NOTIZIARIO TECNICO TELECOM ITALIA

CUBA: LE SFIDE DI ETECSA PER LE TELECOMUNICAZIONI

L'IMPATTO DEL COMMERCIO ELETTRONICO SUI GESTORI DELLE RETI TLC

LA SICUREZZA IN INTERNET

anno 7
n. 3
DICEMBRE
1998

TELECOM ITALIA

Ai lettori

Con il vostro ausilio possiamo ancora migliorare

"È cosa singolare come il conto torni *(ratio constat)* o sembri tornare giorno per giorno, ma non torni completamente quando si prendono in esame molti o tutti i giorni" *così scriveva Plinio il Giovane a Minicio Fundano (lettere I,9), confidandogli le sue riflessioni sullo scorrere del tempo e sul giudizio retrospettivo della propria attività. È forse bene che anche noi "ci sottoponiamo a un esame" dopo tre anni d'intenso impegno della redazione del* Notiziario*, anche per constatare che dopo tutto, qualche* conto *sembra tornare.*

Da quando è stato redatto il primo numero, la rivista ha conosciuto numerosi mutamenti. Quelli più appariscenti a prima vista riguardano l'aspetto esteriore e l'impostazione tipografica. Non si è trattato solo di un miglioramento, ma - spero - di modifiche che hanno consentito una migliore leggibilità delle figure e dei grafici e una maggiore espressività dei testi, grazie anche alla riproduzione di fotografie.

Non è però sull'aspetto esteriore che desidero soffermarmi. Senza abbandonare il "cuore" della rivista, costituito dagli articoli tecnici e, in particolare, da quelli organizzati in cicli di ampio respiro, sono state introdotte gradualmente nuove rubriche nei numeri del Notiziario *più recenti: rapporti su conferenze (finora ventisette), un osservatorio, le news (con particolare riguardo agli aggiornamenti sulla normativa internazionale), recensioni di libri tecnici, sommari di alcune pubblicazioni CSELT (scelte tra quelle di maggiore interesse per i destinatari del* Notiziario*), escursioni storiche nell'ambito delle telecomunicazioni (le nostre radici). La definizione del ruolo e dei contenuti di ognuna di queste rubriche è stato oggetto di riflessione del Comitato Direttivo; una conferma di questo sforzo per essere più vicini alle attese di voi lettori può essere ritrovata nell'evoluzione costante delle rubriche. Abbiamo cercato, infatti, di adattare la rivista ai destinatari, anche attraverso sondaggi espliciti mediante questionari, e di attrarli su questioni rilevanti di attualità o su possibilità di formazione o integrazione delle proprie conoscenze tecniche che ci sembravano meritare attenzione.*

Punto di forza della rivista (e in particolare per i testi che richiedono uno sforzo maggiore!) rimangono però gli approfondimenti mediante testi tecnici: negli anni più recenti sono stati pubblicati cinquantotto articoli su un insieme abbastanza esteso di temi riguardanti le novità nelle telecomunicazioni quali, ad esempio: ATM, Internet, DECT, satelliti, cavi sottomarini, SDH, rete di accesso (xDSL), energia. Accanto a testi con connotati tecnico-specialistici sono stati pubblicati articoli informativi o descrittivi e, in particolare, quelli legati all'internazionalizzazione delle attività del Gruppo Telecom Italia. Nei testi abbiamo posto una certa cura per incoraggiare alla lettura il destinatario, anche se non particolarmente esperto nella materia, evitando termini specialistici o sviluppi matematico-logici complessi. Questi chiarimenti sono stati aggiunti, solo nei casi ritenuti veramente necessari, in riquadri che non interrompono la lettura del testo principale, con l'obiettivo di offrire l'occasione di "saperne di più", magari in una seconda lettura o per facilitare l'approfondimento tecnico di coloro che già sono "iniziati" alla materia trattata. Sono stati pubblicati testi difficili da assimilare, a volte magari un po' lunghi: voglio tuttavia ricordare che può essere compiuto uno sforzo per rendere chiara *una materia complessa, ma sarebbe ipocrita e fuorviante farla apparire* semplice*.*

L'organizzazione in cicli dei lavori presentati non è mutata; essa è del resto una formula efficace che consente un'esposizione esauriente di argomenti, spesso molto ampi e articolati. Non è un caso che circa un terzo degli articoli pubblicati dal 1996 (18 su 58) fa parte di cicli su materie attuali come ATM e Internet. Sono state affrontate anche tematiche relative alle infrastrutture trasmissive, in particolare a larga banda (14 articoli sono stati dedicati ai satelliti, ai sistemi trasmissivi SDH, agli apparati xDSL ed ai portanti sottomarini). In questo quadro è previsto di avviare fra breve un ciclo di articoli sul WDM (Wavelength Division Multiplexing) *e sulle tecniche di* optical networking*, tema che in questi ultimi tempi è uscito dai laboratori di*

Ai lettori

ricerca o dalle applicazioni speciali (ad esempio i portanti sottomarini) per tradursi in prodotti e in realizzazioni di rete. Il Comitato di Direzione desidera anche promuovere l'approfondimento di temi sui servizi e sulle esperienze in campo. Ha inoltre deciso di dedicare uno dei prossimi numeri al pressante argomento dell'interconnessione tra le reti di telecomunicazioni.

Sotto il profilo della diffusione del Notiziario*, vale la pena infine ricordare l'iniziativa che ha riscosso un successo quasi inatteso: la predisposizione di un sito sull'Intranet di Telecom Italia per consentire la consultazione elettronica ai tecnici della Società. I quasi quattordicimila accessi raccolti nel corso di poco più di un anno di attività del sito dimostrano l'utilità dell'iniziativa e anche, penso, l'interesse suscitato dalla rivista.*

Ho cercato fin qui di tratteggiare le novità vissute dalla rivista nell'ultimo triennio, indicando anche cosa si prepara per il prossimo futuro. Può sembrare questo scritto un'apologia; ma per sgombrare subito il campo da sospetti di celebrazione voglio sottolineare la mia convinzione che non tutti i "conti" tornano.

In primo luogo l'assenza di lettere: invitai tutti i destinatari a scrivere alla redazione per indicare i punti non chiari o quelli da approfondire nei testi pubblicati o per proporre nuovi temi di interesse. Quando feci questa proposta temetti di essere sommerso dalle lettere. Il canale a ritroso, dai destinatari alla rivista, è stato invece a "traffico" praticamente nullo. Sempre con Plinio il Giovane vorrei ripetere l'invito che lo scrittore latino rivolse a Fabio Giusto (lettere I,11): "Olim mihi nullas epistulas mittis ...".”Da molto tempo non mi scrivi. Tu dici: non ho nulla da scriverti. Ebbene scrivimi proprio questo ... Fai ch'io sappia che cosa fai, giacché il non saperlo mi dà la maggiore inquetitudine".

Ripeto quindi che noi della Redazione gradiremmo ogni contributo di idee di persone dell'Azienda che considerano la rivista tecnica della Società nella quale operano come un patrimonio per la propria professione ed un segnale dell'importanza del proprio ruolo.

Altro aspetto del quale sono finora parzialmente soddisfatto è la realizzazione *della rivista. Parafrasando Quintiliano* (non multa, sed multum) *non è alla produzione di massa che la Società punta ma piuttosto alla qualità. Ma* qualità *implica anche puntualità e regolarità. E quindi tra gli obiettivi prioritari di chi lavora alla rivista, e in particolare del suo Direttore, è compreso quello relativo all'eliminazione degli ostacoli che non consentono il regolare flusso dei numeri della rivista. Dovrò quindi impegnarmi maggiormente in futuro anche su questi aspetti.*

Non voglio sottrarre altro spazio alla rivista (e altro tempo ai lettori!). Mi fa però piacere affermare che tre anni passati ad occuparmi del Notiziario Tecnico *mi hanno dato l'opportunità di vivere ancora sul* leading edge *(sulle nuove frontiere) del mondo professionale. È con l'entusiasmo che mi deriva da questa opportunità che mi accingo ad affrontare il 1999, sperando di poter continuare ad interagire con sempre maggiore interattività con voi lettori.*

r.c.

Nota: I testi di Plinio il Giovane sono ripresi da "Lettere ai familiari", Volume primo, libri I-IX - traduzione di Luigi Rusca - Biblioteca Universale Rizzoli.

L'internazionalizzazione di Telecom Italia

Le telecomunicazioni a Cuba

DOMENICO CAPOLONGO

Dal punto di vista storico le telecomunicazioni cubane occupano un posto di primo piano a livello internazionale. L'evoluzione del servizio di base segue l'evoluzione economico-politica del Paese, che si caratterizza in tre fasi temporali: dal 1881 al 1901, dal 1902 al 1958 e dal 1959 ai nostri giorni. Nel 1994 i servizi di telecomunicazioni sono stati unificati - con l'esclusione di quello cellulare - nell'unica impresa ETECSA. Nel 1997 la partecipazione azionaria di Telecom Italia, attraverso STET International Netherlands, è passata dal 12,25 per cento al 29,29 per cento e per la componente italiana la responsabilità nella gestione dell'impresa è cresciuta fino alla quasi parità con quella cubana.

La pianificazione poliennale di sviluppo e ammodernamento di ETECSA è stata messa a punto nel corso del 1997. In quest'articolo sono presentati i principali risultati ottenuti nel biennio 1997-98 e alcune previsioni per il medio termine.

1. Un antesignano storico

Quella che potrebbe essere indicata come la prima comunicazione telefonica a livello mondiale si svolse all'Avana nel 1849. Fu un accadimento del tutto involontario perché avvenne durante una seduta di elettroterapia. Più che normali parole fu trasmesso un urlo di dolore dal paziente - un cubano affetto da reumatismi alla testa - al terapeuta, l'italiano Antonio Meucci, esule dal Granducato di Toscana e residente nella capitale cubana dal 1835. La terapia prevedeva, infatti, di somministrare scariche elettriche al paziente e di inserire lo stesso terapeuta nel circuito che includeva una batteria. In questo storico esperimento la batteria sviluppava una tensione superiore ai 100 V ed era collocata nel laboratorio; il paziente si trovava in un'altra stanza, relativamente distante; un filo conduttore collegava la batteria al paziente al quale Meucci aveva chiesto di mettere in bocca i due capi del conduttore tra i quali aveva inserito una linguetta flessibile. Meucci, che si trovava nel laboratorio, s'inserì a sua volta nel circuito tenendo in mano una linguetta simile a quella del paziente e l'avvicinò ad un orecchio mentre attivava la scarica. La terapia era evidentemente ancora in fase sperimentale per cui la tensione - piuttosto elevata - provocò una scossa molto forte al paziente; questi urlò e il suono o, forse sarebbe meglio dire, questo rumore, fu trasmesso in qualche modo elettricamente al terapeuta che lo percepì attraverso la propria linguetta.

Antonio Meucci all'Avana faceva il "meccanico teatrale" nel teatro Tacón, e si dedicava nel contempo a diverse altre attività in quanto era dotato di notevoli capacità applicative nelle novità tecnologiche del

Cuba, sul margine settentrionale del Mar dei Caraibi.

tempo. L'episodio dell'urlo trasmesso elettricamente non lo lasciò perciò indifferente; al contrario ripeté e perfezionò l'esperimento anche quando - l'anno successivo - dovette lasciare L'Avana e si trasferì negli Stati Uniti. Conscio ben presto di aver individuato un

sistema di grande importanza e utilità lo battezzò *telegrafo parlante* e successivamente lo chiamò *telettrofono.*

Per una serie di sfortunate vicende Antonio Meucci non riuscì a sfruttare industrialmente la propria invenzione; Alexander Graham Bell brevettò infatti ufficialmente il *telefono* nel 1876, anno in cui, per mancanza di fondi, Meucci non poté rinnovare il proprio!

Ritratto a carboncino di Antonio Meucci, eseguito da Bistolfi nel 1884 [1].

Un'informazione completa e ricca di particolari sulle vicende dell'intera vita di Antonio Meucci, inventore italiano in terra cubana del telefono, è fornita dall'opera di Basilio Catania che ha pubblicato già due volumi assai documentati su questo singolare e complesso personaggio ottocentesco.

L'Avana è stata quindi la città che ha visto nascere la trasmissione elettrica della voce. Come vedremo in seguito, non è questo l'unico motivo per collocare Cuba in una posizione di avanguardia a livello mondiale nella nascita e nello sviluppo iniziale della storia delle telecomunicazioni.

2. Cuba: un excursus generale

Il territorio cubano è costituito dall'*isola grande* di Cuba, dall'isola della Gioventù e da uno straordinario numero di oltre quattromila piccole isole e isolotti, chiamati "cayos". Cuba è perciò un Paese insulare, con una popolazione di poco più di undici milioni di abitanti e con un'estensione di 110.860 km quadrati, che portano a una densità di 99,6 abitanti per km quadrato, con una netta prevalenza di popolazione che vive in ambiente urbano. Con 1.299 km di lunghezza Cuba è anche l'isola più grande delle Antille. L'Arcipelago cubano è limitato a ovest dal Golfo del Messico; il resto è bagnato dal Mar dei Caraibi a sud e ad est e dall'Oceano Atlantico a Nord. Questa posizione geografica, che fa dire che *la Isla mira hacia todos los caminos,* ha reso fino ai nostri giorni Cuba crocevia primario delle rotte marittime e aeree. Fin dalle prime epoche coloniali l'isola è servita come punto di partenza per la conquista di altre terre, nonché come luogo per il transito di primo piano negli scambi commerciali tra l'Europa e le Americhe, guadagnandosi così la denominazione di *Chiave del nuovo mondo.*

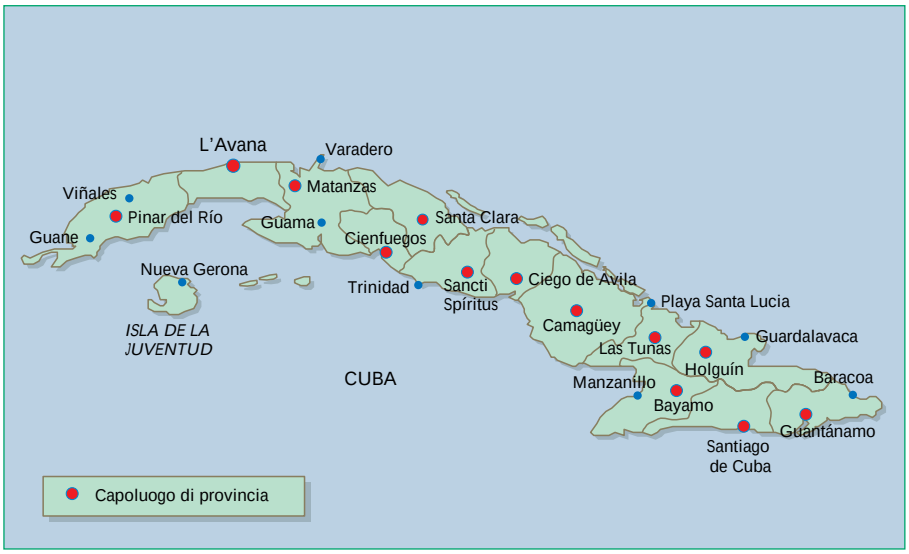
Il Paese è organizzato secondo una divisione politico-amministrativa basata su quattordici provincie e su un "municipio speciale" *(Isla de la Juventud);* le provincie sono divise in 169 municipi. Questa struttura favorisce lo sviluppo socio-economico del Paese perché tiene conto della distribuzione della popolazione, dell'attività economica e del suo sviluppo, di tradizioni e vincoli tra le differenti località, di reti viarie e migrazioni, e di altri aspetti di primaria importanza. La divisione del Paese ha l'obiettivo di facilitarne la politica di sviluppo regionale, equilibrando le differenze presenti nelle diverse zone e permettendo di sfruttare al massimo le risorse umane e naturali disponibili.

Base fondamentale dell'economia cubana è la canna da zucchero e l'industria zuccheriera. Altre coltivazioni importanti sono il tabacco, gli agrumi ed il caffè. Anche l'industria della pesca costituisce un elemento importante per l'economia del Paese. Altri prodotti di base per Cuba sono il nichel, il rum, il miele, il tabacco, il cacao, e, inoltre, il manganese, l'asfaltite, i marmi. Negli ultimi anni si sono sviluppate l'industria farmaceutica e la biotecnologia. È, infine, in pieno sviluppo il turismo e una sua futura ulteriore crescita potrà rappresentare un'importante fonte di entrate di valuta per il Paese.

Per un riferimento storico essenziale su Cuba si deve risalire all'insediamento spagnolo che - dopo il primo sbarco di Colombo nel 1492 - iniziò concretamente nel secondo decennio del sedicesimo secolo. A differenza di quanto avvenne nel resto delle Americhe la presenza coloniale in Cuba durò fino al primo gennaio 1899, allorché l'ultimo "gioiello" della Corona di Spagna si separò definitivamente da Madrid, dopo tre guerre di indipendenza ed un intervento degli Stati Uniti.

Le insufficienze iniziali del regime di sfruttamento imposto dagli spagnoli furono risolte con l'introduzione di schiavi africani, una volta eliminati i rari aborigeni e dopo aver saccheggiato il poco oro trovato nell'Isola. Verso la metà del sedicesimo secolo la minaccia crescente di corsari e pirati fece riflettere il

L'Avana: il Castillo de Los Tres Reyes del Morro, progettato dall'italiano Battista Antonelli. Assieme al Castillo de San Salvador de la Punta - realizzato sulla sponda opposta dell'imbocco al canale di accesso alla baia della città - le due fortezze garantirono dal 1610 la sicurezza de "La Habana Vieja".



Suddivisione in province e principali città di Cuba.

governo spagnolo sull'importanza strategica della *Mayor de las Antillas* che si convinse sull'opportunità di convertire L'Avana in una piazza fortificata nella quale riunire ogni anno le due flotte che dovevano salpare assieme verso la Spagna con l'oro e l'argento delle colonie americane.

Sul finire del sedicesimo secolo cominciarono a essere costruiti i primi zuccherifici *(ingenios azucareros)*; la produzione dello zucchero risultò, in misura sempre più marcata, direttrice fondamentale nella storia di Cuba. Questa industria si espanse in maniera significativa verso la fine del diciassettesimo secolo mentre in quegli stessi anni fu avviata quella del tabacco. Da quel momento la struttura della proprietà terriera si caratterizzò per la presenza di estesi latifondi con livelli di produttività molto contenuti.

L'Avana - come piazza fortificata - crebbe di importanza, mentre la Spagna si debilitò a causa di conflitti interni e internazionali, in particolare europei. A Cuba - in un contesto economico di lento sviluppo - si accentuò progressivamente una certa differenziazione nella popolazione tra i funzionari spagnoli e i nati a Cuba, anche se da matrimoni misti, chiamati *naturali* o creoli *(criollos)*.

I cambi introdotti a partire dal regno di Carlo III (1759-1788) contribuirono paradossalmente, assieme alla cosiddetta politica del *despotismo ilustrado*, a causare una maggior differenziazione della colonia rispetto alla metropoli e alla formazione dei precursori della nazionalità cubana nell'ultimo decennio del secolo diciottesimo e la prima parte di quello successivo.

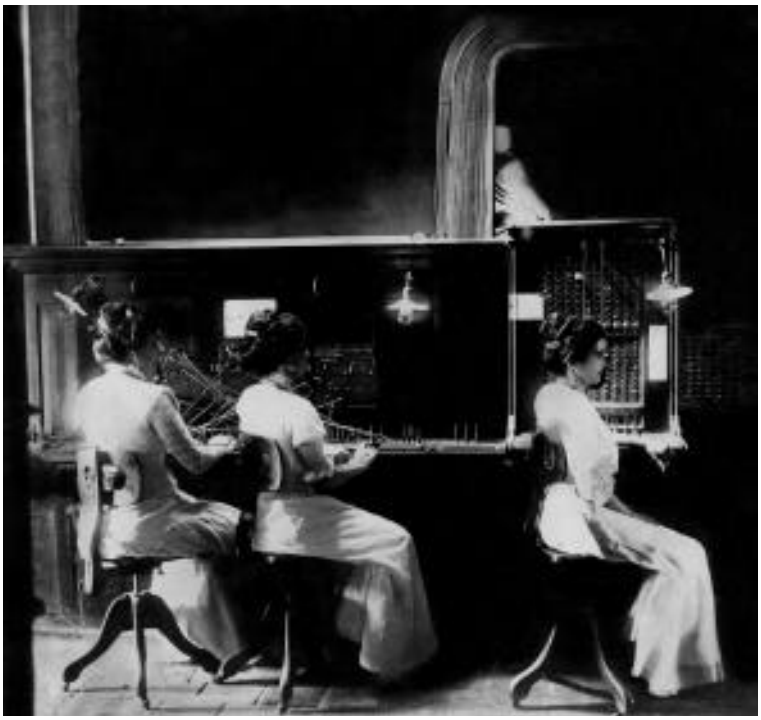
L'evoluzione storica di Cuba continuò su questa direttrice di consolidamento dell'identità nazionale, che si raggiunse definitivamente con le lotte per l'indipendenza dal dominio coloniale e la piena affermazione della coscienza nazionale nel secolo diciannovesimo, a partire dalla "Guerra dei dieci anni", iniziata nel 1868.

Il secolo diciannovesimo risulta quindi caratterizzato da forti contraddizioni da diversi punti di vista, perché si ritrovano insieme, in una coesistenza certamente non pacifica, componenti socio-economiche in contrasto tra loro e difficilmente conciliabili.

Con la schiavitù ancora presente, la struttura della base economica - essenzialmente agricola - mostra ancora segni di una sorta di sopravvissuto feudalesimo che si protende verso un nascente capitalismo con l'introduzione della macchina a vapore negli zuccherifici e lo sviluppo del commercio internazionale di zucchero, tabacco e di altri prodotti.

In questo singolare contesto politico-economico Cuba era spesso all'avanguardia mondiale per le realizzazioni innovative, come le ferrovie e l'illuminazione elettrica, precedendo talora la stessa Spagna.

L'indipendenza cubana da Madrid fu ottenuta, come si è già detto, dopo ben tre guerre, nel 1898 con l'intervento militare degli Stati Uniti. La presenza militare degli Stati Uniti durò solo pochi anni; nel 1902, si instaurò infatti in Cuba la prima repubblica, sotto un controllo spiccato statunitense.



Commutazione manuale all'Avana nei primi anni del Novecento.

Tra il 1902 ed il 1952 si susseguirono una serie di governi - spesso autoritari - sempre sensibili all'in-

fluenza degli Stati Uniti.

Con il colpo di stato del 1952, la dittatura del governo militare di Fulgencio Batista provocò, in un crescente sentimento popolare di forte ripulsa, il rafforzamento del movimento rivoluzionario diretto da Fidel Castro, che trionfò definitivamente il primo gennaio 1959 e che avviò così una nuova era nella vita del Paese.

Con le misure che definirono il carattere democratico-popolare della rivoluzione nella sua fase iniziale - essenzialmente con le grandi nazionalizzazioni realizzate mediante l'esproprio del capitale straniero e dell'oligarchia nazionale - la forma fondamentale della proprietà cubana divenne statale. Allo stesso tempo fu avviato un programma di interventi pubblici orientato fondamentalmente allo sviluppo socio-economico del Paese.

Nell'anno 1961 iniziò una campagna di alfabetizzazione della popolazione che permise di raggiungere questo obiettivo in pochi mesi quasi completamente; per un successivo fenomeno di disuso, il tasso di analfabetismo è oggi del 3,8 per cento nella popolazione con oltre dieci anni. L'accesso a tutti i sistemi di insegnamento è gratuito, con una presenza molto alta di insegnanti ai diversi livelli scolastici. Il Paese dispone ora di ben quindici Università.

