IL COSTO DELL'IGNORANZA NELLA SOCIETÀ DELL'INFORMAZIONE

PierFranco Camussone

Nella società dell'informazione la capacità di usare appropriatamente le tecnologie informatiche è ormai una condizione necessaria. Recenti studi effettuati nel nord Europa hanno confermato quanto era già stato evidenziato nel contesto americano: l'ignoranza informatica ha un costo rilevante per le aziende. Esse perdono di produttività se chi lavora con il PC non è in grado di essere autonomo. Nel presente articolo, si è cercato di valutare l'entità di questo onere che si indica come "costo dell'ignoranza informatica".

1. LA SOCIETÀ DELL'INFORMAZIONE

La società dell'informazione è un contesto socio-economico in cui le nuove tecnologie informatiche e telecomunicative (*Information and Communication Technology*, ICT) assumono un ruolo fondamentale nello sviluppo delle attività umane. Queste tecnologie servono a produrre, in forma digitale, messaggi, immagini, testi, musica, filmati e così via. In termini più generali, si può dire che gran parte delle informazioni e delle conoscenze del genere umano può essere riprodotta, o generata, in modo digitale con una riduzione di costi, fino a qualche tempo fa, impensabile. Questo fatto ha determinato molteplici conseguenze: per esempio, ha dato origine a un nuovo settore economico, quello della produzione e commercializzazione delle tecnologie informatiche e delle comunicazioni digitali. Ha favorito la crescita della domanda di informazioni da parte degli utenti aziendali provocando un aumento della complessità dei sistemi informativi automatizzati nelle imprese. La disponibilità di informazioni tempestive e affidabili ha determinato la revisione e la semplificazione di molti processi interni alle aziende, e tra le aziende, con un incremento della efficienza e della produttività complessiva. Infine, l'informazione è diventata in molti settori una risorsa produttiva determinante, come le materie prime per le imprese di trasformazione.

Il contributo dell'ICT alla crescita del Prodotto Interno Lordo (PIL) è, indubbiamente, uno degli aspetti positivi della società dell'informazione. Secondo le elaborazioni effettuate dal Dipartimento del Commercio degli Stati Uniti, in quel Paese il settore dell'informatica e delle trasmissioni digitali è cresciuto al punto da generare circa l'8% dell'intero PIL della nazione, come si può vedere in figura 1.

Inoltre, il settore ICT risulta quello che maggiormente contribuisce alla dinamica del PIL, la cui crescita continuativa nell'ultimo decennio è da attribuire, per più di un quarto, al contributo determinante di questo comparto (Tabella 1).

Come già osservato, la diffusione dell'uso di queste tecnologie, in tutti i settori economici,

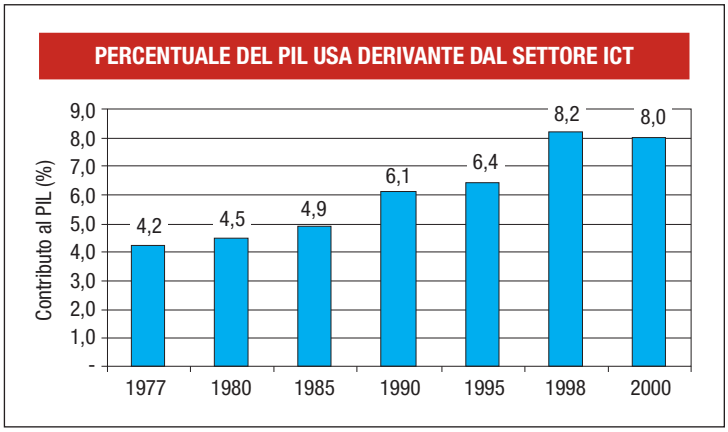


FIGURA 1

Il contributo del settore ICT al PIL degli USA. (Fonte: US Department of Commerce; Economics and Statistics Administration)

	1996	1997	1998	1999	2000
Crescita del PIL dovuta al settore dell'IT	1,1%	1,1%	1,5%	1,2%	1,2%
Crescita del PIL dovuta agli altri settori	2,4%	3,4%	3,5%	3,3%	3,5%
Crescita totale del PIL	3,5%	4,5%	5%	4,5%	4,7%
Quota della crescita del PIL dovuta al settore IT	32%	25%	29%	28%	26%

Fonte: US Department of Commerce; Economics and Statistics Administration

TABELLA 1

Contributo delle nuove tecnologie informatiche alla crescita del PIL degli USA

ha comportato la modifica e il miglioramento di molti processi sia all'interno delle aziende che tra le imprese. I settori maggiormente interessati da questo fenomeno sono, naturalmente, quelli in cui il contenuto di informazioni nel prodotto, o nel suo processo di realizzazione, risulta più rilevante [17], come per esempio il settore finanziario, quello dell'informazione (editoria, *mass media*, istruzione) e quello caratterizzato da lavoro di tipo *brain intensive* (ricerca e sviluppo, consulenza ecc.).

In questi settori, si è verificato un miglioramento significativo della produttività [5] che spesso ha portato al ripensamento dell'intero processo caratteristico dell'impresa, ovvero al *Business Process Reengineering* (BPR) [7, 14]; oppure, all'offerta di nuovi servizi, o prodotti arricchiti da informazioni [6].

Il diffuso utilizzo di Internet come strumento di comunicazione tra le imprese ha modificato i processi interaziendali, consentendo una più elevata efficienza nella filiera produttiva costituita da più operatori [12]. La riduzione dei costi di transazione [20] ha favorito il nascere delle reti di imprese ognuna specializzata in una fase ben precisa della *Supply Chain* (SC) complessiva.

Il Dipartimento del Commercio americano ha misurato l'incremento di produttività che si è avuto in quel Paese nell'ultimo decennio e ha rilevato come le aziende cosiddette "*ICT intensive*", cioè con elevati livelli di investimento nelle nuove tecnologie, abbiano presentato un tasso di incremento annuo della produttività superiore alla media [4].

Mentre, viceversa, le aziende con bassi livelli di investimento in ICT presentano percentuali di aumento della produttività significativamente inferiori (Figura 2).

Sembra confermato, dunque, l'effetto positivo sulla produttività delle nuove tecnologie informatiche e telecomunicative, avvalorando, quindi, quanto affermato da Alan Greenspan, presidente della *Federal Reserve* americana, in una recente testimonianza [11] tenuta presso il Congresso Americano:

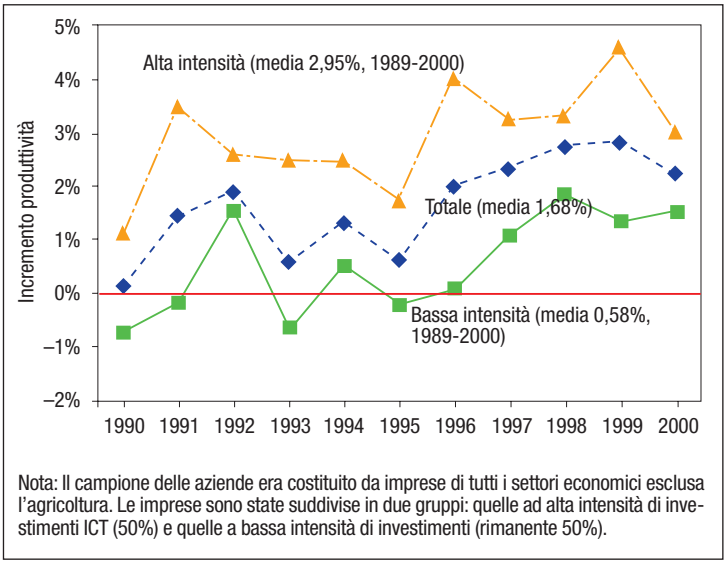
"*... gli Stati Uniti hanno sperimentato in questi ultimi anni una crescita elevata della produttività* (*output per ora di lavoro*). *L'eccezionale incremento nella potenza dei computer e nella velocità delle trasmissioni sembra sia stato l'elemento determinante di tale crescita*".

Una caratteristica peculiare della società dell'informazione è, comunque, l'elevata quota di investimenti informatici effettuata dalle imprese ogni anno. Gli investimenti annuali in ICT delle imprese americane, dopo una lieve flessione nel 2001, sono tornati a rappresentare più di un terzo degli investimenti totali effettuati ogni anno (Figura 3).

Il recente rallentamento dell'economia e lo sgonfiarsi della bolla speculativa, che ha caratterizzato il settore dell'ICT, non hanno cambiato nella sostanza questa visione, anche se hanno ridimensionato le aspettative messianiche che avevano illuso alcuni operatori del settore.

Un effetto importante della diffusione delle nuove tecnologie è consistito nella riduzione

dei costi di produzione delle informazioni. Questo fatto, combinato con l'aumento della complessità del contesto, che richiede maggiori conoscenze in azienda prima di prendere decisioni, ha portato a un significativo aumento, in ogni settore, della domanda di informazioni tempestive e accurate.
La disponibilità di informazioni è diventata una condizione imprescindibile per la gestione di gran parte delle attività economiche, dalla finanza ai trasporti, dalla grande distribuzione organizzata alle imprese manifatturiere e di processo. Il miglioramento della conoscenza del contesto riduce l'incertezza e consente di prendere decisioni migliori. Le informazioni si sono rivelate una risorsa necessaria nello svolgimento delle attività economiche di qualsiasi settore. Le aziende hanno, quindi, sviluppato e adottato sistemi informativi più sofisticati.
Le imprese non solo hanno sviluppato competenze tecniche per la produzione interna di informazioni, ma hanno dovuto addestrare gli utenti a trovare e a gestire le informazioni necessarie allo svolgimento delle proprie mansioni. Gli aumenti di produttività, precedentemente citati, sono certamente dovuti in larga misura allo sviluppo di buone competenze nell'uso dell'ICT da parte degli utenti.
Lo sviluppo della società dell'informazione ha provocato un cambiamento nelle competenze di un gran numero di lavoratori la cui attività è influenzata dall'uso delle nuove tecnologie.
Secondo un rapporto della Commissione delle Comunità Europee:
"*Il lavoratore e il posto di lavoro nella società dell'informazione saranno molto diversi da quelli che conosciamo oggi. Nella società dell'informazione un numero crescente di persone svolge mansioni legate all'informazione e alla conoscenza e fa un uso crescente degli strumenti e servizi della società dell'informazione, sia durante il lavoro che nel tempo libero. I lavoratori dell'èra digitale devono, quindi, essere alfabetizzati verso l'ICT, altamente qualificati, autonomi, mobili e pronti a sottoporsi a una formazione continua (apprendimento lungo tutto l'arco della vita). Analogamente, la società dell'informazione solleva un'enorme domanda di specialisti della società dell'informazione, domanda che finora è rimasta inevasa. Poiché il lavoratore digitale potrà essere sia uomo che donna e che questo tipo di lavoro ridurrà i vincoli dettati da disabilità, distanza e tempo che costituivano barriere all'occupazione, la società dell'informazione rappresenterà per tutti un più ampio accesso al lavoro*" [1].
I settori che sono intrinsecamente basati sulla produzione e gestione di informazioni (banche, assicurazioni, istruzione, editoria ecc.) dovranno investire fortemente nella formazione informatica del proprio personale. Ma per quanto osservato nelle pagine precedenti, si può concludere che tutti i lavoratori dovranno possedere nuove competenze nella società dell'informazione per affrontare le evoluzioni richieste alle loro mansioni, o per fare evolvere il proprio ruolo sul posto di la-



Nota: Il campione delle aziende era costituito da imprese di tutti i settori economici esclusa l'agricoltura. Le imprese sono state suddivise in due gruppi: quelle ad alta intensità di investimenti ICT (50%) e quelle a bassa intensità di investimenti (rimanente 50%).

FIGURA 2

Miglioramento annuo della produttività, misurata come variazione percentuale annua dei PIL per unità di forza lavoro (Fonte: US Department of Commerce; Economics and Statistics Administration)

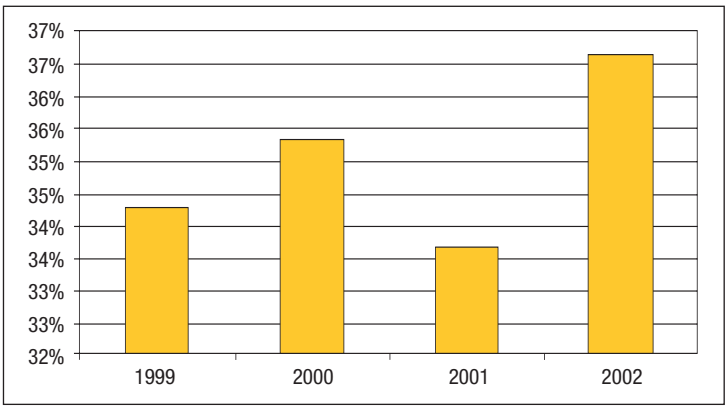


FIGURA 3

Quota degli investimenti in ICT delle imprese USA rispetto al totale degli investimenti annuali (Fonte: US Department of Commerce; Economics and Statistics Administration)

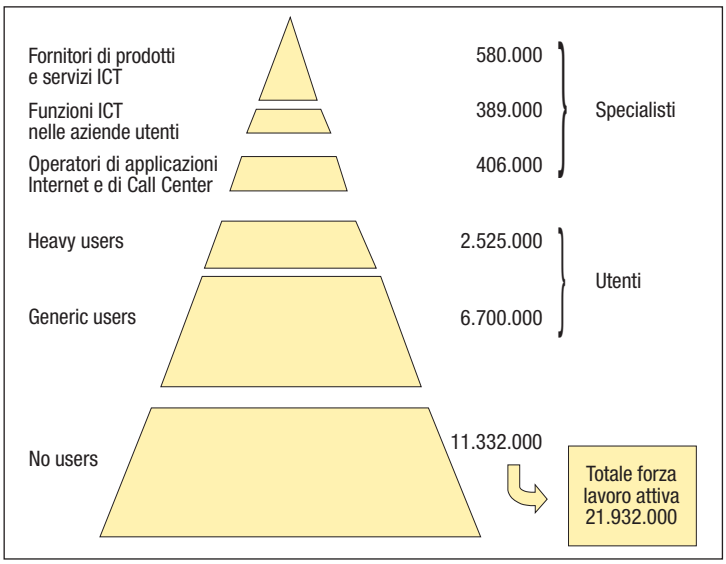


FIGURA 4

Analisi del mercato del lavoro in Italia dal punto di vista delle competenze ICT nel 2002

TABELLA 2

Diffusione dell'uso del PC tra i lavoratori europei

	Percentuale di lavoratori Europei che usano il PC
Novembre 2000	45%
Ottobre 2001	53%

TABELLA 3

L'uso dell'ICT sul posto di lavoro in Europa (Nov. 2000)

	Percentuale degli utenti di strumenti ICT
Manager	79,8%
Impiegati	68,8%
Operai	21,8%
Lavoratori autonomi	41,5%

	Modalità di apprendimento (% degli utenti, risposte multiple)
• A casa per proprio conto	45%
• Al lavoro per conto proprio o aiutati da colleghi	30%
• A scuola	24%
• Tramite formazione *ad hoc*	22%
• A casa di amici	14%

TABELLA 4

Come gli utenti europei imparano ad usare il PC

AICA e **SDA Bocconi** hanno ritenuto di comune interesse svolgere una ricerca sul costo dell'ignoranza informatica nel nostro Paese. Tale lavoro si è svolto in due momenti successivi. In un primo tempo si è raccolto tutto il materiale che è stato poi reso di pubblico dominio, con particolare attenzione alle pubblicazioni che trattano il costo che deriva alle aziende dalla insufficiente preparazione informatica degli utenti. Con questi elementi si è cercato di stimare il valore dell'onere per le aziende italiane derivante dalla impreparazione informatica degli utenti.
In una seconda fase, si è cercato di valutare con una ricerca empirica se la formazione, e in particolare i corsi ECDL, potessero ridurre tale impreparazione e di conseguenza determinare una contrazione del costo dell'ignoranza.

voro. L'alfabetizzazione generalizzata alle tecniche della società dell'informazione è, quindi, un'esigenza degli ambienti che aspirano a far parte di questo contesto.
Secondo un'analisi svolta dalla **SDA Bocconi** su dati Istat, Federcomint, Anasin, Assinform ed EITO la situazione delle conoscenze informatiche richieste dal mercato del lavoro in Italia si presenta come illustrato in figura 4.
Sul totale degli occupati, in Italia, gli specialisti ICT rappresentano il 6,2%; mentre gli utenti sono addirittura il 42% della forza lavoro attiva. Questa situazione non è molto lontana da quanto riscontrato da uno studio della Comunità Europea [2] (Tabella 2), da cui si evince anche che la diffusione dell'uso dell'ICT dipende dalla professione, o dalla mansione esercitata (Tabella 3).
A dispetto della larga diffusione degli strumenti ICT, l'apprendimento all'uso di tali strumenti è largamente sottovalutato dalla maggior parte delle imprese. Secondo il già citato studio della Comunità Europea in Europa prevale l'auto-apprendimento e l'aiuto di colleghi più esperti (Tabella 4).

2. LA NECESSITÀ DELLA FORMAZIONE INFORMATICA

La Comunità Europea si è posta l'obiettivo di diventare la società dell'informazione più sviluppata al mondo. Ciò richiede uno sforzo di preparazione di tutto il potenziale umano che lavora, o lavorerà nei prossimi anni, nel Vecchio Continente. Si calcola che 81 dei 117 milioni di giovani con meno di 25

anni seguono, attualmente, corsi presso istituti di formazione [1].
Questa è la forza lavoro del futuro che deve essere predisposta a lavorare in un contesto ad alta intensità di tecnologie informatiche. I sistemi educativi attuali devono preparare gli studenti ad affrontare questa realtà. Le scuole devono essere attrezzate con le infrastrutture tecnologiche necessarie e attivare i programmi formativi adeguati, provvedendo, se necessario, a formare anche gli insegnanti.
L'intervento non deve, però, riguardare solo i futuri lavoratori, ci si deve preoccupare di preparare anche coloro che già lavorano e che devono utilizzare le nuove tecnologie. I lavoratori dell'èra digitale devono essere quasi tutti alfabetizzati nell'uso del PC e delle applicazioni di uso individuale più comune quali Internet, la posta elettronica, il *word processing* e il foglio di lavoro ecc..
La società dell'informazione fa nascere anche un'enorme domanda di specialisti ICT e di utenti con capacità di utilizzo elevato delle nuove tecnologie. Per queste persone la formazione deve essere più profonda e più lunga. La percentuale di *heavy user* tenderà a crescere e le aziende dovranno prepararsi a fronteggiare la carenza di queste competenze (*skill*).
Se si prende in esame la situazione attuale, però, l'alfabetizzazione informatica tocca una parte minore della forza lavoro cui spetterebbe questo tipo di formazione. Solo il 29% della forza lavoro in Europa ha ricevuto una formazione di base, e si sa che questo è un valore medio tra i contesti scandinavi più evoluti e quelli mediterranei che presentano percentuali ben inferiori.
Ma l'aspetto forse più sconcertante è che solo il 22,6% dei lavoratori, in Europa, ha seguito un corso offerto dalla propria azienda. Molti hanno dovuto addestrarsi da soli, o con l'aiuto di colleghi. Solo un 10,8% ha fatto della formazione nel corso dell'ultimo anno. Pare un po' poco se si considera la velocità di cambiamento e il tasso di innovazione che caratterizza le nuove tecnologie informatiche e telecomunicative.
La formazione in ICT non può fermarsi alla fine dei corsi scolastici. Le aziende devono favorire e incoraggiare l'aggiornamento delle conoscenze informatiche. Per le persone più dotate e promettenti vanno definiti dei corsi per **heavy user** e la loro formazione va pianificata, così come dovrebbe essere fatto per la loro carriera e il loro sviluppo professionale.
Per i cosiddetti ***generic user***, l'azienda deve procedere con un intervento di formazione più estensivo che intensivo, senza curarsi se ciò che viene insegnato possa tornare subito utile nella mansione che in quel momento viene svolta dal lavoratore. Insegnando i rudimenti dell'ICT si creano potenziali utenti che possono più facilmente adattarsi a cambi di mansione e possono intravedere essi stessi miglioramenti organizzativi nelle modalità di svolgimento dei propri compiti [9].
E qui si introduce una nuova riflessione. La formazione tecnica dovrebbe essere affiancata da corsi con un taglio più organizzativo in cui si illustrino le nuove modalità di lavoro che l'ICT consente.
Gli aumenti di produttività dipendono da come le persone sanno usare gli strumenti informatici, da come rivedono e semplificano il proprio lavoro grazie a questi strumenti, per ricavare spazi di tempo da dedicare ad attività più ricche e che possano determinare un maggior valore aggiunto [8].
In altri casi, non è il risparmio di tempo che ci si deve aspettare dall'uso dell'ICT, quanto piuttosto un miglioramento dell'output del lavoro che risulta più completo, più ricco di contenuti. Le misurazioni dei vantaggi tangibili hanno rilevato che entrambe queste aspettative trovano riscontro nella verifica empirica [5].
Un ostacolo che le aziende incontrano nel fare formazione per i propri dipendenti consiste nel fatto che evidentemente ciò comporta dei costi. Le aziende maggiori, quelle quotate in borsa, sono restie a investire in formazione perché nessun indicatore di questo genere di investimenti viene abitualmente preso in considerazione dagli analisti finanziari, per cui le spese in formazione non contribuiscono al rialzo delle quotazioni di borsa. Anzi, trattandosi di costi, riducono gli utili del periodo e fanno apparire meno brillante il risultato economico. Le aziende che fanno investimenti in forma-

Gli **heavy user** sono utenti le cui mansioni prevedono un uso specialistico della tecnologia informatica come nel caso dei progettisti che usano apparecchiature CAD, o degli specialisti di controllo di processo che regolano il processo con il computer; oppure persone che utilizzano quasi esclusivamente il computer per lo svolgimento delle proprie mansioni.
I **generic user** sono persone che pur usando il computer non si possono definire specialisti in senso stretto, oppure lo usano saltuariamente.

zione lo fanno, dunque, a dispetto della pressione per i risultati di bilancio a breve termine.

3. IL COSTO DELL'IGNORANZA INFORMATICA IN UN CONTESTO EVOLUTO

La società dell'informazione si sviluppa se chi vive e lavora in tale società sa fare un buon uso delle possibilità offerte dalle nuove tecnologie informatiche e telecomunicative. Per esempio, il PC e gli strumenti di informatica individuale sono strumenti che tutti dovrebbero saper usare. Metaforicamente parlando, l'informatica equivale a un linguaggio che tutti dovrebbero apprendere, perché consente di interagire con un mondo che, ormai, si esprime mediante questa lingua. L'ignoranza informatica pregiudica il successo dei piani e dei progetti europei che vorrebbero far divenire il Vecchio Continente la prima società della conoscenza a livello mondiale. Non solo, riduce anche la capacità delle singole imprese di raggiungere livelli di efficienza consentiti dall'impiego diffuso delle nuove tecnologie.

Già nel 1997, una ricerca [3] effettuata negli Stati Uniti indicava che il problema più critico nel campo del lavoro era la formazione e l'addestramento all'uso dell'ICT.

Come mai questo risultato?

Molte organizzazioni ad alta intensità di lavoro sono coscienti che le risorse più preziose per la propria sopravvivenza e il proprio sviluppo sono le persone. È altrettanto noto che nella società dell'informazione una risorsa fondamentale è rappresentata dalle informazioni medesime, che si devono poter acquisire, elaborare e trasmettere in modo efficiente ed efficace.

Nel nuovo contesto si dovrà, quindi, investire in tecnologia, ma anche nelle risorse umane, per far sì che queste ultime sappiano ricercare o produrre informazioni senza fatica e con grande dimestichezza. Una società che ha recepito questo concetto è, per l'appunto, quella americana in cui gli investimenti in ICT, da parte delle aziende, rappresentano il 45% del totale degli investimenti e per l'addestramento informatico si spende circa un terzo dell'intera spesa di formazione delle imprese [4].

Dal momento che la spesa in formazione non produce ritorni immediati e tangibili sul risultato economico del periodo, molte aziende europee, e in particolare italiane, sono restie a predisporre programmi di formazione per molti dei propri dipendenti, pur esigendo da questi ultimi che sappiano usare gli strumenti informatici. La mancanza di una formazione adeguata può, però, produrre costi nascosti che derivano da una minor produttività delle persone (risultati prodotti rispetto alle ore di lavoro). Oppure, nei casi più gravi può determinare un uso erroneo degli strumenti informatici, con conseguenze difficili da valutare.

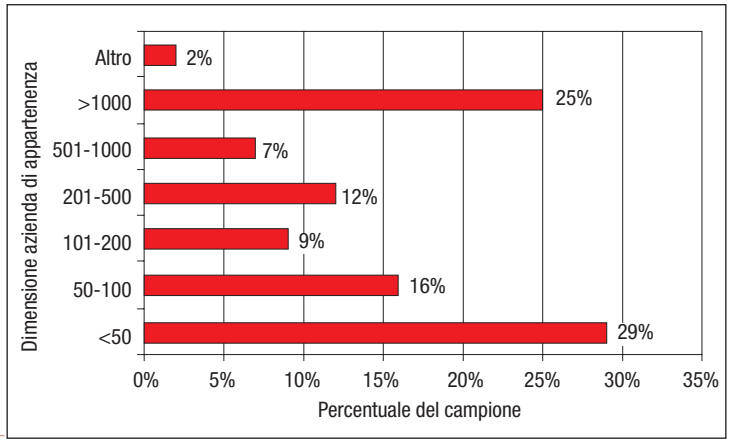
Seguendo questo ragionamento l'Istituto di Statistiche Norvegese ha cercato di determinare il "costo dell'ignoranza" nell'uso dei normali strumenti informatici, cioè del PC, del *software* di uso individuale (MS/Office), dei servizi di rete (*e-mail*, Internet) e delle applicazioni *legacy* (sistemi informativi interni istituzionali). Questa ricerca è stata condotta intervistando un campione di 800 utenti, per il 69% appartenenti alle aziende private e per il 31% operanti nel settore pubblico.

La struttura del campione dal punto di vista delle mansioni svolte era la seguente:

Manager di livello elevato	16%
Manager operativi e quadri	30%
Impiegati	54%
	100%

Per quanto concerne la dimensione dell'azienda di appartenenza il campione era distribuito come illustrato in figura 5.

FIGURA 5
Distribuzione del campione per dimensione dell'azienda di appartenenza



Le applicazioni, di cui si è riscontrata la maggior diffusione sono state, ovviamente, il word processing, l'e-mail e l'uso di Internet (Figura 6). In seconda battuta, sono state citate le applicazioni predisposte dai sistemi informativi interni (*legacy system*); mentre solo un terzo degli intervistati ha nominato applicazioni di interesse individuale o di *project management*.
Gli intervistati hanno successivamente quantificato il loro tempo assorbito, mediamente, ogni settimana dalla nascita di problemi derivanti dall'uso degli strumenti informativi. Come si può vedere dalla figura 7 ogni settimana si perdono 22 min in attesa di un supporto richiesto alle strutture di assistenza. Dal momento che si hanno a disposizione colleghi che probabilmente hanno già dovuto affrontare un problema simile, spesso si ricorre a loro per avere un aiuto immediato. Questo comportamento spiega la presenza al primo posto della voce "aiuto ai colleghi".
Come è facile comprendere molti dei problemi che sorgono (dall'uso delle applicazioni in rete, all'impiego di Internet e degli strumenti MS/Office) potrebbero essere ridotti con una formazione specifica su tali strumenti. In particolare, una formazione di base come quella necessaria per l'acquisizione della Patente europea del computer (ECDL, *European Computer Driving Licence*) potrebbe ridurre, notevolmente, il totale del tempo "perso" ogni settimana per problemi connessi all'uso degli strumenti ICT.
Secondo le rilevazioni dell'Istituto di Statistiche norvegese, gli utenti passano, mediamente, 24 h ogni settimana davanti al

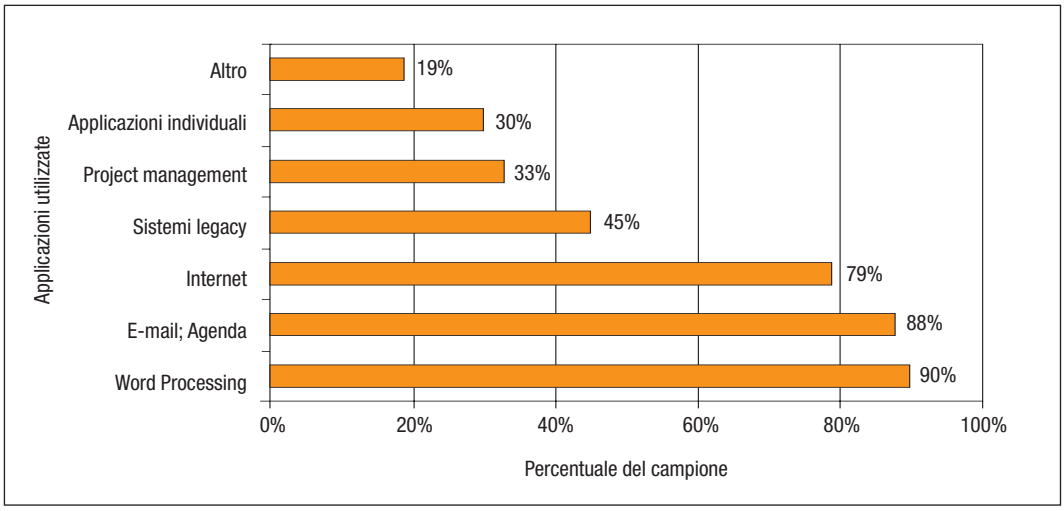


FIGURA 6
Diffusione dell'uso delle diverse applicazioni

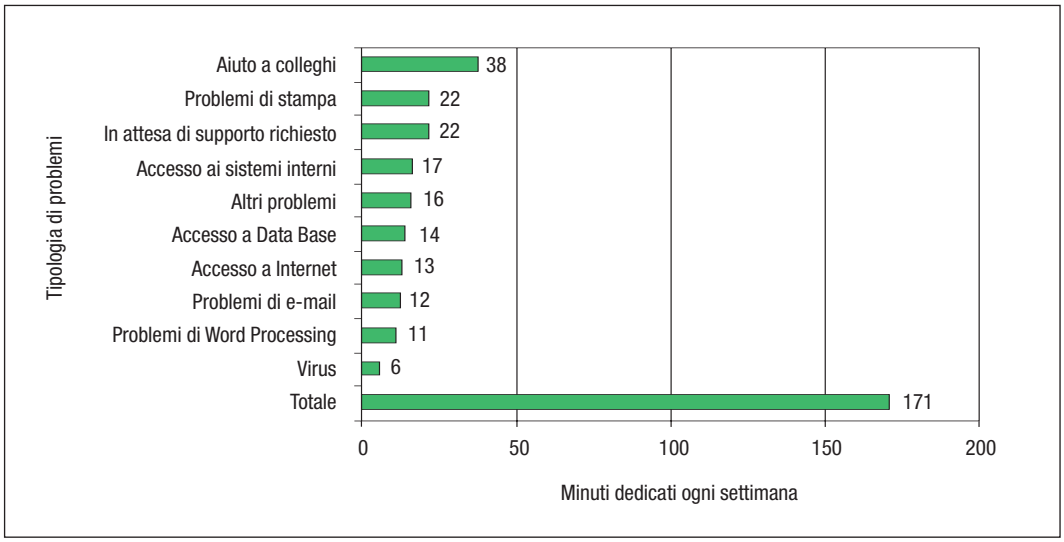


FIGURA 7
Tempo settimanale non produttivo per ogni utente di strumenti informatici

computer sulle 40 teoricamente lavorabili. Si tratta di un 60% del tempo lavorativo, ormai assorbito dall'interazione con i sistemi ICT. Ma la ricerca effettuata indica che 171 min ogni settimana, ovvero 2 h e 51 min, sono improduttivi, a causa dell'insorgere di difficoltà che bloccano il normale svolgimento dell'attività che ogni utente deve eseguire in relazione alla propria mansione. Quindi, ogni lavoratore che utilizza il PC "perde" il 7,13% del proprio tempo lavorativo (171 min su 5 giorni di 8 h).
I risultati di questa ricerca sembrano attendibili e certamente possono dare una indicazione di quello che potrebbe essere il costo della ignoranza informatica in una società molto informatizzata, verso la quale anche l'Italia deve assolutamente tendere.

