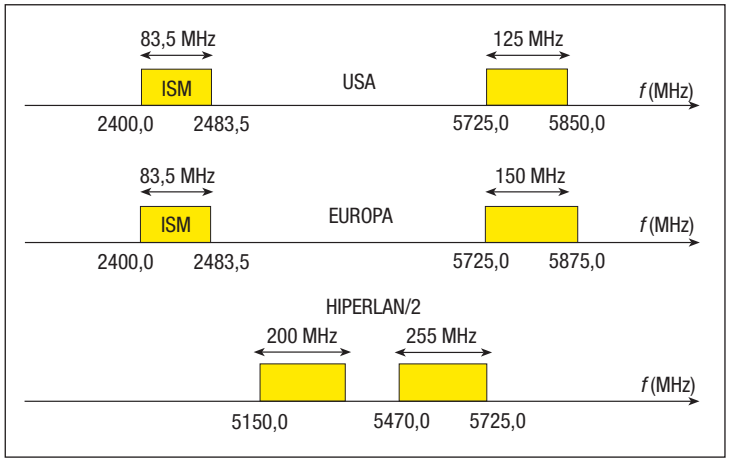


FIGURA 1
Le bande impiegate dallo standard IEEE 802.11 e la banda per lo standard europeo HiperLAN/2

Le bande ISM sono impiegate per sistemi di identificazione a radiofrequenza (*Radio Frequency Identification Device*, RFID), dispositivi di comunicazioni a corto raggio e a bassa potenza per collegamenti audio, video e dati (inclusi WLAN, *Bluetooth e HomeRF*), sistemi di telecomando e telecontrollo ecc.. Queste bande sono anche interessate dalle radiazioni di sistemi elettrici ed elettronici tra i quali alcuni sistemi di illuminazione e i forni a microonde. Considerate le modalità d'uso non coordinato e non sorvegliato delle bande, si opera, di norma, in condizioni di interferenza imprevedibile e incontrollabile: si pone, pertanto, un problema specifico di coesistenza di sistemi differenti. Inoltre, a causa della imprevedibilità dei livelli di interferenza che si possono presentare, la Qualità del Servizio (*Quality of Service*, QoS) può risultare variabile anche in maniera sensibile. Nei casi in cui ciò rappresenti un problema, si potrà realizzare sistemi WLAN a standard IEEE 802.11a (o a standard HiperLAN/2) alle frequenze, non di tipo ISM, intorno a 5 GHz che offrono una larghezza di banda, e quindi una capacità di traffico, più ampia e che renderanno meno critici i problemi di interferenza che si presentano nelle bande ISM.
Nell'articolo sono state approfondite le nuove opportunità di servizio offerte dal Wi-Fi a partire dall'esame degli aspetti generali e tecnologici. Sono stati analizzati, inoltre, i problemi ancora aperti per una diffusione del Wi-Fi in ambito pubblico: sono allo studio diverse soluzioni per affrontare tali problemi,

tra cui verranno considerati, in questa sede, i più sentiti (semplicità d'uso, sicurezza, qualità di servizio, mobilità e gestione della rete). Sono stati esaminati, infine, alcuni aspetti rilevanti per l'attuazione di questo nuovo *business*, che presenta caratteristiche specifiche rispetto ai tradizionali servizi radiomobili.

2. STANDARD IEEE 802.11 E WI-FI

IEEE 802.11 è oggi il nome impiegato per designare una famiglia di standard WLAN, non tutti ancora pienamente finalizzati. Una rete WLAN basata su IEEE 802.11 è un sistema di comunicazioni adatto a realizzare un'estensione o una alternativa per le reti LAN d'ufficio di tipo Ethernet. Una prima versione dello standard base (dal nome generico IEEE 802.11) è stata pubblicata nel giugno 1997.
Oggi si dispone di una la famiglia di standard IEEE 802.11 che si compone di [8]:

- ***IEEE 802.11b*** (emesso nel 1999): opera a 2,4 GHz (banda ISM) con 83 MHz di larghezza di banda e velocità di trasmissione lorda di 11 Mbit/s; usa in prevalenza la tecnica di modulazione DS-SS (*Direct Sequence – Spread Spectrum*): attualmente, è operativo sia negli Stati Uniti che in Europa e sono disponibili prodotti realizzati da numerosi costruttori;
- ***IEEE 802.11a*** (emesso nel 2002): opera a 5 GHz con 150 MHz di larghezza di banda e velocità di trasmissione lorda di 54 Mbit/s; usa la tecnica di modulazione OFDM (*Orthogonal Frequency Division Multiplex*): attualmente, è già operativo negli USA ma non è ancora autorizzato in Italia.
- ***IEEE 802.11e*** (in preparazione): definisce le caratteristiche del sottostrato MAC (*Medium Access Control*) delle interfacce IEEE 802.11b e IEEE 802.11a in modo da garantire i requisiti di QoS;

FIGURA 2
Il marchio Wi-Fi

- ***IEEE 802.11g*** (in preparazione): estende, per mezzo di una modulazione aggiuntiva, le caratteristiche dello standard IEEE 802.11b (2,4 GHz); con esso è pianificata la compatibilità, per offrire una velocità di trasmissione teorica massima fino a 54 Mbit/s lordi;
- ***IEEE 802.11i*** (in preparazione): definisce le caratteristiche del sottostrato MAC per migliorare la sicurezza, con riferimento sia all'autenticazione dell'utente che alla *privacy* della connessione.

Poiché lo standard IEEE 802.11b non è uno standard completo, ossia si occupa soltanto degli strati OSI 1 e 2 (parzialmente), possono sussistere diverse incompatibilità tra prodotti di diversi costruttori che, in generale, non sono in grado di interoperare; questa limitazione rappresenta un evidente freno alla diffusione dello standard e, pertanto, è stato deciso di adottare un marchio, denominato Wi-Fi, sotto l'egida della Wi-Fi Alliance, cui hanno già aderito molti costruttori.
Wi-Fi Alliance [11] è un'associazione no profit, costituita nel 1999 con il nome provvisorio di WECA (*Wireless Ethernet Compatibility Alliance*), che si propone come ente indipendente di certificazione della interoperabilità dei prodotti WLAN basati sulle specifiche IEEE 802.11. Essa ha perciò realizzato alcuni laboratori negli Stati Uniti, in Europa e nell'Estremo Oriente, dove verifica l'aderenza dei prodotti alle specifiche e rilascia, quindi, il "marchio Wi-Fi", riportato nella figura 2, ai prodotti che superano i *test* di interoperabilità. Chiunque voglia realizzare un'infrastruttura WLAN aperta, ossia senza sfruttare specifiche tecniche proprietarie, dovrà verificare che i prodotti che adotta si fregino del marchio Wi-Fi, a garanzia della possibilità di interoperare con sistemi di altri produttori almeno a livello di strato fisico e di strato di collegamento.
Il successo di Wi-Fi Alliance può essere ben compreso sulla base del numero di prodotti testati: a partire da marzo 2000, data in cui è stato aperto il primo laboratorio dell'associazione, sono stati certificati 580 prodotti di 200 produttori. È particolarmente rilevante notare che ben 140 prodotti sono stati certificati nel solo autunno del 2002, a conferma del crescente interesse industriale attorno a queste tecnologie e al relativo mercato.