Anche nel campo della Salute Pubblica i risultati ottenuti sono molto apprezzabili. I servizi medici sono gratuiti per tutta la popolazione. La vita media è già di 75 anni e l'indice di mortalità infantile ha raggiunto il 7,1 per mille nati, cioè essa è pervenuta a valori di assoluta avanguardia specie se confrontata con quella di altri Paesi dell'America Latina.

Con la caduta del blocco socialista e la disintegrazione dell'Unione Sovietica, l'economia cubana è entrata nel 1990 in una delle crisi più acute della sua storia, per la quasi completa interruzione delle principali relazioni commerciali internazionali: il PIL nel 1993 si è ridotto del 40 per cento rispetto al 1989 (figura 1); la svalutazione del peso cubano rispetto al dollaro ha raggiunto il massimo (130 pesos per un dollaro), la depressione economica è risultata essere assai elevata potendosene apprezzare gli effetti negativi nella scarsità di beni e servizi disponibili nonché nell'inflazione dei prezzi.

Questa situazione di debolezza economica è stata anche esasperata dalla posizione rigida degli Stati Uniti verso Cuba attraverso misure restrittive - diverse e onerose - per gli scambi reciproci, iniziate fin dal 1960 e oggi ancora presenti con numerose leggi, ben note a livello internazionale.

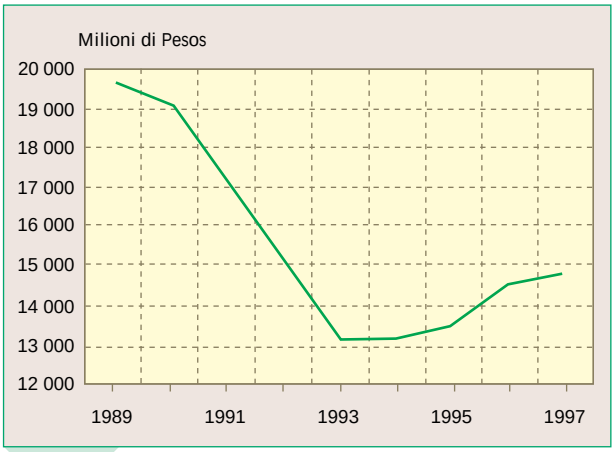


Figura 1 *Variazione, a prezzi costanti, del prodotto interno lordo negli ultimi anni.*

A partire dal 1994 sono state adottate un serie di riforme per adattare l'economia cubana alla nuova realtà internazionale.

È cominciato così un lento processo di recupero che continua tuttora, con una crescita media annua del PIL di circa il 3 per cento, in un quadro di miglioramento macroeconomico generale, specialmente nei settori dei servizi e in quello manifatturiero.

Tra le principali riforme adottate negli ultimi anni occorre segnalare il riconoscimento di altre forme di proprietà (oltre quella statale); l'apertura del mercato nazionale agli investimenti stranieri (attraverso società miste); l'autorizzazione all'uso del dollaro degli Stati Uniti d'America; l'istituzione del "peso cubano convertibile" (con cambio paritetico, 1:1, con il dollaro); la riforma del sistema bancario; la possibilità di iniziative commerciali private entro dimensioni contenute; la riorganizzazione dell'appara-

La sala operatrici dell'Avana nel 1920.

Posa a Cuba di un cavo sottomarino all'inizio degli anni Venti.

to statale attraverso una massiccia riduzione di enti e un significativo decentramento in particolare per le imprese statali.

In questi anni si è assistito infine a una sensibile e continua crescita del turismo con un apporto vitale di valute pregiate all'economia nazionale. Si prevedono due milioni di turisti nel Duemila e quattro milioni nel 2007.

Le prospettive economiche a medio termine prevedono un ridimensionamento dell'industria zuccheriera compensato da significative crescite in altri settori, e in particolare il turismo, l'estrazione del nichel e le biotecnologie.

3. Lo sviluppo delle telecomunicazioni cubane

La nascita della telefonia cubana si colloca storicamente ai primi posti a livello internazionale, indipendentemente dall'essere stata L'Avana sede dell'invenzione di Meucci nell'ormai lontano 1849: infatti, nello stesso anno 1877 in cui si realizzava in Boston il primo collegamento telefonico tra due edifici distanti tra di loro, si svolse all'Avana la prima comunicazione telefonica in lingua spagnola. Solo l'anno successivo, nel 1878, si iniziarono le prove a Madrid - con apparecchi trasferiti da Cuba - negli stessi anni in cui venivano effettuate le prime, timide prove in un numero limitato di importanti capitali e di altre città europee.

Tra il 1877 e il 1881 la telefonia cubana, come avveniva peraltro in altri Paesi all'avanguardia, visse un periodo di prime prove e di un numero limitato di installazioni con apparecchi importati dagli Stati Uniti, in una percezione ancora debole sull'importanza che di lì a poco il nuovo servizio avrebbe avuto nello sviluppo delle comunicazioni, sostituendosi e migliorando sensibilmente quello telegrafico, introdotto sperimentalmente nell'Isola nel 1851 e avviato regolarmente a partire dal 1853 con una linea tra la Capitale e Bejucal.

La nascita del servizio telefonico pubblico a Cuba avvenne nel 1881, lo stesso anno dell'Italia (figura 2): il 30 giugno di quell'anno l'asta pubblica per questo servizio all'Avana fu aggiudicata all'unico concorrente V.F. Butler, residente in città, domiciliato al numero 1 di Calle Mercader, rappresentante per Cuba di una società statunitense. Il 21 dicembre dello stesso anno la rete telefonica della Capitale presentava un'estensione di 23 km e aveva già settantotto clienti.

Nel marzo del 1882 la *Compañía Telefónica de Cuba* (ufficialmente *Compañía Eléctrica de Cuba)* dichiarò di avere centodieci apparecchi in funzione con prospettive di un rapido sviluppo e con ottimi risultati economici. Nel 1883 la rete dell'Avana risultava costituita da 600 km di linee e da 450 apparecchi in servizio con 1500 chiamate giornaliere instradate dall'unica centrale di commutazione manuale.

Nel 1895 alla compagnia di Butler si sostituì la Società denominata *Red Telefónica de La Habana*,

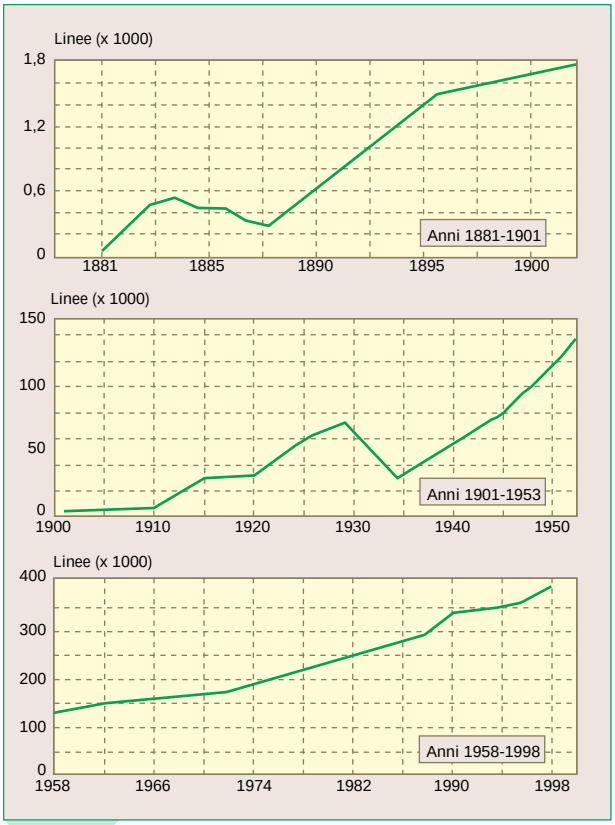


Figura 2 *Crescita negli anni delle linee telefoniche.*

L'Avana. Vista parziale della città; al centro della foto l'Hotel Nacional (uno degli edifici più noti di Cuba), realizzato negli anni Trenta in art-déco, si affaccia sull'Oceano.

mentre veniva introdotto un servizio in poche altre città, fornito solo localmente, senza possibilità quindi di interconnettere tra loro queste aree urbane.

Nel 1909 fu concessa dal Capo dello Stato un'autorizzazione a tempo indefinito all'esercizio del servizio in tutta l'Isola, compresa l'interconnessione per i collegamenti di lunga distanza nazionale, alla *Cuban Telephone Company*, Società costituita negli Stati Uniti.

Con la *Cuban Telephone Company* lo sviluppo della telefonia acquistò nuovo slancio sull'intera Isola. Nel 1910 fu inaugurato il servizio nazionale e fu installata all'Avana una centrale automatica Strowger tra le prime al mondo[1]. Nel 1915 questa centrale risultò tra le prime otto a livello mondiale con oltre diecimila linee installate.

Nel 1916 la *Cuban Telephone Company* e la *American Telephone and Telegraph Company (AT&T)* dettero vita alla *Cuban-American Telephone and Telegraph Company* con l'obiettivo di collegare le due reti nazionali con un cavo sottomarino: fu realizzata così una rete telefonica internazionale che costituì un altro primato a livello mondiale. Il cavo fu rapidamente posato tra Key West e L'Avana; esso presentava una lunghezza di 195 km (un vero record per l'epoca) e scendeva fino alla profondità di 1.800 metri. Il servizio fu inaugurato l'11 aprile 1921, data memorabile nella storia delle comunicazioni telefoniche internazionali in quanto furono interconnesse in quel giorno l'isola di Santa Catalina in California con L'Avana, mediante un collegamento, lungo complessivamente 8.800 km, realizzato con un cavo sottomarino, terminato con linee aeree e interrate e con una tratta radio. Altri cavi sottomarini furono successivamente posati lungo lo stesso percorso tra la Florida e L'Avana; nel 1950 furono immersi gli ultimi due cavi, tecnologicamente avanzati perché impiegavano, per primi e con successo, ripetitori dei segnali telefonici sommersi a grandi profondità.

Tra il 1953 e il 1957, per difficoltà operative, la *Cuban Telephone Company* interruppe l'installazione di nuove linee. Il Governo Rivoluzionario instaurato a Cuba il primo gennaio 1959 nazionalizzò ben presto la *Cuban Telephone Company* (il 6 agosto 1960), e costituì, nell'ambito del Ministero delle Comunicazioni, la *Empresa Telefónica "13 de Marzo"*.

Nel 1972 iniziò una fase di frammentazione strutturale: l'Impresa unica nazionale *13 de Marzo* fu sostituita dalle *Direcciones Provinciales de Comunicaciones*. Nel 1976 il quadro organizzativo divenne maggiormente complesso, risultando composto rispettivamente da: quattordici *Empresas Integrales de Comunicaciones Provinciales*, cinque *Empresas Especializadas* e una *Unidad Presupuestada*. Nel 1989 si aggiunse infine la *Sociedad Mercantil Privada para las Telecomunicaciones Internacionales (INTERTEL)*.

Dopo una fase di sviluppo piuttosto limitata nel primo decennio, si è assistito ad una crescita annuale della densità telefonica più elevata tra il 1972 e il 1982 (3,58 per cento) e nuovamente più contenuta nel decennio successivo (2,26 per cento). Nel 1973 fu attivata la stazione terrena satellitare di Caribe, a circa 30 km dall'Avana (che inizialmente impiegava il sistema Intersputnik). Nel periodo compreso tra il 1976 e il 1980 fu realizzata la rete nazionale di lunga distanza in cavo coassiale.

Nel 1990, in collaborazione con l'Italcable, furono istallate cinque stazioni mobili satellitari collegate al sistema Intelsat.

4. Avvio della fase presente (1994-1997)

Dal 1994 il quadro delle telecomunicazioni cubane si è di molto semplificato: il 17 agosto di quell'anno, con il Decreto 190 del Consiglio dei Ministri, il Governo Cubano ha emesso la Concessione Amministrativa in favore di *ETECSA (Empresa de Telecomunicaciones de Cuba S. A.)*, per la gestione dei principali servizi pubblici di telecomunicazioni, a eccezione, in particolare, del servizio di radiotelefonia cellulare concesso il 22 gennaio 1992 all'Impresa CUBACEL.

ETECSA realizza con propri tecnici la maggior parte degli impianti.

Nel periodo compreso tra il 1994 e l'inizio del 1997 il principale obiettivo di ETECSA, in un quadro di

(1) *In Italia la prima centrale automatica realizzata dalla Siemens, con 2 mila linee, fu messa in servizio nel 1913 a Roma Prati.*

	1996	*1997*	*1998*	*1999*	*2004*
Linee in servizio (per mille)	354,9	370,8	409	460	1.060
Tasso di numerizzazione (%)	11	18,3	36,7	46,4	85
Densità telefonica (%)	3,4	3,5	3,9	4,4	9,4
Telefoni pubblici* (per mille)	4,73	5	7,1	12,3	56

** A scheda e moneta*

Tabella 1 *Andamento dei principali indicatori della telefonia di base.*

livelli degli investimenti ancora ridotti e di una crescita assai limitata, ha riguardato il recupero della qualità del servizio telefonico *(detener el deterioro)*.

Un forte impulso operativo è stato impresso a ETECSA nel febbraio 1997, quando è stata semplificata la costituzione azionaria dell'Impresa risultando *STET International Netherlands* l'unico socio straniero tra i quattro che compongono l'Impresa e con un sensibile aumento della quota di partecipazione, che ora è del 29,29 per cento (figura 3).

Il 14 maggio 1997 è stato approvato dal Consiglio di Amministrazione di ETECSA il Piano di Sviluppo poliennale *(Plan de Expansión, Modernización y Económico-Financiero 1997-2007)*, che ha richiesto l'aggiornamento del precedente Decreto N.190 mediante la promulgazione del Decreto N. 221 del 28 luglio 1997.

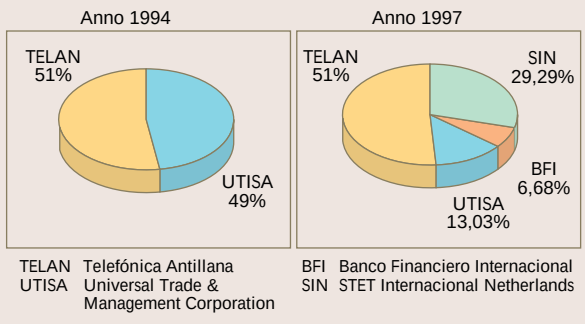


Figura 3 *Suddivisione azionaria di ETECSA nel 1994 e nel 1997.*

5. Piani e prospettive future di ETECSA

In un quadro generale di compatibilità economiche e finanziarie e con il soddisfacimento degli obiettivi di qualità del servizio indicati nel nuovo Decreto 221, il Piano Poliennale di ETECSA prevede per i prossimi anni obiettivi significativi di sviluppo e di modernizzazione per le telecomunicazioni cubane. Nella tabella 1 sono riportati i principali risultati pianificati per gli anni 1999 e 2004 per la telefonia di base, e sono confrontati questi dati con i valori a consuntivo degli anni precedenti.

Nel 1998 è stata attivata la rete di trasmissione dati (riquadro di pagina 12, figura A), mentre l'apertura alla rete Internet avverrà nel corso del 1999. Da notare che l'accesso Internet è già disponibile da alcuni anni per un numero limitato di clienti, quasi tutti relativi a istituti scientifici e concentrati all'Avana. È previsto inoltre l'avvio della rete intelligente e della ISDN dal Duemila.

Il Piano poliennale di ETECSA è quindi caratterizzato da un sensibile sforzo indirizzato alla sostituzione nei primi anni delle centrali analogiche obsolete (in particolare nel triennio 1997-99), seguito in quelli successivi da un altrettanto significativo incremento della rete di accesso e in conseguenza dell'utenza (tabella 2). Il piano per la progressiva numerizzazione degli autocommutatori è mostrato nella figura B del riquadro di pagina 12.

Centrale trasmissiva di San Antonio de los Baños.

Anche per la telefonia pubblica è previsto un sensibile sviluppo negli anni finali del Piano, mentre la sostituzione degli apparecchi a moneta oggi in servizio sarà attuata tra il 1999 e il 2000.

È stata introdotta nel corso del 1998 la telefonia pubblica a scheda in misura significativa con 1.800 apparecchi disponibili a fine anno. Nel campo della rete nazionale di lunga distanza tra il 1997 ed il 1998 è stata installata la dorsale nazionale in ponte radio *(Red Nacional de Microondas)* in sostituzione dei sistemi trasmissivi obsoleti su cavi coassiali (figura C del riquadro di pagina 12).

Nel 1999 sarà avviata l'installazione della dorsale nazionale con portanti ottici; lo sviluppo completo di questa rete, che prevede vari anelli, sarà di circa 3 mila chilometri (figura D del riquadro di pagina 12).

Oltre alla telefonia pubblica a schede prepagate e

	1997	*1998*	*1999*
Linee numeriche (per mille)	39,8	108,1	88,3

Tabella 2 *Linee numeriche messe in servizio di recente o in corso di installazione.*

AMMODERNAMENTO DELLE TELECOMUNICAZIONI CUBANE

Figura A

Sviluppo attuale della rete di trasmissione dati.

Figura B

Piano per la numerizzazione delle centrali.

Figura C

Rete nazionale di trasporto SDH in ponti radio.

Figura D

Rete nazionale di trasporto in fibra ottica che sarà completata entro il 2004.

alla rete nazionale trasmissiva su ponti radio, il 1998 è da considerare "storico" per ETECSA in quanto in quest'anno è stata attivata anche la rete nazionale di trasmissione di dati *(Cubadata)* e l'indice di numerizzazione ha compiuto, come già riportato in tabella 1, un balzo di quasi il 20 per cento.

Con la numerizzazione degli autocommutatori e dei collegamenti trasmissivi è stata definita la nuova struttura della rete. Uno schema della rete regionale è riportato in figura 4.

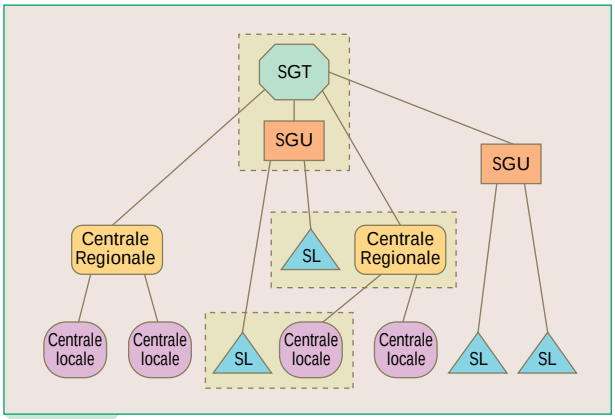


Figura 4 *Struttura della rete regionale al 2004.*

I collegamenti internazionali di ETECSA risultano ancora realizzati quasi interamente via satellite, attraverso la stazione terrestre di Caribe, collocata a pochi chilometri dall'Avana. Restano solo alcune decine di circuiti in cavo sottomarino con gli Stati Uniti. Sono perciò in corso di valutazione alcune ipotesi di collegamento in cavo ottico sottomarino, che possano assicurare una seconda via di collegamento internazionale di maggiore potenzialità terminata a Cuba (paragrafo 6).

La coesistenza in Cuba, dal punto di vista monetario, del dollaro USA e del peso cubano, comporta per ETECSA due conseguenze: anzitutto la presenza di clienti per i quali la fatturazione è effettuata in dollari (circa il 5,5 per cento) e di altri clienti la cui tassazione è in pesos cubani (circa il 94,5 per cento); in secondo luogo la necessità per l'Impresa di gestire una doppia amministrazione per le due monete circolanti.

	1996	*1997*	*1998*	*1999*
Milioni di dollari	29	98	123	130*

** Valore previsto*

Tabella 3 *Investimenti di ETECSA negli ultimi anni.*

Gli investimenti (tabella 3) sono quasi esclusivamente in dollari. Dopo un lungo periodo di livelli di investimento molto contenuti per le telecomunicazioni cubane il 1997 è stato il primo anno che ha presentato una significativa ripresa, con prospettive analoghe per il breve-medio termine. Nel quadriennio 2000-2004 sono previsti investimenti per 550 milioni di dollari.

Figura 5 *Il progetto Nautilus con sistemi trasmissivi in cavo sottomarino.*

6. Il progetto "Nautilus"

Il rafforzamento dei collegamenti internazionali della rete pubblica cubana prevede di collegare Cuba ai Paesi limitrofi con uno o più sistemi trasmissivi in cavo sottomarino realizzati in fibra ottica. Il *Progetto Nautilus* (figura 5) si inserisce in questo contesto ed è interessante per almeno due motivi: anzitutto esso è un progetto di ETECSA e in secondo luogo la sua concezione risulta innovativa e complementare con quella di altri progetti che interessano l'area caraibico-centroamericana.

Il Progetto Nautilus è stato ufficialmente presentato e discusso all'Avana il 22 e 23 luglio 1998 con la partecipazione esterna di rappresentanti delle Società di telecomunicazioni di Haiti, Porto Rico, Repubblica Dominicana e Messico, oltre che di Telecom Italia e di France Télécom.

La lunghezza complessiva del cavo sarà di circa 3 mila km. Tre diramazioni sono previste nel Paso de Los Vientos. Il progetto, il cui costo totale è di circa 100 milioni di dollari, prevede cavi che contengono due coppie di fibre, ciascuna progettata per una velocità massima di cifra di 10 Gbit/s.

Uno dei sessanta "Caddy-Phone" installati di recente a Cuba.

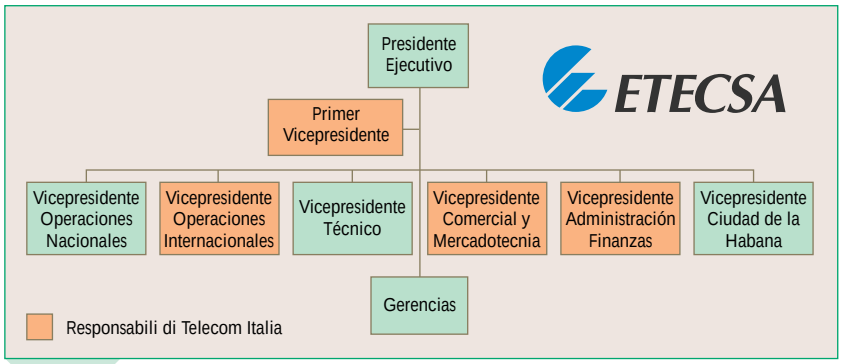


Figura 6 *Struttura organizzativa di ETECSA.*

7. La presenza di Telecom Italia

Telecom Italia, come è già stato anticipato, è presente in ETECSA attraverso *SIN (STET International Netherlands)*. Nel Consiglio di Amministrazione il Presidente è italiano ad anni alterni, mentre sei dei dodici consiglieri sono scelti dal Gruppo Telecom Italia. Nella Direzione Esecutiva dell'Impresa (figura 6), al Presidente esecutivo, che per Statuto è cubano, si affianca il *Primer Vicepresidente*, scelto da Telecom Italia, con ampi poteri statutari che riguardano la supervisione ed il coordinamento delle Vicepresidenze, nonché poteri abbinati con il Presidente esecutivo per tutti gli impegni di spesa eccedenti i 200 mila dollari. Tre delle sei Vicepresidenze operative sono affidate a responsabili italiani e ognuna delle altre tre Vicepresidenze è affiancata da un Direttore aggiunto di nomina italiana. Completano il quadro dei rapporti con il Gruppo Telecom Italia in ETECSA la vigenza di un contratto generale di assistenza tecnica da parte di *SIN (Technical Assistance Agreement)* e l'assistenza specifica in alcuni *progetti speciali* (quali quelli relativi a fatturazione, gestione clienti, contabilità, logistica, gestione della rete, pianificazione della rete, organizzazione aziendale).