4. IL COSTO DELL'IGNORANZA INFORMATICA NEL CONTESTO ITALIANO

Un'estrapolazione dei valori riscontrati nel contesto norvegese alla realtà italiana porterebbe a risultati impressionanti.
Secondo i valori riportati in figura 4, in Italia, ci sono, attualmente, 2.525.000 di heavy user e 6.700.000 di generic user per un totale di 9.225.000 di utenti in totale.
Applicando i risultati scandinavi ai soli ***generic user***, in quanto si suppone che gli heavy user siano più preparati e, quindi, perdano meno tempo rispetto ai primi, si ottengano le seguenti stime di perdita di produttività settimanale:

2 h e 51 min × 6.700.000 utenti = 19.095.000 h per settimana

che in un anno (composto da 48 settimane lavorative) determina una perdita di:

19.095.000 h × 48 = 916.560.000 h = 114.570.000 di giornate lavorative

Ci si può domandare che cosa significhi, da un punto di vista economico, questa "perdita di produttività" per il sistema produttivo italiano.
Il CNEL (*Consiglio Nazionale dell'Economia e del Lavoro*) elaborando la base statistica dell'ISTAT fornisce i seguenti dati del costo del lavoro in Italia per addetto nel 2001:

Industria	30.831 €/anno
Servizi	30.335 €/anno

Naturalmente, questi valori si riferiscono al *mix* completo delle mansioni presenti nel contesto industriale e dei servizi e, quindi, comprendono gli operai, oltre che gli impiegati e i dirigenti per l'industria, così come per i servizi sono compresi anche gli operatori di qualifica più bassa.
Se, dunque, si volesse essere più precisi si dovrebbe far riferimento ai costi del lavoro degli addetti (impiegati e dirigenti) che costituiscono la parte principale dei generic user.
Per maggiore prudenza nella stima è possibile, però, utilizzare il valore del costo del lavoro medio per settore come indicato dal CNEL, sapendo che i generic user dovrebbero avere una remunerazione un po' superiore al valore medio, essendo prevalentemente impiegati e dirigenti.
Un costo annuo di 30.000 € corrisponde a un costo per giornata di 136,36 €, tenuto conto che un anno è costituito da 220 giorni lavorativi.

Il costo annuo per il sistema produttivo italiano è, quindi, il seguente:

136,36 € × 114.570.000 giornate = 15.6 miliardi di €

Se questa cifra, che riguarda l'intero Paese, può sembrare difficile da apprezzare, viste le sue dimensioni, si può ragionare partendo dal basso e calcolare che, per ogni utente generico, le aziende sostengono un "costo dell'ignoranza informatica" rappresentato dal tempo improduttivo perso annualmente dall'interessato.
Esso equivale al seguente costo del seguente tempo improduttivo:

2 h e 51 min × 48 settimane/anno = 17,1 giorni/anno

per un importo di:

136,36 €/giorno × 17,1 giorni = 2.331 €/anno

Per completezza di analisi, si dovrebbe aggiungere i costi dell'ignoranza informatica degli ***heavy user***. Essi dovrebbero, certamente, essere più preparati rispetto ai generic user per cui il costo annuo della loro "impreparazione" dovrebbe essere una frazione dei 2.331 € calcolati per gli utenti generici.
Se solo si pensasse che, nel loro caso, il tempo perso per la soluzione dei problemi informatici fosse non più di un 1/4 di quello dei generic user, si avrebbe un costo aziendale annuo di 582 €. Il che significa per il sistema produttivo italiano un costo annuo ulteriore di:

582 € × 2.525.000 utenti = 1,47 miliardi di euro

Questi numeri sono così rilevanti che si può pensare ai vantaggi di una loro riduzione anche solo parziale. Gli investimenti formativi sono una delle strade che l'Italia deve percorrere con maggiore convinzione. Ciò riguarda sia il sistema scolastico e universitario, sia le aziende che devono pensare al completamento e all'aggiornamento delle conoscenze informatiche.

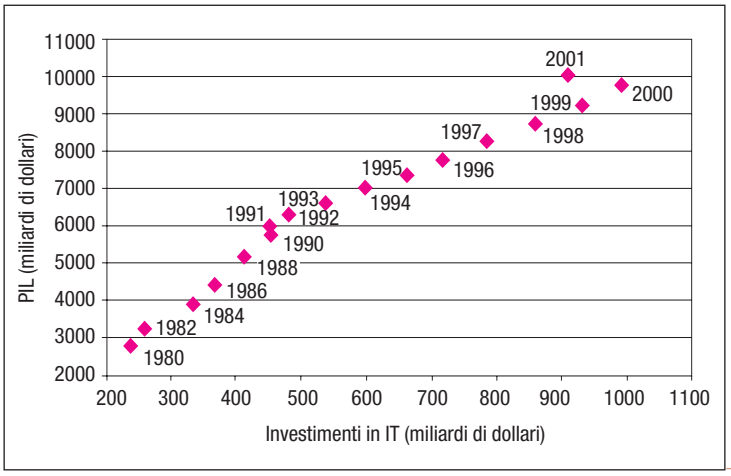
5. LA SPESA INFORMATICA PER L'UTENZA FINALE: UN'ANALISI DEI COSTI

In anni recenti, la spesa informatica delle aziende è diventata molto significativa. Secondo stime accurate [19] circa il 41% degli investimenti annuali delle aziende americane in beni capitali ha riguardato l'ICT.
È, generalmente, riconosciuto che un elevato livello di spesa informatica si accompagna con un elevato tasso di sviluppo dell'economia (Figura 8). È altrettanto provato [5] che le tecnologie informatiche sono un elemento importante nella crescita della produttività degli individui e - di conseguenza - delle imprese.
Un aumento indiscriminato della spesa informatica non produce, tuttavia, in maniera automatica, effetti positivi di miglioramento della produttività aziendale e di sviluppo dell'impresa o della società. Spesso, un maldestro incremento di investimento in tecnologie può determinare l'insorgere di altri costi

Il *Total Cost of Ownership*, **TCO**: indica i costi totali che l'azienda sostiene annualmente per l'utilizzo da parte degli utenti di una postazione di lavoro (PC). Tali costi comprendono non solo le quote di ammortamento dell'hardware e i canoni del software, ma anche l'assistenza (help desk) e il coordinamento centrale e gli oneri derivanti dal mancato funzionamento delle apparecchiature per guasti o incompetenza. Tale espressione è stata introdotta a metà degli anni '90 da Gartner Group per significare che i costi di un PC in azienda non erano solamente quelli dell'hardware e del software su di esso installato, ma un insieme di costi nascosti ben più rilevante.

indotti (costi di gestione di apparecchiature più complesse, costi di assistenza agli utenti e così via) che riducono, o annullano, i vantaggi attesi dall'azienda.
Le ricerche svolte da Gartner Group [16] hanno provato che il costo annuale totale, (*Total Cost of Ownership*, **TCO**) di una postazione di lavoro è spesso sottostimato dall'azienda, che prende in considerazione solo la spesa sostenuta per l'*hardware* e il software acquistati. Secondo una ricerca svolta nel contesto americano [13], ogni postazione di lavoro ha un costo reale compreso tra gli 8.000 e i 9.000 $ l'anno suddiviso in diverse componenti come illustrato in figura 9.
Come si può vedere, il decentramento di risorse hardware e software ha indotto costi di governo della rete (gestione) dello stesso ordine di grandezza dei costi diretti per l'hardware e il software delle postazioni di lavoro. Interessante e significativa è anche la quota di costo che, nella ricerca, viene attribuita al tempo perso dall'utente finale. Si tratta di più di 2.000 dollari all'anno. Tale valore appare molto vicino a quanto rilevato dai ricercatori norvegesi nel lavoro precedentemente illustrato.

FIGURA 8
Investimenti informatici e tasso di sviluppo dell'economia



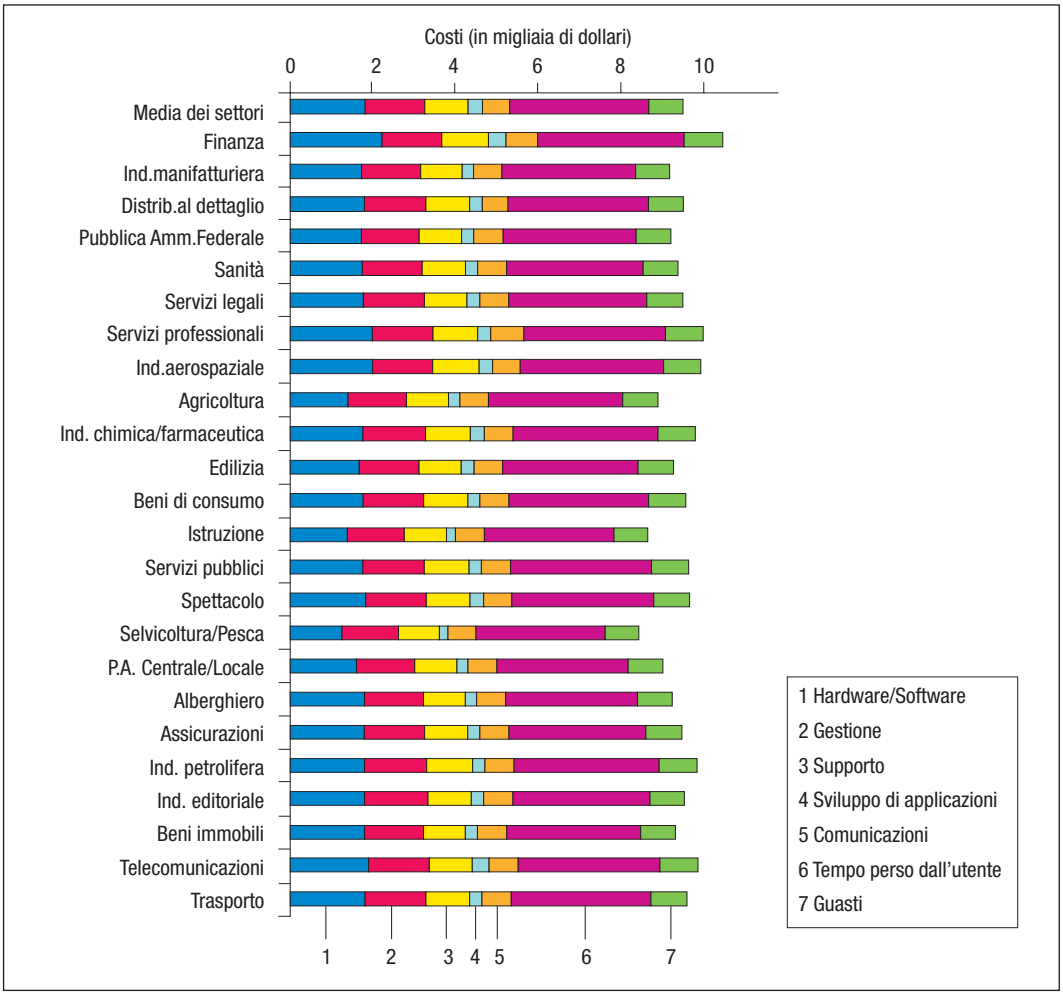


FIGURA 9
Il TCO di una postazione di lavoro per end user (Fonte: Guptill, Gartner Group)

Come si può constatare, lavori di analisi aventi finalità differenti sono arrivati alle medesime conclusioni. Le ricerche di Gartner mostrano, tuttavia, un'interessante peculiarità. Le imprese possono ridurre il costo complessivo del posto di lavoro[1] se investono in tecnologie più stabili (che richiedono minor assistenza centrale) e più facili da usare (ovvero, che riducono la difficoltà d'uso dell'utente finale). Anche la spesa in formazione, se oculatamente indirizzata e incrementata, contribuisce a ridurre il costo della assistenza e il tempo improduttivo degli utenti.
Anzi, dal lavoro svolto dai ricercatori appare evidente che il costo della improduttività delle persone (circa 2.600 dollari all'anno) rappresenta un terzo (34%) del costo complessivo di ciascuna postazione di lavoro. È, quindi, molto più importante per l'azienda ridurre questo costo nascosto, vista la sua incidenza, che ottenere uno sconto dai fornitori di hardware e di software.
Questo costo può essere diminuito con un intervento di formazione e di addestramento, che però richiede una attenzione e un impegno organizzativo molto superiore rispetto a una rinegoziazione dei prezzi di acquisto dell'ICT.

6. LE VIE PER RIDURRE IL COSTO INFORMATICO PER L'UTENZA FINALE

I costi informatici per il funzionamento di ogni postazione di lavoro individuale possono essere suddivisi in costi di acquisto delle apparecchiature (circa il 20% del totale) e costi di uso e di gestione (80%).

[1] L'espressione usata abitualmente per indicare il costo complessivo è la seguente: *Total Cost of Ownership* (TCO).

Molte ricerche sono state svolte al fine di trovare qualche via di riduzione dei costi di gestione, vista la loro rilevanza. Studi effettuati di recente [10], hanno dimostrato che una sensibile riduzione di tali costi (da un minimo del 26% a un massimo del 39%) può essere ottenuta mediante due azioni:

- la standardizzazione della tecnologia impiegata;
- l'accentramento dei servizi di assistenza e di supporto.

L'influenza della prima azione è del tutto evidente [18] se si considera la necessità di duplicare competenze per il governo di postazioni di lavoro basate su differenti tecnologie.

La centralizzazione dell'assistenza, invece, presenta vantaggi e controindicazioni: aumentando il livello del controllo sulla periferia e centralizzando il supporto, un solo tecnico riesce a fornire aiuto anche a 77 utenti, mentre in contesti a basso grado di controllo ne riesce a seguire solo 18 [15]. Apparentemente, è possibile strutturare l'assistenza agli utenti in modo più efficiente (cioè con un tecnico che segue un numero maggiore di utenti), ma la ricerca indica che questo va a scapito del livello di servizio. Tuttavia, è stato messo in evidenza che un accentramento spinto comporta un degrado dei livelli di servizio all'utenza finale. La riduzione del personale di assistenza, possibile grazie alle economie di scala che l'accentramento consente, comporta un allontanamento dalla linea operativa dello *staff* di assistenza e, non poche volte, un allungamento dei tempi di servizio. Ciò determina un aumento del tempo perso dall'utente che, pertanto, in un contesto siffatto deve essere più autonomo e preparato. In ultima analisi, c'è il rischio che ciò che si risparmia nei costi di gestione e assistenza venga largamente controbilanciato da un aumento del livello di inefficienza dell'utenza finale.

Ne consegue la necessità pianificare accuratamente gli investimenti in sistemi di accentramento e controllo, bilanciandoli con opportuni interventi volti a non deprimere il livello di servizio all'utenza finale; per esempio, una conseguenza ovvia è che sarà necessario investire in formazione per rendere più autosufficienti e produttivi gli utenti, se si vuole fruire dei vantaggi dell'accentramento e del controllo senza scontarne le conseguenze negative.

7. UN QUESITO FINALE

Nel corso dello studio sul costo dell'ignoranza informatica, due quesiti si sono, quindi, presentati ai ricercatori.

1. La formazione può ridurre i costi aziendali di ciascuna postazione di lavoro, in particolare può ridurre il tempo non produttivo degli utenti?

2. I corsi per il conseguimento della "patente europea" del computer (ECDL) possono rappresentare lo strumento formativo adatto a ottenere tale scopo?

Per rispondere a questi interrogativi è stata avviata un'indagine empirica sugli effetti di corsi orientati all'acquisizione dell'ECDL su un campione di soggetti, i cui risultati saranno illustrati in un altro articolo che verrà pubblicato sul prossimo numero di Mondo Digitale.

Bibliografia

[1] AA. VV., Commissione delle Comunità Europee: *Strategie per l'occupazione nella società dell'informazione*. Com (2000) Vol. 48, Bruxelles 04/02/2000.

[2] AA. VV., Commission of the European Communities: *Information Society Jobs: quality for change*. Bruxelles, 03/04/2002, SEC, (2002), p. 372.

[3] AA. VV.: National Human Relations Development Executive Survey, 1997.

[4] AA. VV.: Digital Economy 2002, US Department of Commerce: Economics and Statistics Administration.

[5] Brynjolfsson E, Hitt L: 1997, Productivity, profit and consumer welfare: the different measure of IT's value; MIS Quarterly 1996.

[6] Camussone PF: *Informatica, organizzazione e strategia*. McGraw Hill Italia, 2000.

[7] Davenport TH: 94, *Process Innovation. Reengineering work through information Technology*. Boston - Mass., Harvard Business School Press; 1993, (trad. ital., *Innovazione dei processi. Riprogettare il lavoro attraverso l'information technology*, a cura di Ernst&Young Consultants, Franco Angeli; 1994).

[8] Danziger JN, Jenning JA, Park SC: *ICT Training*. Center for research on ICT and Organizations. University of California Irvine, 1999.

[9] Danziger JN, Wang YC: *Enhancing end users' ICT skills in the new economy*. Center for research on ICT and Organizations; University of California Irvine, 2000.

[10] David JS, Schuff D, Louis RS: *Managing your IT total cost of ownership*. Communication of ACM, Jan. 2002. Teach F: How to succeed in IT. CFO Magazine, oct. 1998.

[11] Greenspan A: Monetary Policy Testimony and Report to the Congress, 24 febbraio 1998.

[12] Gouillart FJ, Kelly J: *Transforming the organization*. McGraw-Hill, 1995, (trad. it., Business Transformation, McGRAW-HILL Italia; 1995).

[13] Guptill B: Measurement conference '99: Helpèing to justify IT; Research Note, Gartner, march 1999.

[14] Hammer M, Champy J: *Reengineering the corporation*. A manifesto for business revolution, Harper Business, New York, 1993.

[15] Johnson H: *Technical support cost for dual-platform desktops: managed diversity*. Research Note, Gartner, 1995.

[16] Kierwin B, Mieritz L: *TCO and performance management in architectural choices*. Research Note , Gartner july 2002.

[17] Porter M, Millar P: *How Information Gives You Competitive Advantage*. HARVARD BUSINESS REVIEW, July 1985.

[18] Nash K: *Use of standards save money*. Computerworld, Mar. 8 2001.

[19] Teach E: *How to succeed in IT*. CFO Magazine, july 1997.

[20] Williamson O: *Market and Hierarchies: Analysis and Anti-trust Implication*. THE FREE PRESS, New York, 1975.

PIER FRANCO CAMUSSONE Professore di "Organizzazione e sistemi informativi" presso l'Università di Trento. Direttore dell'Area Sistemi Informativi della Scuola di Direzione Aziendale (SDA) della Bocconi. Membro dei comitati scientifici di diverse riviste (tra cui Economia e Management, Mondo digitale). Autore di numerose pubblicazioni sugli aspetti economici ed organizzativi dell'informatica.
pierfranco.camussone@uni-bocconi.it

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.*"

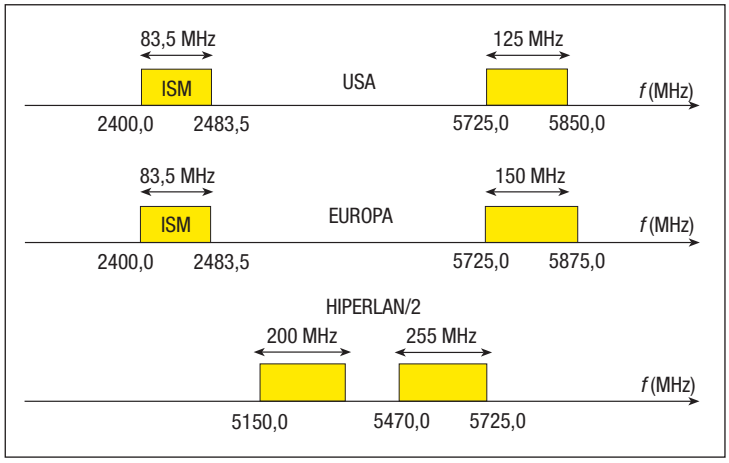


FIGURA 1
Le bande impiegate dallo standard IEEE 802.11 e la banda per lo standard europeo HiperLAN/2

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-

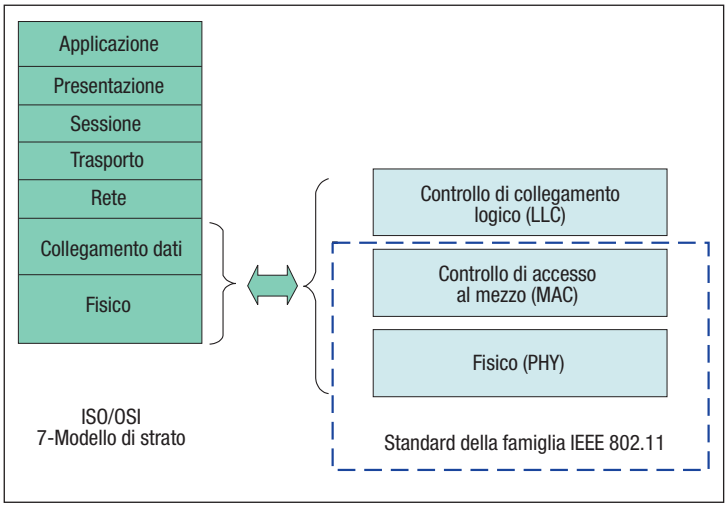


FIGURA 3
Associazione fra strati delle architetture OSI e IEEE 802.11

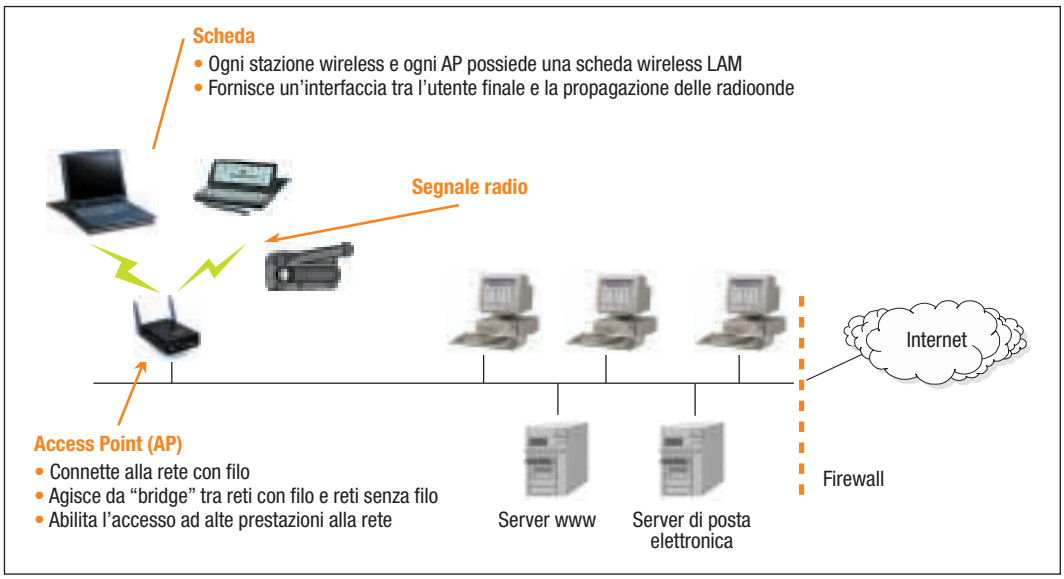


FIGURA 4
Configurazione tipica di rete aziendale IEEE 802.11

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

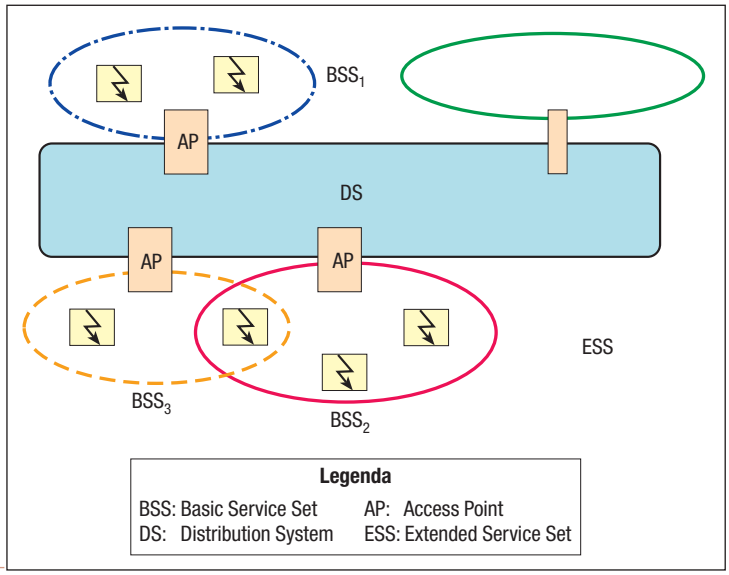
❑ ***Reti "ad hoc"***: si compongono di un insieme di nodi wireless (NIC) che si possono riorganizzare autonomamente in configurazioni temporanee e arbitrarie; i nodi possono servire da *router* e da *host*, e possono instradare pacchetti anche per conto di altri nodi; i nodi possono ospitare e attivare 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.

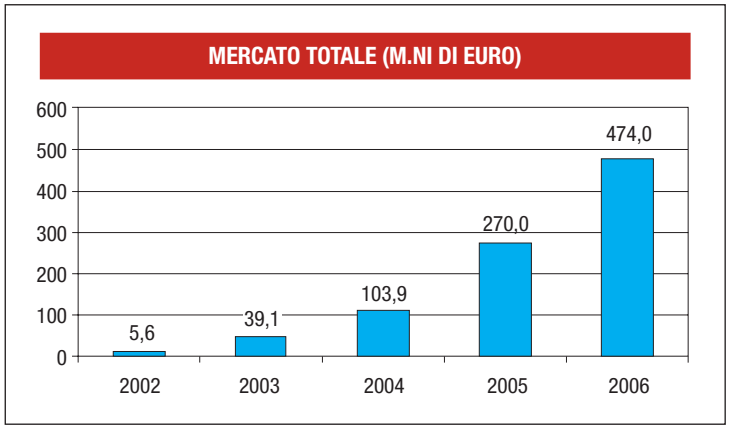


FIGURA 6
Previsioni per i mercati privato e pubblico in Italia (Fonte: Databank)

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-

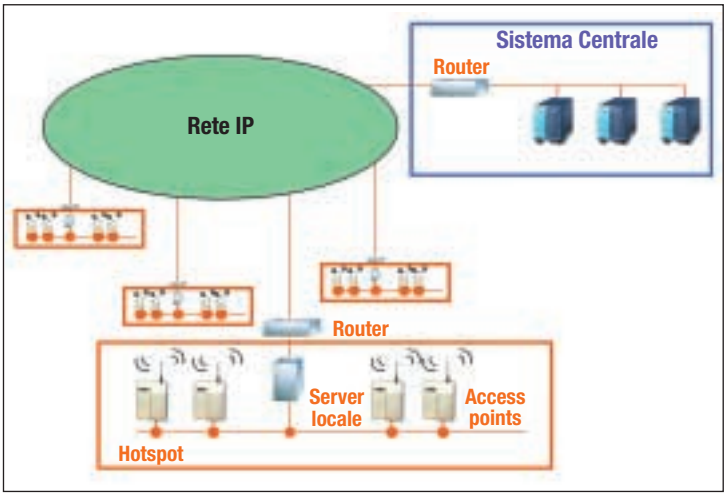


FIGURA 7
Architettura di sistema hotspot pubblico

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.

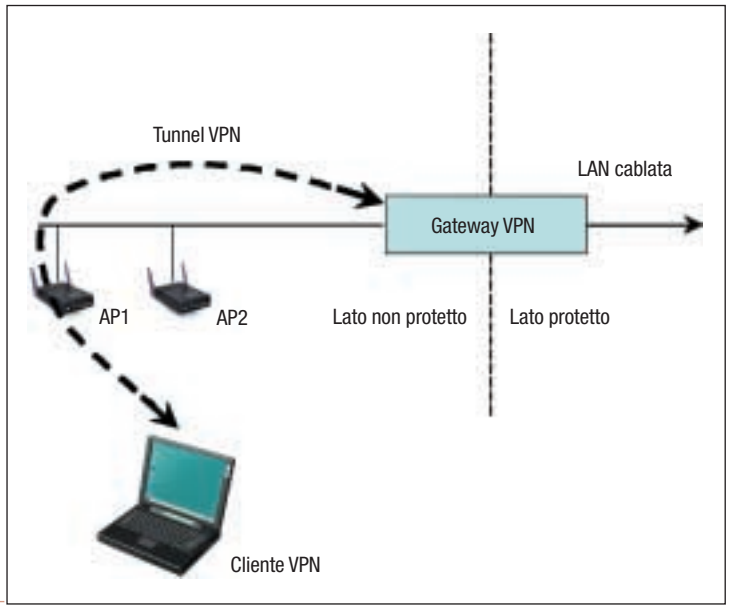
Per risolvere l'insieme dei problemi di sicurezza, si possono proporre sia soluzioni "native" (ossia, a livello di sottostrato MAC) che soluzioni esterne al Wi-Fi (livello OSI 3) che sono studiate nell'ambito del *802.11 Task Group* i incaricato di predisporre lo standard IEEE 802.11 i: le più note di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

SICUREZZA E BUSINESS IN RETE

Marco Mezzalama
Edoardo Calia

La sicurezza è oggi percepita dal mondo occidentale come esigenza fondamentale. Questo senso di incertezza è avvertito anche nel settore informatico e delle TLC. Oggi i sistemi informativi costituiscono il cuore dei processi aziendali e la loro sicurezza fisica e logica diventa un elemento determinante. Se si considera che un sistema informativo odierno non può prescindere dall'infrastruttura di rete si comprende come la sicurezza della rete informatica sia condizione necessaria per la sicurezza del sistema e del patrimonio aziendale.