Impiegando in una rete prodotti certificati Wi-Fi (IEEE 802.11b) sarà lecito attendersi le seguenti principali caratteristiche:

- una porta di accesso (AP, *Access Point*) di un costruttore è interoperabile con qualsiasi scheda cliente (NIC, *Network Interface Card*) di qualsiasi altro costruttore che espone il marchio Wi-Fi;
- il sistema opera alle velocità massime di trasmissione (lorde) di 1 Mbit/s; 2 Mbit/s; 5,5 Mbit/s; 11 Mbit/s;
- le coperture tipiche del servizio, senza degradare la velocità di trasmissione, può arrivare fino a circa 150 m all'aperto (*outdoor*) e fino a circa 50 m al chiuso (*indoor*).

L'intestazione (*overhead*) del protocollo riduce, in effetti, la massima velocità di trasmissione da 11 Mbit/s al valore netto di circa 6 Mbit/s. Inoltre, la velocità di trasmissione può essere dinamicamente adattata alle condizioni del canale, fino a un minimo di 1 Mbit/s, ma può risultare in generale di circa 11 Mbit/s fino a distanze di 50 - 100 m; essa è tuttavia sensibilmente influenzata dalle interferenze e, ad esempio, si è valutato che in presenza di una trasmissione Bluetooth già, a 10 m possa degradare fino al 40%.

3. TECNOLOGIA IEEE 802.11

Come già detto, gli standard attuali della famiglia IEEE 802.11 riguardano lo strato 1 (*physical layer*) e lo strato 2 (*data link layer*) dell'architettura OSI. Più precisamente, lo standard IEEE 802.11b definisce lo strato fisico (*Physical Layer Device, PHY*), lo strato di controllo di accesso al mezzo (MAC), come mostrato in figura 3.

Una WLAN che risponda allo standard IEEE 802.11 si compone essenzialmente di:

- **unità per l'interconnessione alla rete**, dette NIC, che sono le schede di interfaccia tra il terminale mobile e l'accesso a radiofrequenza;
- **le porte (o i punti) d'accesso**, le AP, che rappresentano l'equivalente a radiofrequenza della *hub* delle reti Ethernet.

Una AP è sovente connessa con la dorsale LAN Ethernet ma può anche realizzare una rete solo wireless: la configurazione tipica di una installazione di una rete WLAN aziendale IEEE 802.11 è mostrata in figura 4.

Lo standard prevede differenti modalità di al-

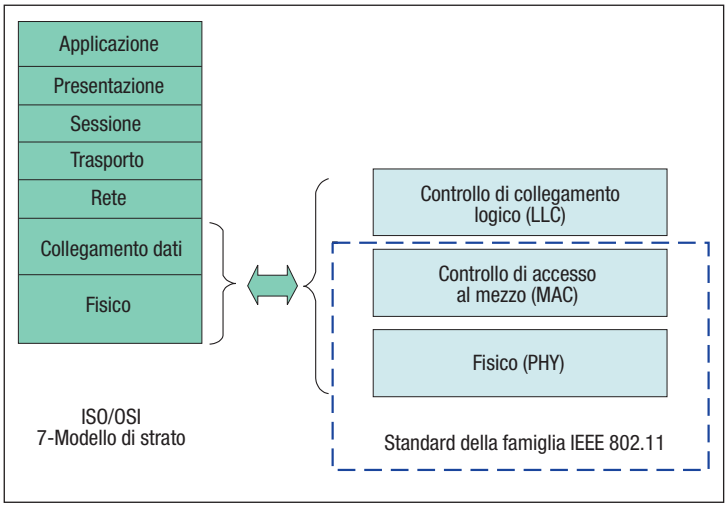


FIGURA 3
Associazione fra strati delle architetture OSI e IEEE 802.11

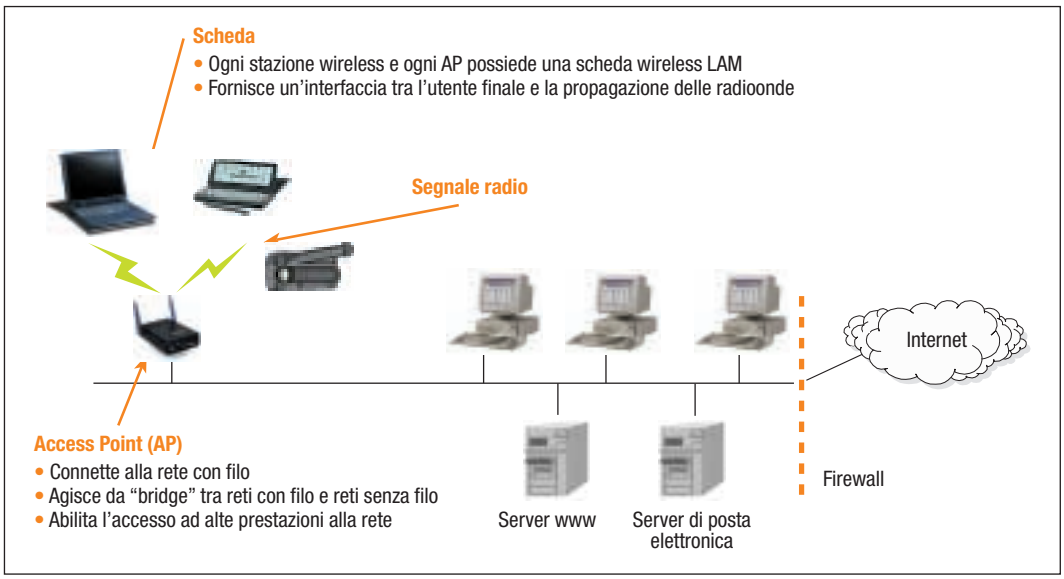


FIGURA 4
Configurazione tipica di rete aziendale IEEE 802.11

lestimento delle connessioni e delle reti, secondo due topologie [4, 6]:

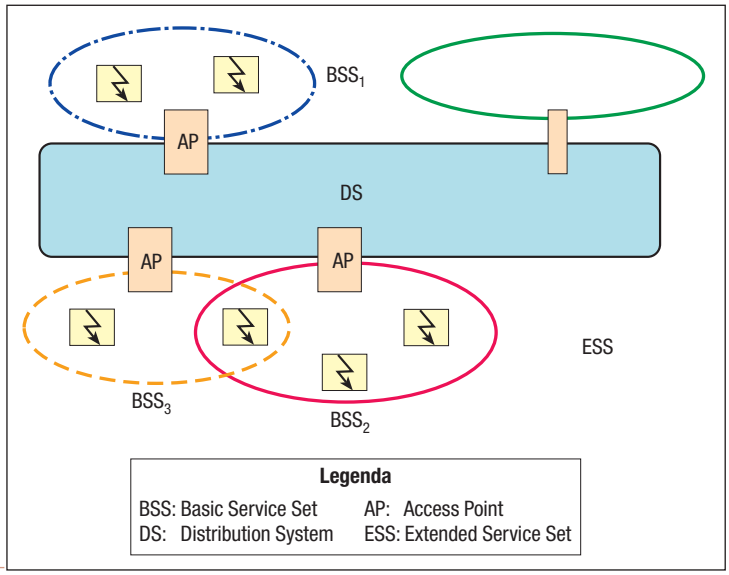
❑ ***Reti "ad hoc"***: si compongono di un insieme di nodi wireless (NIC) che si possono riorganizzare autonomamente in configurazioni temporanee e arbitrarie; i nodi possono servire da *router* e da *host*, e possono instradare pacchetti anche per conto di altri nodi; i nodi possono ospitare e attivare applicazioni d'utente. Le connessioni sono generalmente da pari a pari (*peer-to-peer*).