8. Conclusioni

Le telecomunicazioni cubane si trovano oggi in una fase avanzata di sviluppo e di ammodernamento, specie se confrontata con la situazione degli altri servizi pubblici. In una prospettiva di breve–medio termine il mercato interno cubano si presenta molto promettente e in esso le telecomunicazioni dovranno svolgere il ruolo propulsore che spetta all'infrastruttura di maggior pregio per il sistema socio-economico del Paese.

La posizione di Cuba nell'area caraibico-centroamericana e le sue ampie valenze ambientali e culturali completano questo quadro promettente sullo sviluppo dell'Isola, riportandola, per la sua naturale collocazione geografica, a nodo strategico di primaria importanza nel mondo americano.

Scheda telefonica prepagata di ETECSA.

Ringraziamenti

L'autore ringrazia particolarmente gli amici e colleghi cubani che hanno fornito ausilio nella preparazione di questo articolo: Patricia Soler Silva, José Altshuler, José A. Sánchez, Juan M. Villanueva, Carlos Núñez e José A. Roche.

Bibliografia

[1] Catania, B.: *Antonio Meucci - L'inventore e il suo tempo - Da Firenze a L'Avana.* Edizioni SEAT, Torino, 1994.

[2] Catania, B.: *Antonio Meucci - L'inventore e il suo tempo - New York 1850-1871.* Edizioni SEAT, Torino, 1996.

[3] Gonzàlez Royo, M.: *Comienzos del teléfono en la Habana.* Academia de Ciencias de Cuba, conferencias y estudios, n. 52, La Habana, mayo 1983, p. 31.

[4] Altshuler, J.: *Las Telecomunicaciones en Hispanoamérica. Pasado, presente y futuro. Cuba.* AHCIET, Asociacion Hispanoamericana de Centros de Investigacion y Empresas de Telecomunicaciones, Madrid, 1993, pp. 73-88.

[5] Pillado Ortiz, J.M. et alii: *ibidem, España.* pp. 159-160.

[6] Cuban Telephone Co.: *El servicio telefónico fiel reflejo del progreso nacional.* En: "Libro de Cuba", Talleres Litográficos de Artes Gráficas, 30 de junio de 1954.

[7] Hernández, O.: *Cresce il recupero dell'economia cubana.* En: Business Tips on Cuba (in italiano), vol. 5, n. 11, novembre 1998.

Domenico Capolongo si è laureato in ingegneria elettrotecnica presso l'Università di Napoli nel 1962. In SET, poi SIP, quindi Telecom Italia dal 1963 al 1997. Dal 1997 opera in ETECSA. Tra gli incarichi ricoperti si ricordano quelli di: responsabile delle centrali in Puglia e in Campania/Basilicata, della pianificazione della rete in SIP, della pianificazione e programmazione della rete in Telecom Italia; assistente tecnico del Presidente in Entel Bolivia; Primer Vicepresidente in ETECSA. È stato docente di Telefonia e Traffico presso il Politecnico di Napoli dal 1975 al 1979. Domenico Capolongo è anche autore di una ampia letteratura tecnica, scientifica e letteraria.

Il commercio elettronico: prospettive di sviluppo, tecnologie abilitanti e impatti sui Telecom Operator

Natalino Curci
Domenico Zappi

Il commercio elettronico è ormai una realtà: esso modifica infatti non solo i canali commerciali tradizionali e la gestione operativa delle aziende, ma soprattutto incide sulle loro strategie di business. In questo senso, il panorama italiano, ma più esplicitamente il case study (Amazon) presentato in questo articolo, mostra come il commercio elettronico non sia più solo un'opportunità di vantaggio competitivo, ma una vera e propria dimensione di business da acquisire per non essere estromessi dal mercato e per non perdere la "tradizionale" clientela. La disponibilità di un'infrastruttura universale capace di seguire on-line l'intero ciclo - dalla produzione alla vendita e fino alla consegna al cliente finale - trasforma l'intera natura dei prodotti e dei servizi portando ad una riorganizzazione globale del mercato. Il commercio elettronico realizza così un nuovo paradigma di business: quello della Internet Economy, abilitata e garantita da un insieme di nuovi elementi tra i quali spiccano nuovi ruoli aziendali; l'interoperabilità globale di reti e di protocolli eterogenei; l'applicazione di standard di sicurezza sempre più evoluti; l'adozione di nuovi mezzi di pagamento via rete, semplici e sicuri; la definizione di nuove figure di intermediari "fiduciari" delle transazioni. Un insieme dunque di tecnologie, processi e strategie di mercato capace di incidere fortemente anche sui gestori delle reti di telecomunicazione, i Telecom Operator: il commercio elettronico è, infatti, nella sua generalità, connesso strettamente allo sviluppo di Internet che si pone come contesto prevalente di riferimento abilitante a nuove opportunità di business legate all'applicazione di nuovi modelli di partnership, alla revisione delle tradizionali politiche di pricing, all'offerta di soluzioni infrastrutturali Intranet/Extranet, nonché alla definizione di nuovi rapporti con gli ISP (Internet Service Provider).

Questo scenario spinge i Telecom Operator verso un generale riposizionamento di business che consenta la transizione dall'offerta tradizionale di servizi di trasporto delle informazioni ad un'offerta innovativa di servizi Internet, Intranet ed Extranet, secondo una logica d'integrazione e di sinergie complessive.

1. Introduzione

Nel corso degli anni si è assistito a una mutazione costante della rete Internet, che da mezzo per la comunicazione si è via via trasformato in un media di promozione e informazione, quindi in strumento di cooperazione, fino ad arrivare alle attuali applicazioni di commercio elettronico e di scambio di documenti con validità legale in rete.

Quest'ultima dimensione tende a definire Internet come luogo ideale nel quale sviluppare nuovi modelli commerciali destinati a produrre mutamenti profondi nei rapporti tra fornitori, clienti e acquirenti. Lo sviluppo di questi modelli è favorito dalla disponibilità di nuove tecnologie in grado di fornire le funzionalità necessarie allo svolgimento di transazioni sicure in rete.

In questo scenario il Commercio Elettronico rappresenta un nuovo canale commerciale che offre alle aziende l'opportunità di "aprire" un negozio virtuale, attraverso cui è possibile eliminare la distanza fisica tra le parti contraenti sia in un contesto *Business-to-Business* (tra azienda e azienda) sia *Business-to-Consumer* (tra azienda e cliente finale), avvalendosi delle modalità di comunicazione rese disponibili da Internet.

Il commercio elettronico rimuove qualsiasi vincolo geografico e di tempo tra fornitore e cliente e si basa su una comunicazione che riduce attriti - in costi e flussi informativi - delle tradizionali catene di vendita.

In definitiva si raggiunge un bacino di potenziali clienti molto più ampio ed a costi di infrastruttura sensibilmente più contenuti.

Di rilievo sono le implicazioni, non solo sulla Società, ma anche sulle aziende, in termini sia di ottimizzazione della gestione operativa, sia di business. Basti pensare che il mercato virtuale sul WWW consente al consumatore l'accesso a beni ed a servizi senza limitazioni geografiche, temporali o stagionali. Con un semplice "click" si può infatti accedere dal proprio domicilio, a qualsiasi ora del giorno e della notte, a un volume di beni e servizi praticamente illimitato. Analoga logica può essere estesa nei rapporti clienti-fornitori interni di qualsiasi azienda.

	1996	*1997*	*1998*	*1999*	*2000*	*2001*
Consumer	1	6	21	70	194	475
Business	2	6	24	95	308	905
Totale	3	12	45	165	502	1380

Fonte: IDC

Tabella 1 *Commercio elettronico su Internet: suddivisione del mercato italiano tra clienti affari e residenziali (in milioni di dollari).*

Ma i vantaggi travalicano queste considerazioni; soprattutto per le aziende, conseguenze di rilievo hanno, infatti, la riduzione dei costi di distribuzione, il miglioramento del customer service, la riduzione del "time to market", l'incremento della soddisfazione del cliente e la possibilità di mantenere con lo stesso un contatto diretto. Sono naturalmente evidenziate le possibilità offerte dalla rete di fornire in modo semplice e strutturato tutte le informazioni di vendita sui singoli prodotti e le possibilità offerte dall'interattività di dialogare con il cliente in modo da offrire un servizio ritagliato sulle sue particolari necessità.

Tutti questi servizi non sono più oggi una prerogativa solo di società di grandi dimensioni, con reti di vendita e di assistenza assai distribuite, ma possono essere gestiti - con grande facilità ed a costi estremamente contenuti - anche da piccole e medie aziende, nei confronti delle quali anche la Commissione Europea sta mostrando un crescente sensibile interesse.

2. I settori di mercato

Nel mondo del commercio elettronico è possibile distinguere due diverse aree di mercato che presentano caratteristiche proprie sia dal punto di vista del rapporto tra venditore e acquirente sia per le conseguenze realizzative che da esso derivano. Si delineano così due modelli: il modello *Business to Business* e quello *Business to Consumer.*

Il modello *Business to Business* presenta alcune caratteristiche peculiari quali:

- generalmente, acquirente e venditore, si conoscono a priori;
- sono già consolidati i rapporti con banche e *delivery carriers*, per modalità di pagamento e trasporto;
- è richiesta l'integrazione con i sistemi informativi esistenti *(legacy)* attraverso progetti ad hoc.

Il modello *Business to Consumer* è caratterizzato a sua volta dai seguenti fattori:

- gli acquirenti, in genere, non sono conosciuti a priori da chi vende;
- possono essere proposte modalità di pagamento ad hoc (ad esempio on-line via carta di credito/debito, micropagamenti);
- l'ordine è gestito - almeno nella fase di avvio - indipendentemente dall'integrazione con i sistemi informativi esistenti (la gestione separata presenta elementi di maggiore semplicità soprattutto per cataloghi non molto ampi);
- sono necessari meccanismi di consegna ad hoc (on line per beni *digitali*, servizi di consegna addizionali per il recapito di *beni materiali*).

Queste considerazioni portano a una diversa focalizzazione in termini di servizi in funzione dello specifico settore di mercato: nel *Business to Business* si ha perciò una maggiore attenzione alla fase architetturale e di progettazione; nel *Business to Consumer* si ha invece una maggiore considerazione per la gestione delle problematiche di pagamento e di consegna e per la gestione legata ai problemi della distribuzione.

	1996	*1997*	*1998*	*1999*	*2000*	*2001*
Consumer	1	6	20,6	70,1	194,4	475
Piccole imprese[1]	0	0,2	2,4	14,2	58,5	206,2
Medie e grandi imprese	2	5,3	20,5	74,8	221,7	591,8
Pubblica Amministrazione[2]	0	0,1	0,5	3,3	12,3	62,8
Istruzione *(Education)*	0	0,1	0,7	2,4	15,4	44,8
Totale	3	11,7	44,7	164,8	502,3	1380,6

1) Meno di 100 dipendenti
2) Centrale e locale

Fonte: IDC

Tabella 2 *Commercio elettronico su Internet: mercato italiano (in milioni di dollari).*

In Italia, lo spaccato del mercato tra i clienti *Consumer* e quelli *Business* interessati al Commercio Elettronico su Internet è indicato nella tabella 1.

La suddivisione delle spese tra Consumer, imprese, pubblica amministrazione locale e centrale e istituti di formazione e didattica è riportato nella tabella 2.

A livello di definizione dei nuovi business, connessi al commercio elettronico, risulta rilevante l'analisi dei settori che, oggi ed in un'ottica futura,

possono risultare maggiormente predisposti a introdurre il commercio elettronico in Internet nel *Business to Consumer;* nella tabella 3 si riporta a questo proposito, la previsione EITO '97 relativa al mercato italiano di prodotti e servizi commercializzati attraverso Internet (espressa in valore percentuale rispetto al totale annuo).

	1997	*1998*	*1999*	*2000*	*2001*
Computer e software	28,5	25,6	22,3	19,2	16,0
Vendita al dettaglio[1]	16,1	15,5	15,0	14,5	14,0
Servizi finanziari	3,6	3,5	3,3	3,2	3,0
Materie prime	5,7	7,0	8,3	9,7	11,0
Comunicazione ed informazione	9,8	10,0	10,0	10,0	10,0
Turismo	5,2	5,1	4,7	4,3	4,0
Servizi professionali	16,6	18,5	20,3	22,2	24,0
Pubblicità	11,9	11,7	12,3	12,7	13,0
Altro	20,6	3,1	3,7	4,3	5,0
Totale	100,0	100,0	100,0	100,0	100,0

1) Quali, ad esempio, i prodotti per la casa e per il tempo libero. *Fonte: Eito '97*

Tabella 3 *Previsione dello sviluppo percentuale annuo dei prodotti e dei servizi commercializzati mediante Internet in Italia.*

Più in generale, la figura 1 mostra una crescita potenziale del commercio elettronico tale da giustificare l'elevata attenzione di aziende e settori pubblici per questa tematica.

3. Il commercio elettronico in Italia

Il profondo cambiamento, stimolato dal commercio elettronico e guidato dall'evoluzione e dalla diffusione delle tecnologie informatiche e delle telecomunicazioni, determina un contesto nel quale la localizzazione geografica non rappresenta più una barriera per lo sviluppo di cultura e di opportunità di business. Esso rappresenta il "villaggio globale" dei servizi on-line.

La realizzazione della Società dell'Informazione coinvolge in modo orizzontale i diversi settori della vita economica e sociale del nostro Paese interessando in particolare il nostro sistema industriale e produttivo, il commercio, i servizi pubblici ed i rapporti fra le imprese e la Pubblica Amministrazione. L'Italia può partecipare all'evoluzione di questi fenomeni o può assistervi, e in qualche modo subirli, con evidenti rischi di marginalizzazione; il ruolo che il nostro Paese dovrà svolgere, dipenderà dalla capacità di gestire il cambiamento con il contributo di tutte le parti politiche, sociali ed economiche.

Risulta quindi avere una valenza strategica per l'Italia il ruolo delle tecnologie dell'informazione e della comunicazione, assegnando a esse un'adeguata priorità in termini di attenzione e di risorse. Infatti, le ricadute per l'intero sistema economico, finanziario e produttivo sono evidenti laddove tali tecnologie - e la capacità di gestirle - condizionano lo sviluppo di nuove opportunità di business, l'allocazione delle risorse e delle infrastrutture produttive, l'accesso e la presenza nei mercati. Tutti i settori industriali e del terziario sono pertanto interessati da tale sviluppo. Nel quadro generale sopra descritto il commercio elettronico è considerato, anche a livello governativo, tra gli elementi chiave capaci di spingere la crescita del sistema economico del Paese. Tuttavia, a tutt'oggi, l'avanzamento del commercio elettronico, l'*e-commerce*, appare in Italia ancora in uno stato embrionale.

Sono infatti disponibili solamente una settantina di siti italiani dedicati a questo scopo. Solo una minima parte di utenti ha dichiarato di avere effettuato almeno un acquisto *on-line* e l'andamento alterno degli accessi *consumer* fa presumere che ancora per qualche tempo il commercio elettronico occuperà una posizione marginale per l'Internet del nostro Paese.

Analisi recenti mettono in luce tuttavia uno spiccato interesse dal lato dell'offerta: su mille aziende italiane, appartenenti ad alcuni settori nell'area del commercio, dei servizi e dell'industria il 14 per cento ha dichiarato di avere da tempo avviato progetti specifici sul commercio elettronico e il 25 per cento ha pianificato un intervento nel biennio 1998-99.

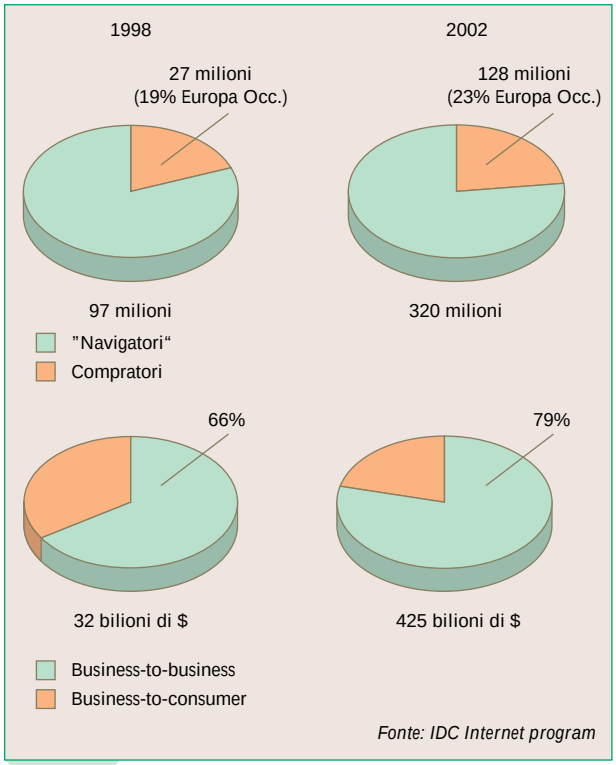


Figura 1 *Evoluzione del mercato mondiale della diffusione del commercio elettronico.*

La maggiore attenzione dimostrata dal lato dell'offerta rispetto a quello della domanda può essere spiegato in diversi modi: barriere culturali, paura dell'insicurezza delle transazioni, mancanza di interazione con il venditore. Inoltre, per il caso italiano, "la navigazione" sulla rete mette in evidenza una disponibilità di categorie di beni ancora assai limitata e, spesso, associata a prodotti di basso valore. Sul ritardo italiano influiscono poi anche problemi connessi agli elevati costi di spedizione che, determinando un differenziale di prezzo, non favoriscono l'utilizzo del mezzo elettronico per l'acquisto degli oggetti di interesse.

Dal lato dell'offerta i giudizi sull'utilità di alcune forme di servizi e di commercio via rete implicano la vendita diretta, la possibilità di trovare nuovi fornitori e di ordinare prodotti, l'accesso e le operazioni sui mercati finanziari, la movimentazione su conti correnti, l'acquisto di beni vari.

Le analisi svolte dalla Commissione Europea (DGXIII) mettono tuttavia in luce, anche per il nostro Paese, le potenzialità del commercio elettronico associate a una diffusione progressiva per i prossimi anni. Alcune stime effettuate dalla DGXIII mostrano una crescita del fatturato complessivo negli Stati Uniti di circa 139 miliardi di ECU nel 2001 a fronte di una crescita prevista per l'Europa di circa 23,4 miliardi di ECU.

4. Case study

In questo panorama spicca il caso di una realtà americana (Amazon) che è sicuramente l'emblema delle potenzialità connesse allo sviluppo del commercio elettronico.

Amazon è una società statunitense, costituita con l'obiettivo di realizzare un modello di business centrato sul commercio elettronico e, in particolare, sulla vendita di libri attraverso la rete Internet. La società, nata nel 1994, ha iniziato la propria attività commerciale nel luglio del 1995, attraverso il web Internet (www.amazon.com).

Per avere un elemento di paragone per valutare la prestazione economica di questa esperienza è utile il confronto con Barnes & Noble, la maggiore catena di librerie statunitense, basata fino a poco tempo fa su un modello di vendita tradizionale. Il confronto tra i fatturati delle due società (la prima, Amazon, nata da poco e la seconda, Barnes & Noble, consolidata da molti anni su mercato) consente di rilevare alcuni dati di interesse (tabella 4).

Come è rilevabile dai dati della tabella, nel 1996 le vendite di Amazon rappresentavano meno dell'1 per cento del fatturato Barnes & Noble, ma già l'anno successivo salivano al 5 per cento e nel 1998 il rapporto dovrebbe essersi attestato intorno al 20 per cento.

Non siamo quindi di fronte al semplice fenomeno di crescita esplosiva tipico di nuove iniziative tecnologiche di piccola capitalizzazione *(small cap)*, ma alla conquista da parte di una nuova società di una considerevole porzione di mercato di un prodotto maturo, grazie alla tecnologia del commercio elettronico.

Le chiavi di questo successo sono quelle tipiche con cui è "venduto" il vantaggio competitivo del commercio elettronico nei confronti della rete di vendita tradizionale: costi più contenuti (che in parte si trasformano in sconti per i clienti), maggiore facilità e potenza per gli utilizzatori del servizio (il web Amazon consente, tra l'altro, ricerche non effettuabili in una libreria tradizionale, avvisi sulla pubblicazione di un nuovo libro interessante; suggerimenti; commenti dei clienti per ogni volume).

Che il commercio elettronico non sia più solo un'opportunità di vantaggio competitivo, ma una vera e propria necessità per non essere emarginati dal mercato, devono averlo percepito anche alla Barnes & Noble che da alcuni mesi ha aperto un web di vendita su Internet (www.barnesandnoble.com).

	1996	*1997*	*1998*
Amazon	15	147	610[1]
Barnes & Noble	2448	2796	3000[2]

1) 252 nell'ultimo trimestre
2) 2015 nei primi nove mesi

Fonte: Fatturati ufficiali delle due società americane espressi in milioni di dollari

Tabella 4 *Confronto tra due società con differenti sistemi di vendita: tradizionale (Barnes & Noble) e on-line (Amazon).*

I risultati sono abbastanza promettenti, anche se essi non hanno ancora raggiunto la misura di Amazon (9,4 milioni nel secondo trimestre 1998 e 12,5 nel terzo). Questa crescita fa ritenere che - anche nel nuovo mondo del commercio elettronico - sia importante arrivare per primi, per cercare di conquistare la fedeltà dei clienti.

È forse prematuro affermare che Amazon diventerà un'azienda di successo (a tutt'oggi deve infatti ancora presentare un trimestre in utile); ma che il suo modello di business sia valido è già palese, così com'è ormai chiaro che il commercio elettronico in tutte le sue forme sarà il campo in cui si svilupperà la competizione e che deciderà il futuro di molte aziende commerciali e di servizi.

5. L'importanza dell'interoperabilità

Il commercio elettronico è però qualcosa di più che la semplice vendita di beni e servizi on-line: con Internet, per la prima volta, si ha infatti a disposizione un'infrastruttura universale capace di seguire on-line l'intero ciclo produttivo dalla produzione, alla vendita fino alla consegna al cliente finale. Non si assiste dunque solo al mutamento del modo tradizionale di individuare la disponibilità dei beni di interesse e quindi di effettuare l'ordinazione dei prodotti (che, come già si è detto, determina un grande impatto sul sistema aziendale): è l'intera natura dei prodotti e dei servizi che viene trasformata e che porta a una riorganizzazione globale del mercato. In questo senso il

CERTIFICATI DIGITALI ED INTEROPERABILITÀ

Per garantire la massima apertura di sistemi e servizi appare sempre più necessario definire un quadro complessivo di regole capace di garantire livelli effettivi di interoperabilità. Alcuni degli elementi tecnici per i quali è urgente procedere ad una normalizzazione sono:

- ***Estensioni dei certificati:*** **i campi selezionati da una specifica *CA (Certification Authority)* per certificati X.509 dovrebbero permettere l'interoperabilità tra differenti domini.**
- ***Richiesta di certificati:*** **il metodo con cui sono richiesti i certificati dovrebbe rispondere a regole comuni in modo da garantire l'interoperabilità tra differenti CA.**
- ***Emissione dei certificati:*** **le diverse procedure di emissione dovrebbero essere compatibili tra loro e garantire l'interoperabilità tra differenti domini.**
- ***Tempo di validità e di utilizzo dei certificati:*** **essi dovrebbero permettere una verifica incrociata *cross-certification* tra differenti CA.**
- ***Politiche di sicurezza:*** **dovrebbe essere possibile determinare un *framework* globale di riferimento per consentire operazioni di *cross-certification* a qualsiasi livello di sicurezza richiesto.**

commercio elettronico abilita un nuovo paradigma di business: quello della *Internet Economy*.