3.7

1. LO SCENARIO

Non molto tempo fa il noto settimanale americano Newsweek indicava come "la sicurezza informatica fosse il fattore abilitante per un reale uso commerciale di Internet". Affermazione suffragata da una recente indagine sugli utilizzatori di Internet che indica in circa l'80% la quota di coloro che non utilizzavano ambienti di *e-commerce* B2C (*Business to Commerce*) a causa di presunti rischi di sicurezza sulla rete.
Una rete è essenzialmente un'infrastruttura costituita da connessioni e apparati che collega calcolatori (*host*) al fine di far interoperare questi ultimi e di realizzare servizi applicativi. Ma la rete e i servizi applicativi che su essa si appoggiano risultano veramente insicuri, e se sì dove sono le cause e quali i rimedi?
Ebbene se si considera l'ultima edizione dello studio condotto da CSI (*Computer Security Institute*) in collaborazione con l'FBI di San Francisco nel 2002 e si valutano le prime 20 criticità rilevate su sistemi in rete, ci si accorge che ben 17 riguardano "debolezze" proprie degli host, e in particolare dei loro sistemi operativi. Un esempio per tutti è lo sfruttamento del cosiddetto *buffer overflow*, tecnica che satura di messaggi opportuni i buffer del sistema operativo, permettendo in tal modo di acquisire il controllo totale o parziale del sistema. Pertanto, nel valutare le problematiche di sicurezza verranno prese in considerazione le azioni, le minacce e le vulnerabilità che riguardano sia la rete come infrastruttura (protocolli e apparati di rete) sia i calcolatori a essa connessi e che realizzano servizi di rete, quali *e-mail* o *web server*.
Per semplicità di esposizione verranno suddivise le criticità in tre aree distinte: quelle che fanno riferimento ai protocolli e agli apparati di rete, quelle che interessano i sistemi operativi e i *data base* e, infine, quelle che riguardano le applicazioni.
Ci si soffermerà soprattutto sulle prime, pur considerando anche il secondo ambito essendo sovente strettamente interdipendente dal primo.

1.1. Attacchi alla sicurezza: tipi ed evoluzione

Il fatto che negli ultimi anni le minacce e gli attacchi ai sistemi in rete siano notevolmente cresciuti è un dato reale. I dati indicati dal CERT (*Computer Emergency Report Team*) relativi a incidenti accertati di intrusione indicano, come illustrato in figura 1, un tasso di crescita esponenziale che negli ultimi anni può essere semplificato indicando un fattore di crescita pari a circa 2,5/anno. Ancora più significativo appare il dato che evidenzia il crescere di nuove tipologie di vulnerabilità, denotando come, al crescere della complessità dei sistemi, protocolli e apparati, cresca di concerto quella delle tecniche di attacco: si passa da circa 300 tipi di tecniche di attacco nel 1997, a 1090 nel 2000, a 3750 nel 2002.

Nella definizione di questo quadro è opportuno citare il rapporto annuale "*Computer Security Issues&Trends*" del CSI/FBI. Esso si basa su una puntuale analisi condotta su un campione di circa 500 aziende americane rappresentative del contesto industriale e dei servizi. Tra i vari dati ottenibili dal *report*, direttamente scaricabile dalla rete, appare interessante citare i seguenti:

- il 90% del campione ha subito attacchi diretti al sistema IT (*Information Technology*);
- l'80% ha rilevato perdite finanziare, con valor medio pari a circa 7.000.000 di dollari in crescita significativa rispetto agli anni passati (un fattore 3 rispetto all'anno precedente);
- le perdite più significative riguardano il furto di informazioni o le frodi finanziarie;
- l'85% hanno subito un attacco da *virus* o *worm*;
- il 38% hanno rilevato accessi non autorizzati al proprio sito web.

Per definire un quadro completo delle criticità cui può essere assoggettato un sistema informatico, è importante conoscere da dove proviene l'attacco e da chi. Anche a queste domande si può rispondere facendo riferimento al già citato rapporto CSI/FBI.

Nella figura 2 è illustrato, nel corso degli ultimi tre anni, quale sia il punto di partenza di un attacco: si noti come sia preponderante la provenienza dalla rete Internet, sebbene risulti notevole ancora la percentuale di minacce portate dall'interno dell'azienda.

Questa lettura, che stempera abbastanza il mito che gli attacchi al sistema aziendale derivino principalmente dall'esterno, è rafforzata dai dati relativi ai soggetti che mettono in atto un attacco riportati in figura 3. Si evince come il rischio "interno" risulti significativo e come, pertanto, una saggia politica di sicurezza debba guardare con attenzione non solo "fuori ma anche dentro le mura".

Un'ultima considerazione in questo scenario preliminare, riguarda i danni economici subiti per attacchi informatici. Il Club Sicurezza Informatica ipotizzava nel 1999, in Italia, una perdita generica dovuta ad attacchi e malfunzionamenti valutabile in circa 1.500 milioni di euro. Sempre dal rapporto CSI/FBI sono, inoltre, desumibili non i valori assoluti delle perdite, bensì quelli relativi per classe

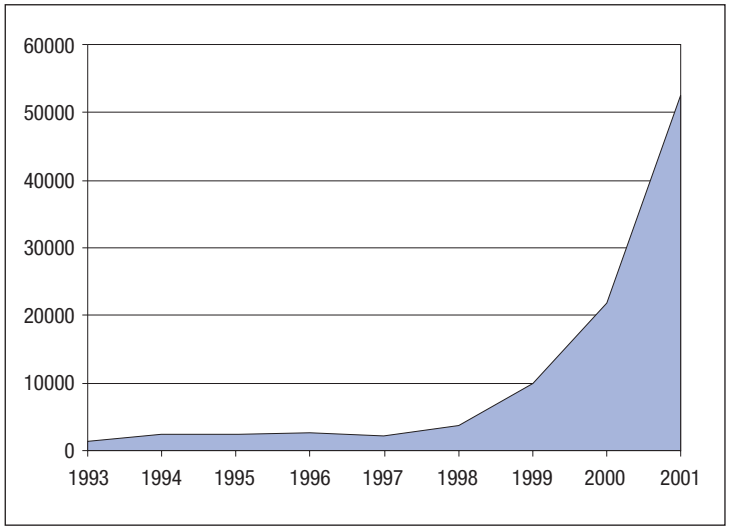


FIGURA 1

Numero di incidenti segnalati dal 1993 al 2001

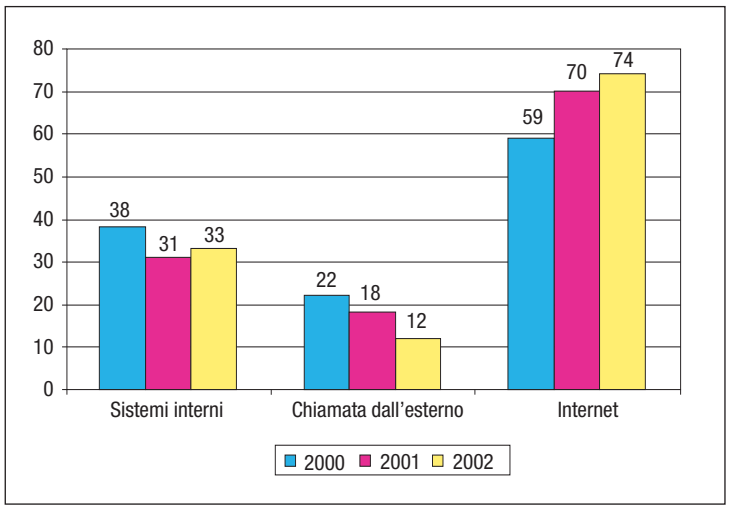


FIGURA 2

Provenienza degli attacchi (Fonte: CSI/FBI 2002)

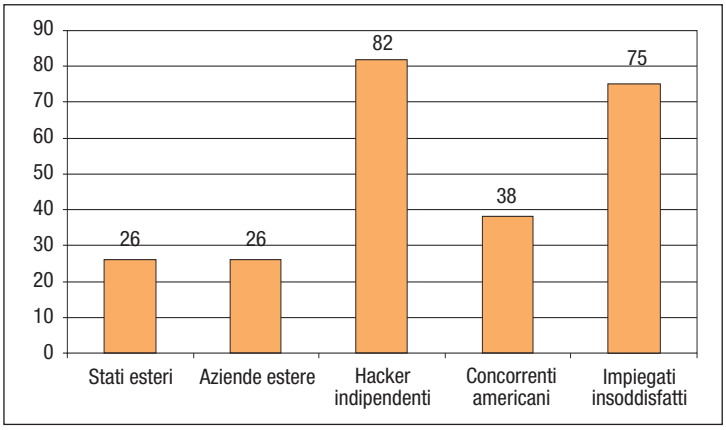


FIGURA 3
Attuatori degli attacchi (Fonte: CSI/FBI 2002)

di vulnerabilità. Normalizzando a 100 le perdite dovute a furti di informazioni riservate, che come si è detto, costituiscono la classe con il valore assoluto più elevato, si ottengono i valori relativi riportati nella tabella 1.
In generale, i dati precisi sulle perdite economiche dovute a intrusioni, minacce e vulnerabilità varie sono difficili da ottenere per problemi sia di riservatezza (l'80% degli attacchi con o senza danni non viene denunciato o, comunque, reso esplicito) sia di valutazione tra costi diretti e indiretti.
È possibile, tuttavia, disporre di alcuni dati attendibili, ad esempio sui costi dei danni prodotti da virus e worm. Nel 1999, si stima che siano stati persi globalmente circa 8 miliardi di dollari per worm di rete, di cui una parte consistente dovuti al *worm Melissa*. Nel 2001, il *worm Red Code*, che in poco meno di 9 min ha compromesso 250.000 computer, si stima abbia provocato danni per 2,6 milioni di dollari. Una cifra assai significativa se si pensa che il danno complessivo alle strutture IT in occasione dell'attacco terroristico dell'11 settembre è stimato pari a circa 12 milioni di dollari.

DOS (*Denial of Service*)	13
Virus/worm	30
Accessi dall'esterno non autorizzati	11
Furti di informazioni riservate	100
Frodi finanziarie	68
Sabotaggi	9
Abuso nell'uso delle reti interne	29

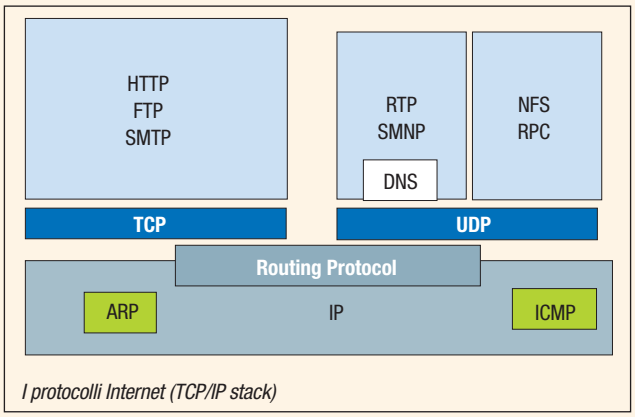
TABELLA 1
Perdite dovute ad attacchi informatici per classi di vulnerabilità

2. SICUREZZA DELLE RETI

L'insieme delle comunicazioni fisse e mobili si sta oggi muovendo verso un significativo punto di aggregazione costituito dall'adozione del paradigma dei **protocolli Internet**. In particolare, le reti basate su *Transmission Control Protocol* (TCP) e *Internet Protocol* (IP) costituiscono, ormai, la quasi totalità delle reti orientate ai dati e stanno diventando predominanti anche per reti orientate ad altri flussi informativi, quali la voce e il video. Ne deriva che la trattazione che verrà fatta in questo articolo si orienterà esclusivamente alle reti di tipo TCP/IP.
Va subito osservato che la genesi dei protocolli Internet, realizzati sostanzialmente negli anni '70 e '80, ha tenuto conto, in modo assai marginale, dei problemi di sicurezza derivanti dall'uso intensivo di tali protocolli in un contesto pubblico, assai complesso, e ancor meno dei servizi applicativi che imponevano vincoli di sicurezza stringenti, si pensi alle transazioni economiche via web. Ciò ha determinato una serie di vulnerabilità, ancora oggi presenti, che costituiscono la base su cui varie minacce, quali virus, worm, attacchi alla disponibilità dei sistemi, si basano. Come per altro già affermato, la vulnerabilità dei protocolli di rete deve essere associata alla vulnerabilità degli ambienti *software* sugli host.
In sintesi, i problemi di sicurezza nascono, *in primis,* dai seguenti fatti:

- Le reti e i relativi protocolli di base sono per loro natura strutture insicure: per esempio, in assenza di specifiche misure, la trasmissione dell'informazione avviene sempre in chiaro, *password* comprese; le reti, specie quelle locali, operano in modalità *broadcast*; la disponibilità agevole di strumenti di gestione per l'intercettazione, la modifica di pacchetti di rete, i cosiddetti *sniffer software*;
- gli ambienti software di sistema (sistema operativo) o applicativi contengono errori e criticità sfruttabili a fini di realizzare minacce: è il caso di errori di codifica o configurazione quali il già citato *buffer overflow*, o la presenza di *backdoor*;
- i dati sono sempre più condivisi tra utenti e applicazioni, e ciò in assenza di politiche forti di protezione o di protocolli di negoziazione

I **protocolli** su cui si basa **Internet** si rifanno allo schema concettuale ISO-OSI, che prevede una serie di livelli logici separati di protocollo, ciascuno con funzionalità ben definite e con interfacce standard verso il livello superiore o inferiore. I protocolli della *suite* Internet possono essere classificati in tre livelli distinti, definiti come livello di rete o di *internetworking*, livello di trasporto e livello di applicazione. Si veda, a tal proposito la figura. Il livello di rete si appoggia sul livello *data-link* che non è considerato nella suite Internet e riguarda più propriamente i tipici protocolli delle reti locali (per esempio, Ethernet) oppure i protocollo punto-punto per le reti geografiche (per esempio, HDLC, PPP). Il livello di rete è caratterizzato dal protocollo IP, responsabile dell'instradamento dei pacchetti tra sottoreti anche disomogenee. Il livello di trasporto prevede due fondamentali protocolli che garantiscono una connessione diretta end-to-end di tipo affidabile o connesso (TCP) o di tipo non connesso. Il livello di applicazione riguarda, invece, un insieme di protocolli ognuno dei quali orientato a un particolare servizio Internet, tra cui il protocollo SMTP per i servizi di posta elettronica e il protocollo HTTP per la navigazione web.



I protocolli Internet (TCP/IP stack)

Va infine ricordato che, in aggiunta ai classici citati protocolli, esistono molti altri protocolli dell'architettura Internet che hanno rilevanza ai fini dell'operatività di Internet stessa. Alcuni sono protocolli relativi a servizi, altri protocolli che realizzano funzioni di controllo. Alcuni di questi ultimi rivestono particolare importanza ai fini della sicurezza. Tra questi si citano:

- il protocollo ICMP (*Internet Control and Management Protocol*), usato per scambiare informazioni sullo stato dei nodi della rete;
- i protocolli di routing (RIP, OSF, BGP ecc.), impiegati dai router per lo scambio di informazioni di instradamento;
- il protocollo DNS (*Domain Name System*) utilizzato per lo scambio di informazioni tra speciali server di rete(DNS server) che effettuano la traduzione tra indirizzi logici (per esempio www.polito.it) e indirizzi binari di rete (per esempio, 130.192.23.13).

idonei a livello di data base, tali da permettere accessi controllati e autenticati ai dati.
In questo contesto, si realizzano un'ampia serie di minacce ai fondamenti della sicurezza. Questi devono garantire la *riservatezza* e *l'integrità* dei dati, *l'autenticazione* del mittente e del destinatario, la *disponibilità* di dati e risorse e il *non ripudio*, ossia la proprietà per cui non sia possibile negare la generazione e/o la trasmissione di informazioni.
Introdurre qui una completa tassonomia dei possibili tipi di attacco o di vulnerabilità risulterebbe assai dispendioso. Si preferisce riassumere in breve le minacce che risultano quantitativamente e qualitativamente più rilevanti.

❑ ***Sniffing (snooping)*** È l'insieme di tecniche mirate a catturare i pacchetti che transitano sulla rete al fine di leggerne i contenuti, siano essi gli indirizzi di partenza o di arrivo, oppure il contenuto vero e proprio del pacchetto, il cosiddetto *payload*. Si tratta, pertanto, di un attacco alla riservatezza dei dati reso assai agevole da alcune tecnologie di rete, come quelle LAN (*Local Area Network*), dove l'informazione viene inviata in modalità broadcast a tutti i nodi. Nel caso di reti punto-punto, è, invece, necessario acquisire il controllo di una delle apparecchiature che costituiscono la rete, per esempio i *router*. Ci si può proteggere da attacchi di tipo *sniffing* sui dati attraverso l'impiego di opportune tecniche crittografiche, come realizzato nelle VPN (*Virtual Private Network*) sicure descritte nel seguito.
❑ ***Address spoofing*** Con questo termine si indicano le tecniche di attacco basate sulla generazione di pacchetti di rete contenenti l'indicazione di un falso mittente. Quando questa modifica riguarda l'indirizzo IP di un pacchetto si parla di *IP spoofing*. Si tenga presente che la manipolazione degli indirizzi di rete di un pacchetto risulta, in genere, assai semplice poiché la maggior parte dei protocolli di rete non ammettono protezioni su tali valori. Falsificando l'indirizzo del mittente si inganna il nodo destinatario con lo scopo di superare alcune protezioni di accesso, se queste sono basate sull'indirizzo del mittente, o di dirottare verso altri nodi le risposte attese o ancora di attribuire, a terzi, azioni richieste o attivate

dal pacchetto modificato, come nel caso di **attacchi DOS** (*Denial of service*) per far ricadere l'origine dell'attacco su altri nodi.

❑ ***Denial of service (DOS)*** Questi tipi di attacchi compromettono la disponibilità di servizi o elaboratori tenendoli impegnati in una serie di operazioni inutili o bloccando totalmente l'attività. Quando l'attacco proviene da diverse stazioni contemporaneamente, al fine di rendere molto più incisiva l'efficacia dell'attacco, si parla di *distributed DOS*, o DDOS. Gli attacchi DOS sfruttano, in genere, un'intrinseca debolezza di un protocollo di rete o una sua non idonea configurazione o implementazione. Esempi ampiamente diffusi sono gli attacchi basati sul protocollo TCP (TCP/SYN *flooding*) e ICMP (*Internet Control Message Protocol*) *smurfing*. Tali attacchi possono essere indirizzati sia a servizi, quali i siti *www*, compromettendo in tal caso le funzionalità del servizio (l'accesso al sito per esempio o a elaboratori di rete come i router o i *server* DNS) determinando notevoli criticità all'operatività complessiva della rete.

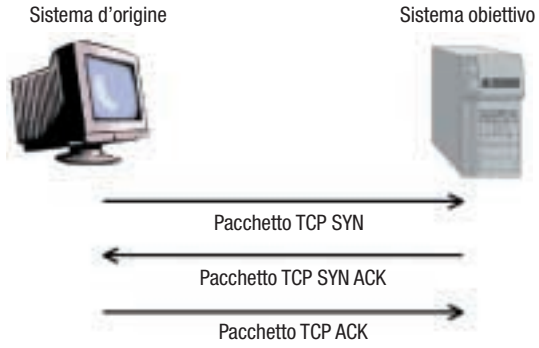
In aggiunta ai tre tipi di attacco in precedenza descritti, debbono essere ricordati ancora due fondamentali elementi che concorrono alla realizzazione di minacce per sistemi. Essi riguardano più gli host che non la rete o i suoi protocolli in senso stretto. Si tratta delle tecniche definite come *Trojan* (cavallo di Troia) e *backdoor*.

❑ ***Trojan*** Un Trojan (o *Trojan Horse*) è una porzione di codice, o più genericamente, un programma che realizza azioni indesiderate o non note all'utilizzatore. Tali programmi possono essere inseriti all'interno di programmi o procedure tradizionali che svolgono, apparentemente, normali funzioni applicative o di sistema. La concezione di virus informatico si basa fondamentalmente sull'impiego di programmi Trojan. Tutti i virus più famosi, da *Nimba* a *Melissa* a *I loveYou*, contenevano un "cavallo di troia", nascondevano cioè il proprio codice virale in *file* eseguibili apparentemente innocui o di sistema.

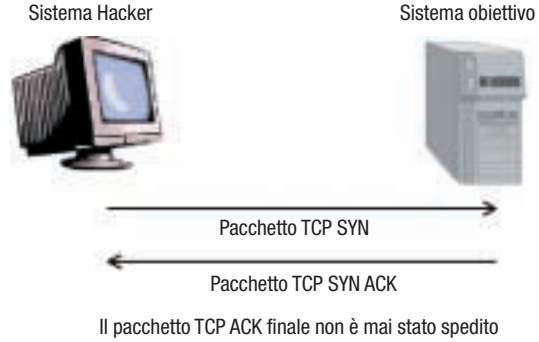
❑ ***Backdoor*** Con questo termine si indica un meccanismo, in generale non noto diffusa-

Per comprendere il meccanismo di un **attacco di tipo DOS** della categoria *SYN flood* è necessario tener presente che l'apertura di una normale connessione TCP si realizza inviando da parte del sistema che vuole attivare il collegamento (*source system*) un pacchetto TCP di richiesta di apertura di connessione, denominato SYN. Il sistema destinazione (*target system*) quando riceve il pacchetto SYN, pone la richiesta di connessione in una apposita lista o buffer contenenti le richieste di connessione e risponde con un pacchetto di accettazione della connessione denominato SYN ACK. Il sistema target si pone, quindi, in attesa di un'ulteriore conferma da parte del sistema *source*, conferma che si realizza mediante l'invio di un pacchetto di conferma di tipo ACK. Quando questo giunge al sistema target esso stabilisce definitivamente la connessione rimovendo dalla lista la richiesta pendente di connessione. La sequenza delle operazioni è illustrata nella figura **A**.

Nel caso, invece, di un attacco di tipo Syn flood, il programma di attacco residente sul sistema source (*Hacker system* in figura **B**) ignora deliberatamente il pacchetto di conferma SYN ACK proveniente dal sistema target e invia in brevissimo tempo una ulteriore richiesta di connessione tramite il pacchetto di SYN. Il sistema target riceverà così in brevissimo tempo molte richieste di connessione saturando in breve la lista delle richieste pendenti. A questo punto il sistema non sarà più in grado di ricevere alcuna ulteriore legittima richiesta di connessione e, pertanto, risulterà di fatto scollegato dalla rete. Ovviamente, se durante l'attacco di tipo Syn flood il sistema source non maschera il proprio indirizzo nel pacchetto TCP, risulta relativamente semplice rilevare l'attacco, attraverso l'analisi degli "indirizzi mittente" dei pacchetti giunti al sistema target, e bloccarlo. Se, invece, il codice di attacco presente sul hacker system modifica l'indirizzo mittente, mediante la citata tecnica di spoofing, introducendo nel pacchetto al posto del reale indirizzo del sistema source indirizzi inesistenti o fasulli, l'identificazione risulta assai ardua e l'attacco difficile da rigettare.



A *Sequenza di richiesta di servizio corretta (3 ways handshake)*



B *Principio dell'attacco di tipo SYN flood*

mente, che permette di "entrare" in un ambiente o programma superando le normali barriere poste per accedervi. Tali percorsi possono essere stati progettati volutamente per garantire un accesso diretto durante le fasi di sviluppo e/o manutenzione del codice, oppure possono derivare da errori di progettazione o di codifica del codice. L'importanza delle backdoor deriva dal fatto che gli *hacker* per iniziare un attacco devono penetrare un sistema sul quale installare il codice di attacco. E ciò di norma è realizzato attraverso lo sfruttamento di backdoor. Lo stesso vale per la realizzazione di meccanismi di propagazione per virus e worm. Per esempio, il recente *worm Sapphire* o *sq hell* che ha generato notevoli danni all'inizio di questo anno sfruttava una tecnica di backdoor per acquisire privilegi di sistema.

Sniffing, *spoofing*, *DOS*, *Trojan* e *backdoor* costituiscono le tecniche di base per realizzare attacchi in rete molto articolati e complessi. Mediante queste tecniche si realizzano le intrusioni informatiche per realizzare furti di informazioni o danneggiamenti, o si creano virus e worm oppure si attaccano apparati o server di rete.
Per esempio, per compromettere il funzionamento e le prestazioni della rete Internet, o di una sua porzione oppure di una rete aziendale basata su tecnologia Intranet, possono essere attaccati router e DNS (*Data Source Name*) server. Si consideri, a titolo esplicativo, quest'ultimo caso.
Si ricorda che la funzione fondamentale di un server DNS è quella di tradurre gli indirizzi logici della rete (per esempio, www.polito.it) nei corrispondenti indirizzi binari o indirizzi IP (per esempio, 130.192.23.13). Il protocollo DNS, permette a ogni nodo della rete di richiedere a un server DNS questa traduzione: viene inviato l'indirizzo logico e si ottiene in risposta quello IP. Gli attacchi ai servizi erogati dai DNS server possono riguardare l'integrità dei dati contenuti nel server o la disponibilità dei servizi. Un server DNS può essere compromesso mediante un attacco DOS, nel qual caso risulta non più accessibile dai nodi di rete. Un risultato analogo può essere ottenuto intercettando le richieste dei vari nodi (sniffing) e inviando indietro falsi pacchetti di risposta (spoofing) o re-indirizzando i pacchetti di richiesta a server senza funzioni DNS. Si otterrà in tutti i casi che i nodi mittenti non otterranno risposta. Un server DNS può essere, inoltre, compromesso attraverso tecniche di backdoor che implicano l'acquisizione del controllo del sistema, potendo in tal caso svolgere funzioni mirate a corrompere il data base di corrispondenza tra indirizzi logici e binari. Queste tabelle di corrispondenza possono essere, infine, corrotte attraverso l'invio di dati di aggiornamento falsi, sfruttando in modo anomalo certe funzioni del protocollo DNS. Per esempio, a un dato indirizzo logico può essere associato l'indirizzo IP non del vero sito web ma di un sito clonato o diverso (*shadow web server*), con evidenti criticità sul piano dell'immagine e del business. Si noti che le funzioni DNS sono tra quelle fondamentali nel funzionamento di Internet: la loro compromissione determina, pertanto, gravi e significativi problemi al funzionamento della rete, tanto è che lo IETF ha introdotto una versione sicura del protocollo DNS, denominata DNSSEC.
Nel concludere questa breve rassegna sulle tecniche di attacco e sulle vulnerabilità presenti nei sistemi di rete odierni, non possono non essere citati i worm. Questi, come noto, sono programmi dotati della caratteristica di auto replicarsi, come i tradizionali virus, e di auto propagarsi in rete. È quest'ultima caratteristica che, almeno sul piano formale, li distingue dai virus, anche se oggi le differenze diventano sempre più labili. Oggi i worm sfruttano tecniche di diffusione assai sofisticate e molto veloci, tali da rendere le contromisure inefficaci se non nel medio termine. Si consideri che il worm Sapphire, attivatosi il 25 gennaio scorso generando notevoli danni nel nostro Paese, ha realizzato una velocità di diffusione, dovuta a tecniche sofisticate di scansione del codice virale, che portava al raddoppio dei calcolatori infettati ogni 8,5 s, contro i 37 min del già citato worm Red Code, considerato a suo tempo il più veloce worm della storia. Sapphire ha infettato più del 90% degli host vulnerabili in circa 15 min, con un numero di host compromessi complessivamente superiore a 100.000. Il maggior danno di questi worm, al di là dei potenziali effetti distruttivi di file eventualmente contenuti, a scadenza, nel codice virale, deriva dalla saturazione della rete che si realizza durante la propagazione

producendo un effetto di DOS su server e apparati di rete, ivi comprese le reti locali soggette alla diffusione del codice virale.

3. COME DIFENDERSI

La necessità di realizzare reti sicure è, come detto, un'esigenza imprescindibile per le applicazioni business. Essa, pur in presenza delle citate vulnerabilità, può essere ottenuta attraverso una idonea politica di sicurezza che si poggia su corrette scelte tecnologiche e su adeguate strategie organizzative. Soffermandosi, per ragioni di brevità, unicamente sulle prime senza per altro trascurare l'importanza fondamentale delle seconde, si può affermare che il raggiungimento di accettabili livelli di sicurezza si ottiene impiegando tecnologie mirate a realizzare le funzioni di segretezza, di autenticazione, di autorizzazione e di *auditing*. Tali funzioni si basano, essenzialmente, sull'impiego di tecniche crittografiche descritte brevemente nel seguito.
La realizzazione delle sopra citate funzioni di sicurezza può essere realizzata con modalità tecnologiche diverse in funzione dei contesti architetturali e dei servizi di cui si vuole disporre. A un primo livello di approssimazione, è possibile suddividere le tecniche per rendere sicuro un sistema in rete in due grandi categorie: le tecniche che operano sui protocolli di rete, modificando quelli tradizionali al fine di introdurre prestazioni di sicurezza (sottoparagrafo 3.4), e quelle di tipo architetturale che mirano a rendere sicuro un sistema introducendo appositi apparati, per esempio *firewall*, e/o modificando la struttura stessa della rete riducendo le vulnerabilità esistenti (sottoparagrafo 3.5).
Prima di poter esaminare, in dettaglio, alcune delle possibili soluzioni atte a rendere sicura una rete aziendale e i suoi servizi, sembra utile riassumere i fondamentali concetti di crittografia, che come noto è la base concettuale per realizzare le fondamentali proprietà della sicurezza: segretezza, autenticazione, non ripudio.

3.1. Cenni di crittografia

Affinché due nodi possano comunicare tra loro in modo sicuro è necessario che il canale che li collega goda delle proprietà di segretezza e autenticazione. Queste vengono realizzate mediante tecniche e algoritmi crittografici. In generale, nella fase più propriamente detta di cifratura, un testo in chiaro (*plaintext*) viene trasformato nel corrispondente testo cifrato (*ciphertext*) mediante l'uso di una chiave predefinita. Un procedimento analogo si realizza nella fase di decifratura che garantisce il passaggio dal testo cifrato a quello originale. La chiave e gli algoritmi utilizzati nella cifratura non necessariamente coincidono con quelli impiegati durante la decifratura.
Esistono due principali categorie di algoritmi utilizzati per la cifratura delle informazioni: quelli che fanno uso di chiavi simmetriche (dove la stessa chiave serve sia per la cifratura dei dati sia per la loro decodifica) e quelli a chiavi asimmetriche, dove le due chiavi sono diverse e intercambiabili: ciascuna di esse può essere utilizzata per cifrare le informazioni, ma solo l'altra può essere usata per decifrarle. In generale, della coppia di chiavi una, detta privata, viene tenuta segreta, l'altra detta pubblica viene, invece, resa disponibile a tutti. In pratica a ciascun soggetto è associata una coppia di chiavi (chiave pubblica e chiave privata). L'associazione tra la chiave pubblica e il soggetto a cui essa è associata, è realizzata mediante un certificato a chiave pubblica, cioè una tabella informatica che contiene gli estremi del soggetto e la chiave pubblica associata. Tale certificato è di norma rilasciato da un apposito ente indicato come autorità di certificazione o CA (*Certification Authority*).
Gli algoritmi basati su chiave simmetrica sono più semplici e, quindi, meno pesanti dal punto di vista computazionale rispetto agli algoritmi a chiave asimmetrica. Esempi di algoritmi simmetrici sono: DES, triplo DES, AES, RC4. Il problema intrinseco degli algoritmi simmetrici risiede nella distribuzione della chiave in modo affidabile e segreto. Se questa non è distribuita in modo sicuro, e qualcuno ne viene a conoscenza, tutto il sistema risulta compromesso. Da qui, l'uso di definire gli algoritmi simmetrici anche come algoritmi a chiave segreta. La distribuzione della chiave segreta ai soli soggetti suoi depositari può essere realizzato in vari modi, tra cui quello di impiegare la crittografia asimmetrica.
Mentre gli algoritmi simmetrici sono impiegati principalmente per realizzare la funzione

di segretezza, quelli a chiave asimmetrica permettono di realizzare sia la *segretezza* sia l'*autenticazione*.