❑ ***Reti "client/server"***: realizzano organizzazioni gerarchiche in cui uno o più nodi rappresentano i centri "stella" della rete (AP); le connessioni tra nodi periferici (NIC) possono di norma essere instradate solo attraverso uno o più centri stella. Esse si possono riconfigurare dinamicamente per inserire o per eliminare nodi periferici.

L'architettura elementare di una rete IEEE 802.11 è indicata nello standard [7] come BSS (*Basic Service Set*) e, nella configurazione minima, è costituita da due soli terminali. Essa si instaura quando due o più stazioni sono in grado di comunicare direttamente tra loro e non esiste una pianificazione preventiva dell'architettura di rete.

Quando non sia possibile realizzare collegamenti entro un solo BSS, per le limitazioni dovute alla radiopropagazione, al traffico o per altri motivi, e quando si voglia, quindi, interconnettere più BSS si ricorre all'architettura di sistema di distribuzione DS (*Distribution System*) riportata in figura 5. Il DS ha il compito di gestire l'indirizzamento dei dati dalla sorgente al destinatario, anche nel caso di terminali portatili, e, al tempo stesso di operare l'integrazione trasparente (a livello di sottostrato LLC) di più BSS indipendenti. L'uso di DS e BSS consente di realizzare reti IEEE 802.11 di dimensione arbitraria e diversa complessità: una rete di questo tipo viene detta ESS (*Extended Service Set*).

FIGURA 5
Architettura di sistema di distribuzione IEEE 802.11 mista con/senza filo



L'integrazione di un'architettura di rete basata su IEEE 802.11 con una rete LAN cablata di tipo IEEE 802.x avviene attraverso un'architettura logica basata sull'impiego di un'interfaccia detta portale. Tutti i dati che provengono dalla rete cablata transitano verso la rete IEEE 802.11 attraverso il portale, e viceversa. Un dispositivo generico può offrire servizi per realizzare sia l'AP che il portale. Ciò si verifica, ad esempio, quando il DS è in realtà esso stesso una rete LAN cablata a standard IEEE 802.x. L'architettura di figura 5 consente anche di realizzare un accesso alla rete Internet. Attualmente, tali architetture miste (con o senza filo) si stanno diffondendo sempre più e si pongono problemi specifici di autenticazione degli utenti e di crittografia dei dati, anche in ambiti relativamente ristretti e controllati come quello aziendale.

4. CRITERI DI PROGETTO DI UNA RETE WLAN AZIENDALE

L'adozione di una infrastruttura a radiofrequenza per la realizzazione dei collegamenti all'interno di un'azienda richiede di valutare con attenzione una serie di aspetti, non soltanto di natura tecnica. Tutti questi aspetti devono essere accuratamente esaminati in fase di analisi del problema, al fine di massimizzare le possibilità di successo del progetto. Nel seguito, vengono illustrate le principali aree di attenzione.

4.1. Analisi delle esigenze

È importante valutare l'entità del traffico a cui la rete wireless sarà sottoposta dall'utenza reale. Si deve, pertanto, valutare il numero e il tipo di terminali, sia fissi che portatili, con particolare attenzione alle aree a maggiore densità, quali ad esempio sale riunioni, sale per didattica o per convegni ecc.. Oltre al numero degli utilizzatori in ciascuna area, devo-

no essere verificate le applicazioni che gli utenti utilizzano, per valutare il traffico dati che la rete dovrà sostenere, in relazione alla capacità dei collegamenti e al numero e al tipo di terminali per cella.

4.2. Copertura radioelettrica

Il secondo aspetto progettuale di grande rilevanza è la copertura radio. Essa, infatti, non dipende soltanto dall'AP e dall'antenna, ma dipende fortemente dalle caratteristiche di propagazione nell'ambiente reale, che possono consentire una copertura a distanza o che possono introdurre forti attenuazioni (per esempio, in prossimità di pilastri in cemento armato, cabine elettriche, trombe degli ascensori ecc.), riducendo così l'estensione di cella. Va comunque sempre tenuto presente che esiste una relazione tra il numero e il tipo di terminali presenti in una cella e il traffico massimo nella rete; pertanto, l'aumento eccessivo della dimensione della cella riduce il numero di terminali che possono essere serviti in modo efficace.
In particolare, non si ritiene di poter superare una ventina di terminali simultanei per cella in caso di applicazioni semplici, mentre al crescere della sofisticazione delle applicazioni questo numero può scendere fino a una decina di terminali o anche meno. Il progetto di una copertura adeguata non può prescindere, dunque, da una preventiva verifica sul campo con opportuni misuratori e, eventualmente, con l'ausilio di strumenti *software*.
Una volta pianificata la distribuzione degli AP, si provvede ad assegnare a ciascuno di essi uno dei tre canali disponibili, in maniera da evitare le interferenze tra celle adiacenti, sia in orizzontale che in verticale: è, infatti, possibile che un'antenna offra copertura, in corrispondenza della propria posizione, anche ai piani immediatamente inferiore e superiore.

4.3. Selezione degli standard

Attualmente, in Italia, è possibile utilizzare solo apparati a standard IEEE 802.11b. Si prevede, comunque, che, a breve, le autorità di regolamentazione diano l'autorizzazione anche per gli apparati IEEE 802.11a. È opportuno, dunque, che la progettazione di un impianto non prescinda dall'analisi di questa possibile migrazione (anche parziale).

4.4. Interoperabilità

Una considerazione importante riguarda l'interoperabilità degli apparati adottati. Sebbene, come già precedentemente accennato, la certificazione Wi-Fi garantisca la piena interoperabilità IEEE 802.11b degli apparati dotati di questo marchio, ciò fa esclusivo riferimento alle caratteristiche previste dallo standard. Nell'impiego effettivo, d'altra parte, sorgono spesso necessità che possono suggerire l'adozione di tecniche più sofisticate di quelle standardizzate. In questo caso, ci si può avvalere delle estensioni del fornitore degli apparati, legandosi ai soli prodotti di quel fornitore, oppure si possono adottare soluzioni offerte da terze parti, per le quali è solitamente disponibile una lista di compatibilità nei confronti di vari produttori. L'opportunità di una interoperabilità completa con qualsiasi fornitore si scontra, dunque, con la necessità di adottare soluzioni per le quali solo un certo numero di prodotti è certificato.

4.5. Sicurezza

L'area della sicurezza è quella a cui fare maggiore attenzione nella progettazione di un impianto WLAN aziendale.
La tematica della sicurezza è relativa a vari aspetti tra i quali si segnalano:

- la protezione del collegamento radio con eventuale crittografia dei dati, per evitare intercettazioni passive;
- l'identificazione e autenticazione dell'utente per autorizzare il terminale ad accedere ai servizi disponibili;
- l'identificazione di estranei non autorizzati per evitare che questi raggiungano i servizi offerti dalla rete o che interferiscano con il buon funzionamento dei servizi a disposizione dei terminali autorizzati.

Questi aspetti vengono affrontati con varie tecniche e con vari prodotti, ma, stante l'attuale sviluppo degli standard, si ritiene che una rete "sicura" non possa fare a meno di prodotti specializzati orientati alla gestione della sicurezza. Sulla sicurezza delle reti WLAN si tornerà nel seguito dell'articolo.