In questo nuovo scenario i fornitori, i consumatori e i nuovi intermediari *(trusted parties)* interagiscono e si scambiano informazioni secondo nuove modalità, che permettono ai consumatori di acquistare cosa, come e quando vogliono indipendentemente da unità di tempo e di spazio. Parallelamente si va più rapidamente realizzando il paradigma di un mercato sempre più aperto e globale, nel quale il problema della interoperabilità si pone come chiave di successo per lo sviluppo integrale dell'*e-commerce*.

Il commercio elettronico è infatti reso possibile grazie a una "federazione" eterogenea di reti e protocolli che, attraverso meccanismi diversificati di interfacciamento, ne garantiscono il carattere globale. In questo sistema la chiave di successo passa attraverso lo sforzo - da parte degli Enti di regolamentazione e delle aziende interessate - di definire piattaforme e tecnologie che assicurino un accesso aperto ai servizi.

Questo concetto di "apertura" implica due elementi: anzitutto, che le specifiche per l'interconnessione siano chiare e trasparenti; in secondo luogo, che esse non possano essere soggette a modiche arbitrarie da parte di una delle parti coinvolte a scapito delle altre. Si tratta di una serie di azioni che - seppure di carattere tecnologico - hanno un forte impatto a livello di regolamentazione e di business cui sarà possibile rispondere solo attraverso una "framework" globale di riferimento.

Queste considerazioni possono sembrare lontane dalla realtà, ma l'esperienza GSM dimostra che l'apertura e la trasparenza degli standard sono gli unici fattori abilitanti per garantire una crescita del mercato e per consentire nuove opportunità di sviluppo. In questo senso è significativo che molti produttori della *Information Technology* siano orientati a rendere di pubblico dominio specifiche applicative e funzionali in modo da garantire requisiti di apertura e di interoperabilità applicativa (ad esempio, Java).

6. La moneta ed i sistemi di pagamento su Internet

Nell'ambito del commercio elettronico è possibile individuare tre ruoli principali per quanto riguarda i sistemi di pagamento su Internet:

- il gestore di flusso finanziario;
- l'acquirente;
- il venditore.

Per quanto riguarda il ruolo del gestore del flusso finanziario, non si è parlato volutamente di banca; si è usato invece il termine generico di "gestore di flusso finanziario" per sottolineare la presenza a livello mondiale anche di società che adempiono a questo ruolo senza essere nate come banche.

In figura 2 sono mostrati i ruoli suddetti: essi sono

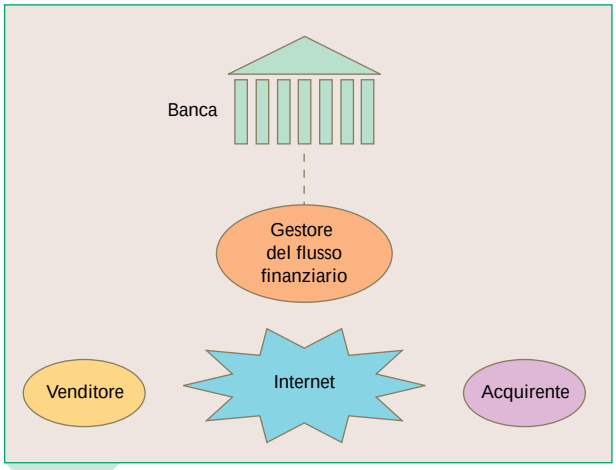


Figura 2 *Distinzione di ruoli in un sistema di pagamento su Internet.*

in genere fisicamente separati, in quanto si ipotizza che nel mezzo sia presente la rete Internet.

Il compratore possiede un *browser*, e, in aggiunta, un applicativo integrato con il browser, che gli permette di effettuare i pagamenti.

Il venditore possiede un *server WEB* cui il compratore si connette; esso possiede anche un software che gli permette di connettersi con il sistema di gestione dei pagamenti (verso il gestore del flusso finanziario). Sia il compratore che il venditore hanno in genere un *account* presso lo stesso gestore, in modo che l'importo che deve essere versato dal compratore possa essere addebitato e quello che riceve il venditore possa essere accreditato. I gestori di account hanno, quasi sempre, una connessione anche con una banca, in modo che essi, come gestori di account, possano fungere da *stanza di compensazione* tra compratori e venditori, riducendo, per quanto possibile, il ricorso a operazioni bancarie.

Per le modalità di pagamento on-line, il problema centrale è connesso all'efficienza, all'affidabilità e alla sicurezza con cui le operazioni sono effettuate. Numerose organizzazioni hanno risolto questo problema mettendo a punto sistemi di pagamento proprietari, differenti tra loro nel progetto, nelle prestazioni e negli standard di sicurezza utilizzati.

Nel campo non elettronico, i pagamenti possono essere effettuati in diversi modi, quali ad esempio la moneta contante, gli assegni, le carte di credito e debito, gli ordini postali.

L'obiettivo attuale è quello di realizzare gli equivalenti elettronici di tutti questi sistemi di pagamento: i negozi virtuali sono rivolti infatti a un pubblico assai differenziato; ma senza dubbio la sopravvivenza delle singole aziende è subordinata a un mezzo di pagamento via rete, semplice e sicuro.

Numerose compagnie e consorzi stanno operando nell'ottica di far evolvere le proprie soluzioni verso standard di sicurezza. È importante tuttavia osservare che protocolli di comunicazione bilaterali sicuri non sono da soli sufficienti: occorrono infatti protocolli di pagamento sicuri che coinvolgono più parti.

Le prime forme di pagamento per servizi offerti su Internet sono state di tipo convenzionale: gli abbonati che usufruivano dei servizi pagavano quote mensili, prelevando il denaro dal proprio conto bancario e versandolo sul conto dei fornitori. Questo metodo risulta tuttavia molto costoso e richiede tempi lunghi di attuazione, soprattutto per transazioni effettuate tra Paesi diversi.

Esso è indicato solo in relazioni commerciali durature e coinvolge tipicamente società. Internet è però una rete aperta a tutti - anche alla clientela residenziale - e il tipo di relazione che in genere lega un acquirente a un venditore è di tipo occasionale. È stato perciò necessario prevedere forme di pagamento alternative.

Le forme di pagamento disponibili per il commercio elettronico on-line, sono raggruppabili in tre categorie principali: i *token* (ovvero particolari stringhe di bit che rappresentano valore monetario), i sistemi basati sull'utilizzo di carte di credito e quelli basati su spostamenti di denaro tra conti bancari equivalenti.

6.1 Sistemi di pagamento basati sui token

I *token elettronici* costituiscono un nuovo strumento finanziario. Progettati come l'equivalente elettronico di numerose forme di pagamento emesse dalle banche o da istituti finanziari, essi si distinguono in:

- *moneta elettronica*, indicata spesso come *e-cash (electronic cash):* rientra, in alcuni casi, nella categoria dei sistemi di pagamento di tipo pre-pagato (o di debito), per i quali sul conto bancario del compratore è addebitato in anticipo l'importo per acquisti futuri. L'*e-cash* può essere memorizzata sia all'interno di *smart card*, utilizzate in numerosi progetti di "borsellino elettronico", sia su altri supporti come i *floppy disk* oppure l'*hard disk* della macchina;
- *assegno elettronico*, chiamato *e-cheque (electronic cheque):* è l'equivalente digitale di quello cartaceo. In questo caso si ha un modello di pagamento post-pagato, detto anche di credito, nel quale è presente un server la cui funzione consiste nell'identificare e nell'autenticare un cliente e nel verificare la disponibilità dei fondi indicati nell'*e-cheque.*

6.2 Sistemi di pagamento basati sulle carte di credito

Per effettuare pagamenti su Internet è possibile anche ricorrere alle carte di credito. Il processo di base rimane invariato rispetto a una transazione tradizionale, regolata con questo strumento, nel mondo non elettronico: quando i consumatori vogliono acquistare prodotti o servizi, inviano gli estremi della propria carta di credito al fornitore ed è poi l'organizzazione che gestisce la carta di credito che si fa carico di concludere il pagamento. Anche in questo caso si tratta di sistemi di pagamento post-pagato, in cui il conto del venditore è accreditato prima dell'addebito al compratore, per l'importo relativo alla vendita.

6.3 Pagamenti effettuabili con addebito presso server di terze parti

Alcune società si pongono come terze parti nel processo di compravendita su Internet; queste società sono in genere le stesse che forniscono la tecnologia per i pagamenti e che hanno deciso di sfruttare i vuoti lasciati dalle istituzioni finanziarie per operare praticamente in loro vece.

Queste società richiedono che venditori e compratori aprano un conto *(account)* presso di loro; gli account sono, a tutti gli effetti, conti correnti coperti (per ogni evenienza) da un numero di carta di credito, ma possono essere regolati, oltre che con carta di credito, anche per mezzo di un bonifico.

Gli accordi tra acquirenti e terze parti per la copertura del conto dipendono dal tipo di contratto stipulato: il conto corrente può essere coperto a priori, oppure a posteriori a scadenze prefissate, o in funzione di un diverso accordo.

Gli acquirenti, quando devono procedere all'acquisto di un bene presso un venditore, usano un codice di identificazione rilasciato dalla società. Il

INFRASTRUTTURA DI SICUREZZA A CHIAVE PUBBLICA

Nelle comunicazioni che utilizzano le reti telematiche, uno dei problemi di maggiore rilievo è quello che riguarda la sicurezza delle transazioni.

Internet, come noto, utilizza il protocollo TCP/IP che permette la trasmissione delle informazioni sotto forma di "pacchetti" informatici. Durante la trasmissione questi "pacchetti", prima di giungere a destinazione, attraversano numerosi computer-nodi che compongono la rete Internet. Durante il tragitto, il messaggio può essere facilmente intercettato ed essere sottoposto ad una serie di manipolazioni (ad esempio, alterazione e/o cancellazione del contenuto, modifica del destinatario e/o del mittente).

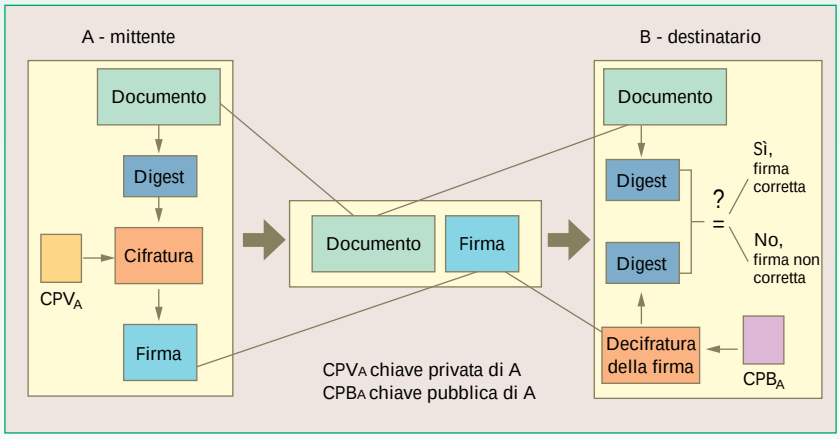
Per garantire la maggiore sicurezza possibile, le moderne tecniche crittografiche offrono numerosi soluzioni, tra le quali, soprattutto nell'ambito del commercio elettronico, riveste particolare interesse la crittografia a chiavi asimmetriche, la firma digitale e il sistema delle certificazioni. Si tratta di requisiti di base necessari per la realizzazione di un canale di trasmissione sicuro e affidabile.

Un sistema di comunicazione è sicuro quando sono rispettati rigorosamente i seguenti requisiti:

- ***confidenzialità:*** **devono essere impedite letture non consentite dei messaggi;**
- ***integrità:*** **il destinatario di un messaggio e il suo mittente devono essere assolutamente certi che il messaggio non venga modificato durante la trasmissione;**
- ***autenticazione:*** **l'origine dei messaggi deve essere assolutamente certa;**
- ***non rifiuto:*** **non deve essere possibile negare di aver inviato o ricevuto un messaggio;**
- ***certificazione:*** **deve essere validata l'idoneità e la facoltà di un soggetto a compiere determinate operazioni, tra cui l'invio del messaggio.**

Il meccanismo di certificazione si basa sull'utilizzo di algoritmi asimmetrici che impiegano due chiavi (una pubblica e l'altra privata): la chiave pubblica è usata per crittografare il testo chiaro, quella privata (mantenuta segreta e conosciuta solo dall'utente) è utilizzata per decrittografare il testo cifrato (o viceversa). L'algoritmo di crittografia a chiavi asimmetriche più impiegato è l'*RSA* (dal nome dei suoi ideatori *Rivest-Shamir-Adleman).*

La firma elettronica *(firma digitale),* riportata su un messaggio, garantisce invece la certezza dell'origine e l'integrità del messaggio.



La firma digitale.

La firma elettronica è il risultato di una procedura di validazione informatica, basata sul sistema delle chiavi asimmetriche, che, rispettivamente, consente al mittente, tramite la propria chiave privata, ed al destinatario, tramite la chiave pubblica del mittente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici (si veda la figura in alto). L'utente "firma" quindi con la propria chiave privata e chiunque è in possesso della chiave pubblica di questo utente è in grado di verificarne la firma e quindi la provenienza certa del messaggio. (Maggiori chiarimenti in proposito sono riportati nell'articolo "La sicurezza in Internet: aspetti tecnologici, amministrativi, legali" che compare su questo stesso numero della rivista a pagina 40).

CERTIFICATION E REGISTRATION AUTHORITY

- **La *CA (Certification Authority)* costituisce una componente importante dell'infrastruttura che rende i sistemi di crittografia a chiave pubblica utili per l'autenticazione della parti presenti in rete anche nel caso in cui esse non siano note. Il livello di confidenzialità dei meccanismi, se gestito correttamente, può essere molto elevato. La CA deve realizzare le seguenti funzioni principali:**
  - **accettare le richieste di certificato;**
  - **verificare l'identità delle persone o delle organizzazioni che richiedono un certificato;**
  - **emettere il certificato;**
  - **revocare il certificato;**
  - **fornire informazioni sui certificati che ha emesso.**
- **Sono spesso distinte le prime due funzioni, dette di registrazione, da quelle di emissione e gestione dei certificati. È introdotta così, accanto alla CA, la *RA (Registration Authority)* che interviene per gli aspetti organizzativi nella costruzione e nella gestione dei certificati.**
  La RA è l'entità responsabile dell'identificazione e dell'autenticazione dei proprietari dei certificati; essa delega la CA per la firma e per l'emissione dei certificati. Questa separazione di compiti e di responsabilità è molto utile soprattutto quando in un'organizzazione le funzionalità di firma e di emissione sono date in outsourcing.
- **I certificati possono essere emessi a fronte di una loro applicazione anche in ambiti specifici e ristretti, così come quelli relativi alla clientela di una banca o ai dipendenti di una società: i certificati possono essere così riconosciuti e permettono un'autenticazione "forte" degli utilizzatori del sistema, trasponendo così logiche nate per il commercio elettronico nell'ambito delle organizzazioni in modo da consentire un'introduzione progressiva nelle aziende dei vantaggi evolutivi associati allo sviluppo delle tecnologie di tipo Internet.**

venditore richiede l'autorizzazione al pagamento, collegandosi via rete al server della società. Quest'ultima, in qualità di terza parte, agisce in pratica come una banca.

7. Principali elementi distintivi di uno schema di pagamento

7.1 Anonimato e tracciabilità

Un tema assai dibattuto sui sistemi di pagamento riguarda l'anonimato e la tracciabilità delle transazioni. Con il termine anonimato si intende che nel pagamento non è utilizzata l'identità del compratore; con tracciabilità si intende invece la possibilità di mettere in relazione pagamenti diversi effettuati da uno stesso compratore, anche senza conoscerne l'identità.

Nei casi oggi usuali (diversi da quelli on-line), l'uso di banconote nell'attività di compravendita garantisce il passaggio di mano di denaro rispettando sia l'anonimato che la non tracciabilità delle transazioni: compratori e venditori possono agire senza essere controllati. Queste caratteristiche, garantite dalla banconota cartacea, possono non essere rispettate quando i pagamenti sono effettuati on-line. La possibilità di non riuscire a garantire l'anonimato e la tracciabilità dei trasferimenti di denaro, ovvero l'opportunità offerta a "qualcuno" di controllare gusti e preferenze dei singoli clienti negli acquisti, preoccupa molto il mondo Internet.

Ciò che più interessa tuttavia un consumatore è che venga salvaguardato il proprio anonimato in modo che, anche se le transazioni sono tracciabili, la sua identità non venga comunque svelata.

Finora sono pochi gli schemi di pagamento che garantiscono l'anonimato e la non tracciabilità dell'acquirente, ma non del venditore: in questi casi, quando il venditore richiede l'accredito delle somme ricevute come pagamento, verifica che i token del cliente siano validi, ma non può risalire all'identità di chi li ha spesi.

7.2 Firma Elettronica e Certification Authority

Molti degli schemi che non prevedono l'anonimato fanno uso della firma elettronica allo scopo di identificare in maniera univoca il compratore, il venditore o comunque chiunque intervenga nella catena di compravendita.

A questo scopo di solito si usa l'algoritmo a chiave

pubblica chiamato *RSA* (dal nome dei tre inventori *Rivest, Shamir, Adleman):* questo algoritmo, detto anche di crittografia asimmetrica, è basato sull'utilizzo di due chiavi, una privata e l'altra pubblica e tali per cui crittografando un qualcosa con l'una è possibile decrittografare solo con l'altra (figura 3).

Questo algoritmo permette di disporre di tutte le funzionalità di sicurezza (autenticazione, controllo degli accessi, integrità, confidenzialità e non ripudio) e, soprattutto, rende possibile la firma elettronica.

Ogni qual volta si convalida con una firma digitale una trasmissione di denaro si perde l'anonimato, cosa in genere gradita nei casi in cui si spostano quantità di denaro di non modesta entità.

Per l'impiego di tecniche di pagamento che facciano uso di firma elettronica occorre una infrastruttura chiamata *CA (Certification Authority)* che

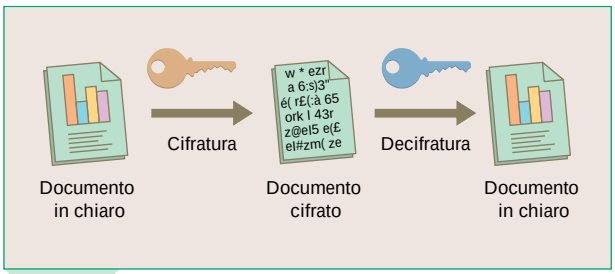


Figura 3 *Utilizzo dell'algoritmo RSA per la cifratura e decifratura dei dati.*

svolge la funzione di certificare le chiavi pubbliche. Questa operazione di certificazione avviene, in pratica, attraverso l'emissione di un certificato digitale: il certificato è un documento elettronico speciale che contiene una serie di informazioni alle quali è aggiunta una firma digitale della CA, riconosciuta e convalidata da una comunità di utenti. Il certificato digitale è paragonabile a una carta d'identità elettronica: la normale carta d'identità garantisce, attraverso la firma di un autorità riconosciuta ed i relativi bolli, che alla fotografia sul documento corrisponde l'identità indicata nel documento

La CA si fa anche carico di mettere a disposizione, in rete, le chiavi pubbliche certificate degli utenti, in modo che esse siano disponibili a chiunque voglia verificare una firma o desideri comunque ottenere la chiave pubblica di un utente.

8. Impatti sui Telecom Operator

Gli effetti del commercio elettronico sui *TO (Telecom Operator)* sono molteplici e hanno un'influenza, a partire dalla rete e dal livello di servizio, fino ad arrivare all'ambito della gestione operativa dell'azienda ed a quello di nuove opportunità di business.

Per quanto riguarda le conseguenze sulla rete, il commercio elettronico non sembra comportare specifiche esigenze: infatti, la "qualità" del dato trasmesso, che è la componente prevalente per il successo dell'*e-commerce* (soprattutto in termini di integrità e di riservatezza), è garantita più dal livello applicativo che dai protocolli di rete. Da questo punto di vista il livello di servizio della rete attuale non sembra costituire un limite alla diffusione del commercio elettronico.

La sua diffusione, considerata strettamente connessa allo sviluppo di Internet e delle tecnologie abilitanti (ad esempio TCP/IP), spinge tuttavia verso una progressiva integrazione di servizi sulla rete IP che a sua volta dovrà essere sempre più adeguata per supportarli tecnologicamente in modo adeguato (per esempio mediante lo sviluppo del protocollo IPv6).

Passando poi a considerare l'impatto sui canali di vendita tradizionali, va messo in risalto come il commercio elettronico comporti l'esigenza di una profonda re-ingegnerizzazione degli attuali processi aziendali. L'adozione di tecnologie Internet in ambito aziendale risulta infatti determinante per suggerire la sollecita revisione delle politiche e dei processi di marketing, di commercializzazione di prodotti e servizi e di *customer service* in modo da permettere di conseguire i benefici economici associati ad un loro impiego.

La diffusione del prodotto su misura per il cliente, l'avvio dell'era della moneta elettronica ed i concetti totalmente nuovi connessi alla creazione di un altro canale - privo di spazio e di tempo - per la commercializzazione dei prodotti e dei servizi, saranno significativi per ridurre i costi, per migliorare l'efficienza e l'efficacia delle azioni operative e per far crescere la qualità dei servizi e del rapporto con i clienti.

Per i nuovi servizi interattivi on-line, è poi da tenere in conto la possibilità di disporre di strumenti che consentano di gestire una forma innovativa di pubblicità basata sul profilo del cliente *(push technology).*

Sul versante delle nuove opportunità di business, è invece l'intero sistema aziendale che è messo in discussione: il commercio elettronico è infatti, nel suo complesso, strettamente connesso allo sviluppo di Internet che si pone come contesto prevalente di riferimento abilitante a nuove opportunità di business.

In questa logica il sistema aziendale, mediante le sollecitazioni derivanti dal commercio elettronico, è vincolato alle regole di un mercato, difficilmente prevedibile, nell'ambito del quale è sempre più necessario sviluppare nuovi modelli di presidio e di riferimento per consentire una gestione dinamica delle strategie, la loro attuazione operativa, pena non solo l'estromissione dai potenziali nuovi settori di business, ma soprattutto la perdita di clienti "tradizionali".

Un primo aspetto che caratterizza il "nuovo" spazio di business è sicuramente quello legato alla definizione di *partnership* strategiche realizzate da parte dei Telecom Operator.

Internet ed i nuovi servizi interattivi on-line (tra i quali il commercio elettronico) sono, infatti, erogati da una molteplicità di attori sensibilmente diversi tra loro. La ricerca dei partner, la flessibilità e la qualità della gestione, rappresentano perciò, un fattore strategico significativo per le aziende che vogliono detenere la *leadership* in questo mercato.

Una lista delle più significative *partnership*, con le specifiche aree di interesse, è riportata in tabella 5.

Un secondo aspetto dei modelli innovativi, è quello associato alla revisione delle politiche di *pricing* dei servizi di telecomunicazione, con specifico riferimento agli accessi dei servizi interattivi. Questo elemento è ritenuto dai Telecom Operator uno degli aspetti strategici più importanti per realizzare il nuovo contesto di business. Anche in quest'ambito è condivisa da molti l'esigenza di definire nuovi modelli di sviluppo che consentano di passare gradualmente, ma velocemente, da un concetto di *pricing* basato su criteri di traffico telefonico a uno nuovo basato sull'importanza e sulla complessità della transazione realizzata e su criteri di impegno dei mezzi trasmissivi, in termini di banda dedicata.