- La funzionalità di *segretezza* si ottiene utilizzando la chiave pubblica per cifrare le informazioni da inviare al soggetto cui la chiave stessa è associata. Solo l'interessato possiede la chiave privata, e pertanto è in grado di decodificare le informazioni.
- La funzionalità di *autenticazione del mittente* (ovvero, la certificazione dell'identità del mittente) è ottenuta facendo sì che l'originatore cifri i dati con la propria chiave privata prima di inviarli. Chiunque sia in possesso della chiave pubblica può utilizzarla per decodificare le informazioni ricevute e avere, quindi, la certezza che esse siano state cifrate con la chiave privata del soggetto in questione.

Gli algoritmi a chiave asimmetrica ricoprono anche un ruolo fondamentale nel garantire la corretta distribuzione di chiavi simmetriche. Esempi di algoritmi asimmetrici sono RSA, DSA e *Diffie-Hellman*, per la distribuzione di chiavi segrete.

3.2. Reti aziendali e sicurezza

Nel caso più generale, una rete aziendale è costituita da un insieme di reti locali, ciascuna corrispondente a una specifica sede dell'azienda, connesse fra loro da collegamenti che possono essere realizzati con un'infrastruttura privata oppure utilizzando una rete pubblica (ad esempio, Internet) come illustrato in figura 4.

In relazione agli aspetti di sicurezza risulta opportuno definire i seguenti tre sottosistemi:

- La rete locale (una per ogni sede). Renderla sicura significa introdurre meccanismi di riservatezza delle informazioni trasmesse, oltre a sistemi che "osservano" il traffico al fine di identificare comportamenti o eventi anomali. La rete locale può prevedere zone che richiedono livelli di protezione diversi, come sarà illustrato nel seguito trattando le soluzioni di tipo firewall.
- La zona di frontiera (una per ogni sede). È il punto di contatto tra la rete locale e la rete "pubblica" utilizzata per le comunicazioni con il resto del mondo (tipicamente la rete Internet). In tale area è generalmente presente un router che collega a un fornitore di servizi di connettività (per esempio, un *Internet Service Provider*, ISP). Rendere sicura questa zona implica attivare, per esempio, sul router di frontiera meccanismi di ispezione dei pacchetti in transito al fine di verificare traffico anomalo in ingresso verso la rete locale o in uscita da essa.
- La rete esterna utilizzata per realizzare le connessioni tra le varie sedi aziendali. Trattandosi nel caso più comune di una rete pubblica (Internet), questa zona dovrà essere sempre considerata insicura, e nel caso si vogliano proteggere le comunicazioni che su essa hanno luogo occorrerà introdurre meccanismi che rendano indecifrabile il traffico tra le diverse sedi dell'azienda.

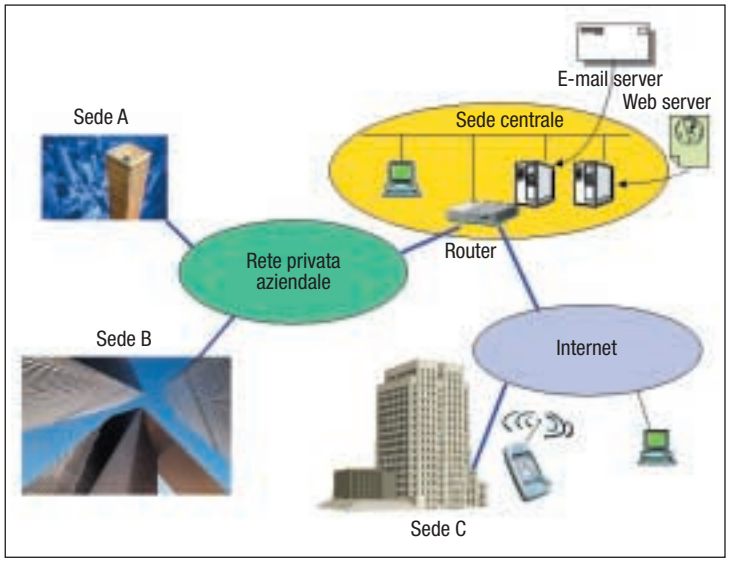


FIGURA 4
Rete aziendale

3.3. Le politiche aziendali per la sicurezza

La messa in atto di meccanismi che rendano sicura una rete aziendale possono essere definiti con precisione solo a seguito di una pianificazione delle politiche di sicurezza dell'azienda, in generale contenute nel documento fondamentale della sicurezza aziendale, il "piano di sicurezza". In esso, tra l'altro, si descrivono le funzionalità di rete che si vogliono concedere e le relative modalità, così come le funzionalità che si decide di proibire.

Esempi di aree interessate dalla definizione delle politiche di sicurezza aziendale sono:

- La possibilità di concedere comunicazione diretta tra i nodi della rete (PC degli utenti) e la rete Internet per scopi di navigazione. Qualora si stabilisca di non voler concedere tale diritto, occorrerà, per esempio, prevedere un nodo *proxy web* (o *web cache*) attraverso il quale gli

utenti che vogliono consultare il mondo web siano costretti a passare (quindi, parallelamente bloccando il passaggio diretto dei pacchetti tra i PC degli utenti e il mondo esterno).

- La presenza di un sistema centralizzato di antivirus in grado di "intercettare" ed esaminare il grado di sicurezza dei messaggi di posta elettronica, delle pagine web e delle eventuali porzione di codice (per esempio, *Java applet*) in esse presenti.
- La presenza di un sistema che analizza periodicamente il traffico presente sulla rete locale, configurato per riconoscere sequenze di attacco e identificare, quindi, tentativi di forzatura originati all'interno della LAN aziendale.
- La presenza di un sistema analogo al precedente, ma installato in posizione tale da permettergli di analizzare il traffico da e verso il mondo esterno (al fine di identificare attacchi provenienti dall'esterno e diretti alla LAN aziendale o viceversa).
- La presenza di un sistema in grado di eseguire autenticazione di utenti aziendali che si trovano all'esterno dell'azienda e che, in caso di riconoscimento di personale autorizzato, conceda l'accesso sicuro alle risorse aziendali con le stesse modalità disponibili per gli utenti interni.

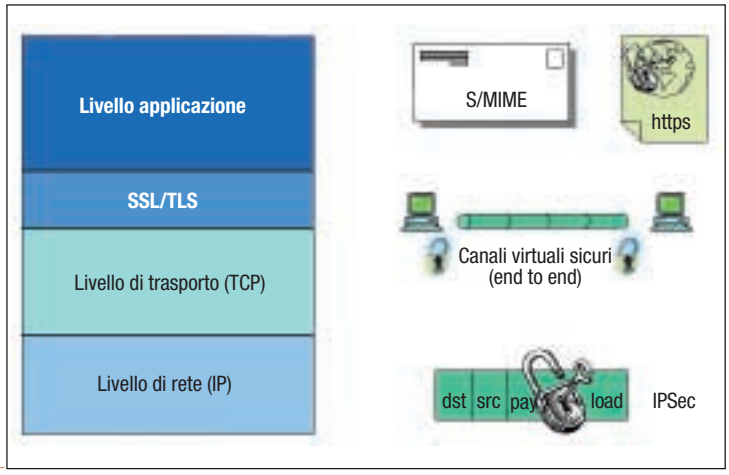
3.4. Sicurezza nelle applicazioni e nei protocolli di rete

La necessità di introdurre sicurezza nel software di comunicazione mediante impiego di applicazioni o protocolli di rete resi sicuri nasce dalla assunzione fondamentale di non avere garanzie di sicurezza offerte dalla rete. Partendo cioè dal presupposto di avere una rete non sicura (alla quale, pertanto, si assume siano connessi soggetti intenzionati a osservare il traffico al fine di carpire informazioni e successivamente perpetrare attacchi), due elaboratori che intendono scambiarsi informazioni devono utilizzare accorgimenti che impediscono l'intercettazione e la manipolazione delle informazioni stesse, nonché la certezza dell'autenticità del mittente e/o destinatario delle informazioni.

Come specificato nel riquadro sui protocolli Internet, il software di comunicazione di rete viene convenzionalmente organizzato e sviluppato in modo stratificato, identificando diversi "livelli" per ciascuno dei quali sono definite funzionalità e modalità di comunicazione verso i livelli superiore e inferiore (interfacce). L'indipendenza (tipica di questa architettura e suo principio fondamentale) di ciascuno dei livelli rispetto agli altri offre la possibilità di modificare il software che costituisce un livello senza dover intervenire su quelli superiori o inferiori.

Le funzionalità di comunicazione sicura possono, quindi, essere introdotte in diversi punti della "pila", ottenendo soluzioni di sicurezza con caratteristiche diverse. Si considerano ora le diverse soluzioni adottabili ai diversi livelli di protocollo, rappresentate in modo sintetico in figura 5.

FIGURA 5
Sicurezza a diversi livelli



3.4.1. Sicurezza a livello di applicazione

Introdurre funzionalità di sicurezza a livello applicativo significa modificare l'applicazione che si vuole rendere sicura aggiungendo, ad esempio, la crittografia dei dati: le informazioni vengono rese indecifrabili a bordo dell'elaboratore che le genera, e nessuna altra applicazione risente dell'effetto di questa operazione. I dati generati dall'applicazione sicura vengono inviati utilizzando normali pacchetti di rete, ai quali non è applicata alcuna operazione di cifratura (per la rete tali dati sono "in chiaro", ma sono di fatto indecifrabili in quanto sono stati cifrati alla fonte). Molto comune è, per esempio, l'impiego di posta elettronica cifrata (per esempio, in conformità con le specifiche S/MIME), che prevede che solo l'applicazione che compone il messaggio e quella che lo riceve rilevino l'uso di crittografia. Ne deriva che lo scambio di chiavi crittografiche riguarda ciascuna applicazione e la sicurezza

si limita alla singola applicazione, per esempio la posta elettronica ma non il web.

3.4.2. Sicurezza a livello di sessione

Introdurre sicurezza a livello di sessione significa creare un canale virtuale sicuro sul quale far transitare una specifica transazione o sessione di comunicazione. Le applicazioni coinvolte, in questo caso, generano e ricevono informazioni senza cifrarle (e, quindi, potrebbero anche ignorare l'esistenza della sicurezza e della crittografia). Ne deriva che più applicazioni possono avvalersi del canale sicuro. Le informazioni vengono "intercettate" prima di lasciare l'elaboratore che le ha generate per essere cifrate e inviate al nodo destinatario. Presso il nodo destinatario è attivo un procedimento speculare che prevede la ricezione delle informazioni stesse, la loro decodifica e il passaggio (in chiaro) alla applicazione che le deve ricevere. Le applicazioni coinvolte non sono al corrente delle operazioni di crittografia. Un caso molto diffuso di questo tipo di soluzione è rappresentato dal protocollo SSL (*Secure Socket Layer*), alla base delle comunicazioni web sicure. Nel caso del trasferimento di pagine web mediante SSL, le pagine stesse non sono crittografate, e possono essere consultate in modo sicuro utilizzando il protocollo HTTP inviato su un canale con protocollo SSL (a sua volta costruito sul TCP) che garantisce l'autenticazione del server e del client e la cifratura di tutti i dati che transitano sul canale.
È importante osservare come la possibilità di stabilire un canale di comunicazione sicuro permetta l'utilizzo di questa soluzione a un numero arbitrario di applicazioni, senza modificare il codice relativo alla applicazione stessa. Nel caso precedente (sicurezza a livello applicativo) viene, invece, risolto il problema della sicurezza solo per l'applicazione che viene modificata per renderla sicura. Il protocollo SSL, introdotto da Netscape, è stato standardizzato con lievi modifiche da IETF ed è denominato TLS (*Transport Layer Security*).

3.4.3. Sicurezza a livello network: IPSec

La costruzione di un canale di comunicazione sicuro mediante SSL implica la realizzazione di un canale virtuale *end-to-end*, cioè tra mittente e destinatario, che rende sicuro tutto il traffico esistente tra i due nodi mittente e destinatario e che utilizza come protocollo il TCP. Di fatto, SSL può essere visto come uno strato aggiuntivo collocato nella architettura TCP/IP al di sopra del livello TCP. Di conseguenza, non tutto il traffico è associato a canali virtuali realizzati mediante TCP (per esempio, il traffico che impiega il protocollo UDP (*User Datagram Protocol*)).
È possibile, tuttavia, introdurre sicurezza anche a livello più basso del trasporto, agendo, ad esempio, direttamente sui singoli pacchetti IP. Una soluzione molto diffusa che fa uso di questa strategia è l'architettura IPSec (*Secure Internet Protocol*), che prevede di eseguire cifratura e autenticazione a livello dei singoli pacchetti IP.
Questa caratteristica svincola questa soluzione dal dover essere messa in atto sul nodo origine del traffico (come, invece, avviene nei due casi precedenti). La cifratura del traffico IP può, infatti, essere effettuata tra due nodi qualsiasi esistenti tra il nodo sorgente e quello destinatario e riguarda tutti i pacchetti IP in transito indipendentemente dai protocolli superiori impiegati, TCP o UDP. Il protocollo IPSec agisce in sostanza tra due nodi qualunque della rete, in genere costituiti da router. È evidente che non è richiesto che il nodo mittente o quello destinatario siano informati dell'esistenza di un canale IPSec lungo il percorso che li unisce. Il nodo mittente immette traffico "in chiaro" sulla rete, quello destinatario riceve traffico "in chiaro". Tecniche quali IPSec trovano frequente impiego nella realizzazione di reti private virtuali o VPN, grazie alle quali diverse sedi possono essere messe tra loro in comunicazione senza utilizzare un'infrastruttura dedicata, ma costruendo canali sicuri su una struttura intrinsecamente insicura. Nella figura 6 è riportata la stessa struttura logica precedentemente illustrata (Figura 4), ma nella quale la rete privata di connessione tra le sedi è stata sostituita da canali virtuali costruiti su Internet. Non tutte le sedi aziendali sono obbligate a essere connesse utilizzando canali virtuali sicuri: nella figura, la sede C, che precedentemente era connessa alla sede centrale utilizzando la rete Internet, continua a essere partecipe della rete aziendale nella stessa modalità.

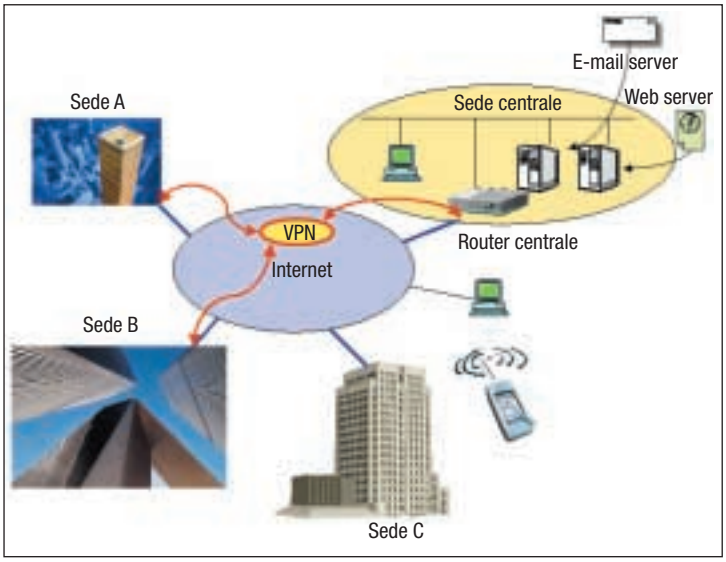


FIGURA 6
Rete aziendale con VPN (Virtual Private Network)

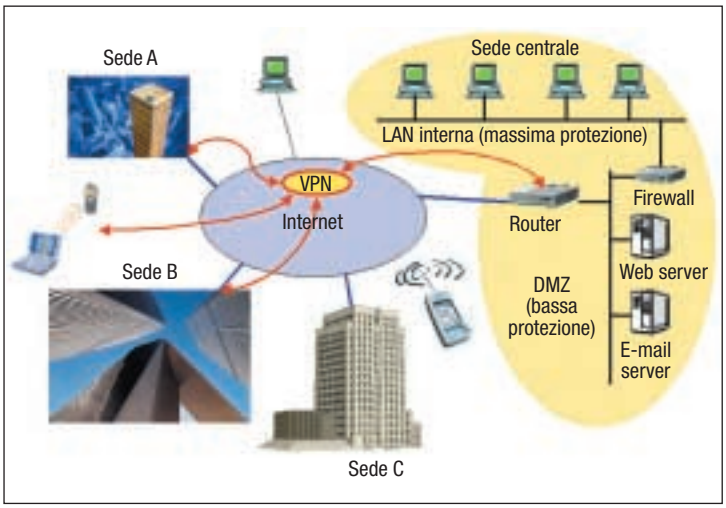


FIGURA 7
Rete aziendale protetta mediante firewall

3.5. Introdurre sicurezza nell'architettura di rete

Le soluzioni sopra citate permettono di ottenere comunicazioni sicure su un'infrastruttura non sicura. Esse, tuttavia, non tutelano nei confronti di attacchi che non hanno come oggetto l'informazione in transito ma le funzionalità della stessa rete, quali ad esempio gli attacchi di tipo DOS (già descritti in precedenza), o la forzatura (*hacking*) di sistemi per ottenerne il controllo.
Molte di queste minacce possono essere vanificate mediante l'introduzione, nell'architettura della rete, di componenti che hanno il compito di "osservare" tutto il traffico e riconoscere situazioni anomale, a seguito delle quali prendere provvedimenti atti a bloccare l'attacco in corso.
Tra i componenti più frequentemente introdotti a tale scopo all'interno delle reti aziendali figurano i firewall, le reti private virtuali o VPN, i sistemi di rilevamento di intrusioni o IDS (*Intrusion Detection Systems*) e i sistemi antivirus.
Nella figura 7, è rappresentata l'architettura di rete aziendale già descritta in precedenza, ulteriormente ampliata introducendo alcune soluzioni mirate alla messa in sicurezza. Per brevità sono state raffigurate solo le soluzioni VPN e firewall. Si osservi come, in questo caso, partecipa alla VPN anche un utente mobile (PC portatile connesso a un telefono cellulare).

3.5.1. VPN

Le reti private virtuali o VPN (*Virtual Private Network*) costituiscono un'applicazione che integra l'uso di protocolli di rete sicuri e tecniche di autenticazione dell'utente. Il servizio di VPN è un meccanismo che permette di stabilire, tra due sedi, comunicazioni sicure e autenticate, permettendo (attraverso una rete pubblica non sicura) lo scambio di informazioni e l'accesso alle risorse aziendali con le stesse caratteristiche di riservatezza e le stesse autorizzazioni garantite agli utenti fisicamente connessi alla rete aziendale.
Due sono i principali ambiti di impiego delle VPN:

- VPN "permanenti" per connessione reciproca di sedi aziendali;
- VPN temporanee per la connessione da remoto di utenti con caratteristiche di nomadicità.

Le VPN permanenti si costruiscono identificando coppie di sedi che devono essere tra loro connesse, e installando in ciascuna di esse un apparato (o un elaboratore che svolge le stesse funzioni) detto terminatore di VPN.
Ciascuno dei due terminatori di un circuito virtuale si preoccupa di cifrare il traffico ricevuto dalla propria LAN e di inviarlo al terminatore di VPN presente nell'altra sede. Il traffico, cifrato, può tranquillamente essere trasportato a questo fine su una rete insicura quale la rete Internet senza che questo rappresenti una minaccia per la sicurezza. Solo i due apparati terminatori del canale VPN conoscono le chiavi per eseguire codifica e decodifica dei pac-

chetti. Di fatto, i pacchetti originali sono prima cifrati e poi imbustati in nuovi pacchetti che viaggiano tra i due soli terminatori della VPN.
Come è semplice intuire, questa soluzione può essere applicata facilmente anche al caso in cui uno dei due terminatori di canale VPN sia su un elaboratore di un utente (per esempio, un PC portatile). Risulta, pertanto, possibile, mediante installazione di opportuno software sull'elaboratore dell'utente, concedere accesso sicuro alle risorse aziendali anche a personale autorizzato che si trovi fuori sede e sia connesso a un comune Internet Service Provider. In quest'ultimo caso è anche evidente la temporaneità del canale virtuale, che viene creato quando l'utente desidera connettersi e cancellato al termine della sessione di lavoro.

3.5.2. Firewall

La posizione di frontiera tra la rete aziendale (che si vuole mantenere sicura) e quella pubblica, è la sede ideale nella quale installare apparati (spesso denominati *firewall*) dedicati a svolgere funzioni di "filtro" del traffico di rete, al fine di impedire il transito di tutto il traffico che non rientra nelle politiche aziendali.
Le funzioni di firewall possono essere anche integrate (nei casi più semplici) all'interno di router esistenti (in particolare, il router principale di connessione verso l'esterno). Anche i router, infatti, sono in grado di eseguire un'analisi (sebbene solo macroscopica) del traffico, e di prendere i primi provvedimenti ove necessario.
Per esempio un router è facilmente in grado di identificare (e bloccare se questo è previsto) traffico di posta elettronica entrante in azienda ma non diretto al server mail aziendale, oppure traffico di navigazione uscente verso il mondo Internet, o altre richieste di connessione provenienti dall'esterno alle quali si sceglie di non voler concedere autorizzazione.
Un router non è, invece, generalmente in grado di identificare pattern di traffico sofisticati quali *port scanning* o TCP SYN attack, così come non è in grado di eseguire sul traffico analisi sofisticate che richiedono la ricostruzione di file di grandi dimensioni quali messaggi di posta elettronica o di intere pagine Web (per esempio per effettuare scansione antivirus).
Vista la sua posizione centrale nell'architettura di rete locale dell'azienda, il firewall viene anche utilizzato per suddividere la LAN in aree a diverso livello di sicurezza, come accennato in precedenza (sottoparagrafo 3.2). Viene a tal fine spesso identificata una zona detta "demilitarizzata" (DMZ) sulla quale vengono rilasciati alcuni dei vincoli che proteggono la rete interna dell'azienda. Sulla DMZ, accessibile più facilmente dal mondo esterno, si trovano elaboratori quali il mail server e il web server aziendali.

4. UN ESEMPIO APPLICATIVO: HOME BANKING

Nei paragrafi precedenti sono state descritte, in modo conciso, le tecnologie disponibili per rendere sicure reti e comunicazioni. Al fine di dare concretezza a tali concetti si ritiene utile descrivere applicazioni di business che si avvalgono di queste tecnologie per realizzare servizi applicativi sicuri.
Tra le varie applicazioni si descrive quella più nota e diffusa: *home* o *Internet banking*. Questa risulta particolarmente interessante in quanto è percepita come estremamente critica dal punto di vista della protezione e riservatezza delle informazioni. Essendo essa basata su una tecnologia ampiamente utilizzata nel mondo Internet (la tecnologia web), permette di evidenziare come, anche in una situazione in cui la sicurezza della rete di comunicazione non è sicura, sia possibile creare una infrastruttura virtuale estremamente affidabile.
In estrema sintesi, il problema dell'Internet banking si riconduce a quello di proteggere la comunicazione tra due nodi connessi alla rete Internet: il *client* utilizzato dall'utente (*browser web*) e il server messo a disposizione dalla banca (web server che svolge funzioni di *front end* verso il sistema informativo bancario).
Condizione essenziale per garantire la sicurezza in questo caso è provvedere alla indecifrabilità delle informazioni trasmesse tra i due elaboratori interessati, mediante tecniche crittografiche (per una descrizione delle quali si rimanda al sottoparagrafo 3.1).
Come precedentemente citato, la creazione di un canale sicuro di comunicazione richiede la condivisione di informazioni segrete (chiavi) tra i due nodi interessati a rendere indecifrabile una specifica sessione di scambio di dati.

Nel caso dello home banking si rende necessaria la generazione di chiavi temporanee che abbiano validità limitata alla sessione di comunicazione di interesse (chiavi di sessione). Parallelamente, occorre un meccanismo grazie al quale due elaboratori che si apprestano a iniziare una comunicazione sicura riescano come azione preliminare a scambiarsi in modo sicuro le chiavi di sessione.
A causa della minore complessità computazionale associata agli algoritmi a chiave simmetrica, questi rappresentano la soluzione preferita per cifrare le informazioni scambiate tra due nodi, i quali devono, quindi, preventivamente condividere un solo segreto (la chiave di sessione, che in questo caso è unica).
La costituzione di un canale sicuro di comunicazione tramite SSL richiede, quindi, due azioni preliminari:

- la generazione della chiave di sessione da parte di uno degli interlocutori;
- la trasmissione della chiave di sessione all'altro interlocutore, *in modo sicuro*.

La *generazione* di chiavi crittografiche, siano esse simmetriche o asimmetriche, è un problema oggi ampiamente risolto mediante opportuni algoritmi, basati su generatori di numeri pseudo casuali, in grado di generare idonee sequenze di *bit* cui le chiavi vengono fatte corrispondere.
Il problema maggiore consiste, invece, nella *trasmissione sicura* di questa chiave dal nodo che la ha generata al suo interlocutore. Ovviamente, tale chiave non può essere trasmessa "in chiaro" prima di iniziare la sessione sicura, perché la sua intercettazione permetterebbe di decifrare tutto il traffico della sessione stessa. Ci si trova, quindi, in presenza di un apparente paradosso: occorre un canale sicuro per trasmettere l'informazione necessaria a creare un canale sicuro di comunicazione.
Il problema della trasmissione della chiave di sessione da un nodo all'altro trova una facile soluzione nell'impiego di una coppia di chiavi asimmetriche. In particolare, le operazioni svolte per trasmettere in modo sicuro la chiave di sessione vengono chiarite nel seguito.
Nel caso dell'applicazione in esame (home banking) il nodo client (utente del servizio) e il nodo server mettono in atto una sessione di comunicazione sicura tra loro mediante la seguente sequenza di operazioni:

1. Il client invia al server una richiesta di creazione di un canale di comunicazione sicuro temporaneo;
2. Il server della banca, che possiede una coppia di chiavi asimmetriche (AK1, AK2, con AK1 chiave pubblica e AK2 privata) invia la chiave pubblica AK1 al nodo client (browser dell'utente);
3. Il nodo client genera la chiave di sessione SK (chiave simmetrica), la crittografa utilizzando la chiave pubblica AK1, e invia il risultato di tale operazione al server bancario. Siccome per decifrare le informazioni è necessaria la chiave privata AK2, solo il server stesso è in grado di decodificare la chiave di sessione (si noti, infatti, che la chiave AK2 non ha mai lasciato l'elaboratore server). La eventuale intercettazione della chiave AK1 non è di nessuna utilità per un eventuale malintenzionato che fosse in ascolto sulla rete.
A questo punto, i due elaboratori condividono il segreto (la chiave di sessione simmetrica SK), e possono iniziare a comunicare in modo sicuro mediante algoritmi simmetrici veloci, trasmettendo le varie informazioni: password, dati finanziari ecc..
Questa sequenza di operazioni è alla base della tecnologia detta SSL (*Secure Socket Layer*) utilizzata per stabilire comunicazioni sicure tra browser e web server. Sul canale SSL (che a questo punto è cifrato e, quindi, sicuro) vengono successivamente inviate le informazioni di autenticazione (username e password nel più comune dei casi). Se la fase di autenticazione viene superata con successo, la banca acquisisce fiducia circa l'identità del cliente e gli rende disponibili i servizi e le informazioni alle quali ha diritto di accedere.
Vista la criticità di questa categoria di applicazioni, misure aggiuntive di sicurezza vengono, generalmente, messe in atto oltre alla creazione di un canale di comunicazione cifrato. Tra queste è possibile citare:

- Scadenza della sessione sicura: qualora l'utente, una volta autenticato, non esegua operazioni di navigazione sul sito per un certo tempo, la sessione "scade" e per continuare le operazioni sarà necessaria una ripetizione delle operazioni di autenticazione.
- Alcune operazioni particolarmente critiche (trasferimento di somme di denaro consistenti) richiedono una ulteriore autenticazio-

ne, spesso basata su tecniche quali *one time password* o similari: per poter portare a termine tali operazioni viene cioè richiesta una informazione aggiuntiva a ulteriore garanzia della identità del cliente.

5. SICUREZZA E TECNOLOGIE WIRELESS

Per completare la rapida panoramica delle architetture di rete aziendale e delle relative tecniche di messa in sicurezza occorre citare la categoria delle soluzioni basate su tecnologie wireless, introdotte diversi anni fa ma per le quali solo in questi anni si sta assistendo a una diffusione consistente sul mercato.
Il principio di base della connettività IP fruibile anche da dispositivi non connessi fisicamente a una rete rende possibile un'ampia gamma di applicazioni. Queste sono in parte semplici estensioni di quelle tradizionalmente fruibili tramite connettività fissa (navigazione su Internet, posta elettronica ecc.), e in parte specifiche del contesto mobile in quanto si basano per esempio su informazioni come la localizzazione fisica dell'utente (telematica per il veicolo, informazioni turistiche ecc.).
La fruibilità delle applicazioni basate su IP da terminali mobili ha visto evolversi parallelamente due settori tecnologici: quello della connettività IP per terminali di tipo telefonico cellulare (quindi connessi alla rete tramite tecnologie quali GSM o GPRS, e WAP per la navigazione Internet), e quello della connettività IP vista come estensione delle reti locali fisse (per terminali connessi alla rete mediante tecnologia Wireless LAN (WLAN), che utilizzano le stesse tecnologie e protocolli tipici delle reti fisse a partire dal livello *network*).
La connettività IP in condizioni di mobilità, e la conseguente trasmissione in aria libera dei dati scambiati tra coppie di elaboratori costituiscono uno scenario nel quale sono ancora più evidenti le problematiche di sicurezza. L'ascolto delle comunicazioni risulta tecnicamente più semplice in ambienti dove queste avvengono via radio rispetto a quanto avviene su rete fissa, dove l'interessato deve almeno trovare un punto di connessione fisica alla rete stessa per avere accesso al flusso di dati. L'uso di tecnologie crittografiche sul canale radio è, quindi, praticamente obbligatorio, sebbene spesso questo aspetto sia effettivamente trascurato. La tecnologia in questo settore è tuttavia già disponibile. Lo scarso successo riscontrato dal protocollo WEP (*Wireless Encryption Protocol*) a seguito della provata possibilità di risalire senza eccessiva difficoltà alla chiave utilizzata per cifrare le informazioni ha incentivato la ricerca di soluzioni alternative quali WPA (*Wi-Fi Protected Access*) o il più generale EAP-TLS (*Extensible Authentication Protocol – Transport Layer Security*), che sono in grado di garantire all'utente la necessaria riservatezza nel dialogo in rete. Per le tecnologie WLAN basate sui protocolli della classe 802.11 sono stati introdotti criteri di elevata sicurezza utilizzando il *framework* di autenticazione fornito dallo standard 802.1x.

Bibliografia

[1] CERT: www.cert.org

[2] CSI/FBI annual report 2002: *Computer security issues & trends*. www.gocsi.com

[3] Mezzalama M, Lioy A: La sicurezza dei sistemi informativi. In *Sistemi Informativi*, Vol. V, Franco Angeli, 2001.

[4] Stallings W: *Cryptography and network security*. 2nd Ed., Prentice Hall, 1999.