4.6. Gestione della mobilità e *hand-over*

Mentre solitamente gli utilizzatori di impianti WLAN in ambito privato (ufficio, abitazione) non si spostano durante una sessione, ossia

una volta collegato il computer portatile questo rimane fisso fino al termine del lavoro, esistono, invece, alcune categorie di lavoratori che utilizzano apparati WLAN, nel corso di spostamenti da una cella a un'altra, su larga scala, anche nell'impiego in azienda (per esempio, nei capannoni, nei magazzini, nei *campus* ecc.).
Diviene in questi casi importante affrontare un altro tema, ossia la mobilità del terminale mobile, che richiede la disponibilità delle funzioni di *IP mobile* [8], nel quale l'indirizzo IP (*Internet Protocol*) si sposta da una cella/sottorete a un'altra cella/sottorete, nonché quello della capacità del sistema di attuare funzioni di *hand-over* da una cella a un'altra su tutti i flussi dati trattati nelle sessioni in corso. Anche per queste problematiche esistono specifiche soluzioni, in alcuni casi proprietarie, in altri casi disponibili per un gran numero di prodotti.

4.7. Gestione della risorsa spettrale

Una nuova esigenza che sta sorgendo riguarda la necessità di gestire in modo controllato la banda disponibile in una cella, assegnando a ciascun terminale una banda massima per la propria trasmissione sulla base delle sue priorità, delle applicazioni a cui sta accedendo e del numero di terminali simultaneamente attivi nella stessa cella. Per affrontare in modo sistematico queste tre problematiche sono stati presentati alcuni prodotti che prendono il nome di *access server*: si tratta, in effetti, di AP particolarmente complessi che, pur interoperando con un grande numero di adattatori WLAN per PC riescono a offrire, con l'ausilio di un software installato nel terminale, una gestione assai flessibile ed efficiente della risorsa spettrale.

5. IL MERCATO DELLE WLAN

Le aspettative del mercato WLAN sono largamente motivate sulla base dell'attesa di incremento della produttività per gli utenti affari che utilizzano il Wi-Fi: infatti, è stato stimato che gli impiegati possano accedere a Internet e alle intranet aziendali una media di 105 minuti al giorno in più (Fonte: NOP *Research Group*), mentre Merrill Lynch & Co. ha già deciso di installare Wi-Fi in ogni suo nuovo ufficio, avendo stimato un aumento di produttività media del 20% [3]. Secondo Cisco, inoltre, per rientrare nel costo dell'infrastruttura Wi-Fi, è sufficiente aumentare la produttività media degli impiegati di soli 1 o 2 min al giorno.
Ma quali sono i vantaggi offerti dalla tecnologia WLAN alla base di questi attesi benefici economici?
I vantaggi principali sono:
- *massima mobilità* – i dipendenti possono liberamente spostarsi, non solo in altri uffici o sale riunioni, ma anche in altre sedi dell'azienda, con la sicurezza di raggiungere immediatamente tutti i servizi (*e-mail*, sistemi informativi aziendali, *web*, applicazioni ecc.): è sufficiente attivare il computer portatile perché questo si colleghi, automaticamente, alla rete aziendale, come se fosse collegato via cavo alla LAN Ethernet;
- *incremento di efficienza* – la tecnologia WLAN rende disponibili strumenti che consentono di raggiungere, immediatamente e in ogni luogo, i dati che interessano, permettendo di aumentare in modo significativo l'efficienza sul lavoro;
- *riduzione dei costi* – le riduzioni di costo sono legate sia alla drastica riduzione dell'entità dei cablaggi, sia alla migliore gestione degli impianti (manutenzioni, aggiornamenti tecnologici, spostamenti e variazioni degli accessi ecc.), che risulta assai semplificata e non richiede più virtualmente alcun intervento "*in loco*";
- *scalabilità* – la modularità del sistema consente di variare il numero di terminali d'utente che si collegano alla rete non richiede più alcun tipo di variazione impiantistica (cablaggi, *patch panel*, apparati attivi di rete ecc.).

Un'associazione di produttori che si occupa di promuovere le tecnologie WLAN, la WLANA (*Wireless LAN Association*), ha provato a misurare il risultato economico conseguente ai vantaggi sopra indicati. In un recente studio realizzato a mezzo di interviste ed analizzando in dettaglio trentaquattro grandi installazioni di infrastrutture WLAN presenti in diversi settori (università, ospedali, aziende manifatturiere, grande distribuzione, servizi finanziari), il 90% circa degli intervistati ha dichiarato di aver ottenuto importanti benefici economici e operativi dall'adozione della nuova tecnologia e di voler ampliare la propria infra-

struttura WLAN in futuro. In tutti i casi, il ritorno dell'investimento è stato ottenuto in meno di un anno [9]. Questi risultati non soltanto spiegano la crescente diffusione del Wi-Fi in ambito aziendale, ma ne motiva l'interesse per un impiego professionale sempre e dovunque, e rappresenta una spinta energica alla sua diffusione in ambito pubblico.
In accordo con i risultati sopra riportati, Gartner Dataquest stima che nel 2002 siano stati consegnati 15,5 milioni di unità NIC, con un aumento del 73% sul 2001, per un volume complessivo di transazioni di 2,1 miliardi di US$, con un aumento del 26% sul 2001 [10]. Il tasso di crescita per il 2003, con consegne che raggiungeranno 26,5 milioni di unità per un totale di 2,8 miliardi di US$. Ci si aspetta, inoltre, una significativa crescita fino a tutto il 2007. Il volume di affari cresce a un tasso minore del numero di unità consegnate, segno inequivocabile di un generale processo di riduzione dei prezzi, dovuto sia alla crescita della concorrenza, sia alla produzione in grandi volumi, sia al processo di integrazione nei computer *notebook*.
Il mercato principale della tecnologia WLAN è, infatti, attualmente costituito da adattatori per PC (NIC esterne), che vengono acquistati separatamente dall'acquisto dei PC. Le stime del 2002 indicano che un 10% di computer notebook è già venduto con l'adattatore WLAN integrato: pertanto questi notebook non richiedono l'aggiunta di una scheda PCMCIA (Gartner Dataquest prevede che esse rappresenteranno il 31% nel 2004 e il 68% nel 2007).
Questa soluzione è naturalmente più economica della scheda esterna ed è destinata a contribuire alla riduzione dei prezzi e, quindi, alla diffusione della tecnologia WLAN, non più solo in ambiti professionali ma sempre più rapidamente anche in ambiti domestici.
La sensibile crescita del mercato fa anche prevedere una fase di selezione nel corso dei prossimi 2-3 anni, con la sopravvivenza di un solo numero molto ridotto di produttori di adattatori WLAN.
Il segmento dei fornitori di infrastrutture WLAN e degli integratori di sistema che adotteranno queste soluzioni rimarrà, invece, presumibilmente molto ampio, per la grande differenza tra le esigenze dei vari mercati, segmentati sia su base geografica che su base applicativa.

