Mobilità e reti wireless

Franco Canna

Assintel ha reso disponibili i risultati di una ricerca realizzata da Mate su reti wireless e tecnologie a supporto. L'indagine, basata su un campione di 400 aziende italiane di medie dimensioni, ha evidenziato una serie di punti - costi, interferenze, sicurezza - sui quali si è articolato un interessante dibattito che ha coinvolto le aziende presenti, con un occhio di riguardo all'aspetto funzionale della questione: la mobilità.

Partendo da un'indagine di mercato, attraverso anche alcuni *speech* tecnici e interventi di carattere aziendale, un convegno organizzato da Assintel dal titolo "Reti wireless e tecnologie a supporto" è stato l'occasione per approfondire le tematiche legate al concetto di mobilità: un tratto emergente dell'organizzazione sociale che sempre più riceve il supporto della tecnologia.
Wireless e mobilità sono temi strettamente correlati: sempre più, infatti, il luogo di lavoro tende a essere il luogo dove sta il lavoratore e non l'ufficio. Manager, operatori sul campo, forze vendita, operatori dei servizi pubblici di mobilità, attraverso una vasta gamma di dispositivi, dagli smartphones ai palmari, ai tablet, ai notebook, accederanno a servizi tradizionali adattati al mondo *mobile* e a servizi nuovi appositamente sviluppati e resi disponibili, in taluni casi, negli *hot-spot*, i luoghi ad accesso pubblico con copertura wireless.
Il rilievo sociale delle trasformazioni in atto mette in gioco l'attività politica e normativa degli Enti (sindacati, governo, sanità ecc.) e questo introduce un considerevole fattore di incertezza sulla velocità della diffusione delle tecnologie.
I temi caldi sono quello della disponibilità del dispositivo in termini di durata delle batterie, della disponibilità di vari *form factor* degli schermi, delle diverse capacità di archiviare e trasportare i dati e, soprattutto, della sicurezza.

Tecnologie e mercato

Che diffusione hanno le tecnologie wireless nella media azienda italiana? A questo interrogativo hanno risposto 400 aziende, con risultati in alcuni casi sorprendenti. Innanzitutto va chiarito che il mondo delle comunicazioni wireless è composto da due grandi parti: la comunicazione *wide area* e quella di tipo locale più o meno ristretta. Alla prima tipologia di comunicazione fanno capo, in ordine cronologico e di capacità tecnologica, il Gprs e l'Umts: in altre parole, il mondo Telecom. Alla seconda tipologia fanno invece capo le tecnologie (Bluetooth, Wi-Fi e HyperLan) indirizzate alla comunicazione intra- e inter-aziendale (nonché ad uso domestico); ed è quest'ultimo il campo di indagine prescelto. Va detto, peraltro, che Marco Pancotti – relatore dello studio Mate – non esclude una possibile concorrenza del Wi-Fi anche sul terreno wide-area dell'Umts: dato il basso costo di implementazione e la maggiore disponibilità di banda, sarebbe infatti possibile che, grazie ad accordi di roaming, una successione ordinata di Access Point permetta anche di realizzare collegamenti a distanze ragguardevoli.

A) Il Wi-Fi

Il mondo dell'802.11 è estremamente vario. Nella Tabella 1 sono riassunte le caratteristiche dei principali protocolli standardizzati dall'Ieee. Esistono, poi, anche altri protocolli – molti dei quali ancora in fase di sperimentazione – studiati per andare incontro a specifiche esigenze.
Le reti wireless possono essere strutturate su due diverse architetture: una basata su un Access Point, a sua volta collegato alla Lan aziendale, al quale si connettono le unità mobili dotate di dispositivi di ricezione; una seconda modalità di creazione di network è il peer-to-peer. In tale configu-

1) I principali protocolli di trasmissione del tipo 802.11

	802.11a	802.11b (Wi-Fi)	802.11g	802.11b+
Frequenza (GHz)	5,15 - 5,35 e 5,47 - 5,72	2,4 - 2,497	2,4 - 2,497	2,4 - 2,497
Modulazione tipo	Ofdm	Dsss	Dsss/Ofdm	Dsss/Pbcc
Canali non overlapping	8	3	3	3
Bit Rate teorico (Mbps)	54	11	54	22/44
Bit Rate reale	25 - 31	3 - 5,7	21 - 26	5,7 - 14
Copertura reale (metri)	30	100	100	100