[5] SSL specification: www.netscape.com/eng/ssl3

Marco Mezzalama è Professore ordinario di Sistemi di Elaborazione presso la Facoltà di Ingegneria dell'Informazione del Politecnico di Torino, dove attualmente ricopre la carica di Pro Rettore. Autore di numerose pubblicazioni scientifiche, ha collaborato e coordinato parecchi progetti di ricerca in ambito nazionale ed europeo. La sua attività scientifica si è svolta principalmente nei settori dell'architettura dei sistemi di elaborazione, delle reti di calcolatori e dei sistemi informativi aziendali. Ha fondato il Laboratorio di Sicurezza Informatica del Politecnico di Torino e recentemente l'associazione Assosecurity.
marco.mezzalama@polito.it

Edoardo Calia è direttore dei laboratori di ricerca presso l'Istituto Superiore "Mario Boella" di Torino. Presso il Politecnico di Torino è stato responsabile dei Sistemi Informativi e di Telecomunicazioni tra il 1994 e il 2001, ed è attualmente professore a contratto per la docenza del corso di Reti di Calcolatori. Nel 1992 ha ottenuto presso il Politecnico di Torino il titolo di Dottore di Ricerca. Durante il corso di dottorato ha trascorso un anno presso i Laboratori di Ricerca della Digital Equipment Corporation di Marlboro, MA (USA).
calia@ismb.it

SISTEMI OLFATTIVI ARTIFICIALI

Ada Fort
Santina Rocchi
Nicola Ulivieri
Valerio Vignoli

I nasi elettronici sono sistemi complessi caratterizzati da una struttura simile a quella del sistema olfattivo umano: una matrice di sensori chimici a bassa selettività fornisce una firma caratteristica di una miscela chimica che viene successivamente classificata sulla base delle conoscenze acquisite in una fase di addestramento del sistema. Le prestazioni di questi sistemi dipendono in maniera critica da tutte le scelte progettuali, cioè dalla tecnologia realizzativa dei sensori, dalla struttura del sistema di misura, dagli algoritmi di classificazione.

4.3

1. INTRODUZIONE

L'applicazione di sistemi elettronici dedicati nel campo della misura e caratterizzazione di odori è un obiettivo di rilevanza economica e scientifica. I sistemi attuali di rilevazione e misura degli odori basati su *panel* di esperti supportati da sistemi di analisi chimica come la Gas Cromatografia (GC) e la Spettrometria di Massa (MS) sono costosi e richiedono tempi di analisi lunghi. Quindi è di grande interesse lo sviluppo di sistemi a costi contenuti che siano in grado di effettuare tale rilevazione sul campo in tempo quasi reale. Un sistema elettronico elimina anche gli svantaggi legati alla presenza di panel umani, quali per esempio la soggettività del giudizio, cioè la variabilità individuale, e l'adattamento, cioè la diminuzione della sensibilità durante esposizioni prolungate a un odore. Per rispondere a questa esigenza negli ultimi dieci anni sono stati proposti e sviluppati diversi sistemi olfattivi artificiali, noti con il nome di "nasi elettronici", che hanno in comune un'architettura basata su di una matrice di sensori di gas e su di un sistema complesso di elaborazione dei segnali misurati.

2. L'ARCHITETTURA DEL NASO ELETTRONICO

L'architettura dei nasi elettronici deriva dalla struttura del sistema olfattivo dei mammiferi, e può essere suddivisa in tre diversi componenti: il sistema di rilevazione dei gas, il sistema di elaborazione dei segnali provenienti dai sensori e il sistema di identificazione/riconoscimento degli odori [2, 4, 11]. Questi tre componenti con differenti funzionalità sono connessi in cascata. In un tipico naso elettronico il sistema di rilevazione dei gas è composto da un sistema di campionamento chimico e da una matrice di sensori, normalmente caratterizzati da una scarsa selettività, cioè sensibili a una vasta gamma di composti chimici. La matrice di sensori è costituita da un insieme di sensori con caratteristiche diverse, in modo che l'insieme delle loro rispo-

ste rappresenti un *pattern* caratteristico per ciascuna miscela chimica.
In genere, la matrice di sensori è alloggiata in una camera di misura realizzata con un materiale chimicamente inerte (PVC, vetro o acciaio inossidabile), in cui fluisce un gas di riferimento (per esempio aria sintetica o azoto). Il gas di riferimento viene utilizzato per stabilire una linea base per la risposta dei sensori. Per effettuare la misura vera e propria il sistema di campionamento chimico provvede a iniettare, in condizioni controllate, l'odorante nella camera di misura, producendo una variazione quasi istantanea dell'atmosfera chimica e, dunque, un transitorio della risposta dei sensori.
La condizione di regime viene raggiunta in un tempo che varia, nei sistemi utilizzati in pratica, da pochi secondi fino ad alcuni minuti, a seconda della tipologia dei sensori, delle condizioni operative e dell'odorante sotto esame. La misura si conclude iniettando nuovamente nella camera il gas di riferimento, ripulendo, così, il materiale attivo che costituisce i sensori e riportando la loro risposta alla linea base.
Il sistema di elaborazione provvede, dapprima, alla pre-elaborazione delle risposte dei sensori, che consiste nella riduzione delle derive, attraverso opportune tecniche di compensazione, e nella normalizzazione dei dati. Successivamente, esegue la compressione dell'informazione attraverso l'estrazione di alcuni parametri caratteristici (*feature extraction*) e l'eliminazione delle informazioni ridondanti.
Il sistema di riconoscimento degli odori non è altro che un classificatore implementato, in genere, con una rete neurale. Durante la fase di apprendimento, il classificatore neurale impara a distinguere i pattern rappresentativi delle miscele di interesse utilizzando gli esempi contenuti in un *data base*. Un tipico classificatore neurale consiste in due o più strati di neuroni. Le uscite dei neuroni appartenenti a uno strato sono connesse con gli ingressi dei neuroni dello strato successivo. Durante l'addestramento la rete adatta i pesi sinaptici (coefficienti moltiplicativi associati alle connessioni) in modo da imparare quali siano i pattern caratteristici per un insieme di odoranti. Dopo l'addestramento, un pattern da classificare posto in ingresso alla rete viene propagato attraverso i diversi strati di neuroni, producendo l'assegnazione di un'etichetta e, in genere, un livello di confidenza relativo all'assegnazione. In realtà, i nasi elettronici, oltre a una classificazione di odori, possono fornire, sfruttando la medesima architettura ma strutturando in maniera diversa la rete neurale, una stima della concentrazione di un odorante o le caratteristiche dell'odore stesso come potrebbero essere percepite da un esperto umano [5, 7, 8].
Il funzionamento di un naso elettronico ricalca, perciò, quello del sistema olfattivo umano: si basa su di una struttura fisica che prevede un numero elevato di sensori (recettori), in grado di rispondere a una vasta gamma di odoranti, su di un sistema efficiente di compressione dell'informazione (bulbo olfattivo) e, infine, su di un sistema di elaborazione sofisticato che apprende da un insieme di esempi (cervello).

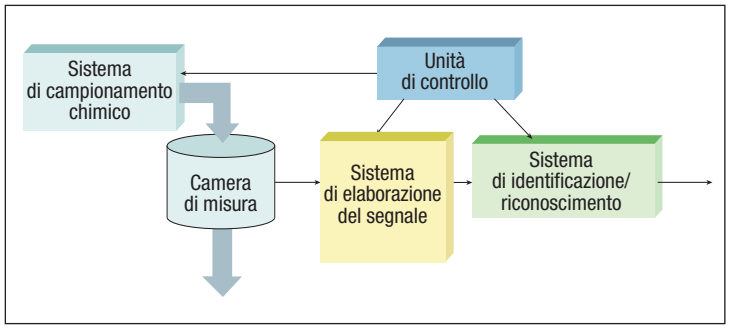


FIGURA 1
Architettura dei nasi elettronici

3. APPLICAZIONI DEI NASI ELETTRONICI

Attualmente, i nasi elettronici trovano spazio specialmente nel settore alimentare [1]. In questo ambito sono documentate applicazioni per la verifica della freschezza di alimenti nell'industria ittica (pesce, molluschi ecc.) [13], la valutazione della stagionatura dei formaggi, il controllo dell'idoneità degli imballaggi, o il controllo della cottura dei cibi. Sempre in questo settore, vengono applicati alla valutazione della qualità di birra e liquori [12]. Vengono applicati anche nelle industrie cosmetiche e farmaceutiche per il controllo dei profumi [14]. Il settore del monitoraggio ambientale e quello della medicina

rappresentano, invece, mercati emergenti per i nasi elettronici. In entrambi questi campi, vengono utilizzati per la rilevazione di specie chimiche prodotte da batteri, per esempio, per applicazioni ambientali il *cianobatterio* presente in specchi e corsi d'acqua, o nel campo medico per rivelare la presenza di *Escherichia coli* [3, 10].
Infine, un mercato che rappresenta uno sbocco economicamente molto promettente per i nasi elettronici o, più in generale, per i sistemi automatici di rilevazione di gas è rappresentato dal settore automobilistico. In questo campo, i produttori sono interessati al controllo della qualità dell'aria nell'abitacolo delle vetture e al controllo dei gas di scarico. Questa applicazione che pure rivestirebbe una particolare importanza resta ancora oggetto di ricerca: infatti, i nasi elettronici attualmente disponibili sono troppo ingombranti e costosi per il mercato di massa. La soluzione a questi problemi è offerta dalla miniaturizzazione dei sistemi attuali, che implica la realizzazione di sensori intelligenti, cioè di microsensori integrati realizzati sullo stesso *chip* che contiene il sistema elettronico di elaborazione. Questo tipo di soluzione consente di aumentare la riproducibilità dei sensori e diminuire sensibilmente i costi. È proprio in questo ambito che negli ultimi tempi si sono concentrati gli sforzi di numerosi gruppi di ricerca, uno dei cui scopi è lo sviluppo di tecnologie realizzative per i sensori che siano compatibili con le tecnologie standard dei circuiti integrati come, per esempio, la tecnologia CMOS (C*omplementary Metal Oxide Semiconductor*).

4. NASI ELETTRONICI COMMERCIALI

La maggior parte dei nasi elettronici presenti attualmente sul mercato sono prodotti nati dai risultati ottenuti nell'ambito della ricerca universitaria (per esempio, l'Alpha MOS delle Università di Warwick e Southampton).
I nasi elettronici commerciali si differenziano, essenzialmente, per le diverse soluzioni tecnologiche utilizzate per la realizzazione dei sensori.
Il costo di questi strumenti commerciali è ancora molto elevato, con prezzi che variano dalle decine alle centinaia di migliaia di euro e sono, in genere, strumenti di uso generale. Inoltre, sono per lo più strumenti con ingombro notevole e potenza dissipata elevata, pensati per l'utilizzo in laboratorio in condizioni ambientali controllate. Recentemente, tuttavia, la Cyrano Sciences ha sviluppato un naso elettronico palmare (Cyrano A320) basato su sensori polimerici conduttivi a costo contenuto (circa 12.000 €). Questo è il primo strumento portatile pensato per applicazioni sul campo.

5. I SENSORI UTILIZZATI NEI NASI ELETTRONICI

Come è stato sottolineato fin qui più volte, l'elemento chiave di un naso elettronico è costituito dalla matrice di sensori. Ci sono varie possibili scelte per la realizzazione dei sensori. In particolare, tra i più utilizzati si distinguono sensori a variazione di conducibilità, piezoelettrici, e MOSFET (*Metal Oxide Semiconductor Field Effect Transistor*). Tra questi i sensori a ossido di stagno (SnO_2), un particolare tipo di sensori a variazione di conducibilità, sono certamente i più utilizzati e studiati, e verranno perciò descritti in questo paragrafo con maggior dettaglio degli altri. Il meccanismo di funzionamento di questi sensori non è stato ancora del tutto chiarito e modellato. La possibilità di utilizzare l'SnO_2 come sensore di gas fu dimostrata nei primi anni Sessanta. Da allora, i sensori a ossido di stagno sono stati prodotti e utilizzati per la rilevazione di gas combustibili, di monossido di carbonio, vapore acqueo, ammoniaca ecc.. Il principio su cui si basano è una variazione della conducibilità dell'ossido in presenza di odoranti rispetto al valore assunto dalla conducibilità stessa in condizioni di riferimento. La variazione è dovuta a una reazione irreversibile tra l'odorante e specie di ossigeno adsorbite sulla superficie del semiconduttore come O^-, O_2^-, e O^{2-}. La specie più reattiva è O^-, che si forma quando l'ossigeno viene adsorbito, legandosi alle vacanze del semiconduttore secondo la seguente equazione:

$$\tfrac{1}{2}\, O_2 + e^- \rightarrow O^- \text{ (adsorbito)}$$

Nei semiconduttori di tipo *n*, l'adsorbimento degli ioni O^- crea una regione di carica spaziale sulla superficie dei grani di SnO_2 e una barriera di potenziale sui bordi di grano che si oppone alla conduzione (Figura 2). Lo spessore della regione di carica spaziale dipende dalla concentrazione di ossigeno adsorbita, che dipende a sua volta dalla concentrazione di ossigeno nel gas in cui è posto il sensore. Perciò, quando il sensore è immerso nell'aria la concentrazione di ossigeno è elevata e il materiale è caratterizzato da una resistenza elevata. D'altra parte, quando il sensore viene esposto a un gas X riducente, questo reagisce con le specie di ossigeno adsorbite O_m^- come segue:

$$X + O_m^- \rightarrow XO_m + e^-$$

Questa reazione brucia ossigeno e libera gli elettroni che si trovavano legati agli ioni di ossigeno, abbassando la resistenza del sensore. Viceversa, se il sensore è esposto a un gas ossidante come il biossido di azoto (NO_2) la resistenza aumenta poiché il gas viene adsorbito sotto forma di ioni negativi sulla superficie del semiconduttore.
La variazione della resistenza è perciò dovuta all'adsorbimento del gas ossidante, nell'ipotesi, però, che la quantità di ossigeno adsorbito resti costante [2].
Sono stati proposti molti approcci per modificare la selettività e la sensibilità dei sensori a ossido di stagno. Un metodo largamente utilizzato consiste nel drogare con metalli nobili il *film* semiconduttore, ottenendo una variazione della sensibilità verso alcuni gas. I metalli hanno, infatti, una funzione catalitica verso alcuni gas e l'aggiunta di metalli modifica la formazione della regione di carica spaziale. I metalli che hanno lavoro di estrazione maggiore dell'affinità elettronica del semiconduttore si legano con gli elettroni in banda di conduzione producendo un innalzamento della resistenza del sensore. L'ossigeno viene adsorbito sia dal metallo che dall'ossido di stagno e, quando viene rilasciato da entrambe le superfici per effetto dell'interazione con un gas, si ottiene una più elevata variazione della resistenza dell'ossido e, dunque, una risposta maggiore. I metalli utilizzati come droganti sono, tipicamente, il platino (Pt) e il palladio (Pd), ma sono stati utilizzati anche l'alluminio (Al) e l'oro (Au). È stato dimostrato che il Pt e il Pd aumentano la sensibilità verso composti organici volatili ossigenati rispetto alla sensibilità verso composti aromatici e alifatici.
Un'altra tecnica per modificare la risposta dei sensori a ossido di stagno si basa sul controllo e la variazione della temperatura di lavoro del film attivo. Questi sensori vengono utilizzati a elevata temperatura (in genere superiore a 300 °C) e ciò produce un sensibile miglioramento della loro risposta sia in termini di prontezza che di sensibilità. Ciascuna specie chimica ha una diversa temperatura ottimale di ossidazione e questo giustifica, anche intuitivamente, come al variare della temperatura operativa

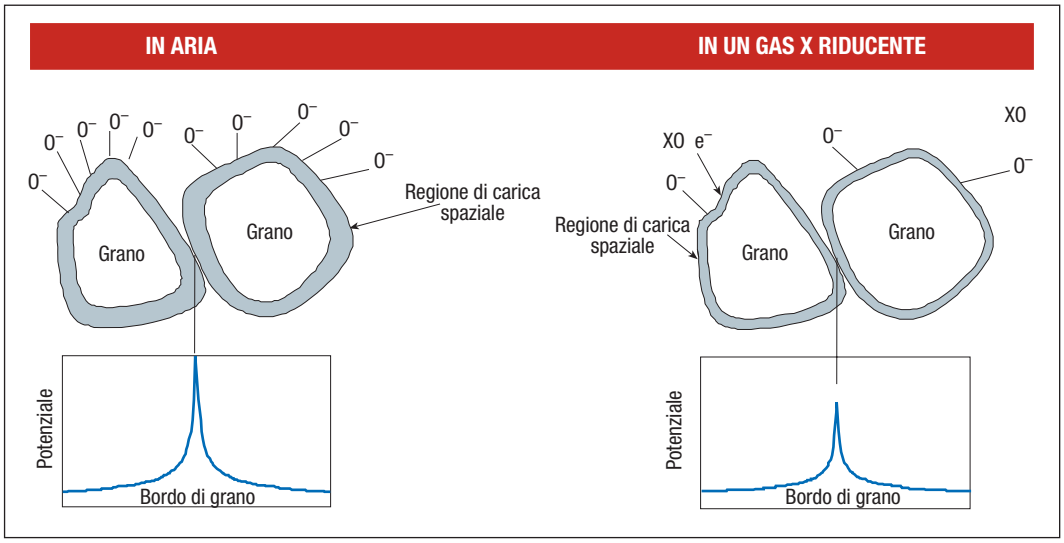


FIGURA 2
Barriera di potenziale sui bordi di grano in aria (figura a sinistra) e in un gas riducente (figura a destra)

possano essere modificate sia la sensibilità che la selettività del sensore. L'elevata temperatura facilita, inoltre, la liberazione (desorbimento) degli ioni OH^-, rendendo i sensori meno sensibili alla presenza di vapor acqueo.
Tra i sensori chimici a variazione di conducibilità vanno ricordati anche quelli basati su polimeri conduttori, che operano normalmente a temperatura ambiente. Il ricorso a processi di polimerizzazione diversi consente di ottenere una vasta tipologia di sensori e, quindi, di specializzare la risposta nei confronti di specifiche classi di odoranti. In analogia ai sensori a ossido di metallo, i polimeri conduttori presentano una spiccata sensibilità alle variazioni di umidità e una deriva temporale sensibile. In aggiunta a ciò, minori sensibilità e costanti di tempo maggiori rispetto al caso degli ossidi di metallo rendono meno efficiente e più lento il processo di misura.
Nei nasi elettronici vengono impiegati anche sensori piezoelettrici: tra i più utilizzati si possono considerare le microbilance al quarzo (*Quartz Crystal Microbalance*, QCM) e i sensori a onda acustica superficiale (SAW). Nei nasi elettronici i QCM vengono utilizzati come sensori a variazione di massa [6]. Un QCM è costituito da un disco di quarzo metallizzato sulle due superfici, con frequenze di risonanza tipiche dal MHz alle decine di MHz. Su una superficie del quarzo viene deposto un strato sottile di materiale sensibile, in genere di tipo polimerico. Il polimero tende ad assorbire alcuni gas in presenza dei quali la massa del sensore cambia causando una variazione della frequenza di oscillazione del quarzo (Figura 3).
I sensori a onda acustica superficiale SAW (*Surface Acoustic Wave*) sono costituiti da un substrato di materiale piezoelettrico, da due coppie di elettrodi a pettine e da uno strato di materiale attivo deposto sul substrato nella zona che separa le due coppie di elettrodi. Una delle coppie di elettrodi è utilizzata per eccitare un'onda acustica superficiale di Rayleigh, l'altra rivela l'onda acustica che si è propagata attraverso il materiale attivo. Il ritardo di fase del segnale ricevuto rispetto al segnale trasmesso dipende dalla velocità di propagazione sulla superficie del sensore ed è, pertanto, influenzata dall'adsorbimento del gas sul materiale attivo. Un tipico sensore SAW opera a frequenze dell'ordine delle centinaia di MHz. I SAW possono essere realizzati utilizzando le tecniche fotolitografiche della microelettronica, e sono, quindi, poco costosi. I rivestimenti attivi polimerici utilizzati per realizzare sensori SAW sono gli stessi che si impiegano nella realizzazione dei QCM. La sensibilità di questi sensori è, in genere, più elevata rispetto a quella dei QCM, d'altra parte l'elettronica di *front-end* risulta, in genere, più complessa.
L'ultima tipologia di sensori utilizzati nei nasi elettronici presa in esame in questo lavoro è quella dei MOSFET. I MOSFET hanno il vantaggio di poter essere interamente realizzati utilizzando la tecnologia dei circuiti integrati. La struttura di un sensore chimico di tipo MOSFET (Figura 4) ricalca la struttura di un normale transistor MOS, nel quale l'elettrodo di *gate* sia ricoperto da un

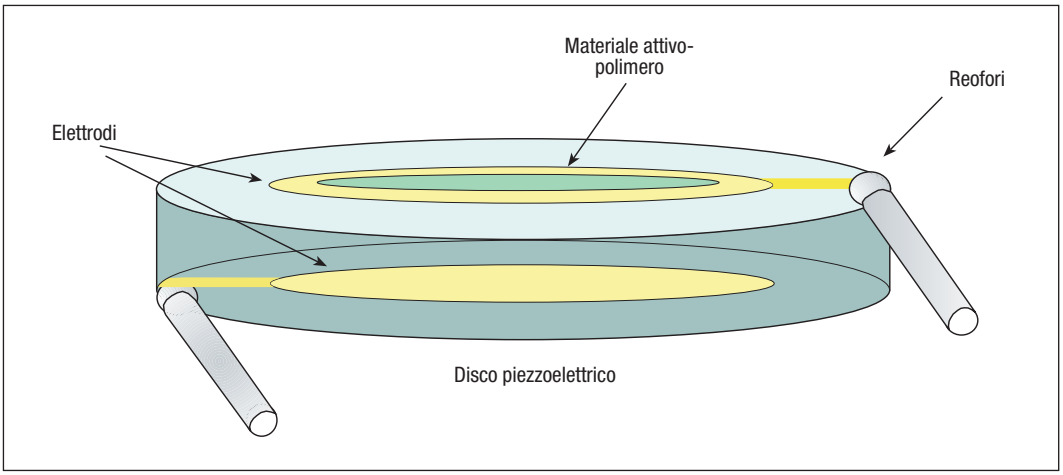


FIGURA 3
Tipica microbilancia al quarzo

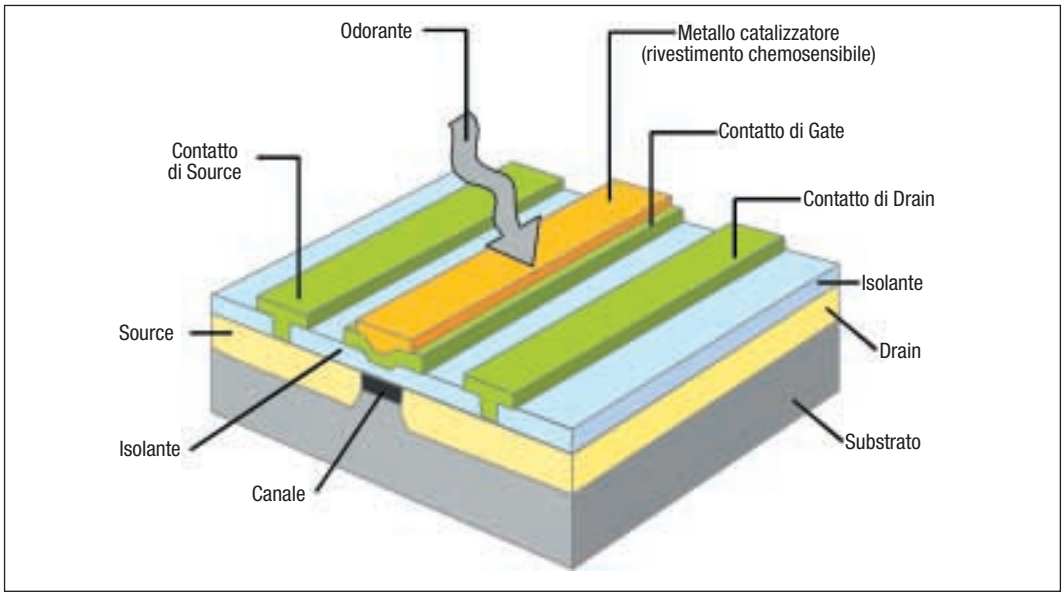


FIGURA 4
Tipica struttura MOSFET

metallo catalizzatore (per esempio, Pt o Pd). Il principio di rivelazione si basa sulla variazione della conducibilità del canale del transistor provocata dalle reazioni chimiche che avvengono sullo strato attivo, che modificano la carica del gate. L'ottimizzazione della sensibilità e selettività dei dispositivi può essere ottenuta variando natura e spessore del rivestimento catalizzatore del gate o la temperatura di funzionamento. Analogamente ai sensori chimici a variazione di conducibilità, i sensori di tipo MOSFET presentano derive delle caratteristiche nel medio periodo.

6. IL FUTURO DEI NASI ELETTRONICI

Un aspetto significativo e interessante che riguarda gli sviluppi futuri dei nasi elettronici, ma più in generale di tutti i sistemi complessi basati su sensori, è la recente tendenza alla standardizzazione dell'*hardware*, dei formati dei dati utilizzati per i risultati delle misure e dei protocolli di comunicazione tra sistemi diversi (cominciano a essere proposti e commercializzati, per esempio, sensori *plug and play* basati sullo standard IEEE1451 [9]). In questo senso anche il protocollo TCP/IP (*Transmission Control Protocol/Internet Protocol*) giocherà probabilmente un ruolo primario, e renderà possibile, tra l'altro, la realizzazione di reti di sistemi di misura, aprendo nuovi possibili scenari applicativi. In quest'ambito, la ricerca è attualmente molto attiva anche nel settore dei nasi elettronici. Se detta tendenza si concretizzerà, porterà a una nuova generazione di nasi elettronici che potranno essere utilizzati ad alto livello, senza che il generico operatore abbia una conoscenza di dettaglio degli aspetti hardware e *software* di basso livello.

Bibliografia

[1] Bartlett PN, Elliott JM, Gardner JW: Electronic noses and their application is the food industry. *Food Technology*, Vol. 51, n. 12, 1997, p. 44-48.

[2] Gardner JW, Bartlett PN: *Electronic Noses – principles and applications*. Oxford University Press, 1999.

[3] Gardner JW, Craven M, Dow C, Hines EL: The prediction of bacteria type and culture growth phase by an electronic nose with a multi-layer perceptron network. *Meas. Sci. Technology*, Vol. 9, 1998, p. 120-127.

[4] Gardner JW, Bartlett PN. A brief history of electronic noses. *Sensors and Actuators B*, Vol. 18, 1994, p. 211-220.

[5] Gutierrez-Osuna R, Nagle HT: A method for evaluating data-preprocessing techniques for odour classification with an array of gas sensors. *IEEE Transactions on Systems, Man and Cybernetics*, Vol. 29, Issue 5, Oct. 1999, p. 626-632.

[6] Hartmann J, Auge J, Hauptmann P: Using the quartz-crystal-microbalance principle for gas detection with reversible and irreversible sensors. *Sensors and Actuators B*, Vol. 18-19, 1994, p. 429-433.

[7] Hines EL, Llobet E, Gardner JW: Electronic noses: a review of signal processing techniques. *IEE Proceedings on Circuits, Devices and Systems*, Vol. 146, Issue 6, Dec. 1999, p. 297-310.

[8] Keller PE: *Overview of electronic nose algorithms*. IJCNN '99, International Joint Conference on Neural Networks, Vol. 1, 1999, p. 309-312.

[9] Licht TR: The IEEE 1451.4 Proposed Standard. *IEEE Instrumentation & Measurement Magazine*, Vol. 4, n. 1, March 2001.

[10] McEntegart CM, Penrose WR, Strathmann S, Stetter JR: Detection and discrimination of coliform bacteria with gas sensor arrays. *Sensors and Actuators B: Chemical*, Vol. 70, Issues 1-3, 1 November 2000, p. 170-176.

[11] Nagle HT, Gutierrez-Osuna R, Schiffman SS: The how and why of electronic noses. *IEEE Spectrum*, Vol. 35, n. 9, Sept. 1998, p.22-31. Publisher: IEEE, USA.

[12] Pearce TC, Gardner JW, Freil S, Bartlett PN, Blair N: Electronic nose for monitoring the flavours of beers. *Analyst*, Vol. 118, 1993, p. 371-377.

[13] Schweizer-Berberich M, Vaihinger S, Gopel W: Characterisation of food freshness with sensor arrays. *Sensors and Actuators B*, Vol. 18-19, 1994, p. 282-290.

[14] Ulmer H, Mitrovics J, Noetzel G, Weimar U, Gopel W: Odours and flavours identified with hybrid modular sensor systems. *Sensors and Actuators B*, Vol. 43, 1997, p. 413-422.

ADA FORT laureata in Ingegneria Elettronica presso l'Università di Firenze, dove ha conseguito il titolo di Dottore di Ricerca in Controlli non Distruttivi nel 1992.
È professore associato di Misure Elettriche ed Elettroniche. La sua ricerca riguarda lo sviluppo di sistemi di acquisizione e di elaborazione di segnali provenienti dai sensori.
ada@dii.unisi.it

SANTINA ROCCHI laureata in Ingegneria Elettronica presso l'Università degli Studi di Firenze. Ricercatore presso l'Università degli Studi di Firenze. Dal 1992 è Professore Associato in Elettronica presso l'Università degli Studi di Perugia. Dal 1993 entra a far parte dell'Università degli Studi di Siena dove è attualmente Professore Ordinario in Elettronica. Il suo campo di interesse è rivolto al progetto di sistemi elettronici integrati e non, basati su sensori ottici, acustici e chimici.
rocchi@dii.unisi.it

NICOLA ULIVIERI ha conseguito il Dottorato di Ricerca in Ingegneria dell'Informazione presso il Dipartimento di Ingegneria dell'Informazione dell'Università di Siena nel 2003. La sua principale attività di ricerca riguarda lo sviluppo di sistemi di riconoscimento di odori (nasi elettronici) basati su sensori ad ossido di metallo, polimerici e al quarzo.
nicola@dii.unisi.it

VALERIO VIGNOLI ha conseguito presso l'Università di Firenze la laurea in Ingegneria Elettronica nel 1989, ed il titolo di Dottore di Ricerca in 'Controlli non Distruttivi' nel 1994. Dal 1997 è Ricercatore in Elettronica presso il Dipartimento di Ingegneria dell'Informazione dell'Università di Siena. Tra i suoi interessi vi è lo sviluppo di sistemi elettronici basati su vari tipi di sensori tra cui, negli ultimi anni, i sensori chimici.
vignoli@dii.unisi.it

DSL: UNA FAMIGLIA DI SISTEMI TRASMISSIVI PER L'ACCESSO AI SERVIZI A BANDA LARGA

Andrea Bonati
Bruno Costa
Guido Vannucchi

Lo sviluppo di Internet ha prodotto una serie di servizi innovativi per le diverse fasce d'utenti che annunciano profondi cambiamenti nella società odierna. *Web*, *e-mail*, *file transfer*, stanno sempre più assumendo importanza anche a livello d'utenza residenziale, di studi di professionisti e di piccole aziende. In questo scenario le esigenze di banda per l'utente finale sono destinate a crescere in misura straordinaria: in tale ambito s'inserisce uno dei possibili metodi per potenziare le strutture d'accesso, la *famiglia dei sistemi DSL*.