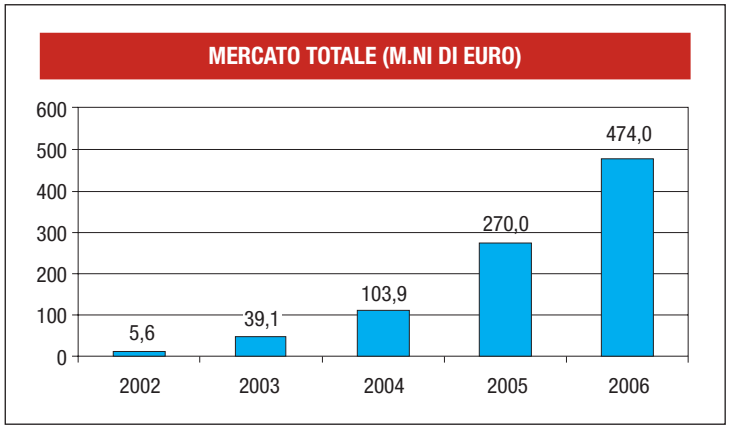


FIGURA 6
Previsioni per i mercati privato e pubblico in Italia (Fonte: Databank)

Anche in Italia, sia pure in ritardo rispetto agli USA, si prevede un mercato in rapida crescita. La figura 6 mostra le previsioni di Databank per i mercati privato e pubblico in Italia [5]. La stima riguarda i servizi di connettività Wi-Fi e include costi per hardware (punti d'accesso e schede wireless) e per servizi di rete e di connettività.
Nel settembre 2002 si contavano circa 50 operatori che operano in Italia nel settore delle WLAN, fra questi vi sono circa 10 aziende manifatturiere di apparati (per esempio, Cisco, Compaq ecc.).
Si è avuto, inoltre, un significativo incremento nel numero delle aziende che offrono prodotti di gestione di rete o soluzioni di integrazione di sistema. Contemporaneamente, operano, inoltre, circa 20 operatori che offrono connettività Internet, apparati e soluzioni per WLAN sia nel settore degli affari che in quello residenziale.

6. SERVIZIO WLAN IN AMBITO PUBBLICO: ASPETTI TECNOLOGICI

Come precedentemente accennato, le WLAN possono essere utilizzate anche in ambienti aperti al pubblico e non solo all'interno delle aziende. Sta di conseguenza nascendo un nuovo business finalizzato all'offerta al pubblico di servizi di accesso a Internet a larga banda in tecnologia *Wi-Fi*. Presso specifici luoghi aperti al pubblico, che vengono detti hotspot, quali aeroporti, stazioni ferroviarie, alberghi, centri congressi, fiere ecc., il forni-

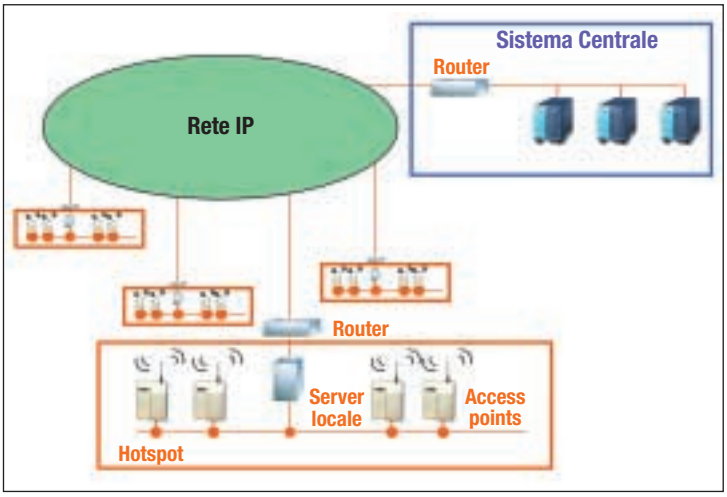


FIGURA 7
Architettura di sistema hotspot pubblico

tore del servizio, che prende in tal caso il nome di WISP (*Wireless Internet Service Provider*), installa una o più AP mettendo a disposizione di un utente, equipaggiato di computer portatile o di PDA (*Personal Digital Assistant*), un collegamento wireless alla rete. Il servizio può essere limitato all'accesso a Internet oppure può includere la realizzazione di una rete privata tramite VPN (*Virtual Private Network*), con la propria azienda, con o senza garanzia di QoS.

Per offrire un servizio pubblico gli aspetti progettuali sopra elencati con specifico riferimento all'ambito aziendale devono essere affrontati sulla base di criteri maggiormente restrittivi, specialmente per quanto concerne la sicurezza. Una volta prese le decisioni di progetto fondamentali, la realizzazione di un'architettura per erogare i servizi Wi-Fi è di norma semplice: a titolo esemplificativo, può essere fatto riferimento alla configurazione mostrata in figura 7, pur tenendo a mente che sono attuabili soluzioni diverse in funzione dell'ampiezza e della complessità dell'area pubblica da servire:

a. presso gli hotspot si dispone di un *server* locale (che può anche servire più hotspot direttamente collegati tra loro), che provvede solitamente alle funzioni di:

- servizio web informativo aperto a tutti;
- identificazione dei terminali mobili;
- gestione dell'indirizzamento IP locale;
- interrogazione dei sistemi centrali circa la validità delle credenziali dei terminali mobili;
- protezione dei collegamenti locali;
- controllo dell'accesso ai servizi oggetto di contratto (per esempio, solo accesso a Internet, oppure anche una VPN aziendale ecc.);
- gestione delle eventuali procedure di handover e di gestione della banda;

b. gli hotspot sono connessi direttamente a Internet, e dispongono di un collegamento protetto (per esempio, VPN) verso i sistemi centrali;

c. i sistemi centrali offrono a tutti gli hotspot e al gestore una serie di funzioni comuni, che comprendono almeno:

- l'attivazione dei contratti con i clienti, e relativa fornitura dei codici e delle schede prepagate;
- il servizio di autorizzazione delle credenziali presentate dai clienti;
- l'autenticazione da e per gli altri operatori per i clienti in *roaming*;
- la gestione amministrativa dei contratti e delle fatturazioni;
- l'interfaccia dei clienti con *help desk* e *call center*;
- gli altri servizi analoghi a quelli forniti da un tradizionale ISP (*Internet Service Provider*) quali, per esempio, il portale, *webmail*, *mail server* ecc..

In attesa che venga emanato un quadro regolamentare chiaro e armonizzato con le direttive europee, sono in allestimento in Italia diversi hotspot in aree aperte al pubblico a fini sperimentali, seguendo il dettato del D.P.R. 447/2001. L'obiettivo perseguito da queste sperimentazioni riguarda l'esigenza di superare alcuni problemi tecnologici legati all'estensione del servizio WLAN in aree pubbliche, oltre all'opportunità di verificarne sul campo l'impatto sui potenziali utilizzatori. Per lo più i problemi tecnologici da affrontare dipendono dal fatto che le WLAN non sono state concepite per la fornitura di servizi al pubblico ma come estensione wireless della Ethernet aziendale. Essi possono essere così classificati [6]:

- semplicità d'uso
- sicurezza
- qualità di servizio
- mobilità
- management di rete.

6.1. Semplicità d'uso

La semplicità d'uso è un requisito assai sentito dalla clientela che non dispone in gene-

rale di approfondite conoscenze di informatica e di reti di telecomunicazioni. Le operazioni oggi richieste sono ancora ardue, dalla configurazione delle chiavi per crittografia dei dati, a complesse impostazioni di parametri per l'accesso alla rete, all'installazione di software per il funzionamento dei dispositivi. Molte di queste operazioni sono motivate dalla necessità di assicurare un adeguato livello di sicurezza nell'autenticazione del cliente. Il requisito operativo richiede, quindi, un compromesso accettabile tra facilità di utilizzo e grado di sicurezza garantito, tenendo sempre conto che semplicità e sicurezza sono comunque requisiti conflittuali.