TO (Telecom Operator) con:	
ISP (Internet Service Porvider)	per il roaming degli accessi e per l'integrazione dei servizi
la Pubblica Amministrazione	per i servizi al cittadino
i fornitori di informazione	per il publishing
gli editori e i pubblicitari	per il disegno delle interfacce di utente
i fornitori IT	per lo sviluppo di servizi e prodotti
i fornitori di sistemi TLC	per l'Internet Telephony
le aziende commerciali	per la posta elettronica
le associazioni professionali	per lo sviluppo di servizi professionali
le aziende di trasporto	per i servizi di consegna dei prodotti
le banche e gli enti finanziari	per i servizi di pagamento
gli studi di consulenza	per i servizi di Groupware e di telelavoro

Tabella 5 *Potenziali partnership strategiche tra Telecom Operator e fornitori di servizio per ottenere un vantaggio strategico nel campo dell'Information & Communication Technology.*

Un terzo aspetto è legato allo sviluppo di applicazioni software destinate al cliente finale. In tale ambito il concetto Internet abilita nuovi paradigmi per l'Information Technology che facilitano l'evoluzione delle applicazioni verso un insieme di sistemi di servizi interattivi on-line e che determinano nuove opportunità di business connesse allo sviluppo, alla commercializzazione e alla gestione di soluzioni Intranet/Extranet.

Un quarto aspetto infine è quello dei rapporti fra i TO e gli *ISP (Internet Service Provider)*, soprattutto nel nostro Paese: ancora prima che i TO percepissero la valenza strategica del comparto Internet, sono nati in Italia molti ISP, a carattere prevalentemente locale, che offrono soprattutto servizi di accesso alla rete. Si è determinata perciò una situazione di contrasto fra ISP e TO, per i quali l'offerta di servizi di accesso a Internet rappresenta la naturale evoluzione dei servizi telefonici.

Il commercio elettronico potrebbe rappresentare uno stimolo per superare questi contrasti, in quanto gli ISP potrebbero occupare nuovi spazi di business in modo da innalzare il livello dell'offerta (dal business dell'accesso a quello dei servizi). Dal canto loro i TO, gestendo il business dell'accesso in un'ottica infrastrutturale evolutiva (servizi di rete TCP/IP, servizi di identificazione, autenticazione e certificazione, servizi di accoglienza personalizzata, servizi per ISP), potrebbero mettere a punto, in accordo con gli ISP, modelli di compartecipazione agli utili reciproci.

9. Conclusioni

Il quadro illustrato in questo articolo costituisce la descrizione di una situazione "de facto". Il Commercio Elettronico favorisce l'integrazione di aspetti di processo, di comunicazione e di Information Technology: questa integrazione costituisce un vantaggio competitivo per le aziende innovative che intendono presidiare con successo lo spostamento del business attuale dei TO (figura 4).

Telecom Italia, rispondendo alle sfide dell'innovazione, ha sviluppato servizi e progetti specifici basati su architetture e tecnologie Internet quali, ad esempio, piattaforme per servizi interattivi (TIN, Village ed Interbusiness, Village Trust, Village Commerce) e sistemi Intranet per l'ottimizzazione di alcuni processi aziendali (Centro di Servizi Intranet, Progetti EtaBeta).

L'esperienza finora acquisita consente di rendere stabile e di accrescere il presidio strategico dell'intero contesto, anche se le azioni finora effettuate sono

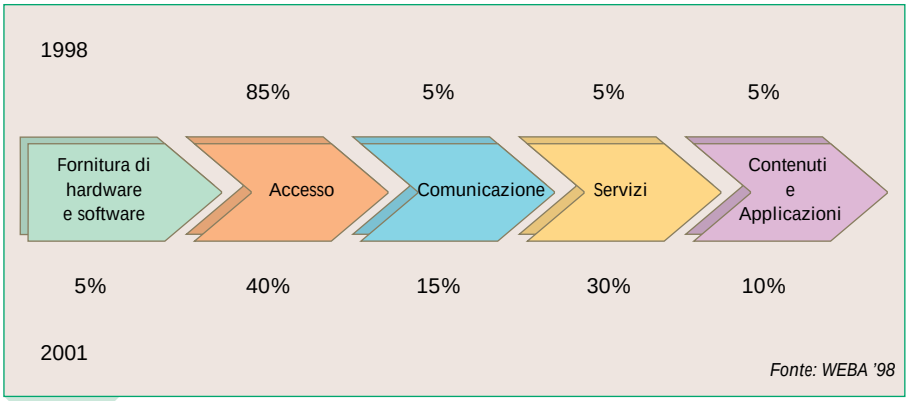


Figura 4 *Spostamento del business dei Telecom Operator.*

migliorabili in modo da consentire di acquisire organicità sufficiente per costituire una scelta strategica di un Gruppo che, potenzialmente, è in grado di garantire la gestione integrata di due elementi fondamentali della catena del valore dei business connessi al commercio elettronico: le infrastrutture di comunicazione e l'Information Technology.

La chiave di successo potrà essere dunque quella di sviluppare un'unica piattaforma infrastrutturale che consenta di elevare il livello di offerta, determinando un riposizionamento del business di Telecom Italia: da fornitura di servizi di trasporto dell'informazione a fornitura di servizi di comunicazione interattiva online e multimediale (figura 5).

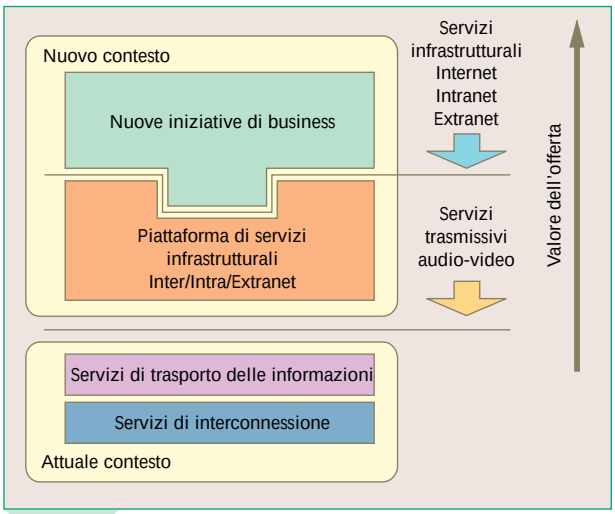


Figura 5 *Evoluzione dell'offerta di servizi dei Telecom Operator.*

Questo nuovo posizionamento, oltre a salvaguardare il presidio dell'attuale *core business* (servizi di trasporto) ed a permettere di sviluppare un nuovo mercato connesso alla commercializzazione di servizi infrastrutturali Internet/Intranet/Extranet, consentirebbe di giocare un ruolo trainante per nuove iniziative di business, che troverebbero nei servizi di piattaforma il contesto abilitante.

Abbreviazioni

CA	Certification Authority
GSM	Global System for Mobility
ISP	Internet Service Provider
IT	Information Technology
RA	Registration Authority
RSA	Rivest-Shamir-Adleman (dal nome degli inventori dell'algoritmo)
TO	Telecom Operator
WWW	World Wide Web

Bibliografia

[1] Ministro Bersani: *Linee di politica industriale per il Commercio Elettronico*. Luglio 1998. http://www.minindustria.it/Osservatorio/Pol_CE/Pol_CE_ita.htm.

[2] *Commercio Elettronico e Unione Europea*. http://www.ispo.cec.be/ecommerce/.

[3] *Multimedia Services Affiliate Forum*. http://www.msaf.org.

[4] *Search the book you want*. http://www.amazon.com. Amazon.com.

[5] *The World at a Click*. http://www.barnesandnoble.com. Barnes&Noble.com.

[6] *NUA Internet surveys*. http://nua.ie/surveys/how_many_online/ index.htm.

[7] *Atti del convegno del Terzo Forum Italiano sul commercio elettronico*. 25 giugno 1998. http://www.mate.it/atti/ce/atti.html.

[8] Merini, L.; Prosperetti, L.: *Lo sviluppo di Internet in Italia*. «Società dell'Informazione», SSGRR, VI, n. 4, 1998.

Natalino Curci: laureato in Ingegneria Elettrotecnica nel 1972, ha conseguito successivamente il Diploma di Specializzazione in "Telefonia", presso il Politecnico di Torino. Dopo il servizio militare, prestato in Aeronautica Militare, è stato assunto in SIP nel 1974. Nominato Dirigente di Azienda nel 1984, opera oggi in Telecom Italia come responsabile del Settore "Studi e Scenari Innovativi" della Direzione Risorse Informatiche. In SIP/Telecom Italia ha ricoperto responsabilità variegate nell'ambito della Direzione Rete (Programmi, Budget e Procedure della Linea Trasmissioni), della Pianificazione Strategica (Architetture e tecnologie di OSS e TMN), della Direzione Clienti Privati (Filiale di Piacenza). Dal 1994 si occupa di strategie, architetture e tecnologie Internet, Intranet ed Extranet. Ha fatto parte del gruppo di studio che ha definito e realizzato il servizio Telecom Italia Net; ha coordinato la Task Force STET per il Commercio Elettronico ed il Team di Progetto Intranet.

Dal 1995 è Chairman del Working Group on the Internet dell'Associazione Europea dei Telecom Operator (ETNO) ed è consulente dell'Unione Europea, con attività svolte in numerose "task force" (quali i Top Level Domains management, Illegal and Harmful Content in Internet, Protection of minors and human dignity for audiovisual and information services, Electronic Commerce, Education, Interoperability). Partecipa alle attività di Organismi internazionali per l'Internet Governance (ICANN, WIPO, ITU, ETSI).

Domenico Zappi: si è laureato in Scienze Politiche, presso l'università di Roma, nel luglio 1995. Nel 1996 ha operato presso la Commissione Informazione del CNEL dove ha sviluppato una ricerca sul tema: "Società dell'Informazione: il caso del Telelavoro". Nel 1997 è entrato a far parte della Direzione Strategie della STET, dove si è occupato di servizi innovati quali il telelavoro, il commercio elettronico, i servizi per le PMI (Piccole e Medie Imprese). Opera ora in Telecom Italia nel Settore "Studi e Scenari Innovativi" della Direzione Risorse Informatiche. In Telecom Italia si è occupato di architetture e tecnologie Internet, Intranet ed Extranet e della definizione delle Policy aziendali; ha inoltre curato gli aspetti normativi e tecnologici connessi alla realizzazione di soluzioni di sicurezza basate su certificati digitali, su smart card e su sistemi di profili d'utente. Ha partecipato a progetti relativi allo sviluppo di sistemi per la condivisione della conoscenza aziendale.

Tecnologie emergenti nel mondo World Wide Web

ARMANDO LIMONGIELLO
VITTORIO TRECORDI

Il principio ispiratore del World Wide Web è la creazione di un sistema aperto e potente per la condivisione di informazioni in una comunità virtuale di soggetti distribuiti geograficamente. Gli sviluppi delle tecnologie abilitanti e l'applicazione del WWW a una moltitudine di contesti, ciascuno con requisiti e vincoli specifici, sono le leve del profondo processo di revisione cui è sottoposto il WWW. La tendenza affermata all'impiego del WWW nell'ambito industriale e commerciale stimola le principali linee di sviluppo. Il commercio elettronico, la realizzazione di sistemi informativi aziendali distribuiti e l'offerta di servizi multimediali in reti a larga banda rappresentano contesti applicativi particolarmente ricchi di spunti. L'introduzione del WWW ha fatto assumere a Internet il ruolo di mass media in grado di affiancare e completare il compito svolto dai mass media tradizionali.

L'articolo si struttura come segue: il primo paragrafo fornisce un'introduzione. Il secondo delinea le basi e le linee di sviluppo della tecnologia. Il terzo descrive i sistemi che abilitano lo sviluppo di applicazioni e tecniche per la scalabilità. Nell'ultimo paragrafo si riportano le conclusioni.

1. Introduzione

Uno fra i fenomeni rilevanti dei tempi più recenti è lo straordinario successo della rete Internet: essa è innanzi tutto una rete di reti a copertura mondiale fondata su un insieme di scelte tecnologiche basate sugli standard aperti[1] dell'*Internet Engineering Task Force (IETF)* e su una famiglia di protocolli nota come TCP/IP, della quale l'*Internet Protocol (IP)* costituisce il nucleo. Originariamente concepita per lo scambio di informazioni nell'ambito della comunità scientifico-accademica, oggi la rete è un formidabile veicolo per la comunicazione e lo scambio di informazione. Gli utenti della rete Internet sono decine di milioni e sono distribuiti su tutto il globo. Le finalità del collegamento alla rete sono estremamente eterogenee: professionali o di svago. Il collegamento alla rete Internet è un requisito essenziale per le aziende moderne che intendono ricoprire una posizione competitiva nei mercati globali virtuali che stanno emergendo. Il proposito realizzativo della rete e della tecnologia delle origini era ispirato dalla necessità di individuare meccanismi per la comunicazione fra elaboratori geograficamente distanti e realizzati da costruttori eterogenei. Fra i requisiti aggiuntivi più significativi si ricordano la capacità di rendere il servizio di comunicazione indipendente dalla tecnologia con cui è realizzato il collegamento tra gli elaboratori e funzionale, anche nel caso di collegamenti particolarmente inaffidabili e soggetti a errori. Il maggiore impulso all'esplosione del fenomeno Internet è da ricercarsi nell'introduzione del *World Wide Web (WWW)*. Il modello proposto dal WWW ha impostato lo scambio di informazioni tra utenti in rete Internet sulla realizzazione di una banca dati distribuita in rete di documenti ipertestuali - ossia la cui consultazione può essere non sequenziale grazie alla presenza di collegamenti *(link)* che possono rimandare ad altri documenti - e ipermediali, ossia di documenti i cui contenuti informativi possono utilizzare varie forme di espressione, quali testi formattati, immagini e sequenze audio e video. Il collegamento fra documenti può legare tra loro contenuti distribuiti su una moltitudine di elaboratori geograficamente distanti e il grafo dei collegamenti riproduce metafori-

(1) *La partecipazione alle attività di normalizzazione è su base volontaria; le normative sono pubblicamente disponibili e il processo di standardizzazione prevede una aperta collaborazione nella fase realizzativa.*

TAPPE FONDAMENTALI DELLA STORIA DEL WWW

Anni Settanta *Nasce Internet*

- **Internet nasce come progetto del Dipartimento della Difesa statunitense e poi si sviluppa in ambito accademico. Internet è essenzialmente una rete di calcolatori per enti di ricerca universitari.**

Anni Novanta *Nasce il World Wide Web*

- **Presso il CERN di Ginevra si sviluppa un sistema per l'elaborazione di documenti ipertestuali con interfaccia amichevole.**
- **Presso il National Center for Supercomputing Applications di Chicago si sviluppa il primo browser: Mosaic. Internet diventa un mass media.**

camente la tela del ragno che realizza la struttura articolata di accesso alle informazioni in rete. In linea con uno dei principi posto alla base della rete Internet, la creazione di documenti e la realizzazione di un collegamento avviene in maniera del tutto distribuita e senza alcun coordinamento. L'utilizzo dei collegamenti consente di creare associazioni fra entità in modo molto libero e la realizzazione del collegamento può avvenire in modo semplice e incrementale.

La chiave dell'emancipazione della tecnologia WWW - da strumento appannaggio di una ristretta élite di utenti esperti della comunità accademico scientifica per mezzo dei mass-media destinato ad un sempre più ampio bacino di utenza - è l'introduzione del browser ossia dello strumento intuitivo e amichevole per la "navigazione" in rete. L'interfaccia grafica e l'uso del dispositivo di puntamento o mouse per la scelta del percorso di navigazione sulla tela ipertestuale hanno reso appetibile anche per l'utente non particolarmente esigente l'accesso al WWW, per lo meno per la consultazione delle informazioni. La fase stessa di creazione dei documenti è stata resa particolarmente semplice grazie allo sviluppo di strumenti per la realizzazione di documenti Web che richiedono un impegno e una competenza analoga a quella dell'uso di un elaboratore di testi e che permettono di produrre documenti anche molto complessi. Sulla ragnatela del Web la tessitura delle informazioni si sviluppa a un ritmo frenetico con un evidente vantaggio di rapida condivisione di informazioni da parte della comunità virtuale degli utenti della rete e con tutti gli svantaggi derivanti dalla totale distribuzione del fenomeno (informazione falsa, fuorviante o contraddittoria, obsoleta, di fonte incerta, lesiva dei diritti altrui). L'evoluzione repentina e pervasiva del mondo WWW si auto-alimenta attraverso la propria capacità intrinseca di condivisione sinergica dei progressi acquisiti su scala globale e di dialettica aperta alla gran moltitudine di soggetti che popolano la ragnatela delle informazioni.

1.1 Le radici di Internet

Nata negli anni Settanta dallo spunto offerto da un progetto avviato dal Dipartimento della Difesa statunitense, l'iniziativa Internet ha dato luogo allo sviluppo di una rete di reti eterogenee con copertura mondiale basata su una serie di principi e una tecnologia comune [1]. La rete delle origini si sviluppò in ambito accademico e l'uso delle risorse di rete era regolato da una politica di utilizzo ispirata a fini *no-profit:* era la rete per la circolazione dell'informazione prodotta dagli Enti di ricerca, con modalità di utilizzo di capacità ristrette all'uso della posta elettronica, del trasferimento di archivi elettronici e del collegamento a elaboratore remoto attraverso un terminale virtuale. L'inclusione nel sistema operativo UNIX della pila di protocolli della rete Internet ha legato le sorti del modello Internet alla diffusione di elaboratori che disponevano di questo sistema operativo. L'integrazione dei protocolli Internet si è successivamente estesa in modo accessorio e nativo a più diffusi sistemi operativi, in particolare quelli Microsoft, riconoscendone il successo indiscusso. Quest'ultima transizione ha coinciso con l'apertura della rete Internet all'utilizzo da parte degli utenti affari. Il modello iniziale per la condivisione delle informazioni in rete consisteva nella realizzazione di serventi *FTP (File Transfer Protocol)* ai quali era possibile accedere per prelevare informazione (documenti, programmi) resi disponibili alla comunità Internet. *Archie* fu introdotto per consentire di trovare informazioni nelle banche dati dei serventi FTP sulla base di parole chiave. *Gopher* rappresentò un primo passo verso l'evoluzione dell'accesso all'informazione in rete in modo ipertestuale e trasparente attraverso un sistema di menù gerarchici con un collegamento alle informazioni in rete. L'esplosione della dimensione dei menù portò all'introduzione di *Veronica,* uno strumento con il quale è possibile effettuare ricerche su parole chiave nelle voci che compongono la maglia di menù.

Tim Berners-Lee, presso il laboratorio del CERN di Ginevra, sviluppò alla fine del 1990 un sistema, basato su NeXTStep, per l'elaborazione di documenti ipertestuali con la possibilità di visualizzazione per consentire un approccio amichevole anche denominato *WYSIWYG (What You See Is What You Get* - Ciò che vedi è ciò che otterrai), gettando le basi del WWW [2]. L'architettura del WWW era stata specificata nel 1989.

Ispirandosi al principio di definire delle specifiche minimamente vincolanti, il progetto originario fissava i seguenti elementi di base:

- identificatori associabili ad ogni entità senza limi-

tazioni, *URI (Uniform Resource Identifier);*
- un protocollo di livello applicativo orientato al trasferimento di ipertesti e di informazioni multimediali, *HTTP (HyperText Transfer Protocol);*
- un formato di documenti basato su una sintassi ricca *HTML (HyperText Markup Language)*, ben definita ed estensibile, mutuata da *SGML (Standard Generalized MarkUp Language)* [3].

La comunità Internet sviluppò successivamente i principi basilari portando il modello architetturale del WWW su altre piattaforme (ad esempio Viola-WWW di Pei Wei per X-Windows e Cello per Windows). Nel 1993, Marc Andreessen del *NCSA (National Center for Supercomputing Applications)* sviluppò il primo browser grafico per ambiente X-Windows, *Mosaic.* Nel 1994, Navisoft sviluppò il primo browser con capacità di elaborazione integrata, in linea con lo spirito del progetto iniziale del CERN. L'introduzione di uno strumento per l'accesso grafico alle informazioni ipermediali ha sancito il passaggio della rete Internet da strumento di interesse solo della élite dei ricercatori e degli accademici a potente strumento per la comunicazione in ogni contesto. In particolare, nel 1994 fu aggiornata la politica di utilizzo della rete Internet in modo da identificarne la porzione ad uso no-profit e quella per utenza affari. La rete di reti a copertura mondiale si sviluppa con fornitori di servizi *Internet ISP (Internet Service Provider)* strutturati in modo da realizzare una rete gerarchica orientata ai clienti affari e collegata alla struttura similare nata per uso *no-profit* e centrata sul *backbone* statunitense *(NSFnet - oggi vBNS).*

Nel 1995 fu coniato il termine *Intranet* (rete aziendale interna) a contrassegnare non solo una rete in grado di veicolare i protocolli della famiglia IP ma più propriamente una porzione del sistema informativo aziendale distribuito basata sui protocolli della famiglia IP e in particolare sull'uso di serventi WWW. Una rete *Intranet* è realizzata tipicamente collegando fra loro reti locali distribuite sul territorio attraverso collegamenti di rete geografica dedicati (siano essi circuiti virtuali o circuiti diretti numerici); oppure si impiega la rete Internet con l'avvertenza di utilizzare la cifratura dei pacchetti IP per salvaguardare nella rete Internet pubblica i requisiti di sicurezza dei flussi informativi privati[2]. Una rete *Intranet* è in genere collegata alla rete Internet attraverso sistemi, i *firewall* (muro di fuoco o barriera), in grado di proteggere la rete privata da minacce alla sicurezza provenienti dalla rete Internet.

La dicitura *Extranet* (rete aziendale aperta all'esterno) è stata coniata da Jim Barksdale e Mark Andreessen di Netscape Communications per indicare una infrastruttura telematica che abilita la comunicazione fra aziende per scopi commerciali. Generalmente la *Extranet* è l'infrastruttura che collega tra loro le *Intranet* di fornitori e clienti utilizzando la rete Internet con opportuni accorgimenti di sicurezza per la protezione degli scambi di dati di rilievo, tipicamente ordini e pagamenti.

1.2 Gli standard Web

Gli standard del mondo Web sono collocati nell'area degli Organismi di standardizzazione dell'Internet, ossia l'ISOC e l'IETF. Tuttavia, nel 1994, nacque il *W3C (World Wide Web Consortium)* con lo scopo di evitare i pericoli della frammentazione relative alle iniziative di standardizzazione. Il consorzio vanta più di centocinquanta membri fra i maggiori sviluppatori di tecnologia Web e rappresenta un foro in cui le aziende concorrenti dal punto di vista del mercato trovano un terreno per le decisioni strategiche per portare al più alto sviluppo il potenziale del Web. I protagonisti del mercato dei sistemi distribuiti, ossia Microsoft, Sun, Oracle rappresentano forti centri di spinta per la promozione di soluzioni innovative nei contesti aperti della standardizzazione alla quale possono contribuire anche le numerose aziende emergenti che si affacciano sul terreno fertile del mercato aperto creato dal modello Internet. Anche i tradizionali attori del mondo dei sistemi informativi aziendali, ossia ad esempio IBM e DEC, sono molto attivi nel processo di migrazione dei sistemi informativi aziendali verso l'impiego di tecnologie distribuite e basate su standard aperti.