3.4

1. NUOVE ESIGENZE PER LE RETI D'ACCESSO

1.1. Sviluppo di Internet

Lo sviluppo di Internet sta aprendo la strada all'introduzione di una sempre più ampia gamma di servizi innovativi per le diverse fasce d'utenti (grandi, medie e piccole imprese, uffici professionali, clienti residenziali ecc.), con la prospettiva di indurre profondi cambiamenti sia nel mondo dell'economia, sia, più in generale, nella società attuale. In particolare, le tre grandi classi di servizi offerti da Internet (*Web*, *e-mail*, *file transfer*), fondate su un'architettura di rete a pacchetto con protocollo IP (*Internet Protocol*) stanno sempre più assumendo importanza anche a livello d'utenza residenziale, di studi di professionisti e di piccole aziende.
Gli effetti in ambito sociale si prospettano rilevanti grazie alla disponibilità diffusa di nuove forme di comunicazione (e-mail, *chat line*, *videocomunicazione*, *comunità virtuali*), allo sviluppo di servizi *on line* nei più svariati settori (*servizi finanziari*, *home banking*, *rapporti con la Pubblica Amministrazione*, *acquisti in rete*, *telelavoro*, *telemedicina*, *teledidattica ecc.*), all'accesso pressoché illimitato a qualunque tipo d'informazione, al diffondersi di nuove forme d'intrattenimento (*TV a richiesta e interattiva*, *canali tematici*, *musica*, *giochi ecc.*).
La tabella 1 dà un'indicazione del numero di utilizzatori di Internet a livello mondiale e chiarisce i motivi per cui si vuole rendere disponibile a vasti strati di popolazione una rete a larga banda, compiendo un salto quantico rispetto al lunghissimo periodo di tempo durante il quale gli unici servizi offer-

Europa	191
Asia/Pacifico	187
Canada & Usa	182
America Latina	33
Africa	7
Medio Oriente	5
Totale	605

TABELLA 1
Numero utenti Internet a livello mondiale (in Milioni) (autunno 2002 Fonte: NUA)

ti a livello residenziale sono stati il telefono e il *fax* con una banda richiesta che non superava i 4 kHz del canale fonico.
In questo scenario, le esigenze di banda per l'utente finale sono destinate a crescere in misura straordinaria, richiedendo, quindi, la disponibilità di una rete per il trasferimento delle informazioni con elevatissime prestazioni. In tale ambito s'inserisce, in particolare, uno dei possibili metodi per potenziare le strutture d'accesso - la *famiglia dei sistemi DSL* (*Digital Subscriber Line*) - che sembra poter rappresentare una metodologia d'estremo interesse dal punto di vista tecnico-economico nell'ambito dei vari sistemi d'accesso che si sono sviluppati in quest'ultimi anni.

1.2. Costituzione dell'attuale rete telefonica dell'operatore dominante

Prima di procedere ad approfondire l'argomento che verrà trattato nell'articolo è utile ricordare che, per l'operatore dominante, la rete pubblica di telecomunicazioni PSTN (*Public Switched Telephone Network*) è oggi organizzata, a livello fisico, da tre domini principali:

- la **rete di trasporto** per le comunicazioni a lunga distanza costituita, in particolare, dalle grandi dorsali di comunicazione;
- la **rete di giunzione** che collega i nodi a commutazione di circuito di una ristretta area geografica, quali quelli di una città;
- la **rete d'accesso** (**o distribuzione**) verso l'utente finale, a sua volta suddivisa in *rete primaria* fino all'armadio di distribuzione e r*ete secondaria* dall'armadio di distribuzione all'utente finale.

Accanto alla rete telefonica tradizionale a commutazione di circuito operano un insieme di altre reti specializzate a copertura nazionale, e in particolare quelle per la trasmissione dati, tra cui occorre citare quelle di Telecom Italia ossia la rete *ITAPAC*, utilizzata per il trasporto dei dati a pacchetto, la *rete ATM* (denominata "Atmosfera") e la *rete professionale IP* (con evoluzione prevista della rete ATM verso questa rete IP) che sono fondamentali per la raccolta dati sulla trasmissione a lunga distanza.
Tutte queste componenti infrastrutturali della rete debbono essere potenziate per adeguarsi alle nuove esigenze, ma l'elemento più critico è senza dubbio costituito dalla rete d'accesso.
Nel presente articolo non sarà presa in considerazione, per semplicità, l'evoluzione necessaria delle reti di livello superiore, peraltro già in atto da qualche anno, ma ci si concentrerà sull'obiettivo più critico delle infrastrutture d'accesso. In particolare, tra i possibili sistemi d'accesso, la famiglia DSL - che sfrutta l'attuale *doppino* d'utente - si presenta con prestazioni e costi interessanti, tali da permettere la fruizione da parte degli utenti, con una certa universalità, di un insieme di servizi quali quelli sopra evidenziati.
Prima di entrare in maggiori dettagli su tale famiglia di sistemi sembra però opportuno chiarire le mutate esigenze di rete che nascono dalle nuove utilizzazioni.

1.3. Fattori che condizionano l'evoluzione della rete d'accesso

Quattro sono fondamentalmente gli elementi che distinguono il servizio Internet dal tradizionale servizio voce a commutazione di circuito, per il quale le reti d'accesso e di trasporto sono state progettate inizialmente. Questi fattori, infatti, comportano la necessità di impiegare nuove e più idonee soluzioni di rete.

- ***Il tipo di traffico***. Il traffico telefonico tradizionale è caratterizzato da un flusso informativo costante su circuiti *end-to-end*, precostituiti nella rete con banda prestabilita e simmetrica nei due sensi di trasmissione. Il traffico Internet è, viceversa, essenzialmente contraddistinto da un flusso informativo discontinuo, a *burst*, costituito da "pacchetti" di dati di lunghezza variabile e che si succedono a intervalli di tempo più o meno lunghi.
- ***Natura asimmetrica della comunicazione***. Le applicazioni Internet, quali il *World Wide Web*, sono fondamentalmente di natura asimmetrica, con il flusso dati *downstream* (verso l'utente) notevolmente maggiore di quello *upstream* (verso la centrale). La tradizionale rete telefonica a commutazione di circuito - che presenta caratteristiche simmetriche nelle due direzioni - non è la più adatta a trasportare tale tipo di traffico e viene utilizzata con bassa efficienza: occorre individuare soluzioni diverse di rete se si vogliono migliorare le prestazioni.
- ***La durata della connessione***. La durata di una normale chiamata fonica è mediamente dell'ordine dei tre minuti, mentre una

sessione Internet dura, in genere, almeno venti minuti, se non addirittura ore. Nel caso ancora molto frequente d'impiego di *modem* in banda fonica, il traffico Internet va a impegnare la centrale telefonica: si tende, in tal modo, a creare (a meno di provvedimenti particolari) problemi di congestione nelle centrali di commutazione tradizionali che non sono dimensionate per sostenere un traffico (*erlang*) di così lunga durata. Inoltre, la lunga durata delle sessioni Internet tende a rendere indisponibile la linea per le normali chiamate foniche, almeno per quanto riguarda l'utenza POTS (*Plain Old Telephone System*), facendo nascere l'esigenza di una seconda linea.

I requisiti di banda. L'affermarsi di Internet, come fenomeno di massa, ha portato alla creazione di pagine Web sempre più ricercate e ricche di contenuti multimediali. Sono richieste, di conseguenza, sempre maggiori disponibilità di banda alle attuali reti di telecomunicazione e, in particolare, alla rete di accesso che crea i maggiori problemi di strozzatura. Escludendo i grandi utenti affari che, in genere, hanno accessi dedicati a velocità elevate, gli altri utenti accedono generalmente a Internet tramite modem in banda fonica a 28,8; 33,6 o 56 kbit/s. Si è, quindi, in presenza di una situazione spesso frustrante per l'utente che deve attendere tempi intollerabili per accedere a una pagina Web o per scaricare un *file* tramite FTP (*File Transfer Protocol*). Anche per l'utente ISDN (*Integrated Services Digital Network*) la situazione non migliora di molto, soprattutto se si tiene conto che il contenuto multimediale d'Internet (filmati, immagini ecc.) è sicuramente destinato a crescere, mettendo ulteriormente in crisi l'attuale struttura di rete.

2. LA FAMIGLIA DSL NELL'AREA D'ACCESSO

Con l'acronimo DSL si indica una famiglia di apparati, concepita agli inizi degli anni '90 per applicazioni di VoD (*Video on Demand*), che opera con una tecnologia che consente di impiegare il "rame" esistente, trasportando su di esso il traffico numerico con velocità di cifra molto più estese di quelle fino a quel momento utilizzate. L'incremento di prestazioni non comporta alcun cambiamento delle infrastrutture (si sfrutta cioè il cablaggio esistente), ma consiste soltanto nell'introduzione di nuovi apparati presso la residenza dell'utente e in centrale.

La tipologia impiegata per il servizio consente di poter, con continuità, trasmettere dati e, conseguentemente, l'utente non deve necessariamente selezionare o attendere che il collegamento venga stabilito (*dial-up*) per iniziare la comunicazione. In altre parole, è possibile instaurare, analogamente ad altri sistemi avanzati, una connessione del tipo *always on*, senza impegnare la centrale telefonica.

Gli apparati DSL sono da considerarsi interessanti sistemi di transizione, in particolare per l'ex monopolista che governa la tradizionale rete d'accesso su coppie telefoniche. La soluzione gode, inoltre, del vantaggio di una rapida installazione, in particolare per l'operatore dominante. In effetti, anche agli altri operatori concorrenti è concesso, dagli Organi preposti alla regolamentazione, di utilizzare le coppie dell'ex monopolista secondo modalità, approfondite più avanti, che prendono il nome di *unbundling*, ma rimangono spesso per questi soggetti alcune limitazioni d'ordine pratico.

Una caratteristica fondamentale dei sistemi della famiglia DSL è, come si è già detto, la prerogativa di non richiedere scavi e/o la posa di nuovi cavi. Inoltre, dal punto di vista degli investimenti necessari alla diffusione del sistema, un altro vantaggio fondamentale deriva dal fatto che la parte d'investimenti centralizzati è alquanto limitata, mentre per la restante parte (modem in centrale e presso l'utente) la spesa risulta proporzionale alle richieste d'accesso al servizio da parte dell'utenza.

La famiglia d'apparati DSL può suddividersi in due categorie (per maggiori dettagli si veda il paragrafo 4). La prima, indicata col nome di *asimmetrica*, consente un traffico sbilanciato nei due sensi di trasmissione ed è tipicamente indirizzata all'utenza residenziale per applicazioni Internet o per distribuzione di segnali multimediali di tipo unidirezionale. Il capostipite di tale categoria di sistemi è l'apparato denominato ADSL la cui sigla significa *Asymmetrical Digital Subscriber Line*.

La seconda categoria è indicata col nome di *simmetrica* e, consentendo uguale traffico nei due sensi di trasmissione, è maggior-

mente indirizzata all'utenza *business* per uffici o piccole aziende. Il capostipite di questa famiglia è il sistema HDSL (*High data rate Digital Subscriber Line*).
Per quanto nel seguito non sia trascurata la seconda categoria, l'obiettivo del presente articolo si concentra maggiormente sull'applicazione domestica e di essa si daranno maggiori particolari sia tecnologici sia di sistema.

3. CARATTERISTICHE E CRITERI DI REALIZZAZIONE

3.1. Caratteristiche di un impianto ADSL

La figura 1 illustra il modello di riferimento dell'inserimento in rete dei sistemi ADSL.
Si può notare come il flusso digitale non transiti attraverso la centrale di commutazione, evitando così i problemi legati al tipo di traffico e alla durata della connessione sopra

NASCITA DEL SISTEMA ADSL

Nel febbraio del 1992 viene fondata a Palo Alto da John Cioffi, un dottorando dell'Università di Stanford, un'azienda denominata Amati che si propone di sviluppare sistemi ADSL su un singolo doppino, per impieghi del tipo VoD (all'epoca non era ancora diffuso il concetto di Internet) in cui il flusso nei due sensi di direzione (*uploading* per la richiesta e *downloading* per il servizio) richiede capacità digitali nettamente differenti. L'obiettivo di velocità digitale da raggiungere per il downstream (6 Mbit/s) era molto ambizioso per coprire distanze sulla rete terminale fino a 3 km. Un ulteriore requisito era quello di garantire la coesistenza sulla stessa coppia con il servizio di telefonia analogica (POTS) e anche l'ISDN.
Cioffi decise di impiegare per tale applicazione, in luogo della modulazione CAP (*Carrierless Amplitude Phase modulation*) studiata dai Laboratori Bell per il sistema HDSL appena introdotto, la modulazione *multicarrier* DMT (*Discrete Multi Tone modulation*), introdotta originariamente negli anni '80 in IBM e ripresa successivamente dallo stesso Cioffi per portarla a prestazioni d'elevato livello. La DMT è sostanzialmente un miglioramento e un raffinamento, ottenibile solo a sistemi con linea di ritorno (upstream), della modulazione OFDM introdotta molti anni prima (e non brevettata) da parte dei laboratori Bell e il cui impiego si stava estendendo a molti sistemi diffusivi digitali studiati in quegli stessi anni quali il DAB (*Digital Audio Broadcasting*) e il DVB-T (*Digital Video Broadcasting-Terrestrial*).
Le due prime società interessate alla tecnologia dell'Amati per le applicazioni sul doppino d'utente sono state una società israeliana e la Northern Telecom. L'Amati fin dall'inizio si applicò anche a studi per applicazioni differenziate quale, per esempio, la trasmissione di canali digitali audio in tecnica DAB negli interstizi della canalizzazione a radiofrequenza in modulazione di frequenza (FM), senza disturbare i canali FM analogici esistenti.
Nel 1994, viene fondato l'ADSL Forum e nel 1995 viene firmato tra Italtel e Amati un contratto di licenza per l'Italia con una serie di sperimentazioni estese sul campo da parte Italtel.
Una forte accelerazione alla società Amati e a questi processi fu data dall'inizio della diffusione di Internet che, indipendentemente dal successo o meno del *Video on Demand*, richiedeva applicazioni asimmetriche e senza l'esasperazione di capacità necessaria per segnali video di qualità.
Le tecniche proposte rappresentavano il trionfo della teoria della comunicazione permettendo di aumentare di tre ordini di grandezza la capacità iniziale di 4 kHz della coppia telefonica e consentendo di avvicinarsi ai limiti teorici indicati da Shannon per i vari tipi di canali di trasmissione.
Per concludere questo breve *excursus storico*, è interessante ricordare le ragioni del nome della società Amati cui va indubbiamente il gran merito iniziale dello sviluppo dell'ADSL e delle sue molteplici applicazioni. Il motivo è spiegato nella *brochure* iniziale della società: "*Amati, maestro di Stradivarius, ha accettato il rischio di perseguire vie non convenzionali nelle metodologie di costruzione dei violini, rompendo antiche barriere e preconcetti e raggiungendo risultati tuttora insuperati. Analogamente la tecnica multicarrier alla base della DMT, rappresenta la forma e il progetto, i moderni "signal processor" sono il legno e la colla e la società Amati è l'abile artigiano che mette insieme questi componenti: come la chiocciola del violino, tutti questi fattori sostengono le corde della migliore musica*".

menzionati. A tale scopo è necessario introdurre, lato centrale, un apparato, denominato in campo internazionale DSLAM (*Digital Subscriber Line Access Multiplexer*) e, in sede di utente, un diramatore (*Splitter*) e un terminale di rete attivo ATU-R (*ADSL Terminal Unit - Remote*).
Nella figura sono mostrate le funzioni principali dell'apparato DSLAM e del terminale di rete ATU-R. Entrambi contengono la funzione *Modem* ADSL preposto alla trasmissione dei flussi digitali ad alta velocità sul doppino telefonico. Il DSLAM provvede a multiplare i flussi provenienti dai singoli utenti, connettendosi verso la rete dati ATM "a pacchetto" a larga banda (con una *bit-rate* di 155 Mbit/s) e viceversa. Lato centrale, il modem ADSL relativo a un utente entra a far parte di una delle schede dell'apparato DSLAM, potendo una singola cartolina contenere, oggi, fino a 48 modem d'utente.
Dal lato utente, il modem ADSL (costruito da diverse aziende) ha le caratteristiche (meccaniche ed estetiche) di un apparato per uso domestico ed è connesso al computer (PC) attraverso una porta USB (*Universal Serial Bus*) o mediante una porta Ethernet (con standard *10 BaseT*), o con un'interfaccia ATM (con standard *ATMF* 25 Mbit/s), tutte interfacce che normalmente sono parte integrante del PC stesso. Si sta anche affermando una connessione di tipo radio (*Wireless LAN*, ossia lo standard IEEE 802.11b, con velocità nominale fino a 11 Mbit/s ma con velocità effettiva dell'ordine di 6 Mbit/s) molto pratica poiché non richiede l'uso di cavi, allenta il vincolo della contiguità fisica degli apparati e permette il collegamento di diversi apparati in una rete locale. Il modem ADSL, se l'utente lo desidera, può anche essere acquistato in versione a scheda per essere introdotto nel computer.
Il complesso del modem ADSL e dell'interfaccia verso il computer è l'ATU-R che si inserisce nell'ambito dell'area *Broad Band* (BB) mentre il telefono rimane confinato a quella *Narrow Band* (NB).
Come mostrato nella figura 2, che riporta maggiori dettagli, l'infrastruttura della rete in rame rimane totalmente inalterata quando si realizza una connessione ADSL.
Ogni sede di utente è collegata allo Stadio di Linea SL attraverso una coppia in rame che costituisce il *rilegamento* d'utente (SLL, *Subscriber Local Loop*). La rete d'accesso (o di distribuzione) si estende fra il permutatore urbano, posto all'interno del sito sede di SL, e la borchia d'utente posta presso la residenza dell'abbonato.
La borchia è il confine tra la rete pubblica di responsabilità dell'operatore e quella privata (o d'abbonato) di pertinenza dell'utente.
È importante notare che la rete d'accesso attuale ha già una topologia a *stella* che si adatta particolarmente alle applicazioni mul-

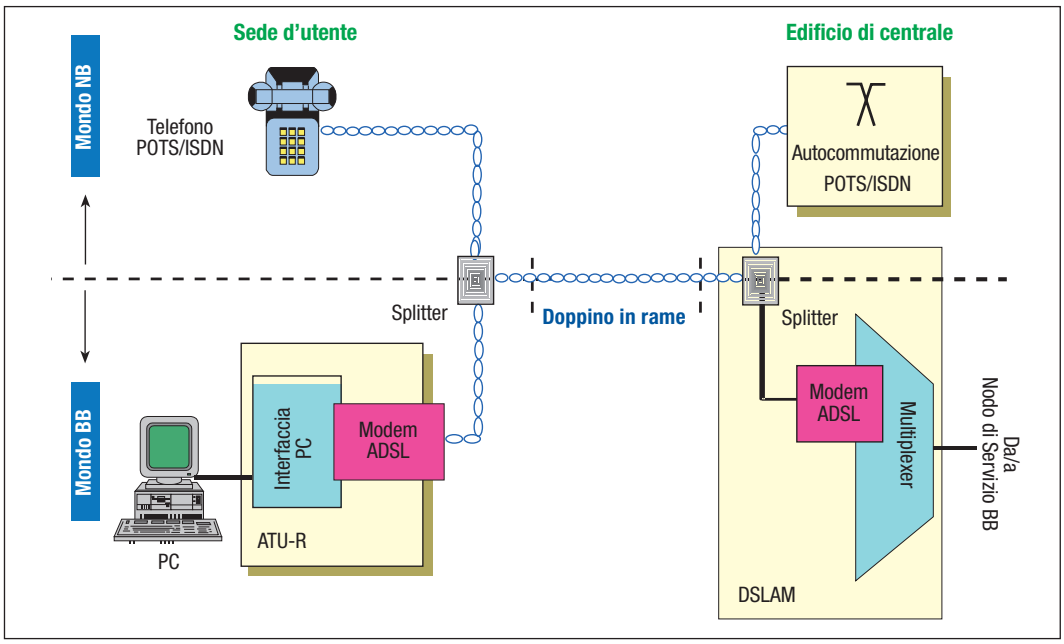


FIGURA 1
Schema di principio della connessione ADSL (NB =Narrow Band; BB = Broad Band)

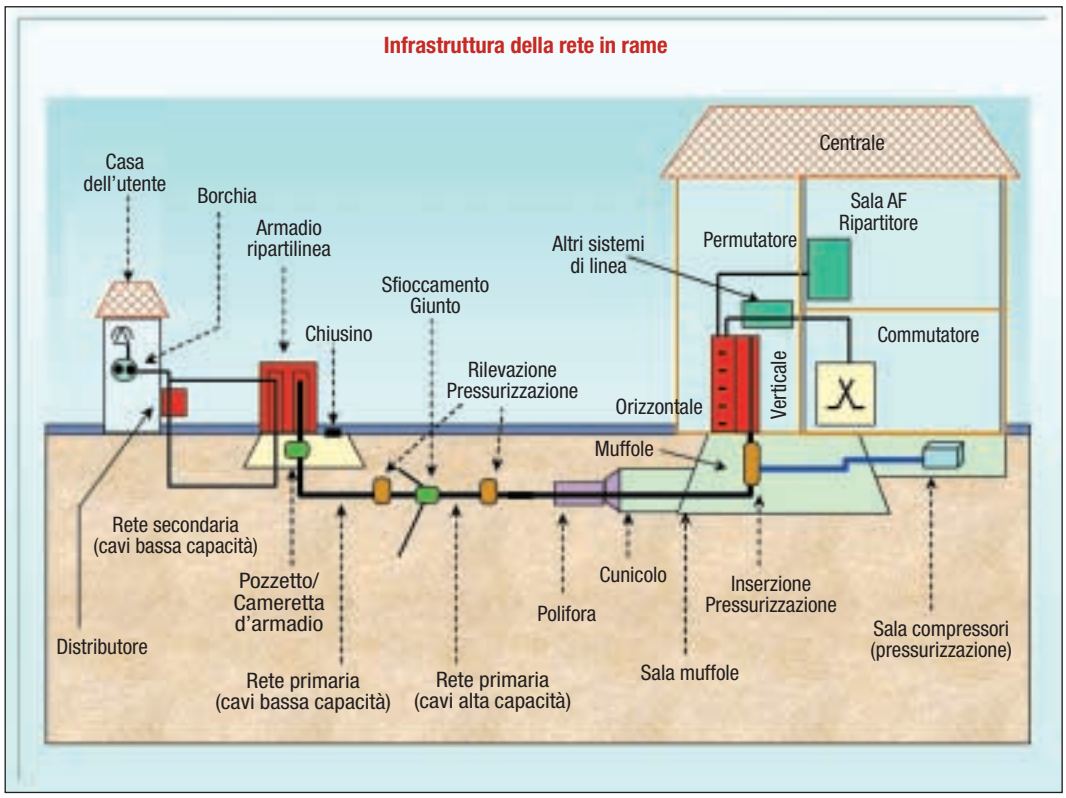


FIGURA 2
Infrastruttura della rete in coppie di rame

timediali interattive. L'area di centrale tipicamente copre una superficie geografica con un raggio, in genere nei maggiori centri urbani, di circa 2 km d'ampiezza, e si sviluppa secondo alcune direttrici dette "area-cavo".
Ogni area-cavo è suddivisa in tratte di cavo a differente potenzialità di coppie (2400, 1200, 800, 400, 100, 50) che diminuisce con la densità della popolazione nell'area servita e con la distanza dalla centrale. In ogni area-cavo è tipicamente presente un armadio di distribuzione (*ripartilinea*) che separa la rete primaria (lato centrale) da quella secondaria (lato utente).
La rete di Telecom Italia dispone di oltre 45 milioni di doppini per una lunghezza di 100 milioni di km. Un elemento particolarmente favorevole in Italia, come si vedrà poco più avanti, è la ridotta *lunghezza media* (1,5 km) dei rilegamenti di utente, oltre che la buona qualità e la relativa giovinezza dei cavi impiegati, fattori che predispongono a un uso ottimale delle tecnologie DSL in Italia. In più, a partire dal finire degli anni '80, Telecom Italia ha posato cavi a coppie con caratteristiche di diafonia sensibilmente migliori rispetto ai precedenti e, quindi, idonei alla trasmissione di segnali in alta frequenza con ridotta interferenza tra coppie adiacenti.

3.2. Caratteristiche tecnologiche e di banda del modem ADSL

Il sistema ADSL è diventato negli anni '90 uno standard *de iure*. La base di tutti le varie versioni di standard che interessano la famiglia è l'*ANSI.413* sul quale si basa lo standard più specifico *ITU.DMT*. Le caratteristiche di maggior rilievo sono descritte qui di seguito.
Tipo di modulazione. La sofisticata tecnica di modulazione impiegata nel sistema ADSL, denominata DMT (*Discrete Multi Tone modulation*), si è ormai universalmente affermata, dopo essere stata in competizione con la modulazione CAP (*Carrierless Amplitude Phase modulation*) proposta dai Laboratori Bell.
Il tipo di modulazione DMT è diventato lo standard per i sistemi ADSL e la relativa tecnica impiegata equivale - dopo avere operato una trasformazione del segnale seriale in un flusso di segnali paralleli - a modulare un elevato numero di portanti (denominate anche "toni" nel caso ADSL), allocate nella banda utilizzabile del portante. Il numero di toni complessivi di un ADSL, distanziati di 4,3 kHz,

è di 255 allocati tra la funzione di upstream (dall'utente verso la centrale) e quella di downstream (dalla centrale verso l'utente). Il metodo si adatta molto bene a tipi di sistemi trasmissivi (quali le coppie) con caratteristiche di rapporto segnale-disturbo discontinue sulla banda di linea occupata dal sistema ADSL, permettendo di individuare i toni più disturbati ed, eventualmente, eliminarli nel caso di una qualità troppo scadente (Figura 3). La modulazione si presenta, di conseguenza, con caratteristiche di grande flessibilità ma anche di robustezza ai disturbi.

Flusso digitale trasmesso. La massima velocità di upstream è fissata in 640 kbit/s e quella di downstream in 8 Mbit/s. L'effettivo bit-rate raggiungibile dipende dalla distanza, dalla qualità del doppino e dai disturbi presenti sullo specifico percorso.

Allocazione in banda. Il sistema ADSL, come già detto, si propone di non disturbare il segnale fonico tradizionale (POTS) e i segnali ISDN nel caso quest'ultimi siano presenti sulla stessa coppia o su altre coppie dello stesso cavo. Il flusso digitale trasmesso è asimmetrico e, per i due sensi di trasmissione, è allocato in bande separate di frequenza, cosi come illustrato nella figura 4. L'allocazione in banda è, pertanto, prevista con due varianti dello standard: iniziando lo sfruttamento della banda al disopra del canale fonico (a partire da 32 kHz) o, eventualmente, al disopra del canale ISDN (iniziando, in questo caso, a partire da 271 kHz ma mantenendo fissa la massima frequenza di utilizzo di 1100 kHz). In quest'ultimo caso si limita, di conseguenza, la banda di downstream con una leggera perdita di prestazioni.

Trasporto dei dati. Il trasporto dei dati è previsto possa essere fatto in modalità asincrona ATM (*Asynchronous Transfer Mode*) oppure in modalità sincrona. L'impiego dei sistemi ATM è quello che offre più vantaggi in termini di flessibilità nell'allocazione della banda disponibile ai vari servizi.

Lunghezze delle tratte da servire. Le potenzialità del sistema ADSL dipendono dalle lunghezze tipiche del cosiddetto "ultimo miglio" e cioè dalla distanza della centrale terminale dalla residenza dell'utente. Al crescere della distanza aumenta la criticità di pianificazione del sistema sia agli effetti della massima banda che il sistema è in grado di portare sia per il numero di sistemi ADSL diversi che possono coesistere sullo stesso cavo.

La risposta all'interrogativo sul massimo numero di sistemi DSL che è possibile far coesistere su uno stesso cavo apre una problematica complessa poiché i problemi ingenerati da fenomeni di interferenza risultano difficilmente inquadrabili in termini teorici. Per di più si pongono questioni di coesistenza anche con altri tipi di sistemi trasmissivi eventualmente presenti sullo stesso cavo dei quali alcuni sono più pericolosi di altri. Semplificando molto e in termini assai grossolani, si può affermare che ci si porta vicino a una situazione critica quando il riempimento di un cavo con sistemi ADSL si avvicina al

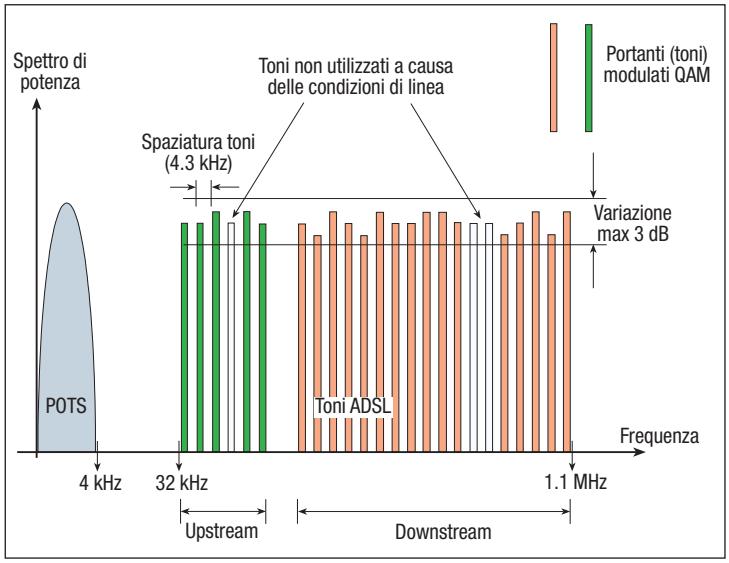


FIGURA 3

Spettro del segnale in linea di un modem ADSL con modulazione DMT

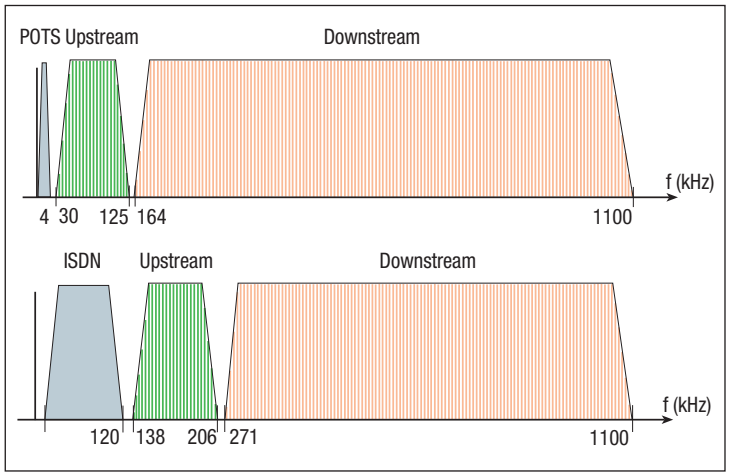


FIGURA 4

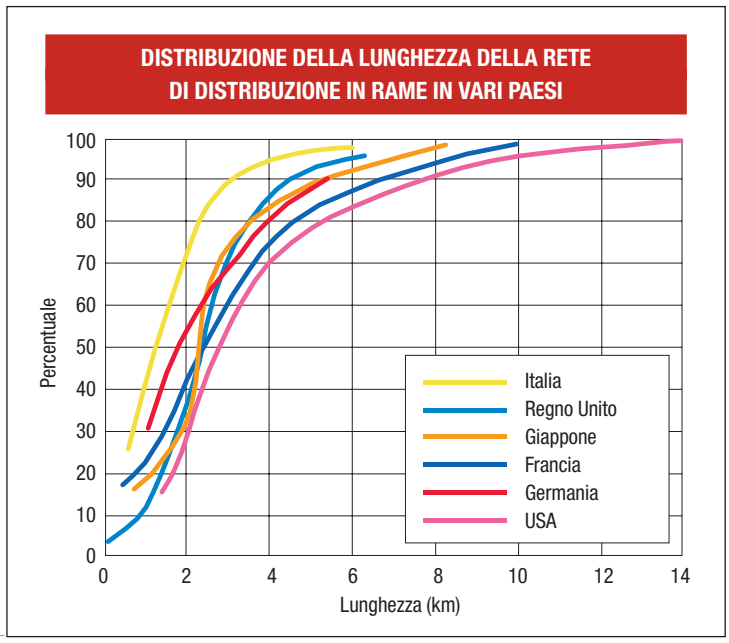
Spettro del segnale del Modem ADSL con POTS o ISDN

50%. Va anche detto, peraltro, che tale percentuale mediamente sulla rete italiana viene a corrispondere al numero di coppie di un cavo che è percorso da correnti foniche. Tuttavia, poiché il grado di riempimento dei cavi non è uniforme, non sarà in generale possibile raggiungere tutte le abitazioni o, se lo si vorrà fare, occorrerà fornire il servizio a velocità più ridotta. Questa tematica potrà, pertanto, costituire il limite per la densità di penetrazione di sistemi ADSL: per superare tale confine si renderà inevitabile, a suo tempo, il ricorso alla trasmissione ottica.
La figura 5 mostra la lunghezza tipica del rilegamento d'utente di diversi Paesi rispetto alla rete italiana. Da essa si vede che il nostro paese ha caratteristiche particolarmente favorevoli all'applicazione di tali sistemi, per la ridotta lunghezza di tratta dei doppini che collegano gli utenti alla centrale più vicina. La distanza media è, infatti, di 1,5 km per un totale complessivo di oltre 100 milioni di km (e per il 90% delle tratte rimane entro i 3 km), il che consente connessioni ADSL con alte prestazioni per una gran parte dei potenziali utilizzatori.