6.2. Sicurezza

La sicurezza nelle reti informatiche presenta vari aspetti tra cui:

1. la prevenzione dell'accesso non autorizzato e l'identificazione dei clienti autorizzati, (l'autenticazione);
2. la garanzia della segretezza dei dati (confidenzialità o *privacy*);
3. la protezione contro le manipolazioni dei dati in transito (integrità);
4. la garanzia di paternità dei dati (autenticità);
5. l'accertamento incontrovertibile della transazione (non ripudiabilità).

Fra questi, nei sistemi che impiegano l'accesso wireless gli elementi che richiedono una specifica attenzione sono l'autenticazione e la confidenzialità.

L'autenticazione può in generale avvenire con uno dei due sistemi di crittografia con chiave privata (o pre-condivisa) e con chiave pubblica. Nel Wi-Fi, attualmente, si adotta la tecnica di autenticazione a chiave pre-condivisa, conosciuta con il nome di SKA (*Shared Key Authentication*).

L'autenticazione è il processo di identificazione dell'utente, che di solito avviene sulla base di *username e password* (oppure attraverso certificati digitali). In ogni caso, in ambito wireless conviene eseguire la trasmissione criptata dei dati di autenticazione. Quando il punto di accesso (AP) riceve una richiesta d'accesso in rete da parte di un terminale risponde con un numero casuale. Il terminale firma il numero casuale utilizzando una chiave segreta pre-condivisa e invia la risposta all'AP. Quest'ultimo calcola la firma e confronta il risultato ottenuto con quello inviato dal terminale: se i due risultati coincidono, il terminale è autenticato e gli viene consentito l'accesso.

L'attuale protocollo per la confidenzialità nel WLAN a standard IEEE 802.11b è il WEP (*Wireless Equivalent Privacy*): il protocollo, attuato a livello MAC, è opzionale nello standard ed è stato concepito in origine con l'obiettivo di assicurare una privacy equivalente a quella offerta da Ethernet via cavo. Se il WEP è attivato, il flusso dati trasmesso dal NIC è criptato utilizzando un algoritmo standard (detto RC4), basato su una chiave segreta a 40 bit e su un vettore di inizializzazione a 24 bit e che comprende anche un dato di controllo per assicurare l'integrità dei dati; la stazione ricevente, che deve conoscere esattamente la chiave, descrive la trama ricevuta. Sia la tecnica di autenticazione che l'algoritmo WEP risultano poco efficaci [12]. Molte reti non sono sicure semplicemente perché il WEP non viene attivato e, quindi, le trasmissioni avvengono in chiaro. Inoltre, la scelta della chiave pre-condivisa rappresenta un elemento di vulnerabilità in quanto la chiave deve essere scambiata via radio fra NIC e AP. Poiché lo standard 802.11 non supporta la funzionalità di scambio dinamico delle chiavi, queste rimangono in uso per tempi anche molto lunghi (mesi o addirittura anni) senza essere modificate dal gestore di sistema.

Un altro elemento di vulnerabilità della sicurezza discende dall'unidirezionalità della tecnica di autenticazione dello standard IEEE 802.11b: il punto d'accesso, infatti, può autenticare il terminale ma quest'ultimo, in nessun modo, può autenticare il primo. Pertanto, un nodo di rete intruso può spacciarsi per AP senza che il terminale possa verificarne l'autenticità. Si noti che questa eventualità non è remota, in quanto la semplicità della connessione in rete degli AP è considerato proprio uno dei punti di forza del Wi-Fi.

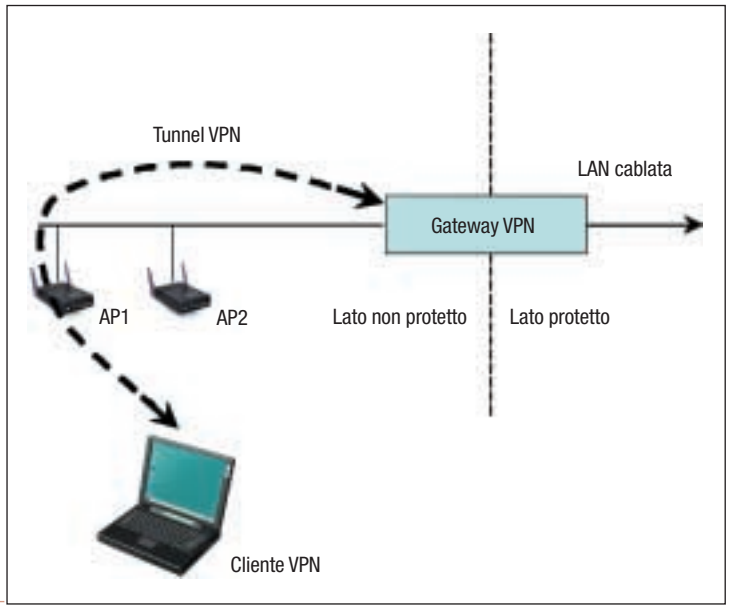
Per risolvere l'insieme dei problemi di sicurezza, si possono proporre sia soluzioni "native" (ossia, a livello di sottostrato MAC) che soluzioni esterne al Wi-Fi (livello OSI 3) che sono studiate nell'ambito del *802.11 Task Group* i incaricato di predisporre lo standard IEEE 802.11 i: le più note di esse vanno, rispettivamente, sotto il nome di *Enhanced*

WEP e *Tunnel VPN*. Per rispondere ai requisiti di semplicità d'uso si potrà ricorrere a un'autenticazione con username e password criptate (SSL, *Secure Socket Layer*, SE ACRONIMO VA ESPLICITATO) e alla protezione dei dati con tunnel IPSec. Il tunnel IPSec (*Secure Internet Protocol*), impiegato nelle applicazioni Intranet aziendali, deve essere realizzato tra il terminale d'utente e il *gateway* VPN situato a monte del AP: questa soluzione mostrata in figura 8, fornisce un'ottima protezione ma con costi addizionali (*gateway* VPN).

6.3. Qualità di servizio

Un altro requisito di rilievo per la fornitura di un servizio pubblico è la garanzia di qualità di servizio (QoS); d'altra parte, nel caso di accesso condiviso alla risorsa comune da parte di molteplici utenti, alcune richieste possono non risultare soddisfatte. Per la risoluzione del problema è impegnata la IEEE 802.11 *Task Force* e; inoltre, alcune manifatturiere hanno implementato negli AP la funzionalità detta PCF (*Point Coordination Function*) che attribuisce priorità sul profilo di utente o sul servizio. Tale soluzione è però solo parziale poiché oltre a non assicurare una banda predefinita all'utente, agisce solo nella tratta radio in discesa.
Attualmente, non è ancora possibile assicurare livelli differenziati di QoS entro le WLAN. La possibilità di differenziare su diversi livelli la qualità della connessione va considerata almeno in relazione a due evenienze: in relazione al protocollo utilizzato (per esempio, con l'attribuzione di una priorità più elevata a un flusso video rispetto alla posta elettronica); in relazione alla WLAN di appartenenza (per esempio, con la creazione di diversi profili d'utente con diverse priorità nella fornitura del servizio).
Per gestire la QoS risulta fondamentale il controllo remoto della rete, indipendentemente dal produttore dell'AP o dalla scheda per l'accesso. Infatti, sia i WISP che gli utenti usufruiranno, in generale, di dispositivi prodotti da differenti manifatturiere senza che ciò debba rappresentare una limitazione al servizio.