Fonte: D-Link

2) Le estensioni future del protocollo

802.11d	semplifica il roaming internazionale
802.11e	implementa elementi di QoS (Quality of service) aggiuntivi rispetto a 802.11b e 802.11a
802.11f	permette di non avere problemi di roaming tra access point di produttori diversi
802.11h	uno sviluppo dell'802.11a che intende fornire un miglior controllo sulla trasmissione e sulla selezione dei canali radio
802.11i	affronta i problemi di sicurezza di dati e trasmissioni

razione più unità terminali possono comunicare tra loro direttamente realizzando una piccola rete paritetica, generalmente impiegata quando serva una piccola rete per breve tempo o specifiche esigenze (riunioni, convegni, stand, dimostrazioni). La modalità di gran lunga più diffusa è comunque la prima. La tecnologia attualmente dominante è quella basata sullo standard 802.11b, in grado di garantire una banda di 11 Mbps. La tecnologia che sostituirà presto l'802.11b probabilmente non sarà la 802.11a, che, operando sulla banda di 5 GHz, non è compatibile con i dispositivi 802.11b, bensì la 802.11g che, con una banda di 55 Mbps migliora significativamente le performance senza introdurre discontinuità. I nuovi prodotti della Apple hanno già adottato questo standard.
Lo standard 802.11g rimarrà sul mercato probabilmente fino alla fine del 2004. Dal 2005 è previsto lo sviluppo degli standard 801.11i e 802.11h che permetteranno larghezze di banda ancora superiori e migliore gestione della sicurezza, in attesa del nuovo 802.15, destinato a risolvere i problemi di compatibilità tra Bluetooth e Wi-Fi. Gli Access Point si stanno evolvendo, integrando capacità proprie di altri dispositivi di rete. Sempre più comune, e sempre più economica, è l'offerta di Access Point in grado di essere allo stesso tempo Access Point, modem Adsl o Isdn, router, firewall e Dhcp server, risolvendo in modo definitivo il problema della disponibilità dell'accesso ad Internet di una rete SoHo. Alcuni produttori hanno poi recentemente (fine 2002) introdotto sul mercato Access Point in grado di sostenere contemporaneamente la connettività Bluetooth e quella 802.11, che permettono la gestione di una connettività verso laptop e Pda dotati del solo dispositivo Bluetooth, integrandoli in un contesto di larga banda e di local networking misto. La fascia alta dei notebook comincia ad integrare una connettività Wi-Fi.
Nel contesto dei notebook, il dispositivo Wi-Fi seguirà probabilmente il corso dei modem e delle connessioni Ethernet che in pochi anni sono passati da optional a built-in in tutta la gamma di prodotto. Interessante al riguardo, è la campagna da 300 milioni di dollari iniziata il 12 Marzo 2003 da parte di Intel a favore di Centrino, un chipset a basso consumo studiato per andare incontro alle esigenze del lavoratore mobile, che sarà utilizzato nei computer portatili garantendo la connettività 802.11.

Mercato
Nel 2002 sono state vendute 18 milioni di unità (tra schede e Access Point) a livello mondiale. I due terzi della domanda circa (65%) proviene dal comparto business, ma è la quota consumer, che ha, tuttavia, mostrato segni di crescita più rapida. Per l'intera offerta si prevede una crescita del 40% annuo (Cagr, Compound Average Growth Rate) fino a raggiungere nel 2006 70 milioni di unità. Il fatturato attuale ammonta a circa 2 miliardi di dollari e non è destinato a crescere in misura proporzionale ai quantitativi: nel 2006, infatti, il valore del venduto ammonterà a cinque miliardi di dollari. Il perché va imputato alla prevista erosione dei prezzi in atto. I calcoli Mate fissano i prezzi asintotici per le schede in 90-100 euro, mentre quelli per le schede a 20-30 euro (per prezzo asintotico si intende quel livello di prezzo considerato "giusto" dal mercato, che non diminuisce e non aumenta). Raggiunti questi livelli (e non si è troppo lontani) il prezzo rimarrà costante anche a fronte di miglioramenti tecnologici.
Va messo in conto che un'ulteriore possibilità di sviluppo del Wi-Fi è legata allo sviluppo della possibilità di implementare sulle sue frequenze servizi di comunicazione Voice-over-Ip.