FIGURA 5
Distribuzione della lunghezza del doppino nel rilegamento d'utente

3.3. I sistemi ADSL leggeri

Si può osservare che la *velocità di cifra* caratteristica dello standard ADSL, sia nella variante POTS sia in quella ISDN, è comunque elevata. Questa rilevazione si spiega ricordando che la tecnologia ADSL nasce attorno al 1992



con l'intento di fornire agli utenti il *servizio VoD* per il quale le esigenze di banda (più corretto sarebbe dire di bit-rate) erano considerevoli. Il VoD sul televisore domestico non si è, tuttavia, dimostrato un servizio trainante per l'ADSL, non essendo competitivo con l'affitto di videocassette. Con il crescere degli utenti e del traffico di Internet, sia con i modem in banda fonica che su ISDN, si comincia a prendere atto, attorno al 1995, che la banda sul rilegamento d'utente costituisce potenzialmente una strozzatura della rete e l'ADSL diviene, di conseguenza, un sistema di accesso estremamente interessante ed economico.
Si comprese anche, all'epoca, che l'ADSL, per diventare una tecnologia d'accesso universale per una diffusione di massa di applicazioni Internet, non doveva necessariamente fare i conti con le pesanti specifiche dovute alle sue origini e che si possono fondamentalmente così riassumere:

- ***i modem sono più costosi del necessario*** essendo progettati per 8 Mbit/s: inoltre, se non si vogliono discriminare gli utenti, è bene dare a tutti una banda garantita, anche se inferiore, in ogni condizione d'impianto e, in particolare, per lunghezze massime della rete d'accesso;
- ***l'installazione per la velocità massima è delicata*** e richiede l'intervento del personale dell'operatore telefonico, al contrario di quanto avviene per i modem in banda fonica: è, infatti, necessario inserire un diramatore prima della borchia d'ingresso (che costituisce il limite del campo di competenza dell'operatore telefonico) e da esso stendere un nuovo doppino fino al modem ADSL.

Per superare questi problemi, nel caso delle applicazioni in cui non si richiedono elevate prestazioni di banda, e per accelerare l'introduzione sul mercato di questi sistemi, è nato uno standard che si affianca a quello visto sopra indicato, il cosiddetto UADSL (*Universal ADSL*) o ADSL-Lite o G.Lite, focalizzato sul servizio *Fast Internet* per l'utenza residenziale e caratterizzato fondamentalmente da:

- ***riduzione della velocità di cifra downstream*** a 1,5 Mbit/s eliminando tutti i toni sopra i 552 kHz;
- ***autoinstallazione*** da parte dell'utente grazie all'eliminazione del diramatore d'ingresso e alla possibilità di collegare il modem

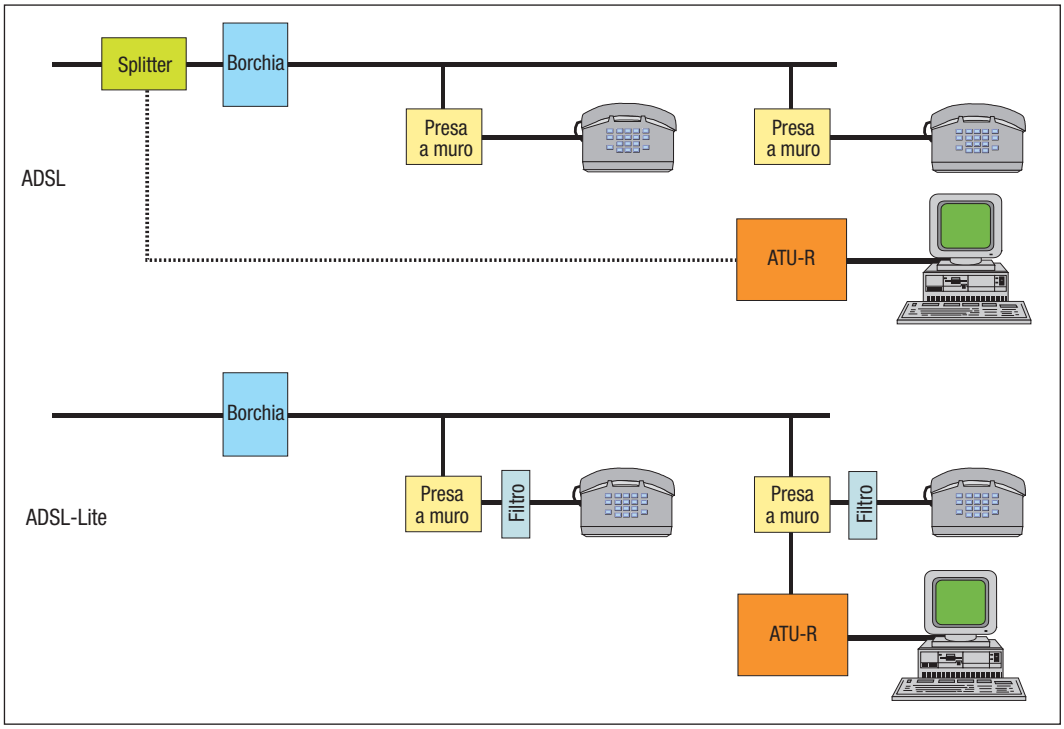


FIGURA 6
Cablaggio domestico per ADSL e ADSL- Lite

ADSL a una qualsiasi presa telefonica. Generalmente, è richiesto l'inserimento di piccolissimi filtri (*passa-basso antidisturbo*) tra le prese e gli apparecchi telefonici come mostrato in figura 6.
La soluzione ADSL standard rimane comunque interessante laddove le esigenze di banda siano superiori a quelle che l'ADSL-Lite è in grado di fornire. Un esempio è il caso d'utenza affari medio/piccola che prevede la connessione di più terminali all'ATU-R (reso possibile attraverso un *Ethernet Hub o un Router*). Un altro caso potrà presentarsi in futuro quando si abbia uno sviluppo di contenuti multimediali tale da richiedere un ulteriore incremento della banda da mettere a disposizione dell'utente. Va poi rilevato che l'ADSL standard è comunque l'unica scelta possibile oggi per gli utenti ISDN (soluzione peraltro non adottata in Italia ma largamente usata in Germania): infatti, l'ADSL-Lite è, dal punto di vista spettrale incompatibile con la linea ISDN.

4. CLASSIFICAZIONE DELL'INTERA FAMIGLIA DSL

Una classificazione più precisa di tutta la famiglia DSL (soluzioni asimmetriche e simmetriche) è riportata nel seguito. Poiché si è di fronte a una tecnologia in marcata evoluzione, quest'elencazione potrebbe, anche nel breve, essere superata in qualche sua parte.

4.1. Soluzioni asimmetriche

Le soluzioni asimmetriche comprendono: ADSL, G.Lite ADSL (o semplicemente, G.Lite), RADSL e VDSL. Le forme standard dell'ADSL utilizzano lo stesso tipo di modulazione: DMT e la piattaforma degli standard facilita l'interoperabilità tra le varie soluzioni.

- **ADSL** (*full rate Asymmetrical DSL*): lo standard ADSL consente di trasmettere contemporaneamente voce e dati sui doppini telefonici esistenti e offre diverse velocità sia downstream (verso l'utente) sia upstream (verso la centrale). Può essere configurata per velocità fino a 6 Mbit/s per i segnali ricevuti dall'utente. Questo tipo di DSL è quello ora più diffuso a livello mondiale sia presso l'utenza privata sia presso quella affari. La Raccomandazione G 992.1 e lo Standard ANSI T1.413-1998 specificano il "*full rate*" ADSL.
- **G.Lite ADSL** (o semplicemente G.Lite): lo standard G.Lite è stato sviluppato specificamente per soddisfare il requisito di facilitare l'installazione *plug-and-play* del segmento

residenziale del mercato. G.Lite consente velocità fino a 1,5 Mbit/s verso l'utente. Lo standard ITU a esso relativo è il G. 992.2.

- **RADSL** (*Rate Adaptive DSL*: è una versione non standardizzata di DSL). Va notato che anche l'ADSL standard consente di adattare la velocità di trasmissione alle condizioni di linea.
- **VDSL** (*Very high bit rate DSL*): fino a qualche decina di Mbit/s su doppino per brevi distanze. È il caso delle terminazioni del *Fibre To The curb* verso l'utente finale. Il sistema VDSL è particolarmente utile all'interno di *campus* e può essere configurato in modo simmetrico.

4.2. Soluzioni simmetriche

Le soluzioni simmetriche comprendono: HDSL, HDSL-2, SDSL e SHDSL. L'uguaglianza delle velocità di trasmissione per i due sensi di propagazione rende il *Symmetrical DSL* particolarmente utile per le LAN (*Local Area Network*).

- **HDSL** (*High date rate DSL*): questa varietà creata sul finire degli anni '80 porta segnali simmetrici a velocità fino 2,3 Mbit/s. È disponibile a 1,5 o a 2,3 Mbit/s. Impiega due o tre coppie ed è standardizzata in ETSI e ITU.
- **HDSL2** (*2nd generation HDSL*): rappresenta un'evoluzione dell'HDSL solo per 1,5 Mbit/s. Utilizza una sola coppia per la trasmissione bidirezionale.
- **SDSL** (*Symmetrical DSL*): è sempre una soluzione di tipo proprietaria che fornisce velocità che vanno da 128 kbit/s fino a 2,3 Mbit/s su una singola coppia. Il sistema SDSL raggruppa oggi una gran quantità di soluzioni specifiche di ogni costruttore. Si dovrebbe progressivamente attuare la convergenza verso il nuovo standard *G. SHDSL* sviluppato in *ITU* con il supporto di *T1E1.4* (*USA*) e dell'*ETSI*.
- **SHDSL** (*Symmetrical High data rate DSL*): è lo stato dell'arte delle soluzioni simmetriche conformi alla Raccomandazione ITU G. 991.2, conosciuta anche come *G.SHDSL* e approvata in *ITU-T* nel febbraio 2001. Il sistema SHDSL raggiunge prestazioni del 20% migliori in termini di lunghezza di tratta superata rispetto ai precedenti sistemi simmetrici. Genera minori diafonie e l'interoperabilità tra costruttori è facilitata dalla standardizzazione più spinta rispetto agli altri sistemi.

5. UNBUNDLING E POSIZIONAMENTO NEL BUSINESS

Risulta chiaro da quanto fin qui presentato che i sistemi DSL costituiscono la tecnologia di elezione per chi, come un operatore dominante, possiede già un'estesa infrastruttura di rete che comprende il cruciale segmento dell'accesso. Questa tecnologia permette, infatti, come si è più volte messo in luce, di utilizzare il normale doppino telefonico con cui viene già raggiunta la totalità dei clienti attuali della rete fissa ed evita, quindi, investimenti per realizzare nuove infrastrutture di accesso che rappresentano sempre la parte a costi più elevati per le reti pubbliche di telecomunicazioni. L'investimento fisso per i sistemi DSL, indipendente cioè dalle richieste di essere connessi alla rete, consiste nell'introduzione degli apparati DSLAM - equipaggiati con schede realizzate peraltro in forma modulare - ed è relativamente contenuto, oltre che graduabile, poiché, anche in quest'apparato centralizzato, è presente una componente proporzionale al numero di clienti da servire (le schede dei modem di centrale). Occorre però tenere presente che sul costo complessivo del servizio incide l'uso d'altre risorse di rete dedicate, quali, ad esempio, le connessioni numeriche ad alta velocità con i POP (*Point of Presence*) o i server d'accesso, nonché l'utilizzo delle reti dati, ATM o IP, dotate rispettivamente dei necessari apparati di commutazione ATM o, in alternativa, dei *router*.
È comprensibile, pertanto, che l'operatore dominante metta in atto una forte politica d'espansione nella diffusione dell'ADSL o, più in generale, dei sistemi DSL, perché capaci di portare ricavi aggiuntivi sia attraverso il pagamento della connessione sia mediante nuovi servizi resi possibili dalla larga banda (*video-comunicazione, TV digitale, gaming on-line* ecc.). Telecom Italia, in particolare, prevede di raggiungere nel 2004 una quota di oltre 1,5 milioni d'accessi *broadband* nel mercato residenziale e, per fine, 2005 il *target* è di oltre 3 milioni d'accessi a larga banda (residenziali, business, e affittati ad altri operatori).

È, d'altra parte, evidente qualche cautela di gestione da parte dell'operatore dominante nei settori professionali e affari che sono già serviti con collegamenti numerici ad alta velocità e con elevati livelli di qualità: la transizione verso nuove offerte è, in questi casi, opportunamente gestita, compatibilmente con la concorrenza, per essere sicuri della qualità e dell'affidabilità del servizio offerto e senza che siano gravemente compromessi i ricavi e i margini di guadagno.

Diversa è la situazione degli operatori concorrenti, gli OLO (*Other Licensed Operator*). Non partendo in generale dalla disponibilità di una propria infrastruttura d'accesso, essi per offrire agli utenti connessioni a banda larga possono ricorrere ai seguenti approcci.

❑ ***Realizzare ex-novo una propria infrastruttura d'accesso***: sono presenti in Italia esempi di questo tipo (in particolare, quello di Fastweb). In questi casi la soluzione tecnologica adottata è essenzialmente l'impiego della fibra FTTB (*Fibre To The Building*) o addirittura FTTH (*Fibre To The Home*). Le bande consentite con la fibra sono assai estese e il servizio è con altissime prestazioni potenziali, ma l'elevato costo di realizzazione rende critica la profittabilità, almeno nel breve-medio periodo. Il servizio può peraltro diffondersi solo in alcune aree cittadine che dispongono di tubazioni (*cavodotti*) e, pertanto, è oggi da considerarsi, in ogni caso, una soluzione relativamente d'*elite*.

❑ ***Affittare infrastrutture per l'accesso di altri operatori*** e, in particolare, di proprietà dell'operatore dominante.

La situazione più tipica è il cosiddetto unbundling e cioè la politica regolamentare stabilita nel 1999 dall'UE che ha definito un quadro normativo generale per l'accesso, da parte degli operatori OLO, ai rilegamenti in rame di proprietà dell'operatore dominante. A livello nazionale, le *Authority delle telecomunicazioni* procedono a definire i modelli di connessione in tale regime e a definire le corrispondenti tariffe. A quest'ultimo proposito, in Italia sono stati definiti due modelli:

a. unbundling fisico: s'intende la possibilità per un operatore alternativo (OLO) di noleggiare linee in rame di proprietà dell'operatore dominante, alle quali si collega fisicamente, posizionando propri apparati (DSLAM) nella centrale o nei siti di proprietà dell'operatore dominante. In questo caso, l'OLO eroga il servizio attraverso proprie infrastrutture in modo end-to-end. La situazione è rappresentata in figura 7;

b. unbundling logico (condivisione delle infrastrutture dell'*incumbent*). In questo caso l'OLO condivide le infrastrutture dell'operatore dominante e per esso sono disponibili due possibilità.

La prima è lo *Shared Access* (SA) e cioè il solo affitto della banda dati del doppino telefonico, che rimane di proprietà dell'*incumbent*, il quale, per suo conto, offre sulla stessa coppia i suoi servizi di telefonia. Per l'OLO gli investimenti e i costi sono analoghi al caso dell'*unbundling* fisico, ma il costo del servizio è molto inferiore essendo l'infrastruttura condivisa. Questa alternativa si adatta agli OLO che offrono servizi a larga banda e non la fonia base (abilitata, eventualmente, solo con

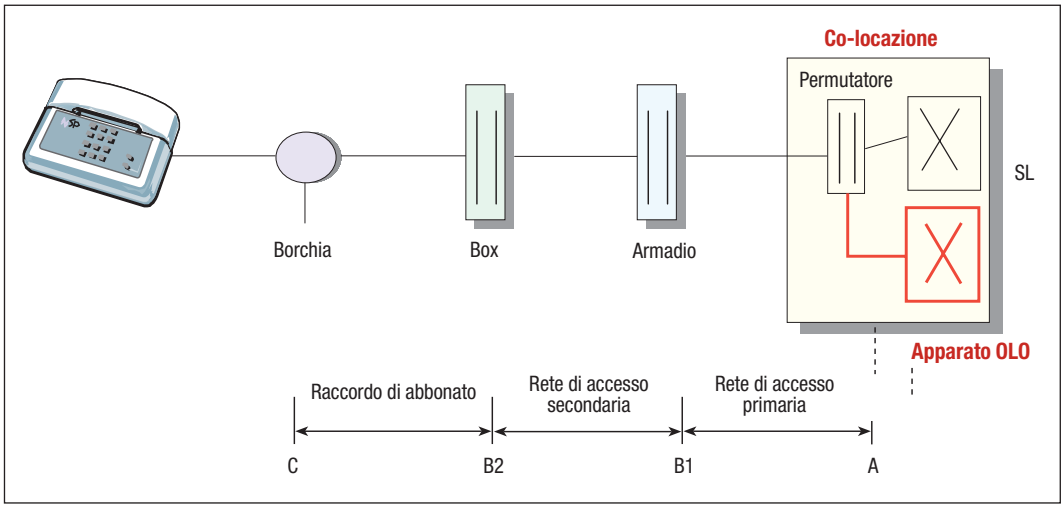


FIGURA 7
Schema di collegamento nel caso di unbundling fisico

tecnologia VoIP, *Voice over Internet Protocol*, nel flusso dati).
La seconda possibilità riguarda il servizio cosiddetto *wholesale*: in tale modello l'OLO, invece, condivide con l'*incumbent* sia l'infrastruttura di accesso sia la rete (connettività, DSLAM e rete ATM), riducendo fortemente i propri investimenti. Infatti, in questo caso, gli utenti ADSL dell'OLO di una determinata area sono raccolti dalla rete dell'incumbent, il quale consegna il traffico all'OLO in opportuni *punti di consegna* attraverso un VP (*Virtual Path*) ATM. L'offerta Telecom Italia prevede 79 aree geografiche di raccolta con 81 punti di consegna (due ciascuno per Roma e Milano). I circuiti virtuali ATM semi-permanenti che collegano gli utenti - i cosiddetti VC di classe ABR (*Available Bit Rate*) caratterizzati da una banda di picco e da una banda minima garantita - sono concentrati nei VP ATM e sono consegnati all'OLO. L'OLO può scegliere per ogni utente la velocità di linea e la banda che vuole garantire, dimensionando quindi opportunamente il VP di raccolta (sino a un massimo di mille accessi per VP). La gestione dell'utente finale rimane comunque di competenza dell'OLO, che dovrà provvedere alla fornitura del modem, micro-*filtri/splitter* e all'assistenza.
Ovviamente, la completa dipendenza dall'operatore dominante rappresenta in quest'ultimo caso una debolezza strategica dell'OLO i cui margini di manovra risultano assai ristretti.
In ambedue i casi sopra esaminati le tariffe di interconnessione dell'OLO verso l'operatore dominante vengono fissate dall'*Authority per le Comunicazioni* sulla base dei costi presentati dall'operatore dominante e verificati dall'ente regolatore.

6. LE OFFERTE COMMERCIALI DELLA FAMIGLIA DSL

6.1. Potenzialità attuale dell'offerta della famiglia DSL dal punto di vista commerciale

I servizi a larga banda sono realizzati i sistemi di accesso DSL che collegano gli utenti finali ai POP degli ISP (I*nternet Service Provider*) da cui sono erogati i servizi Internet quali posta elettronica, contenuti Web, commercio elettronico, *Web-hosting ecc.*.
L'accesso fisico DSL del cliente è realizzato sul normale doppino telefonico, ma la fruibilità effettiva del servizio dipende dalla copertura geografica della rete e dalla distanza dell'utente dalla prima centrale equipaggiata con apparati di multiplazione DSLAM (*Digital Subscriber Line Access Multiplexer*).
È quindi importante assicurare un'adeguata copertura del territorio italiano con DSLAM, installati in centrali telefoniche non distanti dagli utenti finali per assicurare una buona qualità del servizio offerto. Per esempio, i servizi ADSL di Telecom Italia sono presenti in 1115 comuni (copertura del servizio *Alice* al 18 aprile 2003), potendo così raggiungere oltre il 60% della popolazione italiana. La copertura è, comunque, prevista in continua espansione per cui è ragionevole ritenere che nel prossimo futuro i servizi ADSL saranno disponibili alla quasi totalità della popolazione italiana.
I DSLAM (ciascuno in grado di equipaggiare 4608 linee ADSL), sono collegati da una rete ATM di concentrazione tipicamente con flussi numerici a 34 e 155 Mbit/s. Gli elevati investimenti e i costi operativi conseguenti richiedono economie di scala efficienti per rendere il business sostenibile.
L'utente dispone di un modem ADSL (ATU-R) e di micro-filtri per presa telefonica o di un derivatore centralizzato, usati per separare la banda fonica tradizionale da quella per il trasporto dati. I derivatori sono necessari solo nel caso in cui siano presenti centralini, sistemi di telesorveglianza, *smart box* ecc.. Ai suddetti apparati vanno sommati i DSLAM che, nel caso dei competitori dell'operatore dominante, vengono posti in genere, come già sopra visto, nelle stesse centrali di Telecom Italia.
Il più efficace dei concorrenti di Telecom Italia è Fastweb che, nei casi in cui non ritiene conveniente installare la fibra ottica, offre ADSL realizzando, fra tutti i concorrenti, oltre il 50% del totale delle richieste degli OLO a Telecom Italia. Vale la pena ricordare che Fastweb offre connessioni ADSL ai propri clienti al massimo delle caratteristiche tecniche (4-6 Mbit/s) per essere in grado di riproporre agli utenti la maggior parte dei servizi già forniti con la fibra (VoD, *videocomunicazione ecc.*).

6.2. Segmentazione dei clienti nell'offerta DSL

Dal punto di vista dell'offerta commerciale possono essere distinti diversi casi, sia dal lato del tipo di offerta sia da quello del segmento di clientela considerato.
In particolare si può distinguere:

❑ ***offerta al dettaglio*** (*retail*): essa è tipica, oltre che dell'operatore dominante, degli ISP e degli OLO in quanto rivolta all'utente finale. Si articola sia nella connessione ADSL al POP degli ISP o degli OLO, sia di servizi Web, quali caselle di posta elettronica, spazio Web, invio *SMS ecc.*. Il modem non è compreso nell'offerta base verso gli utenti residenziali, mentre sono disponibili servizi aggiuntivi a pagamento, quali la casella elettronica e i siti Web personalizzabili, il *gaming on line* ecc..

❑ ***offerta all'ingrosso*** (*wholesale*) che è tipicamente un'offerta dell'operatore dominante, rivolta ad altri operatori (OLO) o a ISP. Si compone, come già visto poco sopra, della sola connessione ATM su linea ADSL dall'utente finale sino al POP degli OLO o degli ISP (OLO e ISP possono coincidere in un'unica organizzazione). Il *Provider wholesale* (*operatore dominante*) può fornire, su richiesta degli OLO o degli ISP, anche il modem e il router nel caso, chiarito più avanti, di un servizio diretto alla raccolta di traffico da clientela business.

Dal lato del segmento di clientela conviene, invece, distinguere i clienti residenziali, quelli professionali di piccole dimensioni denominati SOHO (*Small Office Home Office*) e i clienti business:

❑ I ***clienti residenziali***: si può avere a che fare sia con utilizzatori che, in una prima fase di approccio ai servizi a larga banda, impiegano Internet per *divertimento*, *comunicazioni*, *ricerca informazioni*, essendo tipicamente più attenti al costo del servizio che alle prestazioni, sia con utilizzatori evoluti che usano in modo intensivo Internet per *scaricare grossi documenti*, *release software*, *file musicali e video* e che sono particolarmente interessati alla velocità effettivamente disponibile nel collegamento, apprezzando o criticando le caratteristiche tecniche e prestazionali del servizio.

❑ I ***clienti SOHO***: sono uffici di professionisti ovvero di piccole imprese o di attività commerciali varie che utilizzano i servizi a larga banda per motivi professionali; richiedono migliori prestazioni della prima categoria (*banda minima garantita*) e un'elevata *affidabilità* e desiderano anche *servizi aggiuntivi* (*hosting* del sito Web, sicurezza nello scambio di dati, maggiore spazio di posta elettronica ecc.) nonché un'assistenza affidabile da parte del fornitore.

❑ I ***clienti "business"*** sono, in genere, piccole e medie imprese (le grandi imprese hanno comunemente l'accesso in fibra) che tipicamente utilizzano l'accesso della famiglia DSL per *collegamenti Intranet* tra le differenti sedi; richiedono la simmetria del collegamento nelle due direzioni, elevate prestazioni e un *livello elevato d'affidabilità* e *sicurezza* dei servizi nonché una serie di servizi aggiuntivi evoluti che si elencheranno più avanti.

6.3. Tipologie d'offerte nell'ambito della famiglia ADSL

Per quanto riguarda i *contenuti* dell'offerta ADSL, i principali elementi caratterizzanti sono:

❑ ***Velocità massima di connessione a Internet***: la linea ADSL è contrassegnata da una velocità massima con servizio di carattere asimmetrico, in grado di fornire verso l'utilizzatore (downstream) e dall'utilizzatore verso la rete (upstream) rispettivamente le seguenti coppie di valori tipici: 256/128, 640/128, 1280/256 e 2048/512 kbit/s (senza alcuna garanzia che la velocità si mantenga nell'intera catena). Tipicamente, le velocità minori sono orientate alla clientela residenziale e a quella del SOHO, mentre quelle maggiori sono rivolte alla clientela business. La scelta è, tuttavia, maggiormente influenzata dalle tariffe (crescenti con la velocità) piuttosto che non dalle effettive necessità d'uso. Uno degli impieghi maggiori di Internet presso i giovani è, ad esempio, lo scambio, in configurazione *peer to peer*, di file audio e ora, sempre più, anche video che diventa ben più praticabile ed efficiente alle alte velocità anche se questa utilizzazione è limitata da un costo troppo elevato. Tutto ciò rende molto discutibile l'equazione "alta velocità per utenti affari" e "bassa velocità per utenti residenziali". L'apparente paradosso si accentua nel caso in cui, nell'immediato futuro, si diffondano sempre di più servizi video (televisivi e di vi-

deocomunicazione) che richiedono bande più estese e meglio garantite.

❑ ***Banda garantita***: in questa modalità di contratto è garantita una velocità minima anche in caso di congestione della rete erogatrice del servizio. La velocità, nel caso dell'ADSL, viene garantita, generalmente, in direzione downstream e può assumere valori che vanno da 0 kbit/s (nessuna garanzia di banda, tipicamente per clienti *residenziali*) a valori di 5 - 64 kbit/s (in genere, per clienti *SOHO*), e da 32 a 1024 kbit/s (per i clienti business).

❑ ***Indirizzo IP***: può essere dato al cliente un indirizzo IP fisso (*statico*) o assegnato quando è stabilita una nuova connessione o si abbia una variazione di rete (*dinamico*).

❑ ***Modem / Router***: il modem ADSL può essere acquistato dall'utente o preso in comodato, a fronte di un canone mensile aggiuntivo. Inoltre, per reti SOHO e business, è, in genere, consigliata l'aggiunta di un piccolo router che dà maggiori flessibilità alla rete e permette l'aggiunta di una barriera di protezione per la sicurezza (un *firewall hardware*): anche in questo caso, il router può essere acquistato dal cliente o dato in comodato d'uso.

❑ ***Servizi aggiuntivi***: nelle offerte sono compresi o richiesti a pagamento servizi aggiuntivi quali, per esempio, spazio-posta, spazio-Web, elenco d'indirizzi IP aggiuntivi, dominio-Web ecc..

A tutte le tipologie di offerta suddette corrispondono, naturalmente, diversi canoni tariffari che risultano anche dipendenti dal tipo di pagamento scelto per il traffico, così come illustrato nel sottoparagrafo seguente.

6.4. Politiche dei prezzi e offerte commerciali nell'area residenziale e SOHO

Un elemento di grande rilievo dal punto di vista del marketing è l'articolazione dei prezzi del servizio, in relazione ai diversi segmenti di mercato e alle diverse esigenze dei singoli clienti: la politica di prezzi può condizionare fortemente l'adesione degli utilizzatori e, quindi, un approccio accorto e ben differenziato può favorire grandemente la diffusione del servizio (come insegna la storia di grande successo della telefonia mobile in Italia).

Tra gli schemi tariffari oggi previsti si possono ricordare:

- ***canone mensile fisso*** (incluso l'eventuale affitto del modem e del router) per un accesso continuo e illimitato del collegamento (*always on*);
- ***canone mensile comprensivo di un numero determinato di minuti o di ore*** con una tariffazione del traffico per il tempo eccedente;
- ***canone mensile ridotto*** e tariffazione del traffico per il tempo di utilizzo;
- ***forme di "prepagato"***, che danno diritto a un certo numero di ore di collegamento. Una prima offerta di questo tipo è stata appena introdotta da Telecom Italia al momento della stesura del presente articolo.

Una sintesi delle principali offerte attuali da parte dei diversi operatori, secondo i parametri prima indicati, è riportata nella tabella 2.

La tabella 2, tenuto conto di quanto detto per la politica di unbundling, mostra che i prezzi delle offerte ADSL dei numerosi operatori verso la clientela residenziale non sono tra loro molto differenziati. La competizione in quest'ambito è, infatti, molto alta e i margini di guadagno sono ridotti.

Ancora più critica è la situazione nei casi in cui l'OLO non può mettere in campo un minimo di economia di scala. Per differenziare l'offerta, gli operatori puntano pertanto su promozioni commerciali (attivazione gratuita, servizio gratuito per alcuni mesi ecc.) o sull'offerta di servizi aggiuntivi (spazio e-mail, spazio Web, fonia con Voice over IP, videocomunicazione ecc.).

Le offerte verso la clientela SOHO hanno, invece, prezzi differenti, giustificati da diverse prestazioni tra cui, per esempio, una più alta banda minima garantita, indirizzo IP statico, numero di utenti abilitati all'accesso, modem e router inclusi o meno nell'offerta.