FIGURA 8
Tunnel VPN



6.4. Mobilità

La mobilità in reti WLAN, in realtà, abbraccia molteplici funzionalità non ancora incluse nello standard IEEE 802.11. Il primo requisito di mobilità è il cosiddetto requisito di *close and go - open and resume* che consiste nel mantenere attiva la sessione del cliente che si muove da un'area di copertura a un'altra ponendo in *stand-by* il proprio computer portatile; in tal caso, quando il PC viene riattivato, occorre fornire all'istante una connessione sicura al cliente. Inoltre, se i due hotspot interessati non appartengono allo stesso WISP occorre anche assicurare la trasparenza nel cambiamento di rete servente attraverso la funzionalità di roaming. Un requisito di mobilità a livello di rete ancora più stringente, applicabile al caso di terminali PDA in movimento, concerne il *seamless hand-over*, funzionalità che consente all'utente di muoversi in aree di copertura di AP adiacenti, dello stesso operatore o di operatori differenti, mantenendo il terminale sempre operativo, cioè senza interruzione del flusso dati; tale requisito, meno importante per servizi dati a bassa velocità, è viceversa necessario per servizi in tempo reale come la fonia o l'acquisizione di flussi video (*streaming*).
La tecnologia oggi considerata più adatta ad assicurare la mobilità entro le reti *wireless* è la tecnologia IP mobile [8]; tale tecnologia è basata su una gestione centrale della mobilità mediante il cosiddetto *home agent* e sulla mobilità nella rete ospite mediante *foreign agent*. IP mobile, tuttavia, non è ancora disponibile nei principali sistemi operativi

(Windows, Mac) e quindi non è attualmente di agevole implementazione.
L'ultimo aspetto ancora aperto del problema della mobilità consiste nell'interoperabilità con le reti cellulari di seconda e terza generazione, necessaria a garantire una più ampia diffusione dei servizi WLAN senza pratiche limitazioni geografiche. In tal caso, occorre tra l'altro risolvere problemi di accordi per la tariffazione tra ISP e WISP; è necessario un unico sistema di accesso alla rete (SIM *card*); infine, occorre risolvere congiuntamente i problemi di gestione della rete.

6.5. La gestione di rete

La gestione di rete è, da tempo, un "valore" consolidato nelle reti cablate, ma le WLAN presentano problemi specifici che non consentono un immediato riutilizzo di strumenti software esistenti. Infatti, le prestazioni di una rete wireless sono strettamente legate alle condizioni dello strato fisico e, pertanto, bisogna gestire dinamicamente la rete per assicurare un adeguato segnale radio in presenza di potenza utile fortemente variabile e interferenze di varia natura. D'altra parte, le reti cellulari hanno già affrontato problemi analoghi ma sono state progettate sin dall'inizio come sistemi integrati con *tool* specifici di gestione molto potenti; inoltre, il rilascio delle frequenze sotto licenza in questi casi destina le risorse spettrali a ciascun operatore e, quindi, non insorgono interferenze tra gestori diversi.
Viceversa, la banda WLAN è di libero uso e non è possibile la pianificazione dello spettro radio delle frequenze fra i diversi utilizzatori: pertanto, bisogna operare necessariamente a livello di gestione della rete per limitare i danni prodotti dalle interferenze isocanale. Inoltre, come si è visto, occorre che il management di rete assicuri la diversificazione dei servizi e delle modalità della loro fornitura anche in termini di qualità differenziata, nonché contribuisca a risolvere i problemi di sicurezza. Uno specifico problema di gestione della sicurezza è rappresentato dalla possibile introduzione non autorizzata di un AP nella rete aziendale, da parte di impiegati o altri soggetti, senza rispettare le politiche di sicurezza previste per la rete. L'installazione di un AP è simile all'introduzione di un hub in una rete Ethernet convenzionale e, se non si adottano le necessarie contromisure, chiunque sia dotato di un adattatore wireless può connettersi agevolmente: si tratta del problema del cosiddetto *rogue AP* (AP del monello), in quanto anche un ragazzo scaltro e informatizzato è in grado di installare un AP violando così le regole di sicurezza stabilite per la rete. Evidentemente questa eventualità deve essere contemplata dall'amministratore di rete che deve disporre di strumenti atti a consentirgli di intervenire con tempestività ed efficacia.
Inoltre, il sistema di *management* di rete deve, comunque, rispondere a funzionalità di autodiagnosi, di misura di *throughput* e del livello di segnale ricevuto sia dal terminale che dall'AP. Tutte queste funzionalità saranno contemplate in future versioni dello standard IEEE 802.11.
Infine, attualmente, le maggiori manifatturiere dispongono di strumenti software per gestire i propri apparati: tuttavia, la possibilità per un amministratore di rete di ampliare la propria WLAN in qualunque momento è vincolata dalla necessità di installare dispositivi affini a quelli esistenti, nonostante la standardizzazione Wi-Fi, anche a causa dei differenti e incompatibili prodotti di gestione.

7. SVILUPPO DEL SERVIZIO WLAN IN AMBITO PUBBLICO

È opinione ormai diffusa che i problemi tecnologici ancora aperti siano rapidamente risolvibili e pertanto, tenuto anche conto di un clima regolamentare generalmente incoraggiante, le previsioni di sviluppo di mercato degli hotspot pubblici sono favorevoli. Per esempio, Gartner Dataquest prevede che nel 2006 si conteranno oltre 19 milioni di clienti di questi servizi che accederanno ai servizi da 38.000 hotspot. Per la società BWCS gli hotspot attivi nel medesimo anno saranno addirittura 114.000.
Negli Stati Uniti d'America il mercato ha avuto sostanzialmente avvio nel 2002, quando T-Mobile, il principale operatore cellulare tedesco, ha acquisito la catena MobileStar. T-Mobile ha poi concluso accordi con alcune grandi catene commerciali, prima fra tutte la catena di caffè StarBucks, portando rapidamente il numero di hotspot

TABELLA 1

Servizio Wi-Fi in aree pubbliche: situazione USA nel 2002 - Totale abbonati: ~ 15.000, (Fonte: Insight on Wireless)

Fornitori Wi-Fi	Numero di abbonati	
T-mobile	9.750	(65%)
Wayport	1.500	(10%)
Boingo	900	(6%)
WiFiMetro	450	(3%)
SurfNSip	450	(3%)
Altri	1.950	(13%)
Totale	15.000	100%

TABELLA 2

T-mobile e Wayport hanno coperto insieme, nel 2002, più dell'80% delle aree pubbliche servite dal Wi-Fi (Fonte: Insight on Wireless)

Fornitori Wi-Fi	Percentuale delle aree servite da ciascun fornitore Wi-Fi
T-mobile	60%
Wayport	23%
SurfNSip	5%
WiFiMetro	3%
Joltage	2%
Altri	7%

attivi a 1300 e pianificandone altri 800 a breve con coperture anche in Gran Bretagna e Germania. Nella tabella 1 si riportano il numero degli abbonati e, rispettivamente, nella tabella 2 il numero di hotspot dei principali WISP operanti negli USA. A fronte del ridotto numero di clienti, si conta comunque già su un ampio numero di hotspot: il numero delle aree di accesso a disposizione dell'utenza è chiaramente uno dei fattori chiave per la crescita del servizio.