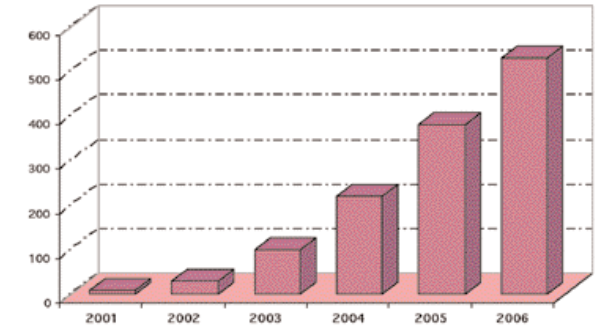
Il nodo sicurezza
È "war driving" il termine che viene in mente quando si parla di sicurezza in ambito Wi-Fi. Il nome nasce in analogia al "war dialing" (una pratica che consiste nel chiamare numeri telefonici alla ricerca della risposta di un modem), e consiste nell'utilizzare indebitamente le reti wireless che "esondano" da appartamenti e uffici, captandole tramite una rudimentale antenna.
I due meccanismi a cui lo standard Wi-Fi affida il compito di gestire la sicurezza sono il Ssid (Service Set Identifier), consistente in una parola chiave condivisa tra tutti i dispositivi connessi all'interno di una rete wireless ed utilizzata per una prima autenticazione dei dispositivi appartenenti alla stessa WLan; e il Wep (Wired Equivalent Protocol), un protocollo che ha il compito di crittografare le informazioni scambiate in rete e di introdurre un controllo di integrità nelle stesse. Con l'adeguata combinazione hardware (scheda WLan) e software (sniffer disponibili su Internet) un *cracker* può identificare l'Ssid, che è trasmesso in chiaro, ed entrare quindi nel processo di autenticazione ed associazione previsto dal protocollo. Anche il protocollo Wep che utilizza l'algoritmo di cifratura RC4, può essere violato: poche ore di

"ascolto" possono essere sufficienti ad un *hacker* adeguatamente attrezzato per impostare i suoi parametri in modo da entrare a far parte della rete. È possibile programmare gli Access Point in modo tale da permettere l'accesso solo a determinati indirizzi Mac, ma vi sono strumenti software che permettono di intercettare anche questi codici Mac. Inoltre un codice Mac identifica al massimo un dispositivo hardware, e non chi lo sta usando: un banale furto di una scheda di accesso, o una dimenticanza nella Acl (Access Control List) di un Access Point permetterebbe ad un malintenzionato un facile collegamento. La conclusione è che, allo stato attuale delle cose, per rendere sicura una rete wireless non basta applicare gli accorgimenti previsti dal protocollo Wi-Fi. Per far fronte a questo problema il consorzio Wi-Fi ha definito un nuovo standard di sicurezza, denominato Wpa (Wi-Fi Protected Access), adottabile come semplice upgrade software dei dispositivi esistenti. Il Wpa sarà basato sul protocollo Temporal Key Integrity (Tkip) che permetterà funzioni di "per-packet key mixing", un controllo dell'integrità di messaggio, un vettore esteso di inizializzazione con regole di sequencing ed un meccanismo di re-keying. Inoltre il Wpa introdurrà l'Extensible Autentication Protocol (Eap) che si baserà su un server centrale di autenticazione Radius (Remote Access Dial-In User Service) e che utilizzerà un sistema di mutua identificazione. Dove non sia disponibile un server Radius, il Wpa prevede l'uso di una password di autenticazione. Il Wpa anticipa l'introduzione del protocollo 802.11i, atteso per il 2004.
In attesa della disponibilità del Wpa, la miglior soluzione perseguibile per garantire un adeguato livello di sicurezza è quello di implementare una Vpn (Virtual Private Network) che permetta una identificazione degli utenti e che introduca un livello di crypting aggiunto a quello Wep.

B) Il Bluetooth

Decisamente più nota – non foss'altro per la sua diffusione a livello di dispositivi consumer come stampanti e telefoni cellulari – è la tecnologia Bluetooth, promossa dalla svedese Ericsson e appoggiata dal Bluetooth Sig, un consorzio di sviluppatori. Bluetooth ha recentemente recuperato credibilità, a seguito di un adeguamento delle aspettative degli utenti: inizialmente infatti si era creato un eccessivo entusiasmo, bruciato da alcuni clamorosi problemi di interferenza. Tra i fattori di sviluppo figura la caduta dei prezzi (fermi oggi a circa 5 dollari per unità). La produzione di chip Bluetooth è stata di 35 milioni di pezzi nel 2002 e arriverà a 100 milioni nel 2003 ed è destinata, secondo In-Stat/Mdr, a crescere con Cagr del 118% fino al 2006, anno in cui arriverà a superare i 500 milioni di unità. Le sue caratteristiche sono molto differenti rispetto al Wi-Fi, sia in termini di copertura sia in termini di capacità di trasmissione, tant'è che mentre per la tecnologia Wi-Fi le applicazioni sono prettamente indirizzate ad ambiti Wireless Lan, per il Bluetooth si parla più correttamente di applicazioni WPan (Wireless Personal Area Network). Le altre caratteristiche distintive sono:

- Bassi consumi e bassa potenza, che lo rendono inadatto alla comunicazione in grandi spazi, ma adatto all'utilizzo in contesti dove l'alimentazione può costituire un problema o dove si teme l'inquinamento elettromagnetico (ad esempio in ambito ospedaliero);



Fonte: In-Stat/Mdr 12/02

Figura 1 - Previsione dei volumi di vendita di chipset Bluetooth su base mondiale

- Riconoscimento immediato dei dispositivi nel momento in cui entrano nel reciproco raggio di azione, con conseguente "presentazione" delle reciproche capacità (profili). Questa caratteristica permette la realizzazione di applicazioni particolari, che sarebbero molto più difficili con altre tecnologie;
- Sostanziale indifferenza al problema della sicurezza, considerate le modalità con cui avviene la comunicazione.

Nel mondo industriale, alcune case automobilistiche hanno cominciato ad inserire dei chip Bluetooth nelle auto di fascia alta, aprendo la strada ad un ambito applicativo nuovo, dove la rete esce dal contesto casa/ufficio e diventa una realtà su cui contare nella quotidianità dei gesti.
Più interessante è però, per l'impresa italiana, l'impiego di Bluetooth in ambito industriale, dove questa tecnologia può essere utilizzata per garantire una comunicabilità tra una macchina o un tool ed un operatore esterno munito di un device compatibile (cellulare, Pda o notebook). Gli impieghi possibili nell'ambito del controllo e monitoraggio della produzione, nel rilevamento di dati da strumenti "mobili" e nel tracciamento di componenti, persone o strumenti sono innumerevoli.

La situazione italiana

In Italia, la situazione è, allo stato, meno rosea di quella generale. Il Wi-Fi ha infatti avuto un decollo decisamente tardivo e solo da poco è decisamente conosciuto. A questo va aggiunto un certo ostracismo da parte delle istituzioni: la regolamentazione tuttora in vigore, infatti, proibisce l'implementazione di servizi a pagamento negli *hot-spot*, consentendone l'adozione solamente a livello sperimentale e proibendo l'installazione di Access Point in zone che comprendano strade, canali, suoli pubblici. Questa limitazione normativa, sottolinea Pancotti, rallenterà - anche se non riuscirà a fermare - non solo la diffusione delle tecnologie wireless in Italia, ma lo sviluppo di un'industria dei servizi legati agli *hot-spot* che negli Stati Uniti ha registrato un fatturato di 60 milioni di dollari nel 2002 (che diventeranno 300 nel 2005).
Delle 400 aziende intervistate, il 18% ha già adottato una soluzione wireless (il 26% ha adottato o prevede di farlo a breve). Di queste, il 61% ha adottato (o progetta di adottare) una soluzione Wlan (Figura 2). Flessibilità, semplicità di installazione, aumento della produttività individuale le motivazioni principali, mentre le aree per le quali è percepita l'utilità spaziano dalla logistica all'area commerciale e alla produzione. Nella scelta dei fornitori, il 61% si è rivolto al fornitore abituale, mentre il 38% ha considerato opportuno rivolgersi a uno specialista del wireless. Infine, alto il grado di soddisfazione: in nessun caso si sono riscontrati risultati inferiori alle aspettative e pochi hanno lamentato gravi problemi di implementazione. I motivi del non-investimento sono stati trovati soprattutto nella sicurezza e nella scarsa maturità delle tecnologie. In ogni caso, come ha sottolineato Giorgio Tosi della Cisco, tra il 2003 e il 2004 si raggiungerà il punto in cui, per un'azienda, rinviare ulteriormente l'investimento in tecnologie wireless costerà più che investire.

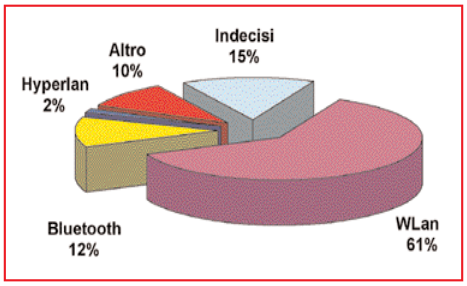


Figura 2 - Le tecnologie impiegate e previste per la realizzazione di collegamenti a breve raggio in Italia
Fonte: Mate