Il numero di OLO e di ISP presenti nel mercato è comunque alto e, perciò, gli operatori cercano di differenziare la loro offerta puntando anche sulle *prestazioni aggiuntive*. Alcuni OLO/ISP che operano in questo ambito offrono a volte, servizi rivolti alla clientela residenziale a prezzi uguali alla concorrenza, solo allo scopo di ottimizzare lo sfruttamento delle proprie infrastrutture, in quanto la fornitura del collegamento non è in ogni caso il loro *core business*.

Gli operatori maggiori quali Wind, Tiscali ed Albacom stanno lanciando offerte congiunte

Target Clientela	Velocità up/down stream [kbit/s]	Banda Garantita [kbit/s]	Indirizzo IP	Modem o router	Traffico [Euro cent]	Operatore	Offerta	Canone mensile [Euro] (IVA esclusa)
Consumer	128/256	0	Dinamico	Opzionale	Incluso	TI	Alice Flat	30.79
					1.5 al min	TI	Alice Time	10.79
					Incluso	Aruba	Aruba ADSL 258	29.00
						Tiscali	Light Sempre	36.95
		10			50 al giorno	Wind	ADSL light	24.95
SOHO	128/256	5	Statico	Incluso	Incluso	IT	Smart 5	44.00
		0				Aruba	ADSL 256 LAN	51.65
Consumer	128/640	0	Dinamico	Opzione	Incluso	TI	Alice 640	41.63
						Aruba	ADSL 640	49.06
						NOICOM	ADSL Famiglia	48.00
		10/20				Albacom	UNY Sprint Light	36.20
		0				Tiscali	Top Sempre	46.95
		32				Wind	ADSL Fast	44.95
SOHO	128/640	5	Statico	Incluso	Incluso	IT	Smart 10	77.00
		0		Opzionale		Aruba	ADSL 640 LAN	72.30
		0		Incluso		Atlanet	Portalis ADSL	75.00
		25	Dinamico	Opzionale		Edisontel	Net ADSL Pro	50.00
		20	Statico	Incluso		Albacom	Alb@DSL Entry	125.00
		0	Dinamico	Opzionale		NOICOM	ADSL Azienda	60.00
		64	Statico			Tiscali	Premium sempre	56.95
		50				Wind	ADSL Pro	55.00
Consumer	256/1280	0	Dinamico	Opzionale	Incluso	TI	Alice Mega	54.13
				Incluso		Fastweb	Int. Senza Limiti	55.83

TABELLA 2
Offerte commerciali ADSL (marzo 2003)

al traffico telefonico, scontando al cliente il canone per il servizio di fonia previsto da Telecom Italia.

6.5. I sistemi DSL per le piccole medie imprese (PMI)

Nel settore business già menzionato precedentemente, le principali applicazioni che richiedono l'uso di banda larga sono le applicazioni *Intranet* (Rete Privata Virtuale), l'*interconnessione LAN tra più sedi, l'accesso a Internet/Intranet* da più postazioni fisse (oltre dieci PC), lo *scambio di informazioni e di documenti, i servizi multimediali* (*VoIP, videoconferenza ecc.*).
Quanto alle caratteristiche del collegamento sono richieste prestazioni elevate: accesso principalmente a 2 Mbit/s simmetrico, con la garanzia di una banda minima alta anche in caso di congestione di rete.

L'abbonamento preferito è il canone mensile *flat* (fornitura di Internet senza limiti di tempo) con modem/router incluso.
I servizi aggiuntivi più richiesti sono caselle di posta elettronica personalizzabili, indirizzi IP statici, *hosting* del sito Web, *security* e firewall *dedicati*. Dal punto di vista del fornitore del servizio, sono elementi vincenti dell'offerta la gestione e manutenzione degli apparati nel sito del cliente, l'elevata qualità del servizio (prestazioni, affidabilità e continuità), un servizio di *customer care* altamente specializzato (a disposizione in maniera permanente durante tutta la giornata di 24 h), un'assistenza tecnica/commerciale specializzata e dedicata con forte presenza territoriale.
La tecnologia di elezione per questo segmento di clientela sono i sistemi simmetrici. In particolare, l'HDSL consente una velocità dati bidirezionale (quindi non asimmetrica come nel caso dell'ADSL) fino a 2 Mbit/s, su una distanza massima di 3,5 km, impiegando due o tre coppie in rame. Questi sistemi, in precedenza impossibili da diffondere in modo generalizzato a causa della loro complessità e dei costi elevati, sono oggi impiegabili in modo relativamente economico. Lo standard HDSL2, pur arrivando solo a 1,5 Mbit/s, permette di utilizzare una sola coppia in rame e ha perciò un notevole interesse.
Le soluzioni simmetriche più innovative sono, però, quelle denominate SHDSL che consentono di ottenere prestazioni anche del 20% migliori in termini di lunghezza dei rilegamenti di utente rispetto ai precedenti sistemi simmetrici. Questo sistema, infatti, genera livelli minori di diafonia tra sistemi coesistenti sullo stesso cavo e, quindi, è facilitata l'interoperabilità tra costruttori diversi che utilizzano gli stessi portanti.
Caratteristiche interessanti dei sistemi forniti alle PMI sono:
- ***connessione simmetrica***: la velocità di trasferimento dei dati, a differenza dell'ADSL, è la medesima sia in entrata sia in uscita (downstream e upstream);
- ***connessione permanente***: la connessione alla rete è permanente, ossia garantita 24 h su 24;
- ***velocità altamente modulare***: usando la prestazione ATM-IMA (*Inverse Multiplexing Application*) l'accesso può essere variato (scalato) a passi di 2 Mbit/s sino a 155 Mbit/s. In questo caso, sono necessari una linea e una coppia di modem per ogni accesso a 2 Mbit/s.

I costi sono naturalmente più elevati che nel caso dell'ADSL, ma minori di quelle della rete CDN (*Circuiti Diretti Numerici*), rispetto ai quali risultano comunque di minore pregio, non presentando le stesse caratteristiche di continuità e di garanzia del servizio.
Da un'indagine dell'Assinform risulta che a fine 2002 ancora una minoranza di imprese (circa il 30% su 110 mila) dispone di collegamenti a larga banda (in fibra ottica o DSL), mentre presso la Pubblica Amministrazione questa percentuale scende al 18%. Il potenziale di crescita è, però, elevato, e si stima che un'ulteriore 24% delle imprese già si trova nella condizione di non poter più fare a meno della connessione a banda larga quale supporto per i servizi integrati d'informatica e telecomunicazioni.
Tra i servizi maggiormente apprezzati e impiegati dalle aziende dotate di connessioni a larga banda spiccano quelli di hosting, di *back up* e di *disaster recovery*. Interesse riscuotono anche i servizi legati alle problematiche che fanno capo alla sicurezza come, per esempio, le reti virtuali private (VPN).
Meno diffusi sono al momento i servizi di *video streaming*, di VoIP e di SAN (*Storage Area Network*).

7. SERVIZI MULTIMEDIALI PER L'UTENZA RESIDENZIALE

Per molto tempo si è cercata (e qualcuno sta ancora cercando) la *killer application* che giustifichi la richiesta di banda larga da parte degli utilizzatori. Come richiamato precedentemente, l'ADSL nacque storicamente per rendere possibile il *Video on Demand* - essendo la trasmissione video l'applicazione che richiede, più di altre, una banda larga - applicazione che, in pratica, si è rivelata essere un insuccesso.
È probabile, invece, che non esista una singola applicazione particolarmente importante: è molto probabile che Internet e l'insieme di applicazioni a essa associate costituiscano nel loro insieme la *killer application*, che si personalizza a seconda dell'utente. Questa esigenza può concretizzarsi in servizi quali: lo scambio di file audio e video e le *chat* per i giovani;

l'accesso alla Pubblica Amministrazione e ai servizi per i cittadini per gli studi professionali; la ricerca documentaria e d'informazione per numerose tipologie d'utenti. In realtà, vi è un intero mondo di applicazioni (Tabella 3), fruibili da diversi soggetti, o dallo stesso soggetto, a seconda delle esigenze e delle circostanze.
L'aumento della velocità delle connessioni fornito dai progressi tecnologici pone, in particolare, la questione d'individuare applicazioni e servizi multimediali interattivi che realmente utilizzino la larga banda. Si fa qui riferimento alle possibilità insite nelle connessioni ADSL che ormai cominciano a essere un'offerta generalizzata sotto la spinta dell'operatore dominante e, con maggiori difficoltà dovute all'unbundling (come chiarito nel precedente paragrafo 6), anche da parte dei suoi concorrenti.
Possono essere innanzitutto distinti due casi. Il primo riguarda lo *scaricamento veloce* da Internet (in particolare, in connessione peer to peer) di file che hanno dimensioni sempre maggiori (i già citati file video che possono anche essere relativi a interi film, ma anche riguardare CD musicali completi). Questa esigenza costituisce probabilmente, in questo momento, il maggiore stimolo alla richiesta di collegamenti a larga banda.
Un secondo caso è, invece, la *fruizione in tempo reale* di programmi audiovisivi, che, a loro volta, possono essere file registrati presenti in archivi, o avvenimenti dal vivo. Questa esigenza è resa possibile dall'invio di flussi (*streaming*) di file multimediali. Si tratta di una tecnologia che permette la diffusione di audiovisivi via Internet, o meglio tramite le reti basate sul protocollo IP.
In generale, questo processo è tanto più efficace, quanto più il collegamento è veloce e ha una banda garantita. Sono disponibili già, anche in Italia, siti appositamente creati per fornire questo tipo di contenuti dedicati agli utenti della banda larga. Uno fra i più famosi è *My-tv*. Oltre ai cortometraggi animati, il sito offre interviste video a diversi personaggi del mondo dello spettacolo, del cinema e della musica; presentazione di *trailer* di film e video musicali.
Un altro settore in cui la banda larga è di grande importanza, soprattutto per giocare on-line, è quello dei *videogame*. Microsoft e Sony hanno, per esempio, lanciato recentemente sui diversi mercati (Giappone, USA, Europa) alcuni servizi orientati ai possessori di *consolle Xbox* e *PS2*, con interfaccia nativa o aggiunta (*add-on*), per collegamenti a larga banda: giochi *multiplayer on-line* con l'eventuale interazione vocale fra i giocatori, e con scene e livelli e personaggi aggiuntivi da scaricare ecc.. Un altro esempio commerciale è quello del cosiddetto GoD (*Game on Demand*), nel quale i titoli per PC sono giocati attraverso collegamenti a larga banda verso server in rete, invece, che essere prelevati dal lettore CD locale. I vantaggi di questa soluzione si ritrovano nella possibilità di provare un gioco con una spesa ridotta, di diversificare le offerte (noleggio per x ore, per un week-end, per una settimana, acquisto definitivo) e in prospettiva anche di controllare meglio il fenomeno della pirateria. Spesso, inoltre, i filmati di presentazione dei giochi sono file che per essere utilizzati al meglio richiedono una connessione a larga banda.

Informazione e Comunicazione	Intrattenimento	Televisione e multimedia
		Foto/video
		Audio-HiFi
		Gioco
	Socio-Culturali	Accesso da remoto a LAN aziendale
		Telelavoro, lavoro cooperativo
		Home news, Info-push e comunità virtuali
		Home banking, acquisti e pagamenti on-line
		Telemedicina, Teledidattica
	Telecomunicazioni	Integrazione con cellulari, PDA ecc. per mobilità
		Servizi telefonici
		Videocomunicazione
		E-mail
Automazione Domestica	Sicurezza	Telesoccorso
		Antintrusione, video controllo
		Antincendio, antifughe gas
	Gestione Ambiente	Distribuzione energetica e consumi
	Robotica Domestica	Gestione automatizzata apparecchi di casa

TABELLA 3
Servizi e applicazioni multimediali per ADSL

Sono stati creati dei siti che raccolgono tutti i contenuti dedicati ai videogiocatori che utilizzano connessioni veloci. È possibile scaricare lunghe sequenze tratte dai giochi in azione o filmati che hanno come protagonisti i personaggi dei videogame.
Sono state anche predisposte alcune sezioni dei principali portali (di solito dedicate ai sottoscrittori del servizio di connettività a larga banda) appositamente per contenuti, quali musica, informazione e documentari, da scaricare in streaming. In Italia, per esempio, sono disponibili i siti *Alice Wonderland, Virgilio X* e *Tiscali Broadband* e ultimamente la Società *RAI-Click* ha reso accessibili i vecchi programmi della RAI.
Da ultimo, ma non meno importante, è l'utilizzo dello streaming per trasmettere i notiziari via Internet, servizio che si va diffondendo sempre maggiormente. Il telegiornale della rete televisiva La7 è già on-line con diverse edizioni al giorno. La RAI fornisce la possibilità di rivedere i principali telegiornali e trasmissioni di vario genere, con connessione a 300 kbit/s. Anche le emittenti radio, già da tempo, hanno capito l'importanza di un mezzo di comunicazione come Internet, soprattutto fra i giovani, e permettono di ascoltare la radio on-line e programmi creati esclusivamente per lo streaming, con *Disk Jockey* dedicati ad appositi contenuti o alla trasmissione di video musicali.
Queste offerte sono di solito gratuite, anche perché non possibile garantire a priori la disponibilità della banda richiesta e, quindi, la qualità finale della fruizione del servizio. Non è ancora chiara la risposta del mercato se queste offerte fossero proposte come servizi a pagamento, prospettiva quanto mai probabile considerati gli scarsi ritorni della pubblicità on-line.
Un tema di particolare interesse per i potenziali sviluppi di business è il rapporto tra ADSL e televisione: in linea di principio, le velocità più elevate offerte con l'ADSL sono sufficienti per fruire di contenuti video in tempo reale che, codificati, ad esempio con MPEG-4, possono raggiungere buoni livelli di qualità già a velocità di 1 Mbit/s (per esempio, nel caso di film codificati *off-line* in modo ottimizzato). Ma, come si è detto, esistono anche offerte di Fastweb in MPEG-2 con ADSL a 6 Mbit/s.
Modelli di pura trasmissione diffusiva (*broadcast multicasting*) appaiono condizionati da aspetti tecnici e di banda disponibile nella rete nella sua interezza (un video di buona qualità richiede 3 Mbit/s), oltre che dalla concorrenza del satellite e della futura televisione terrestre. Sia Fastweb che Telecom Italia hanno allo studio la possibilità di estendere il servizio ADSL anche a trasmissioni televisive multicasting. A lungo termine potrebbero essere più promettenti modelli di Video on demand (nel senso ampio sopra ricordato), e di televisione interattiva, anche se in questo momento non paiono trovare grande risposta da parte del mercato
Una particolare e interessante applicazione della larga banda consiste nella videocomunicazione con buona qualità, che rappresenterebbe la versione in chiave tecnologica moderna e a costi contenuti del vecchio concetto di videotelefonia che non è mai riuscito a decollare per i prezzi elevati. Il servizio è già offerto da Fastweb e anche Telecom Italia si appresta a offrirlo dopo un accordo d'interconnessione con Fastweb.
In quest'applicazione, la natura asimmetrica del collegamento ADSL stabilisce - come limite superiore alla qualità dell'immagine - la velocità di upstream, pur tenendo conto che i più recenti progressi nel campo della compressione video consentono di ottenere con soli 256 kbit/s una qualità paragonabile a quella degli attuali sistemi ISDN professionali a 512 kbit/s.
In tutti i casi di applicazioni in tempo reale, sopra menzionati, si è di fronte a un problema di qualità e di garanzia di continuità, che non è certamente prerogativa dei servizi offerti a basso costo agli utenti residenziali. La banda di picco del collegamento ADSL, anche se apparentemente dedicata al singolo utilizzatore, può essere, secondo la comune esperienza, ridotta sensibilmente dal resto della catena, per motivi attribuibili alla velocità del *server* di erogazione ovvero a problemi di congestione della rete di trasporto o all'accesso contemporaneo di molti utenti sullo stesso sito. Possono aiutare da questo punto di vista (specie per i download, ma non per la videocomunicazione) soluzioni di C*ontent Delivery Network* (CDN), caratterizzate dalla presenza di server periferici che replicano i contenuti più richiesti.
Si può concludere, dunque, che le soluzioni tecniche alla necessità di garantire la qualità dei servizi offerti su reti a larga banda sono già disponibili, ma l'opportunità di introdurle sarà necessariamente legata a considerazioni di mercato e di convenienza economica.

8. GLI SVILUPPI TECNOLOGICI ATTESI DELLA FAMIGLIA DSL

Da quanto si è esposto nei paragrafi precedenti, sembra possibile concludere che, nell'evoluzione delle reti verso le connessioni a larga banda, le coppie simmetriche in rame tradizionali continueranno a svolgere un ruolo importante per un certo numero di anni ancora, anche quando le esigenze di banda supereranno valori di vari Mbit/s per connessione. Sembra, pertanto, opportuno soffermarsi in chiusura di quest'articolo su alcune considerazioni legate alle prospettive tecnologiche dei sistemi DSL.

L'opinione diffusa è che la connessione in fibra ottica dell'utente FTTH è ancora in numerose situazioni d'impianto eccessivamente onerosa e non sempre facilmente realizzabile: essa richiederà, pertanto, un certo tempo per diventare competitiva. Una soluzione economicamente valida nel transitorio potrebbe essere costituita dalla combinazione di una tratta in fibra ottica fino a un punto prossimo a più utenti e l'impiego del doppino telefonico per la connessione finale. Questa topologia è chiamata variamente FTTC (*Fibre To The Curb*) o FTTB, secondo le soluzioni topologiche o realizzative.

Da un punto di vista tecnologico, nello sviluppo della famiglia DSL, il sistema VDSL (*Very High Speed Digital Subscriber Line*), oggi allo studio, può essere considerato, nei casi in cui la distanza lo consenta, l'erede dell'ADSL che ormai tende sempre più ad affermarsi.

Secondo l'attuale impostazione i sistemi VDSL sono in grado di trasportare dati fino a 58 Mbit/s e possono essere realizzati per connessioni simmetriche o asimmetriche, secondo le esigenze dell'applicazione.

A causa delle limitazioni fisiche del portante (l'attenuazione del doppino cresce sensibilmente con la frequenza), la distanza massima su cui un VDSL può operare è limitata a meno di 1,5 km. Nella tabella 4 sono riportate le massime velocità VDSL impiegabili in funzione della lunghezza del doppino di utente.

Il VDSL, di cui oggi esiste qualche primo esemplare, è ancora in fase di definizione: le attuali soluzioni pionieristiche sono, infatti, mirate principalmente a sperimentare la qualità di funzionamento sulle linee telefoniche esistenti.

Un parametro importante, ancora poco conosciuto, è la massima distanza che, con i sistemi VDSL, può essere realizzata in modo affidabile per una certa velocità di trasmissione. La causa principale di questa incertezza è legata al comportamento trasmissivo della linea nel campo di frequenze usate. Mentre, infatti, nel caso degli accessi ISDN e ADSL, le eventuali diramazioni sul doppino, o il suo prolungamento nell'ambito della residenza dell'utente, hanno effetti noti e controllati, nel caso di introduzione di sistemi VDSL si richiedono necessarie accurate sperimentazioni e indagini addizionali. Gli effetti di compatibilità e suscettibilità elettromagnetica sono altresì motivi d'indagine sperimentale sul campo.

Distanza (metri)	"Down-stream" data-rate Mbit/s	"Up-stream" data-rate Mbit/s
300	52	6.4
300	26	26
1000	26	3.2
1000	13	13
1500	13	1.6

TABELLA 4
Velocità VDSL tipiche in funzione della lunghezza del rilegamento di utente

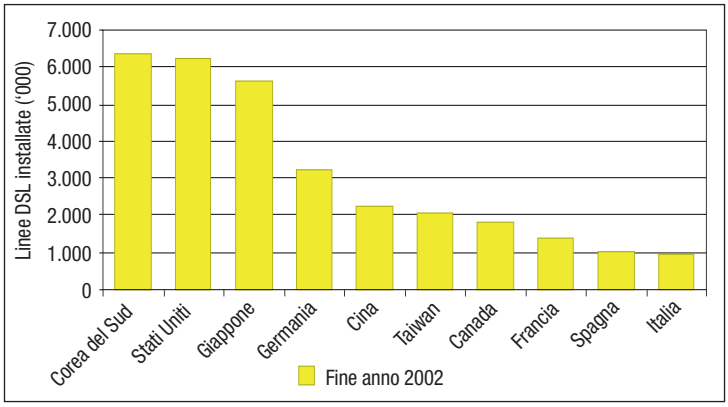
Nel più generale campo delle applicazioni a banda larga, in particolare per il riversamento rapido di un film, il VDSL potrebbe risolvere il problema di entrare a casa dell'utente con più di un canale televisivo con l'impiego di un solo doppino per favorire i diversi componenti di una famiglia che vogliono vedere trasmissioni diverse. Naturalmente, l'evoluzione delle tecnologie, in particolare quella ottica, e dei servizi per l'utente, potrebbero essere tali da accelerare lo scenario presentato e spingere verso la realizzazione di reti più "ottiche" verso l'utenza finale, riducendo o addirittura cancellando la finestra temporale in cui potrebbero collocarsi i sistemi VDSL.

9. IMPIEGO DEI SISTEMI DSL NEL MONDO E PREVISIONI PER IL FUTURO

Il mercato mondiale dell'ADSL, nel 2002, ha mostrato una crescita considerevole nonostante il periodo di stagnazione economica che ha colpito anche il settore delle telecomunicazioni. Le valutazioni degli analisti effet-

tuate sulla crescita di settore a inizio 2002 sono risultate sostanzialmente corrette. Le modalità e le tempistiche di crescita sono, tuttavia, risultate differenti da Paese a Paese.
A fine 2001, si contavano nel mondo poco meno di 19 milioni di ADSL installati mentre a fine 2002 tale numero era cresciuto a circa 36 milioni con una crescita percentuale vicina al 100%. La situazione del 2002 per i principali Paesi è riportata in figura 8.
Secondo molti analisti il mercato dovrebbe mantenere anche nel corso del 2003 tassi di crescita elevati con valori previsti a fine anno compresi tra i 55 ed i 60 milioni di unità. Tuttavia alcuni Paesi, quali ad esempio la Cina, hanno mostrato nel corso degli ultimi mesi dell'anno passato tassi di crescita elevatissimi e, quindi, secondo alcune previsioni anche il valore di 60 milioni di terminazioni potrebbe rivelarsi in errore per difetto. Oggi il 3,6% delle linee telefoniche del mondo risultano equipaggiate con ADSL.
È sicuramente l'Asia con quasi il 50% del mercato complessivo il continente in cui il successo dell'ADSL è più evidente. È notevole osservare in figura 9 il numero di sistemi DSL installati in percentuale della popolazione, tra cui spiccano le particolari situazioni di Corea del Sud e Taiwan ulteriormente rinforzate dalla presenza in questi Paesi anche delle soluzioni in *cable modem*. In particolare, in Corea del Sud il 70% delle abitazioni è raggiunto da sistemi a banda larga con notevole incoraggiamento da parte del Governo e da parte di molti ministeri tra cui, in primo piano, l'impiego per didattica. Un certo rallentamento nei tassi di crescita del Nord America ha consentito all'Europa di raggiungere e superare la quota di mercato detenuta dal Nord America in cui il DSL è diffuso al 10% della popolazione in Canada ed al 3,5% in USA (in ambedue i Paesi i collegamenti in *cable modem* sono più che doppi rispetto a i sistemi DSL).
Negli USA la crescita è risultata inferiore a quella degli anni precedenti: molti operatori, in particolare i CLEC (*Competitive Local Exchange Carrier*) specializzati nel settore, hanno avuto forti difficoltà. La competizione dei cable modem risulta in alcuni Paesi molto efficace: negli Stati Uniti, nel Regno Unito, in Olanda, in Canada e in Austria, per esempio, la diffusione dei cable modem risulta superiore a quella degli ADSL.
In Europa il ruolo di *leader* nel settore è detenuto dalla Germania (oltre 3 milioni di apparati) anche se Danimarca, Belgio e Finlandia vantano la maggior penetrazione percentuale. Buoni valori di crescita si sono ottenuti anche in Paesi, come la Francia e il Regno Unito, in cui la diffusione dell'ADSL era risultata in passato più modesta. Le previsioni di quota di mercato stimate da diversi analisti per le infrastrutture d'accesso indicano le connessioni DSL come un sistema di successo per un lungo periodo transitorio (Figura 10 per il mercato europeo).

FIGURA 8
I primi dieci Paesi in numero di linee DSL installate alla fine del 2002 (Fonte: point-topic.com)



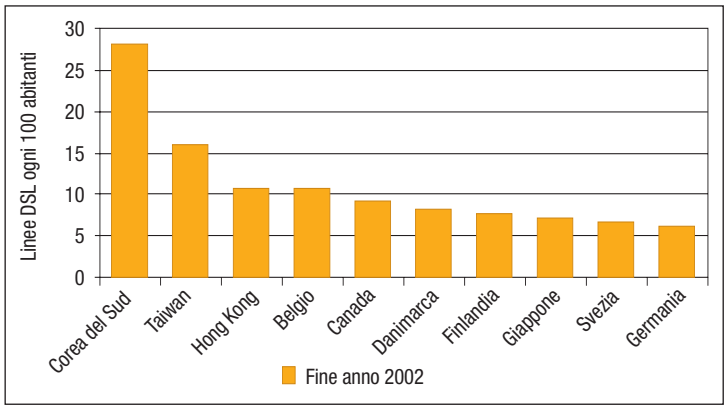


FIGURA 9
I primi dieci Paesi in numero di linee DSL per ogni 100 abitanti (Fonte:point-topic.com)

10. CONCLUSIONI

La numerizzazione del trasporto di informazioni, unita alla codifica numerica dei contenuti e alla compressione di tutti i tipi di informazione e in particolare di quelli audio-video, sta realizzando la famosa (e facile) profezia di Nicholas Negroponte, secondo la quale i bit sono bit, qualunque sia la sorgente informativa da cui provengono e qualunque sia il mezzo in cui sono immagazzinati, diversamente

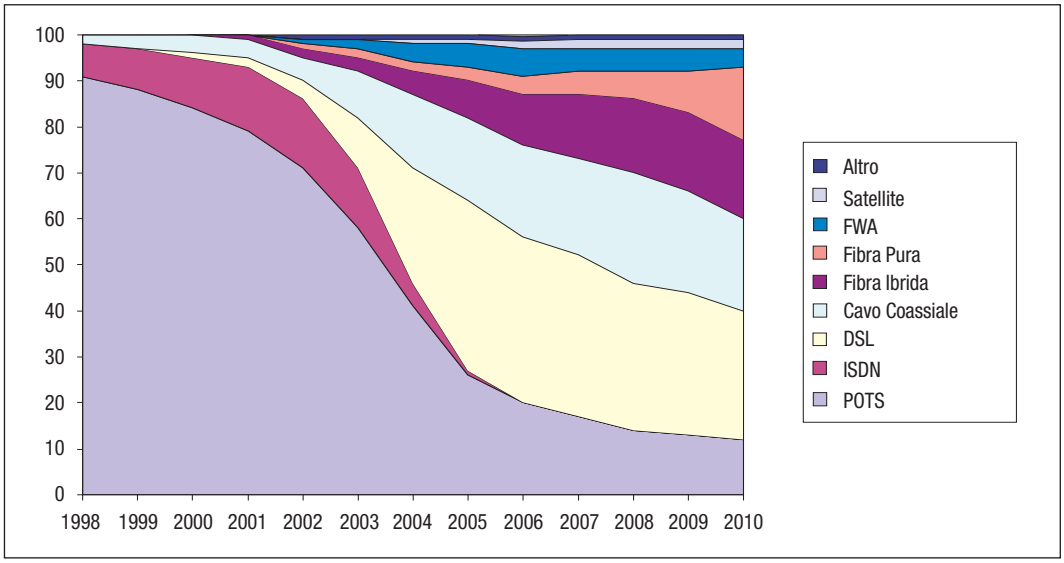


FIGURA 10
Previsione di distribuzione del mercato di accesso nelle case europee tra i diversi sistemi (Fonte: The Development of Broadband Access Platforms in UE–Agosto 2001)

da quanto succede per gli atomi (intesi nel senso dei supporti materiali che costituiscono i diversi media). Si stanno di conseguenza attuando almeno tre convergenze:

- ***la convergenza del trasporto dell'informazione***: il segnale numerico su piattaforma IP porta qualunque tipo di contenuto (voce, dati, segnali audio, video, testi, immagini) sul medesimo canale che arriva a casa dell'utente;
- ***la convergenza dei contenuti***: la numerizzazione dei contenuti rende trattabili da una unica piattaforma mondi fino a poco tempo fa completamente distinti: libri, giornali, fotografie, film, segnali televisivi e musica;
- ***la convergenza delle piattaforme e dei terminali***: un'unica piattaforma basata su architetture tipo quello del PC e un unico terminale diventano di volta in volta giornale, libro, album fotografico, proiettore di diapositive, televisore, radio, registratore e riproduttore audio e video.

In questo quadro, i rilegamenti DSL si pongono oggi come il sistema più potente e "universale" (quasi tutti gli abbonati al telefono possono essere collegati mediante sistemi DSL) per dare l'accesso al mondo digitale a banda larga attraverso la rete pubblica esistente di telecomunicazioni.
Questi sono in estrema sintesi i motivi che giustificano le previsioni di mercato sopra riportate.

ANDREA BONATI, laureato in Ingegneria Elettronica nel 1971 presso l'Università di Padova. Nello stesso anno è entrato a far parte dei Laboratori di Ricerca e Sviluppo in Telettra SpA occupandosi di ricerca e progettazione nell'ambito della Trasmissione su portante fisico con responsabilità crescenti. Nel Settembre 1986 è nominato responsabile della R&S per la Trasmissione su Linea Fisica. Nell'Ottobre 1994 assume la Direzione Tecnica dei Laboratori di Ricerca e Sviluppo di Alcatel in Europa e US per la Divisione Trasmissioni. Attualmente è Assistente Tecnico del Presidente della Divisione Reti Ottiche.
andrea.bonati@netit.alcatel.it

BRUNO COSTA, laureato in Fisica presso l'Università di Torino nel 1969. Dal 1971 ha lavorato allo CSELT (ora *Telecom Italia Lab*, centro di ricerca del Gruppo Telecom Italia), operando e ricoprendo responsabilità nelle aree di ricerca delle comunicazioni ottiche, della fotonica, degli impianti di telecomunicazioni, della rete di accesso e delle reti domestiche. Attualmente è responsabile dei Laboratori riguardanti la rete trasmissiva su cavo. Autore di numerose pubblicazioni scientifiche, ha scritto contributi per libri ed enciclopedie e ha diretto importanti Convegni sulle comunicazioni ottiche.
bruno.costa@TILAB.com

GUIDO VANNUCCHI, laureato in Ingegneria Industriale all'Università di Bologna nel 1958, "Master Science" in "Electrical Engineering" alla Stanford University nel 1963, Libera Docenza in Comunicazioni Elettriche nel 1971. Dal 1960 in Telettra SpA (oggi Alcatel Italia) essendo Direttore Generale dal 1983 al 1990. "Senior Consultant" prima di Italtel e poi di Olivetti Telemedia nonché coordinatore del progetto MxM ("Milano per la Multimedialità"). Vice Direttore Generale della RAI dal 1996 al 1998. Docente al Politecnico di Milano di "Sistemi e Tecnologie della Comunicazione".
Laurea "ad honorem" in Ingegneria delle Telecomunicazioni, conferita dall'Università di Padova nel 1998 per i contributi scientifici e manageriali apportati al campo della trasmissione dei segnali e per gli studi e le realizzazioni pionieristiche nel campo della televisione digitale.
redazione@mondodigitale.com