Un altro elemento di rilievo è rappresentato dallo sviluppo della normativa. In questo settore, il Paese più all'avanguardia è l'Australia che ha temporaneamente esentato i WISP da oneri concessori. Per ottenere l'autorizzazione a operare in qualità di WISP nel prossimo futuro dovrebbe essere richiesto un versamento annuo esiguo (dell'ordine di qualche migliaio di euro) oltre a una modesta percentuale sui ricavi. Come è noto in Europa si è in attesa dell'approvazione del nuovo quadro di regolamento da parte della Commissione Europea, previsto per l'estate del 2003 e, a breve, si prevede anche il varo della normativa italiana. La regolamentazione, attualmente in elaborazione, presumibilmente sarà basata sui seguenti criteri:

- estensione dell'uso della banda ISM dal solo uso privato all'uso pubblico con il conseguente venir meno, o forte limitazione, del concetto di impiego nel solo "fondo di proprietà";
- regolamentazione dell'uso della banda ISM per servizi Wi-Fi sulla base di concetti non discriminatori e di piena concorrenza tra gestori differenti in qualsiasi locazione;
- attuazione di un regime normativo con requisito di autorizzazione generale (molto meno onerosa e più semplice della licenza);
- riduzione delle possibilità di competizione con l'UMTS, al fine di non penalizzare i relativi investimenti.

Dal punto di vista tecnico, d'altra parte, come si è visto, il regime delle interfere radio tipiche della banda ISM, rappresenterà di per se stesso un forte deterrente a realizzare hotspot sovrapposti nella medesima locazione da parte di gestori in concorrenza, per quanto non si potrà escludere, e anzi potrebbe risultare sempre più la regola, che in aree grandi e potenzialmente ad alto traffico si comincino a realizzare coperture da parte di una molteplicità di gestori diversi per servire aree adiacenti. Esempi tipici possono essere un grande aeroporto, ove *terminal* differenti potrebbero essere serviti da differenti gestori Wi-Fi, un campus universitario con molte facoltà anch'esse coperte da gestori differenti ecc..

Il quadro fin qui delineato apre un problema, in prospettiva temporale anche piuttosto ravvicinata (prossimi anni), di esigenza di roaming automatico tra reti differenti, in quanto sarebbe inaccettabile che un utente debba rinunciare al servizio in cui la copertura Wi-Fi è garantita da un gestore cui esso non è abbonato, ovvero, che debba ricorrere a molteplici contratti e a complesse operazioni di inizializzazione, oltre alla scomodità di non poter mantenere la propria sessione attiva. Sono allo studio diversi approcci al problema del roaming multioperatore:

- contratti di roaming bilaterali da stipularsi tra tutti i WISP (in analogia al GSM, *Global System for Mobile Communication*);

Il servizio di aggregazione, fornito da un operatore che rappresenti l'unica interfaccia contrattuale del cliente, indipendentemente dall'effettiva rete che lo sta servendo, verso tutti gli operatori WISP che offrono il servizio di connettività.
Dal punto di vista del modello di business Wi-Fi occorre distinguere quattro fondamentali funzionalità: il servizio d'accesso, quello di autenticazione, il roaming e la tariffazione. Gli attori coinvolti sono l'utente finale, il proprietario della locazione (aeroporto, hotel ecc.), il WISP e, infine, il gestore di rete fissa/mobile. Ciascuno possiede requisiti differenti: l'utente chiede un costo contenuto, servizi a valore aggiunto e personalizzati, facilità d'uso e un accesso sicuro alle risorse aziendali; il proprietario della locazione chiede accesso per tutti i clienti (anche con carte prepagate), un coinvolgimento minimo nella gestione della rete e dei servizi e, infine, la possibilità di inserire contenuti locali; il WISP richiede di avere accesso a molteplici operatori fissi e mobili, ai fornitori di contenuti, l'acquisizione e la manutenzione dei siti Wi-Fi, oltre alla visibilità del proprio *brand*; infine il gestore di rete necessita di assicurarsi una quota del mercato degli hotspot per realizzare utili attraverso la generazione del traffico nella propria rete, fornire servizi addizionali alla propria clientela per una migliore fidelizzazione e, l'integrazione semplice della rete d'accesso Wi-Fi con i propri sistemi/servizi.

8. CONCLUSIONI

Wi-Fi si propone come una soluzione a basso costo, rapidamente installabile, senza specifici requisiti di manutenzione e di facile impiego per sostenere e favorire la crescente richiesta di connettività wireless ubiquitaria e multimediale dell'utente affari.
È in corso un significativo sforzo tecnologico per passare dalle reti aziendali e domestiche alle reti in aree pubbliche. Esistono, tuttavia, ancora alcuni importanti problemi tecnologici da risolvere tra cui: facilità d'uso, sicurezza, qualità di servizio, mobilità, management di rete. Il mercato appare fiducioso su un favorevole sviluppo sia delle necessarie tecnologie che del quadro regolamentare e gli attori potenzialmente coinvolti, dai gestori di rete fissa/mobile, ai WISP, ai proprietari di locazione e, infine, gli stessi utenti finali si stanno già attrezzando per l'impiego delle imminenti reti Wi-Fi pubbliche.

Bibliografia

[1] AEGIS - Spectrum Management Advisory Group: *Demand for use of the 2.4 GHz ISM band*, 1215/AE/ISM2/R/2, Final Report (2001).

[2] Blueprint Wi-Fi – Issue 7, 26 September 2002 – "73 percent WLAN growth in 2002".

[3] Business Week Online: *All Net, All the Time*. Special Report Wireless Internet, April 29, 2002.

[4] Colonna M, D'Aria G: Wireless LAN: tecnologie e applicazioni. *Notiziario Tecnico Telecom Italia*, anno 11, n. 1, giugno 2002, p. 67-86.

[5] Databank Consulting: *Wireless LAN in Italia: Lo scenario evolutivo, i mercati Wi-Fi e la mappa delle "hot spot locations"*. 2002.

[6] Henry PS, Luo H: WiFi: What's Next?. *IEEE Comm. Magazine*, Dec. 2002, p. 66-72.

[7] IEEE: http://standards.ieee.org/getieee802/802.11.html

[8] Perkins CE: Mobile IP. *IEEE Communication Magazine*, maggio 1997, p. 84-99.

[9] Vannucchi G. (a cura di): *Possibili interventi migliorativi della gestione delle risorse spettrali*. Consiglio superiore PT, Gruppo di lavoro 6, Relazione finale, 2001.

[10] Wireless Local Area Network Association: www.wlana.com.

[11] WiFi Alliance: http://www.wi-fi.org

[12] Wi-Fi Alliance, 6 Feb. 2003: *Securing Wi-Fi Wireless Networks with Today's Technologies*. Sito http://www.wi-fi.org

Carlo Alberto Marchi è Amministratore Delegato della PointerCom Spa, azienda che realizza architetture per l'erogazione di servizi di telefonia e videocomunicazione in protocollo IP. L'ing. Marchi è specializzato nel campo delle telecomunicazioni, in particolare nelle reti in protocollo IP sia con connettività fissa che in radiofrequenza. Ha pubblicato alcuni testi e numerosi interventi in conferenze nel settore.
ca.marchi@pointercom.it

Francesco Vatalaro è professore di Telecomunicazioni presso l'Università di Roma "Tor Vergata". È presidente del Consorzio Università Industria – Laboratori di Radiocomunicazioni (RadioLabs) e direttore scientifico del progetto di ricerca VICOM (*Virtual Immersive Communications*) del MIUR. La sua attività scientifica include i sistemi radiomobili e via satellite. È autore di circa 150 pubblicazioni.
vatalaro@uniroma2.it