2. Le basi e le linee di sviluppo della tecnologia WWW

La tecnologia WWW è una tecnologia cliente-servente *(Client-server)* i cui elementi basilari sono descritti nel seguito di questa sezione [3].

I programmi con funzione di servente *(server)* WWW sono in grado di soddisfare direttamente richieste di servizio provenienti dai programmi clienti *(client)* con la finalità di restituire un documento o il risultato dell'esecuzione di un'elaborazione o di indirizzare tali richieste in modo trasparente ad un altro servente. Quando un servente opera il nuovo indirizzamento della richiesta agisce come intermediario *(proxy)* tra il cliente e il servente in grado di soddisfare la richiesta. Il ricorso a un intermediario può avvenire con la finalità di migliorare le prestazioni del colloquio fra il cliente e il servente, nel caso in cui all'intermediario sia demandata la capacità di *caching* (ossia la capacità di archiviare in modo trasparente all'utente i documenti cui abbia acceduto almeno un cliente rendendoli disponibili a clienti successivi, senza doverli prelevare ogni volta dal servente originario). L'intermediario può avere una funzione di disaccoppiamento tra cliente e servente per ragioni di sicurezza: in questo caso esso è progettato con garanzie particolari di salvaguardia dei requisiti di sicurezza ed esporta in modo controllato il contenuto dei serventi WWW mediati, senza esporre questi ultimi a rischi diretti. L'intermediario sicuro è posizionato tipicamente alla frontiera di separazione tra una rete "fidata", *trusted*[3], (ad esempio la *Intranet* azien-

(2) Meccanismi denominati tunneling IP e di reti private virtuali IP.

(3) In una rete "trusted" tra tutti gli elementi componenti la rete esiste una relazione di fiducia reciproca dal punto di vista della sicurezza sancita dalla politica di utilizzo della rete e delle sue componenti ("policy"). Una rete "untrusted" invece non è regolamentata da alcuna relazione.

dale su cui si trovano i serventi WWW) ed una rete "non fidata", *untrusted* (ad esempio la rete Internet cui sono collegati i clienti).

2.1 Il browser

I programmi con funzione di cliente WWW rappresentano l'interfaccia con cui l'utente accede ai servizi resi dai serventi WWW. Indicati oggi come browser, in quanto consentono all'utente di sfogliare l'informazione disponibile in modo molto libero, i programmi cliente consentono di accedere a documenti ipermediali formattati in modo sofisticato con componenti di contenuto audio e video. I browser consentono anche l'accesso alle informazioni attraverso la richiesta semplice di programmi residenti sulla macchina dell'utente (Applicazioni di Aiuto o *Helper Application)* oppure attraverso la visualizzazione dei risultati dell'elaborazione di un programma esterno o di un programma accessorio nello spazio della finestra del browser *(Plug-in*[4]*)*.

I browser possono, anche, eseguire alcuni programmi: ad esempio, eseguono *applet* Java in quanto il browser stesso include un interprete di questo linguaggio *JVM (Java Virtual Machine)*. Esistono diversi clienti utilizzabili per la navigazione dello spazio informativo di WWW anche se, di fatto, i programmi maggiormente diffusi sono *Navigator* di Netscape ed *Explorer* di Microsoft. I programmi serventi e clienti WWW sono disponibili per una vasta gamma di piattaforme hardware e di sistemi operativi.

2.2 Comunicazione tra cliente e servente WWW: il protocollo HTTP e l'URL

Il protocollo usato per la comunicazione tra cliente e servente è l'*HTTP (HyperText Transfer Protocol)*. HTTP è un protocollo di livello applicativo che usa il servizio di trasporto tra le due terminazioni *(end-to-end)* affidabile offerto dal *TCP (Transmission Control Protocol)*. Il protocollo HTTP è fondamentalmente senza stato e ogni richiesta inoltrata dal cliente è trattata come una transazione che prevede l'apertura di una connessione TCP col servente remoto (la porta standard del servizio WWW è la numero 80), il trasferimento della richiesta e della risposta e l'abbattimento della connessione. È possibile salvare localmente al browser un'informazione di stato da parte di un servente WWW per agevolare gli accessi successivi senza richiedere a ogni richiesta la dichiarazione di determinate credenziali di autenticazione, tramite il meccanismo dei *Cookie*. Il browser può essere configurato per impedire l'installazione locale dei *Cookie*, per i quali è possibile specificare un tempo di vita massimo.

Il protocollo HTTP prevede che il corpo del messaggio sia codificato secondo lo standard per la posta elettronica multimediale *MIME (Multipurpose Internet Mail Extension)* sfruttando le comprovate capacità di veicolazione di informazione con una varietà di formati. L'accesso alle risorse secondo il modello cliente-servente WWW (ad esempio "http://www.sito.it/pagina.html") è basato sull'utilizzo di una sintassi particolare, detta *URL (Uniform Resource Locator)*. L'URL aggiunge al nome simbolico usato nella rete Internet per referenziare il servente

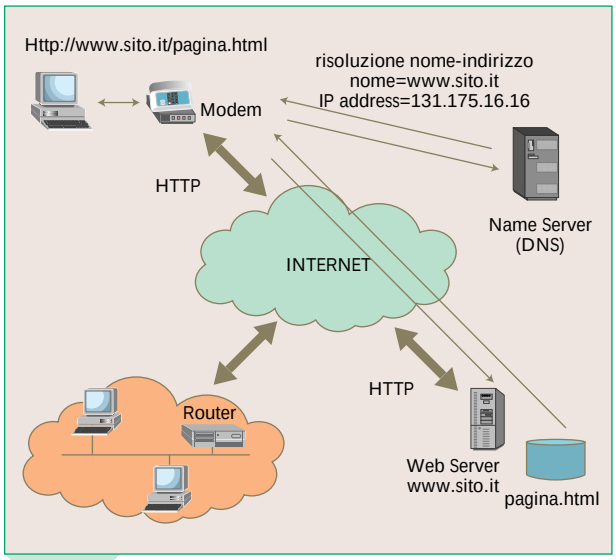


Figura 1 *Uniform Resource Locator e indirizzamento nella rete IP.*

(ad esempio "www.sito.it") cui si intende accedere un prefisso (ad esempio "http:") e un suffisso (ad esempio "../pagina.html"): il prefisso chiarisce la modalità con cui si vuole accedere mentre il suffisso indica la risorsa informativa da recuperare. Avremmo pertanto con http://www.sito.it/pagina.html (figura 1):

- il protocollo applicativo utilizzato: "http";
- la locazione del servente cui si intende accedere utilizzando questo protocollo applicativo. Ad esempio dopo "http://", si indirizza "www.sito.it" che corrisponde al servente relativo all'indirizzo IP "XXX.XXX.XX.XX": la corrispondenza "nome logico" "indirizzo fisico" è realizzata mediante gli usuali meccanismi di traduzione del mondo IP;
- infine si accede al *file* "pagina.html".

Se si vuole accedere in modalità "http" al servente di indirizzo simbolico "www.tin.it" e in particolare alla pagina "intro.html" si avrà così: "http://www.tin.it/intro.html".

L'adozione dell'URL ha consentito di far sviluppare il browser come strumento di interfaccia universale per la comunicazione in rete Internet con la capacità integrata di accedere a serventi WWW, di scambiare posta elettronica, di accedere alle *news* e di trasferire archivi elettronici dal servente WWW.

2.3 Il linguaggio HTML

I documenti ipermediali che popolano il WWW sono scritti utilizzando un linguaggio di descrizione

(4) *I* Plug-in *sono particolari moduli software che possono essere attivati dal* browser *automaticamente in base all'applicazione che ha prodotto il file, scaricato con il reinstradamento dei risultati dell'elaborazione nella finestra del* browser *stesso.*

ELEMENTI BASE COSTITUENTI IL WWW

Modello cliente-servente

- **Concetto necessario per descrivere le comunicazioni tra il consumatore di un servizio (il cliente) e il fornitore di un servizio (il servente).**

Browser

- **Programma cliente che effettua le richieste ai serventi e che è in grado di interpretare i contenuti (scritti in HTML) provenienti dai serventi.**

HTTP (HyperText Transfer Protocol)

- **Protocollo con cui avviene lo scambio di informazioni in rete tra cliente e servente.**

HTML (HyperText Markup Language)

- **Linguaggio (e sue varianti) usato per descrivere i contenuti delle risorse.**

URL (Universal Resource Locator)

- **Sintassi per indirizzare le risorse del WWW.**

chiamato *HTML (HyperText Markup Language)* [4, 5] sviluppato nell'ambito del progetto originario del CERN, prendendo spunto dallo standard *SGML (Standard Generalized Markup Language).*

HTML consente di definire ipertesti multimediali semplicemente inserendo dei marcatori *(tag)* all'interno di archivi elettronici di testo, che indicano ai browser le operazioni da eseguire per presentare ogni componente del documento in maniera appropriata.

Con HTML si può inoltre costruire un'interfaccia la cui ricchezza è limitata solamente dall'immaginazione del suo ideatore e la cui semplicità d'uso è notevole, una volta che si sia acquisita dimestichezza con l'uso del sistema di puntamento e selezione del *mouse.* I collegamenti ipertestuali selezionabili sono evidenziati dal browser con colore, *font* diversi e sottolineatura, e consentono di accedere ad altri ipertesti o archivi elettronici residenti su un qualsiasi servente WWW, tipicamente diverso da quello che ospita la pagina corrente. Dalle origini sono state apportate diverse revisioni[5] a HTML. La versione ora raccomandata da W3C è HTML 4.0 che introduce importanti estensioni allo standard HTML.

La finestra grafica del browser può essere utilizzata in modo molto flessibile mediante l'impiego delle *frame* - ossia la possibilità di suddividere lo spazio della finestra in ambienti affiancati tra loro e con dimensione stabilita dall'utente - indipendenti per capacità di accesso a testi distinti e possibilità autonoma di scorrimento.

Un semplice documento HTML scaricato da un servente WWW è statico, ossia lo stato persistente di un documento testuale non cambia se non dietro esplicito intervento del progettista del documento. Si possono realizzare delle applicazioni basate su WWW che non si limitano al semplice scaricamento nella postazione cliente di documenti HTML statici: la prima alternativa è quella in cui il servente richiami l'esecuzione di un programma esterno che restituisca il risultato dell'elaborazione su dati in ingresso inviati dal cliente realizzando di fatto un'applicazione distribuita. La seconda alternativa si basa sull'uso di una versione evoluta del linguaggio HTML, ossia il *DHTML (Dynamic HTML).* DHTML è la tecnologia che rende possibile il controllo sulla presentazione dei contenuti, indipendentemente dal browser usato. Il controllo comprende sia aspetti statici - come la posizione di un elemento o il comportamento conseguente al verificarsi di eventi (ad esempio il puntamento del mouse per cambiare la posizione dell'elemento puntato, *drag&drop)* - sia aspetti dinamici che possono determinare un cambiamento dell'aspetto e della posizione dell'elemento caricato nel browser (ad esempio effetti di animazione o di dissolvenza). Il DHTML consente di modificare in tempo reale l'aspetto di una pagina WWW senza richiamare programmi sul servente e senza che vengano scaricati programmi sul cliente: i bottoni animati, ossia che cambiano aspetto a seconda della posizione del cursore del mouse, sono un esempio di applicazione del DHTML.

Recentemente il W3C ha rilasciato la specifica per l'*XML (Extensible Markup Language)* [8], un sottinsieme del linguaggio SGML, che definisce un insieme di oggetti, o documenti, ed i metodi per elaborarli. XML supera le limitazioni dell'impostazione dell'HTML in quanto utilizza una sintassi di tipo descrittivo che separa la descrizione del testo marcato sia dalle operazioni di formattazione cui deve essere sottoposto sia dalle azioni che debbono essere eseguite se l'utente le seleziona sullo schermo. In questo modo si potrebbe visualizzare diversamente un medesimo documento se vi si accede da un dispo-

(5) HTML 2.0 fu sviluppato nel 1994 in ambito IETF. HTML 3.0 [6], HTML 3.2 [7] sono estensioni successive.

sitivo video o dal visore di un *PDA (Personal Digital Assistant)*. XML offre una sintassi estensibile attraverso la possibilità di definire nuovi marcatori, di introdurre stili di documenti, o *DTD (Document Type Definition)*, attraverso cui l'utente può definire un proprio stile riusabile. XML[6] consente di estendere anche il concetto di ipertesto in quanto, ad esempio, permette ad esempio la traduzione di un termine in più idiomi.

In alternativa ad XML possono essere usati linguaggi interpretati, come quelli usati negli *applet Java* e nei controlli ActiveX, per realizzare pagine WWW dinamiche con un approccio che sposti il peso dell'esecuzione sul cliente (browser). XML sposa la filosofia che le informazioni appartengono ai loro ideatori e che la gestione ottimale non è legata ad un particolare linguaggio (Java o ActiveX) che potrebbe non essere disponibile presso la totalità dei costruttori.

2.4 Il linguaggio per modellare realtà virtuali o VRML

Una linea di sviluppo del WWW è quella diretta alla costruzione di scene tridimensionali basandosi su un linguaggio di descrizione standardizzato, il *VRML (Virtual Reality Modeling Language)*, introdotto da SGI nel 1994. Nella versione originaria, la VRML 1.0 [9], non si tratta propriamente di un linguaggio di programmazione ma di uno relativo alla descrizione dei dati capace di generare scene tridimensionali statiche con punto di vista dinamico per consentire la navigazione. La versione 2.0 del VRML introduce i comportamenti, ossia dei programmi associati ai nodi VRML, capaci di modificarne gli attributi, consentendo di realizzare scene con oggetti in moto relativo e tra loro interagenti [10].

2.5 Il WWW l'audio ed il video

L'accesso tramite WWW a informazioni multimediali è fortemente limitato dalla notevole mole di dati prodotta dall'informazione in formato grafico o audio cui si contrappone la sensibile limitazione della disponibilità di capacità trasmissiva in particolare per accessi commutati. I browser WWW consentono l'inclusione nei documenti HTML di immagini codificate con tecniche ampiamente utilizzate, quali ad esempio *GIF* e *JPEG*, mentre è possibile accedere a immagini codificate con altre tecniche - anche basate su algoritmi proprietari - utilizzando dei moduli *Plug-in*. Attraverso un browser WWW è possibile accedere a messaggi audio ed a videoclip. I browser sono equipaggiati con la capacità di decodificare flussi audio e video codificati mediante un'ampia gamma di tecniche.

Più complesso è l'accesso a informazioni rappresentate sotto forma di flussi audio e video attraverso browser WWW in quanto questi media presentano requisiti di tempo-reale e di sincronizzazione che vanno rispettati. In alcuni casi il flusso codificato è trasferito completamente al browser prima di intraprendere ogni operazione di decodifica, riducendo così il problema dei requisiti di temporizzazione del trattamento dei dati ad un problema di gestione delle risorse relative alla macchina cliente; in questo caso il protocollo HTTP è utilizzato per trasferire le informazioni in rete. Da questa forma di base si è sviluppata la tecnica di *streaming* ossia di decodifica e riproduzione progressiva del flusso audio o video contestuale al trasferimento dell'informazione in rete: in questo caso il trasferimento dell'informazione si basa su protocolli specifici atti al trasferimento in reti IP di flussi con requisiti di tempo reale e di sincronizzazione. Innanzitutto la famiglia dei protocolli Internet già prevede un protocollo, l'*RTP (Real Time Protocol)* [11], ampiamente usato nella telefonia Internet. RTP consente il trasporto in reti IP di flussi con requisiti di tempo-reale, come la ricostruzione dei timestamp, il rilevamento delle perdite. Recentemente è stato proposto l'*RTSP (Real Time Streaming Protocol)* [12] da Netscape e Progressive Networks, per arricchire le funzionalità di RTP con un supporto alla gestione della sessione. RTSP è stato sviluppato per consentire l'accesso in rete IP a flussi multimediali da parte di un ampio numero di utenti con funzionalità di controllo simili a quelle di un videoregistratore (ad esempio pausa, avanti veloce, riavvolgi). Queste funzionalità sono complementari a quanto previsto dalla raccomandazione ITU-H.323 che definisce lo standard per i sistemi di videoconferenza su reti a banda limitata. Il supporto allo streaming offerto da RTSP e da RTP si integra con la possibilità di un invio simultaneo a più destinatari offerto dall'IP *multicast* e di una qualità di servizio garantita offerto dai protocolli di prenotazione delle risorse *RSVP (Resource ReserVation Protocol)* e di catalogazione dei pacchetti IP nei nodi di rete e nei terminali [13].

La decodifica e la visualizzazione dei flussi multimediali sono disponibili in modo nativo se le informazioni sono codificate utilizzando le tecniche più diffuse (ad esempio WAV, AU per l'audio) mentre si deve ricorrere a *Plug-in* specifici negli altri casi (ad esempio i *Plug-in* RealVideo e RealAudio di Progressive Networks). Si osservi che per quanto riguarda il video, i formati più diffusi sono quelli utilizzati sui CD ROM multimediali, ossia *QuickTime* di Macintosh e *Video for Windows* e *AVI* per Windows.

Sono stati tuttavia sviluppati applicativi, che possono esser utilizzati come *Helper Application* o come Plug-in dei maggiori browser, che consentono di operare le opportune conversioni di formato e di fornire una piattaforma per la comunicazione multimediale sincrona e per il lavoro collaborativo (ad esempio *NetMeeting* di Microsoft e *Communicator* con *Collabra* e *Conference* di Netscape).

Nel novembre 1997 il W3C ha definito il primo documento provvisorio di *SMIL* (e si pronuncia come *smile) Synchronized Multimedia Integration Language*, che definisce un linguaggio dichiarativo standard per consentire la sincronizzazione di flussi audio-video [14].

2.6 Gli strumenti per la realizzazione di pagine Web

Inizialmente le pagine HTML erano sviluppate utilizzando semplici elaboratori di programmi testuali di uso generale. Successivamente è emersa l'esigenza di convertire documenti in formati prodotti da elaboratori tradizionali di programmi e di

testi per renderli accessibili via WWW e pertanto sono stati sviluppati dei convertitori in grado di trasformare un archivio elettronico dal formato originario ad un documento HTML.

Oggi molti strumenti di utilizzo sulla scrivania elettronica per la produzione di documenti e presentazioni prevedono la funzione di esportazione come archivi elettronici HTML già a livello di funzione di base offerta dal pacchetto *software*. Sono disponibili anche numerosi strumenti che consentono lo sviluppo di documenti WWW molto sofisticati con un approccio grafico e senza richiedere la conoscenza di alcuna sintassi specifica.

3. Sviluppo di applicazioni distribuite utilizzando il paradigma WWW

Il successo del WWW ha superato gli ambiti originari di utilizzo ed è diventato un vero e proprio paradigma con cui sviluppare nuove applicazioni (ad esempio il commercio elettronico, telefonia Internet[7]).

Il browser, in particolare, è diventato l'interfaccia di utente universale per una varietà di programmi applicativi, emergono, infine, tecniche per ottimizzare e per velocizzare l'uso delle diverse componenti del WWW (ad esempio *mirroring, caching).*

3.1 Il browser: interfaccia universale

La tendenza all'introduzione dei sistemi distribuiti nell'ambito dei sistemi informativi si interseca con il successo del modello proposto dal WWW per la realizzazione di sistemi per la divulgazione di informazioni. Il WWW si è sviluppato nella direzione di assumere un ruolo centrale nell'infrastruttura che è alla base di un moderno sistema informativo aziendale. Il browser WWW evolve da strumento per la consultazione ipertestuale di documenti ipermediali verso un'interfaccia universale per l'accesso alle risorse dalla macchina personale e del sistema informativo aziendale *(Intranet)* e per l'espletamento di transazioni tra aziende *(Extranet)*. In questa linea sono da interpretare i numerosi sviluppi in direzioni volte ad arricchire le capacità di calcolo e di accesso a risorse e ad informazioni sia sui programmi clienti (i browser) sia su quelli serventi. Una forte spinta allo sviluppo viene dalla valorizzazione del paradigma di ingegneria del *software* basato sull'impiego del *software* mobile. In accordo con questo approccio le applicazioni sono realizzate senza una rigida ripartizione tra le funzioni svolte dai programmi che cooperano in un determinato contesto (ad esempio ripartizione tra cliente e servente) e con la flessibilità di far evolvere dinamicamente le funzioni svolte grazie al caricamento attraverso la rete di *software* altamente portabile. L'affermazione del linguaggio Java ha introdotto lo sviluppo di sistemi distribuiti centrati sulla rete: infatti, esso consente di prelevare da servente WWW sia normali documenti HTML che programmi Java (*applet*), i quali vengono inviati in esecuzione dal browser. I browser sono in grado di scaricare un programma da un servente, di operare un caricamento dinamico e di eseguire il programma. Il trasferimento e l'esecuzione di programmi presentano problemi di sicurezza che sono affrontati attraverso la limitazione dell'accessibilità alle risorse del cliente da parte degli *applet* (ad esempio è impossibile accedere al disco o attivare un programma locale se non si utilizzano *applet* firmate, ossia verifiche atte a rilevare la provenienza benigna comprovata dall'apposizione di una firma digitale). Java è un linguaggio di programmazione orientato agli oggetti introdotto da SUN Microsystems nel 1995. I programmi Java sono precompilati in un formato intermedio detto *byte-code* (codice astratto o intermedio) pronto per essere eseguito nell'ambiente protetto di una *JVM (Java Virtual Machine)* disponibile su una vasta gamma di piattaforme. Questa modalità consente di sviluppare applicazioni altamente portabili che possono essere trasferite in rete ed in particolare scaricate da un servente WWW ad un browser ed eseguite nell'ambito della JVM inclusa nel browser. Pur garantendo il supporto all'esecuzione degli *applet* Java, Microsoft ha sviluppato la propria tecnologia proprietaria *ActiveX* [15] e Netscape ha introdotto *JavaScript* [16]. Le tecnologie qui elencate non sono tra loro confrontabili, anche se rappresentano delle alternative alla realizzazione di applicazioni distribuite evolute in ambiente Web. Infatti, ActiveX rappresenta un approccio allo sviluppo di applicazioni caricabili in modo dinamico che possono essere sviluppate in un qualsiasi linguaggio di programmazione (ad esempio Visual Basic o C++), mentre JavaScript è un linguaggio di programmazione completamente interpretato, senza compilazioni intermedie.

Gli stessi serventi WWW sono stati arricchiti di funzionalità dapprima garantendo la possibilità di attivare programmi. Esiste una modalità standard di interfacciamento per programmi esterni ai serventi WWW, la *CGI (Common Gateway Interface)*, che è disponibile dalla maggior parte dei serventi WWW [17]. Si può pensare a un programma CGI come ad un programma in grado di generare dinamicamente una pagina HTML. La figura 2 presenta tale modalità.

Si è passati in questo caso da un semplice strumento che visualizza informazioni già presenti su un servente WWW (pubblicazione elettronica o *electronic publishing)*, ad un servizio che è in grado di generare automaticamente le informazioni in

---

(6) *Fra gli esempi di applicazione di XML ricordiamo il* RDF (Resource Description Framework), *uno schema per il trattamento dei metadati (dati sulle informazioni quali ad esempio la data, informazioni di sicurezza, note per il copyright), il* CDF (Channel Definition Format) *proposto da Microsoft e il* DRP (Distribution and Replication Protocol) *proposto da Marimba/Netscape per definire modalità di implementazione del modello di push (v. par 4.2), l'*OFX (Open Financial Exchange), *usato da Intuit Quicken e Microsoft Money per lo scambio di informazioni finanziarie, il* MML (Mathematical Markup Language), *usato per rappresentare formalismi matematici e l'*OSD (Open Software Distribution) *di Marimba e Microsoft per la distribuzione del software.*

(7) *In questo paragrafo non si esamina la telefonia Internet, oggetto di un articolo che sarà pubblicato nel prossimo numero del* Notiziario.

formato WWW (pubblicazione dinamica o *dynamic publishing)*. Questo servizio consente un aggiornamento automatico ed una personalizzazione delle informazioni. I programmi richiamati attraverso l'interfaccia CGI dal servente WWW sono programmi scritti con un linguaggio di alto livello e sono compilati per la macchina su cui risiede il servente oppure

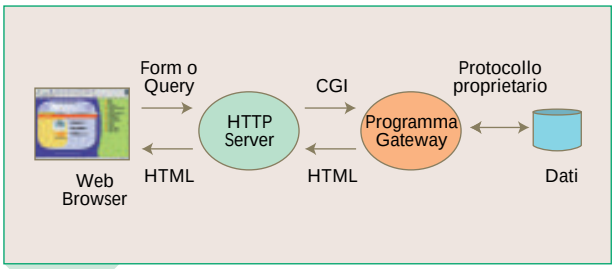


Figura 2 *Modalità di esecuzione di CGI (Common Gateway Interface) Script.*

sono programmi scritti in uno *scripting language* (il più usato è quello *Perl)* e sono interpretati sulla medesima macchina da un interprete. Le limitazioni più evidenti di questo approccio sono legate alla portabilità dell'applicazione richiamata attraverso il CGI su piattaforme eterogenee e alla necessità di attivare un'istanza del processo per ogni richiesta gestita. Per superare queste limitazioni, Netscape ha sviluppato *NSAPI (Netscape Server Application Programming Interface)* e Microsoft ha proposto *ISAPI (Internet Server API)*, interfacce di programmazione proprietarie per i WWW serventi, prodotti dai due costruttori leader del mercato. L'uso di questa *API (Application Programming Interface)* consente di raggiungere obiettivi funzionalmente equivalenti a quelli ottenibili con l'impiego di CGI con vantaggi in termini di prestazioni e di efficienza, in quanto l'applicazione di elaborazione dei dati viene eseguita nell'ambiente del servente WWW eliminando la necessità di un programma *Gateway.*

3.1.1. Il browser e le architetture software e hardware di base

Il successo del modello del browser come interfaccia per l'utente è confermato da Microsoft che ha integrato il browser nel proprio sistema operativo e che anzi consente l'utilizzo del browser come interfaccia unificata per l'accesso alle risorse del PC *(Active Desktop)*. Tuttavia la tendenza a fondare sul modello WWW lo sviluppo delle applicazioni distribuite dovrebbe essere rafforzata operando in una serie di direzioni, tra cui: la creazione di un archivio elettronico globale con garanzie di accesso trasparente e di utilizzo di tecniche di replicazione intelligente e in grado di garantire la coerenza; l'introduzione di nuovi protocolli in grado di consentire l'esecuzione da una postazione remota per applicazioni autenticate e con diritto di accesso alle risorse del sistema; l'introduzione di meccanismi che garantiscano che le applicazioni siano sempre in uno stato noto (meccanismi per le transazioni) [18].

Anche l'architettura *hardware* dei sistemi distribuiti è rimessa in discussione dall'introduzione del *software* mobile: gli alti costi dell'amministrazione delle macchine personali rende infatti interessante l'approccio del cliente leggero, ossia l'impiego di postazioni per l'utente prive di memoria di massa e con costi molto contenuti *(Network Computer)* che caricano i programmi direttamente dalla rete con alte garanzie di aggiornamento del *software*, di caricamento selettivo solamente dei moduli che interessano l'esecuzione corrente, di personalizzazione delle installazioni e di centralizzazione dell'amministrazione del *software.*

3.1.2. Il browser e i servizi di middleware

Il *Middleware* può essere definito come un insieme di servizi di ausilio per una molteplicità di applicazioni, portabili su diverse tecnologie elaborative di rete. Il termine *Middleware* nasce nell'ambito delle reti locali eterogenee (di quelle cioè che integrano protocolli di rete e database diversi) e indica un insieme di prodotti *software* che nasconde al programmatore la complessità dei protocolli di rete e le differenze tra le sintassi di database diversi, offrendo, ad esempio, la possibilità di eseguire transazioni tra differenti piattaforme elaborative.

Anche nel WWW il *Middleware* indica lo strato di *software* intermedio che rende possibile l'interazione tra le componenti di un sistema distribuito offrendo servizi di ausilio per l'interazione di applicazioni distribuite (ad esempio localizzazione di servizi remoti). Sono disponibili diversi approcci alla realizzazione del *Middleware*, fra questi possono essere citati il *Middleware* basato su *RPC (Remote Procedure Call):* il processo cliente invoca una procedura remota (ad esempio invoca una libreria grafica che risiede su un servente); il *MOM (Message Oriented Middleware):* il processo cliente invia un messaggio ad un processo servente (ad esempio un messaggio di guasto per far partire azioni da un processo di diagnosi). Il browser usa o incorpora servizi di middleware quando deve inviare richieste ad un servente.

Microsoft ha proposto il proprio *Middleware*, ossia il *DCOM (Distributed Commom Object Model)* [19]. L'*Object Management Group* ha definito un *middleware* standard *(CORBA)* per l'interazione tra processi/oggetti basato sull'esistenza di *ORB (Object Request Brokers)* che consentono di richiamare metodi di oggetti remoti in modo trasparente alla dislocazione [20], gli ORB usano il protocollo *Internet Inter-ORB Protocol (IIOP)* che utilizza TCP/IP. Sono stati sviluppati dei programmi intermedi che consentono di definire una conversione in IIOP di HTTP; si sta pensando di sviluppare browser e serventi in grado di interfacciarsi con IIOP in modo nativo.

Gli *applet* Java e CORBA sono tecnologie complementari per sviluppare applicazioni distribuite multiutente [21]. L'utilizzo combinato di Java e CORBA consente di superare alcune limitazioni del CGI, quali ad esempio lo stretto legame tra l'interfaccia di utente e la valutazione richiesta al servente remoto e consente di affidare all'*applet* Java locale funzioni di verifica della correttezza dei parametri impostati dall'utente, senza coinvolgere il servente.

A parte prodotti specifici, gli indirizzi generali prevedono l'introduzione della tecnologia ad oggetti e delle architetture basate sullo sviluppo modulare del *software (Componentware)*, con ampia portabilità su macchine eterogenee [22].

3.1.3 Integrazione dei sistemi pre-esistenti *(legacy)*

L'introduzione dei sistemi WWW nell'ambito delle aziende pone naturalmente un requisito di integrazione con i sistemi informativi esistenti. Questa integrazione può essere eseguita in diversi modi. Si possono ad esempio integrare applicazioni riguardanti transazioni del mondo SNA di IBM utilizzando browser convenzionali e programmi di CGI che consentono di effettuare transazioni su un mainframe IBM da una pagina WWW. Un'alternativa è rappresentata dall'uso di browser che hanno incluso un emulatore di terminale 3270, come accade nel caso di Communicator 4.0 di Netscape.

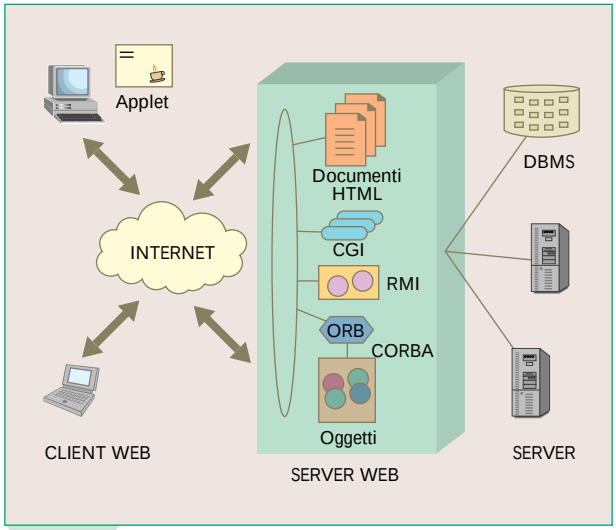


Figura 3 *WWW e il Middleware.*

Altro caso emblematico di integrazione con i sistemi informativi legacy è quello relativo all'accesso alle basi di dati esistenti attraverso un'interfaccia WWW [22]. In questo caso l'accesso ad una base di dati può essere effettuato tramite un programma CGI interconnesso al database in modo proprietario o in modo standard, ad esempio utilizzando l'interfaccia *ODBC (Open Data Base Connectivity)*. Un'alternativa possibile è l'utilizzo di *applet* Java con l'accesso alla base dati tramite l'interfaccia standard *JDBC (Java Data Base Connectivity)*. I vantaggi di questa soluzione sono numerosi: possiamo anzitutto citare i vantaggi in termini di flessibilità tipici delle applicazioni Java: indipendenza dalla piattaforma; indipendenza dal servente WWW e dal browser (purché esso sia in grado di interpretare il codice Java). Inoltre, essendo l'*applet* propriamente una applicazione, lo sviluppo dell'interfaccia grafica consente di realizzare tutte quelle caratteristiche non ottenibili con documenti HTML statici o dinamici (generati da processi CGI), e di aumentare l'interattività tra utente e sistema di gestione di basi di dati. Le soluzioni basate su JDBC hanno anche il grande vantaggio di non richiedere funzionalità aggiuntive sul lato servente, non appesantendone così il carico.

3.1.4 Gestione di sistemi e applicazioni basata su Web

Una delle applicazioni più promettenti della tecnologia WWW è la gestione di reti *Intranet*, di sistemi ed applicazioni *(Web based management)* che consentono di estendere al browser il ruolo di interfaccia per l'accesso al sistema di gestione delle risorse di un sistema distribuito. Alcune aziende, tra cui BMC Software, Cisco, Compaq, Intel e Microsoft, hanno istituito il consorzio per il *WBEM (Web Based Enterprise Management)* definendo: un modello per la descrizione delle risorse oggetto della gestione, *HMMS (HyperMedia Management Scheme)*, un protocollo per la comunicazione di informazioni di gestione, *HMMP (HyperMedia Management Protocol)* e un modello generico per le applicazioni di gestione *HMOM (HyperMedia Object Manager)*. Su un altro fronte, SUN Microsystems ha sviluppato le *JMAPI (Java Management API)* ossia un insieme estensibile di oggetti e di metodi per lo sviluppo di applicazioni di gestione in Java, presumendo che la risorsa da gestire ospiti una JVM in grado di permettere l'esecuzione di agenti di gestione scaricabili attraverso la rete e che l'amministratore del sistema possa operare attraverso un browser generico. Per il colloquio con agenti di gestione basati sugli approcci tradizionali alla gestione *SNMP (Simple Network Management Protocol)*, *CMIP (Common Management Information Protocol)* e *DMI (Desktop Management Interface)* debbono esistere intermediari *(proxy gateway)* che si prendono carico delle opportune trasformazioni sintattiche.

3.2 Motori di ricerca

I motori di ricerca sono lo strumento più semplice per l'accesso mirato all'informazione in Internet. Essi fanno riferimento a informazioni organizzate in indici periodicamente costruiti da programmi detti *robot* che navigano attraverso la rete raccogliendo pagine da elaborare e da inserire negli indici. I termini *robot, crawler, wanderer, worm* sono utilizzati come sinonimi per descrivere programmi *software* dedicati a reperire pagine Web da catalogare. Usualmente questi programmi utilizzano una base di dati nella quale inserire il risultato delle ricerche e la base di dati è spesso direttamente consultabile dagli utenti tramite Web. Comunque il modo di ricercare e indicizzare le informazioni varia molto da robot a robot e quindi le ricerche compiute su motori di ricerca diversi può dare origine a risultati completamente differenti. Un *web robot* esamina un documento e lo indicizza in base al titolo o al testo intero. Inoltre il *software* cerca nel documento anche quei collegamenti a documenti che non sono ancora stati analizzati. I *robot* operano sul principio che le informazioni presenti nel documento possono essere sintetizzate estraendo alcune parole significative e assegnando ad esse un peso; questo valore è ottenuto tenendo in considerazione la posi-

zione della parola nel titolo e nell'intero testo e il numero delle sue ricorrenze.

Gli utenti possono connettersi ad un motore di ricerca e impostare delle chiavi per interrogare l'indice. Al termine è presentata una lista contenente i collegamenti alle pagine Web di interesse (ed eventualmente altre informazioni aggiuntive come un breve sommario e una valutazione sul grado di rilevanza delle informazioni).

Sono disponibili un grande numero di motori di ricerca: essi si distinguono in base a diversi fattori come la dimensione dell'indice, la frequenza di aggiornamento, le opzioni di ricerca, la velocità con cui sono restituiti i risultati e la presentazione dei risultati. È possibile distinguere diverse tipologie di motori di ricerca:

- *Generali:* indicizzano generalmente il Web e spesso anche altre risorse Internet come *FTP, News, Gopher.* Sono caratterizzati in diversa misura da linguaggi sofisticati di interrogazione, interfacce per la presentazione dei risultati e dalla loro valutazione. Esempi sono: *AltaVista* (Web, Gopher, Newsgroup), *Excite* (Web, Newsgroup), *HotBot* (Web, Newsgroup), *Infoseek* (Web, Newsgroup), *Lycos* (Web, FTP, Gopher), *OpenText* (Web, Gopher).
- *Meta motori di ricerca uniformi:* questi strumenti non possiedono le caratteristiche di quelli precedenti ma permettono di avviare ricerche sfruttando le capacità di più motori di ricerca interrogandoli in parallelo, raccogliendone i risultati e inserendoli in una lista unificata epurata dei doppioni. Essi presentano un unica interfaccia verso più motori di ricerca (da qui uniforme). In questa categoria sono compresi *All4One, MetaCrawler, Metafind* e *SavvySearch.*
- *Meta motori di ricerca multiformi:* questi strumenti effettuano interrogazioni dei vari motori di ricerca. Esempi sono *ALL-in-One* (aggregato di interrogazioni di oltre centoventi motori di ricerca) e *2ask.*

3.3 Agenti software

Alternativamente all'impiego dei motori di ricerca, possono essere impiegati agenti software, ossia moduli software dotati di un certo grado di autonomia rispetto all'utente e che agiscono come delegati dell'utente eseguendo operazioni ripetitive e facilmente codificabili, come ad esempio quella della visita di un albero di pagine HTML per inserirle localmente sulla terminazione del cliente o per precaricare la *cache* dell'intermediario/*proxy*. Sono disponibili numerosi studi volti a definire le modalità con cui questi moduli software esprimono il concetto di "autonomia", potendo intraprendere azioni in relazione ad una base ontologica[8] sviluppata (sistemi esperti), potendo muoversi da un sistema ad un altro (agenti mobili), potendo interagire con altri agenti (agenti collaborativi). Sono state avviate alcune iniziative volte a definire un'architettura (ad esempio quella studiata dal *FIPA - Foundation for Intelligent Physical Agent*[9]) e linee guida comuni per la realizzare infrastrutture che consentano lo sviluppo e l'esecuzione di applicazioni basate sugli agenti.

3.4 Introduzione del modello push (o "a spinta")

Il sensibile sviluppo dell'informazione in rete ha reso molto difficile l'accesso a informazioni nuove o a informazioni di interesse attraverso una navigazione in rete anche se con l'aiuto dei motori di ricerca. Un modello alternativo a quello classico basato sulle richieste dell'utente è quello detto *push* basato sulla definizione di condizioni che scatenino automaticamente un invio di informazione ad un utente, senza che vi sia una richiesta esplicita [23]. L'invio di informazioni avviene, inoltre, in modo congruente profilo dell'utente. Il modello si basa sull'identificazione di canali tematici che l'utente può sottoscrivere, esprimendo un proprio profilo per la rappresentazione personalizzata, e in base ai quali i serventi inviano autonomamente informazione ai sottoscrittori (modello a eventi di tipo "pubblica e abbonati"). Il modello *push* ha trovato un impiego esteso nell'ambito dei servizi di divulgazione di notizie. Possono essere citati *Pointcast, Marimba, Backweb, Incisa* fra i principali sostenitori del modello *push.* Alcuni prodotti che offrono un servizio *push* in realtà agiscono inserendo una richiesta periodica da parte dei clienti per verificare se sui canali cui si è abbonati sono presenti variazioni per scaricarle automaticamente. Il modello *push* presenta alcune limitazioni legate alla mole di dati che sono inviati in rete senza che vi sia una esplicita richiesta se non un'espressione di interesse con la sottoscrizione al canale tematico. Inoltre, nei sistemi più avanzati è in corso l'integrazione sull'utilizzo dei protocolli IP *multicast* per evitare che la medesima informazione venga inviata singolarmente ad ogni utente - ignorando la possibilità di un invio contemporaneo a più sottoscrittori con un'unico pacchetto IP indirizzato a più destinatari.

3.5 Il commercio elettronico

La rete Internet consente di istituire una maglia di contatti virtuali tra soggetti che non si conoscono personalmente e che possono essere interessati ad una transazione finalizzata allo scambio di un bene materiale o di uno smaterializzato - un'informazione o un programma che può essere consegnato via rete. Il WWW offre uno strumento potente per consentire le interazioni tra fornitori e clienti in tutte le fasi di una trattativa commerciale, da quella di pubblicità attraverso la vetrina virtuale e di divulgazione di informazione tecnico-economica, a quella di sottoscrizione dell'ordine di acquisto, fino alla fase di assistenza tecnica post-vendita. Per attivare una relazione commerciale è necessario istituire una relazione di credito reciproco fra fornitore e cliente. Questi possono essere convalidati mediante lo scambio delle credenziali autenticate da terze parti fidate che fungono da garante. Inoltre la promiscuità d'uso delle

(8) Il termine ontologico è qui usato nel contesto dei sistemi esperti e può essere inteso come un'accezione più ampia di base di dati.

(9) http://drogo.cselt.stet.it/fipa/

risorse della rete impone la necessità di proteggere le informazioni scambiate nelle varie fasi di una trattativa commerciale dall'accesso indebito da parte di soggetti terzi. È necessario infine avere meccanismi in grado di registrare le transazioni effettuate in modo da consentire il ricorso agli archivi nel caso si verifichino contenziosi.

Il commercio elettronico richiede che siano garantiti requisiti di sicurezza che vanno dalla possibilità di autenticare e autorizzare gli utenti che intendono accedere ai servizi resi da un servente WWW, alla possibilità di garantire confidenzialità, integrità e autenticità delle informazioni, attraverso l'impiego della cifratura e della firma digitale [24].

In ambito WWW sono stati sviluppati meccanismi per la garanzia della confidenzialità ed integrità dell'informazione scambiata tra browser e servente. Alla proposta di emendare il protocollo HTTP con l'introduzione di meccanismi a supporto della sicurezza - attraverso l'introduzione dei *S-HTTP (Secure-HTTP)* [25], è comunemente preferita l'adozione di tecniche di crittografia a livello di presentazione utilizzando il protocollo *SSL (Secure Socket layer)* che permette una comunicazione sicura da un capo all'altro indipendentemente dal protocollo applicativo specifico. Il largo impiego di *script* e in particolare di *applet* Java ha fatto emergere una serie di problemi di sicurezza legati all'accesso alle risorse di una macchina da parte del *software* scaricato dinamicamente dalla rete ed eseguito localmente. Si è provveduto a proteggere il cliente circoscrivendo nei browser l'accesso alle risorse locali (ad esempio l'accesso a disco) o consentendo l'accesso attraverso meccanismi di autenticazione basati sulla firma digitale *(signed applet).* Sono disponibili forme di garanzia nei requisiti di sicurezza, implicite nelle forme di ausilio all'esecuzione dei programmi scritti in Java, che si basano sull'applicazione di misure di base legate al linguaggio (alta tipizzazione del linguaggio, verifica del bytecode, caricamento selettivo dei moduli) e sulla mediazione della *Java Virtual Machine* nell'accesso alle risorse locali della macchina. Meccanismi di filtraggio e di analisi degli *applet* e dei controlli ActiveX sono inclusi anche nei principali *firewall* usati per collegare una rete privata ad una pubblica IP.

3.6 Scalabilità

Lo straordinario sviluppo dei serventi WWW, il tasso di crescita delle informazioni in rete e il considerevole numero di browser mettono in crisi il modello di base del WWW come strumento di condivisione delle informazioni. Per mantenere la possibilità di impiego del WWW è quindi necessario garantire tempi di accesso ai documenti sufficientemente contenuti e ridurre il traffico in rete. Per favorire la scalabilità del modello WWW possono essere utilizzate tecniche di replicazione dell'informazione e d'instradamento intelligente delle richieste. La realizzazione delle repliche presenta tuttavia problemi di consistenza delle copie, di controllo degli accessi e di copyright.

3.6.1 Mirroring *(specchiare)*

Il *mirroring* consiste in una realizzazione sistematica e deliberata di copie dei documenti disponibili presso un servente WWW su altri serventi ospiti. In alcuni casi si tratta di repliche ubicate presso la medesima sede e collegate con reti locali a larga banda in modo da realizzare un gruppo *(cluster)* di serventi identici sui quali è ripartito il carico delle richieste in modo trasparente agli utenti (questo è il caso di serventi addetti a fornire il servizio di motori di ricerca, ad esempio *AltaVista* o *HotBot*, o di serventi WWW di grandi multinazionali, come ad esempio *Microsoft* o *Cisco).* In altri casi le copie sono distribuite opportunamente in rete. Nel caso, ad esempio, della rete Internet è frequente il caso di

CONTESTI APPLICATIVI PRINCIPALI DEL WWW

Browser come interfaccia universale

- **Il browser evolve verso un'interfaccia universale di risorse hardware e software quali, ad esempio, l'interfaccia di mainframe IBM, la configurazione di stampanti, il monitoraggio di reti.**

Motore di ricerca

- **Strumento per accessi mirati ai documenti del Web.**

Agenti Software

- **Moduli software che possono essere eseguiti localmente o in remoto per svolgere operazioni ripetitive e facilmente codificabili.**

Push

- **Invio automatico di informazioni ai clienti.**

Commercio elettronico

- **Scambio di beni materiali, informazioni e programmi con un'eventuale transazione finanziaria oppure come semplice vetrina virtuale di prodotti.**

ORCHESTRA
Open aRCHitecture for the support of Enhanced Services in inTegRAted broadband network

Orchestra è un Middleware per l'erogazione di servizi multimediali di telecomunicazioni. Le caratteristiche principali sono:

- **indipendenza dalle tecnologie di rete;**
- **adattabilità dei servizi alle eterogeneità dei terminali;**
- **personalizzazione dei servizi;**
- **ausilio alla mobilità;**
- **garanzia della qualità del servizio.**

repliche dei contenuti di servente WWW americani in siti europei, in modo da evitare il collo di bottiglia del collegamento intercontinentale.

3.6.2 Caching *(nascondere in una memoria)*

Il caching consiste in una realizzazione occasionale di copie di contenuti posti in memorie temporanee che possono essere presenti sulle terminazioni del cliente o sui serventi in rete. Può essere evitato ogni accesso successivo ai medesimi contenuti per trasferire essi dal servente originario qualora il contenuto possa essere reperito in *cache*. L'intermediario *(proxy)* locale alla macchina cliente rende possibile tramite un semplice caricamento locale dalla RAM o dal disco rigido accessi successivi ad un medesimo documento dal medesimo browser. Tutti i browser che hanno configurato un *proxy* intermedio condividono la *cache* del servente di intermediazione e caricano perciò dalla memoria temporanea del *proxy* i contenuti caricati da almeno un altro browser. Si ottiene così una riduzione dei tempi di accesso, portando i dati in prossimità del consumatore in modo causale e contando sul principio di località spaziale e temporale del riferimento, che assume che i dati cui sono stati fatti accessi recenti e da parte di utenti vicini hanno una elevata probabilità di essere soggetti ad accessi successivi [25].

3.6.3 Distribuzione intelligente *(metriche)*

Tutte le tecniche di replica deliberata od occasionale dell'informazione possono essere abbinate a tecniche di indirizzamento intelligente delle richieste verso la copia più conveniente. Il grado di convenienza a scegliere una replica rispetto alle altre deve essere determinato in funzione di una pluralità di criteri o di metriche. Le metriche valutano sia il carico dei serventi deputati a gestire le repliche (in modo da bilanciare il carico), sia la disponibilità di capacità di trasporto da un capo all'altro della rete, considerando la disponibilità effettiva di banda al netto dello stato di carico corrente. Un meccanismo di distribuzione delle richieste sul cliente deve decidere di attribuire ad una replica utilizzando informazioni disponibili localmente e quindi relative ad una situazione passata.

3.6.4 Pre-caricamento *(Prefetching)*

Le memorie *cache* possono essere precaricate deliberatamente con un'operazione detta di *prefetching* in base ad opportuni criteri, quali ad esempio in base alla visita di un albero di riferimenti ricavato dal profilo degli utenti. Il precaricamento può avvenire a cura di agenti *software* che a seguito del rilevamento di una variazione sull'albero visitato precaricano la *cache* operando nei periodi di inattività della rete.

4. Conclusioni

Il modello Internet introduce un livello di virtualizzazione che ben si presta all'introduzione di nuovi servizi di rete con una modalità *bottom-up*, ossia sulla base dell'iniziativa di soggetti distribuiti e che presentano bassa barriera all'ingresso. Lo sviluppo dei servizi implica lo sviluppo di applicazioni sui terminali della rete anche se un approccio più aggressivo sta proponendo l'apertura di un ambiente in grado di ospitare l'esecuzione di applicazioni nei nodi di rete *(Active Networks)* [26]. La crescente complessità della rete tuttavia è limitatamente scalabile in relazione ai requisiti di utenti che non possono basare l'impiego della rete su un comportamento puramente *best-effort* (tipicamente l'utenza affari). Si stanno perciò sviluppando architetture volte ad assumere un ruolo di rivenditore di risorse e servizi in rete Internet. A questo proposito citiamo il progetto *ORCHESTRA*, sviluppato dal Cefriel per conto di Telecom Italia, che ha condotto negli ultimi tre anni al progetto e alla realizzazione prototipale di una piattaforma per l'esecuzione e lo sviluppo di servizi in reti a larga banda [27].

Le tecnologie abilitanti la ragnatela mondiale del World Wide Web hanno profondamente trasformato il mondo tecnologico in cui i gestori di telecomunicazioni erano abituati ad operare: sono infatti oggi disponibili sistemi di utente che impiegano il PC come terminale intelligente di accesso alla rete; tecnologie di rete con il mondo IP; tecnologie dei serventi di rete con nuove funzionalità software anche di integrazione con il mondo tradizionale (ad esempio la rete intelligente).

La trasformazione si inserisce anche nel contesto della liberalizzazione e le nuove (e forse più economiche) tecnologie forniscono soluzioni a nuovi attori che si pongono in diretta concorrenza con i gestori: all'operatore rimane quindi di utilizzare le nuove tecnologie per sviluppare al meglio nuove opportunità di business.

Articolo pervenuto nel febbraio 1998.

Abbreviazioni

A/D	Analog/Digital
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
AU	Audio
AVI	Audio/Visual interface)
CD	Compact Disk
CERN	Conseil Europeen pour la Recherche Nucleaire
CDF	Channel Definition Format
CGI	Common Gateway Interface
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
CPU	Central Processing Unit
CSS1	Cascading Style Sheet Level 1
D/A	Digital/Analog
DBMS	Data Base Management System
DCOM	Distributed Common Object Model
DEC	Digital Equipment Corporation
DHTML	Dynamic HTML
DII	Dynamic Invocation Interface
DOM	Distributed Object Model
DMI	Desktop Management Interface
DRP	Distribution and Replication Protocol
DTD	Document Type Definition
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
HMMS	HyperMedia Management Schema
HMOM	HyperMedia Object Manager
HTML	HyperText MarkUp Language
HTTP	HyperText Transfer Protocol
IBM	International Business Machine
IDL	Interface Definition Language
IETF	Internet Engineering Task Force
IIOP	Internet Inter-ORB Protocol
IP	Internet Protocol
ISAPI	Internet Server API
ISDN	Integrated Services Digital Network
ISO	International Standard Organization
ISP	Internet Service Provider
ITU	International Telecommunications Union
JDBC	Java Data Base Connectivity
JMAPI	Java Management API
JPEG	Joint Photographic Experts Group
JVM	Java Virtual Machine
LAN	Local Area Network
MIME	Multipurpose Internet Mail Extension
MML	Mathematical Markup Language
MOM	Message Oriented Middleware
NCSA	National Center for Supercomputing Applications
NSAPI	Netscape Server API
ODBC	Open Data Base Connectivity
OFX	Open Financial Exchange
OMG	Object Management Group
ORB	Object Request Broker
PC	Personal Computer
PDA	Personal Digital Assistant
PSTN	Public Switched Telephone Network
RAM	Random Access Memory
RDF	Resource Description Framework
RFC	Request For Comment
RMI	Remote Method Invocation
ROM	Read Only Memory
RPC	Remote Procedure Call
RSVP	Resource ReserVation Protocol
RTP	Real Time Protocol
RTSP	Real Time Streaming Protocol
SG	Study Group
SGI	Silicon Graphics
SGML	Standard Generalized MarkUp Language
SMIL	Synchronized Multimedia Integration Language
SNA	Systems Network Architecture
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Location
VRML	Virtual Reality Modeling Language
VRU	Voice Response Unit
XML	eXtensible Markup Language
WBEM	Web Based Enterprise Management
WWW	World Wide Web
W3C	World Wide Web Consortium

Bibliografia

[1] Leiner, B.M.; Cerf, V.G.; Clark, D.D.; Kahn, R.E.; Kleinrock, L.; Lynch, D.C.; Postel, J.; Roberts, L.G.; Wolff, S.: A *Brief History of the Internet.* http://www.isoc.org/internet/history/brief.html.

[2] Berners-Lee, T.: *The World Wide Web: Past, Present and Future.* http://www.w3.org/People/Berners-Lee/1996/ppf.html, agosto 1996.

[3] Handley, M.; Crowcroft, J.: *World Wide Web: Beneath the Surf.* http://www.cs.ucl.ac.uk/staff/jon/book/book.htm.

[4] Aranson, L.: *HTML, manual of style.* Ziff-Davis Press, 1994.

[5] *Hyper Text Markup Language*. http://www.w3.org/hypertext/WWW/ Markup/MarkUp.html.

[6] Raggett, D.: *HyperText Markup Language Specification Version 3.0.* IETF draft RFC, http://pluto.neurologie.uni-duesseldorf.de/~knorr/html/html30/.

[7] Raggett, D.: *HTML 3.2 Reference Specification.* W3C Recommendation, http://www.w3.org/TR/REC-html32.html, gennaio 1997.

[8] *Extensible Markup Language (XML)*. W3C Working Draft, http://www.w3.org/TR/WD-xml-970807.html, agosto 1997.

[9] Bell, G.; Parisi, A.; Pesce, M.: *The Virtual Reality Modeling Language*. Version 1.0 Specification, http://www.vrml.org/Specifications/VRML1.0/, novembre 1995.
[10] *The Virtual Reality Modeling Language Specification.* Version 2.0, ISO/IEC CD 14772, http://webspace.sgi.com/moving-worlds/spec/, agosto 1996.
[11] Schulzrinne, H.; Casner, S.; Frederick, R.; Jacobson, V.: *RFC 1889 - RTP: A Transport Protocol for Real-Time Applications.* http://www.cis .ohio-state.edu/htbin/rfc/rfc1889.html, gennaio 1996.
[12] Schulzrinne, H.: *A real-time stream control protocol (RTSP).* IETF Draft RFC, ietf-mmusic-stream-00.txt, http://www.cs.columbia.edu/~hgs/rtsp /draft/draft-ietf-mmusic-stream-00.txt, agosto 1997.
[13] Braden, R.; Zhang, L.; Berson, S.; Herzog, S.; Jamin, S.: *RFC 2205 Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification.* Settembre 1997.
[14] Hoschka, P.: *Towards Synchronized Multimedia on the Web.* http://www.w3.org/AudioVideo/W3J.html.
[15] Cluts, N.: *ActiveX Controls Overview.* http://www .microsoft.com/WORKSHOP/PROG/CONTRO LS/CONTROLS-f.HTM, giugno 1997.
[16] *Netscape, JavaScript Guide*. http://home.net-scape.com/eng/mozilla/3.0/handbook/javascript/i ndex.html, 1996.
[17] Robinson, D.R.T.: *The draft WWW Common Gateway Interfce Version 1.1.* Internet Draft http://www.ast.cam.ac.uk/drtr/draft-robinson-www-interface-01.txt, febbraio 1996.
[18] Vahdat, A.; Dahlin M.; Anderson, T.: *Turning the Web into a Computer.* http://now.CS.Berkeley .EDU/WebOS/papers/webos.ps, 1996.
[19] Brown, N.; Kindel, C.: *Distributed Component Object Model Protocol -- DCOM/1.0.* http://www .microsoft.com/oledev/olecom/draft-brown-dcom-v1-spec-01.txt.
[20] Object Management Group: *CORBA 2.0*. http://www .omg.org/corba/corbaiiop.htm, luglio 1996.
[21] Evans, E.; Rogers, D.: *Using Java Applets and CORBA for multi-user distributed applications.* IEEE Internet Computing, http://computer.org /Internet/, maggio-giugno 1997.
[22] Manola, F.: *Towards a Web Object Model*. http://www.objs.com/OSA/wom.htm, 1997.
[23] Hurwitz, J.: *Pushing and Pulling.* DBMS magazine, http://www.dbmsmag.com/9708d04.html, agosto 1997.
[24] *Special Issue on Electronic Commerce*. «IEEE Internet Computing», Vol. 1, n. 6, http://neumann .computer.org/internet/ic1997/w6toc.htm, novembre/dicembre 1997.
[25] Baentsch, M.; Baum, L.; Molter, G.; Rothkugel S.; Sturm, P.: *Enhancing the Web's Infrastructure: from caching to replication*. «IEEE Internet Computing», http://computer/org/Internet/, marzo-aprile 1997.
[26] Tennenhouse, D.L.; Smith, J.M.; Sincoskie, W.D.; Wetherall, D.J.; Minden, G.J.: *A Survey of Active Network Research.* «IEEE Communications Magazine», Vol. 35, n. 1, http://www.tns.lcs .mit.edu/publications/ieee-comms97.html, gennaio 1997.
[27] Limongiello, A.; Roccuzzo, M.; Melen, R.; Trecordi, V.; Wojtowicz, J.: *An Experimental Open Architecture to Support Multimedia Services based on CORBA, Java and WWW technology.* 4th International Conference on Intelligence in Services and Networks IS&N '97, Cernobbio (Italy), maggio 1997.

Armando Limongiello si è laureato in Scienze dell'Informazione presso l'Università degli Studi di Pisa. Dopo aver operato presso aziende italiane ed estere (Kinetics Technology International, Olivetti e Bull) nell'ambito dell'ingegneria del software, programmazione logica e sistemi Ipermediali, è approdato nel 1991 in SIP (oggi Telecom Italia) nella Ricerca e Sviluppo dove si è occupato di evoluzione dei sistemi di commutazione, architetture software di telecomunicazioni, TINA (Telecommunications Information Networking Architecture), Intelligenza in rete e telefonia su Internet. Opera ora nella linea Architetture e Standard Internazionali della Direzione Rete dove si occupa del Piano Tecnologico della Rete.

Vittorio Trecordi ha oltre dodici anni di esperienza nel settore delle tecnologia dell'informazione e delle telecomunicazioni. L'attività svolta ha come caratteristica saliente lo studio e l'applicazione di soluzioni innovative dal punto di vista sia tecnologico e architetturale che organizzativo. I risultati delle attività di ricerca innovativa svolte hanno prodotto oltre trenta lavori di ricerca, presentati a congressi internazionali (IEEE) e nazionali e pubblicati su riviste internazionali. Dal 1997 è membro dell'Editoral Board della rivista IEEE Network Magazine. Dopo aver operato in Laben e in Pirelli Cavi, fra il 1989 e il 1991, Trecordi è stato impiegato presso il Cefriel, ove ha svolto attività di ricerca, formazione, progettazione e consulenza. Ha avuto la responsabilità tecnica di numerosi progetti europei nei programmi co-finanziati dalla UE negli ambiti ACTS, Telematics ed Information Technology (ad esempio Multicube, TeleRegions, Hector). Ha diretto i lavori di consulenza per la progettazione di reti locali e di campus per SEA, SIA, SNAM, Politecnico di Milano e AEM di Cremona. Ha svolto numerose attività di consulenza nell'ambito di progetti di telecomunicazioni avanzati per la Divisione Rete di Telecom Italia. È stato responsabile di numerosi progetti svolti per la pubblica amministrazione. Fra questi, la consulenza per lo studio di fattibilità e per la redazione dei capitolati di gara per la Rete Unitaria per la Pubblica Amministrazione (per AIPA). Da cinque anni Trecordi è Docente a contratto per il Politecnico di Milano, sede distaccata di Cremona, dove tiene un corso di "Reti di telecomunicazioni" per il corso di Diploma Universitario. Dal settembre 1998 ha lasciato l'incarico di Direttore Tecnico del Cefriel, per il quale continua a ricoprire il ruolo di responsabile dei settori reti e piattaforme software, per avviare una nuova società di consulenza, la ICT Consulting.

La sicurezza in Internet: aspetti tecnologici, amministrativi, legali

Stefano Brusotti
Roberta D'Amico
Francesco Marconi
Stefano Montesi

La diffusione di Internet, quale infrastruttura di comunicazione fondamentale per lo sviluppo della Società dell'Informazione, trova un serio ostacolo nella comune percezione dei rischi di un suo uso improprio o illecito. Lo sviluppo delle tecniche di sicurezza fornisce tuttavia molteplici strumenti, che consentono sia la protezione delle risorse (sistemi e dati) da un uso non autorizzato, sia l'autenticazione certa e inoppugnabile degli attori delle transazioni. Il potenziamento di questi strumenti, tra cui la crittografia, i certificati digitali, la firma digitale, i protocolli sicuri (in particolare HTTPS), e infine la tecnologia dei firewall – descritti nel seguito dell'articolo - non sono l'unico processo che contribuisce a rendere la rete Internet un contesto sicuro e affidabile. Di pari passo è infatti in corso di evoluzione il quadro regolatorio e legislativo, sui diversi aspetti dell'uso di Internet: anzitutto la Commissione europea e il Governo italiano hanno promosso l'autoregolamentazione dell'uso di Internet; al riguardo sono disponibili standard tecnici (PICS) che consentono di assegnare etichette ai contenuti disponibili sulla Rete, in modo da consentire il filtraggio di contenuti indesiderati per particolari utenze. Sono in corso di definizione, da parte di una proposta di Direttiva europea e dalla legge italiana, le norme che regolano le attività dei soggetti operanti come Autorità di Certificazione assicurando validità legale alla firma digitale e di conseguenza alle transazioni economiche stipulate sulla Rete. È stato, infine, avviato un processo di armonizzazione internazionale delle regole per la cifratura dei dati in ambito europeo e in quello OCSE. L'impiego delle tecnologie allo stato dell'arte, in conformità con le regole in corso di attuazione, consente lo sviluppo e la diffusione di servizi sicuri su Internet e apre nuove opportunità di sviluppo agli operatori di servizi di informazione e comunicazione.

1. Introduzione

La "rete delle reti", Internet, è stata oggetto nel tempo di trasformazioni che l'hanno portata dalle sue funzioni iniziali di "rete di servizio" per la comunità scientifica degli Stati Uniti di America alle caratteristiche peculiari presenti che ne fanno una infrastruttura emergente per la fornitura di servizi di informazione e comunicazione su scala globale. Questa trasformazione unita all'attuale rapido sviluppo della rete Internet sono accompagnate e sostenute dall'ampliamento della tipologia di applicazioni che ne utilizzano le funzioni di trasporto e, in varia misura, le funzioni di interoperabilità [1].

L'effettiva realizzazione del potenziale di Internet è condizionata tuttavia da una percezione complessiva di "insicurezza", dovuta anche all'eco delle azioni di "pirati informatici". Per fronteggiare questo problema, acuitosi anche per il crescente utilizzo commerciale di Internet da parte di privati e di aziende, negli ultimi anni si è manifestato un progressivo sensibile sviluppo delle tecniche di sicurezza, che permettono oggi di ridurre in modo significativo i rischi connessi all'utilizzo di Internet. Parallelamente allo sviluppo tecnologico è in atto uno sviluppo del quadro di regolamentazione, a livello sia dei singoli Paesi sia internazionale *(OCSE - Organizzazione per la Cooperazione e lo Sviluppo Economico,* Commissione europea), in considerazione del carattere globale della rete Internet e del mercato di beni e servizi per cui essa si propone come infrastruttura di comunicazione avanzata.

In questo articolo, dopo una breve descrizione dello scenario applicativo, è descritto lo stato degli sviluppi relativi alle tecnologie di sicurezza applicabili a Internet, ed è presentato il quadro di regolamentazione nazionale, comunitario e internazionale. Successivamente, è riportata una panoramica di "servizi sicuri" che utilizzano le tecnologie oggi disponibili. L'articolo si conclude con alcune conside-

razioni sulle opportunità che la sicurezza in Internet presenta per gli operatori dei servizi di informazione e comunicazione.

2. La sicurezza in Internet: aspettative e problemi

La sicurezza delle reti e dei servizi di informazione e comunicazione è un tema di per sé molto articolato. Pur fondandosi su alcuni principi e su tecniche comuni, che permettono di definire "come" è possibile raggiungere determinati livelli di sicurezza, il significato stesso di "sicurezza" presenta delle accezioni diverse, in funzione delle tipologie di applicazione. In questo paragrafo, queste accezioni sono esemplificate sulla base di applicazioni emergenti; nel paragrafo successivo esse saranno invece trattate con un taglio più propriamente tecnico.

Tra le applicazioni emergenti, particolare rilevanza spetta - per il potenziale in termini economici e di sviluppo della rete - al "commercio elettronico", ovvero alle applicazioni che permettono di condurre transazioni commerciali tramite Internet, mediante lo scambio di informazioni relative al cliente e al mezzo di pagamento (in genere mediante carta di credito). In questo contesto si fa riferimento al commercio elettronico con un significato specifico di transazioni tra venditori *(merchant)* e consumatori finali, scindendole così dalle transazioni tra aziende che appartengono, da un punto di vista tecnico, al dominio del trasferimento elettronico di documenti *EDI (Electronic Document Interchange)*. In questo secondo caso le minacce possibili sono in qualche modo ridotte in quanto gli interlocutori si conoscono e in considerazione della frequenza relativamente elevata delle transazioni tra aziende, risulta possibile predisporre di mezzi di comunicazione dedicati e dotati di caratteristiche di sicurezza. Nel commercio elettronico in senso stretto le transazioni avvengono invece tra interlocutori che non hanno in genere relazioni prestabilite e che utilizzano un mezzo di comunicazione diffuso e non dedicato come la rete Internet. In futuro si potrà assistere ad una convergenza tra questi due scenari, ovvero ad una migrazione del trasferimento elettronico di documenti tra aziende dalle attuali soluzioni EDI a soluzioni basate su Internet, che fanno presumere dei costi di base sensibilmente più contenuti. Un'aspettativa primaria per le applicazioni di commercio elettronico riguarda la necessità di prevenire l'intercettazione delle informazioni necessarie a perfezionare l'acquisto, scambiate tra il generico cliente e il venditore.

Un'applicazione affine al commercio elettronico è la "banca a domicilio" *(home banking)* che permette ai correntisti di una banca di accedere a uno sportello elettronico per usufruire di servizi bancari: in questo caso, oltre a dover proteggere le comunicazioni da intercettazioni, la banca ha anche la necessità di accertarsi dell'identità del cliente, per evitare sia transazioni indebite da parte di terzi sia anche il semplice accesso indebito a informazioni private del cliente, quali il suo stato patrimoniale.

L'accertamento dell'identità dell'interlocutore *(autenticazione)* è un requisito stringente anche per applicazioni importanti per lo sviluppo della Società dell'Informazione, quali il telelavoro e i servizi forniti al cittadino: nel primo caso, una parte del personale di un'azienda svolge le proprie attività lavorative utilizzando la rete Internet come mezzo di comunicazione per collegare una postazione di lavoro, collocata presso il proprio domicilio - o comunque al di fuori di edifici aziendali -, ai sistemi informativi interni dell'azienda. L'impiego di Internet comporta sia il transito di informazioni confidenziali dell'azienda, sia la possibilità per un estraneo di accedere ai dati mantenuti sui sistemi informativi aziendali. Nel caso dei servizi al cittadino, una diffusione capillare di Internet permetterebbe a cittadini e ad imprese di consultare a distanza le normative della Pubblica Amministrazione, locale o nazionale, di fornire in formato elettronico agli uffici dell'amministrazione le informazioni richieste per i diversi atti, e di ricevere in formato elettronico gli atti da questi uffici.

Le applicazioni citate pongono in luce la necessità di proteggere dalle intercettazioni le informazioni in transito su Internet e allo stesso tempo di garantire alle due parti interessate l'identità del corrispondente.

Un secondo ambito di problemi di sicurezza riguarda le intrusioni in elaboratori collegati alla rete Internet: questi problemi possono essere considerati tecnicamente una categoria a sé stante in quanto non dipendono dalle singole applicazioni: un elaboratore, per il solo fatto di essere collegato *(on-line)* può essere soggetto ad intrusioni "via Internet" da parte di pirati informatici che riescano a forzare i controlli di accesso al sistema e, una volta entrati in esso, possono acquisire, o addirittura distruggere, le informazioni ivi memorizzate. La protezione da simili intrusioni è d'altra parte molto importante nelle applicazioni commerciali: infatti, un pirata che riesca ad accedere ad un elaboratore che costituisce il "negozio elettronico" *(virtual store)* di un venditore potrebbe acquisire tutte le informazioni in esso memorizzate quali ad esempio i codici identificativi delle carte di credito dei clienti, ed aggirare in tal modo le protezioni adottate per impedire intercettazioni dei dati in transito sulla rete. Un problema simile si presenta nel caso in cui si abbia una intrusione sull'elaboratore di un cliente, tipicamente un personal computer: sebbene in questo caso il ritorno per il pirata risulti minore, in quanto potrebbe reperire solo informazioni di un singolo cliente, l'intrusione può essere attuata in maniera assai più semplice rispetto a quella richiesta per accedere ad un negozio elettronico.

La necessità di proteggere da eventuali intercettazioni le informazioni in transito su Internet spiega lo sviluppo e la diffusione su larga scala di soluzioni tecnologiche robuste; essa però deve essere bilanciata dall'esigenza di consentire la repressione di attività illegali eseguite utilizzando i canali di comunicazione di Internet, e allo stesso tempo, di rendere tecnicamente possibile l'intercettazione delle comunicazioni da parte delle autorità competenti. In questo ambito può essere inquadrata la proposta del *key escrow* (chiave in custodia) da parte del Governo degli Stati Uniti, che prevedeva l'introduzione di sistemi critto-

grafici dotati, in aggiunta alle chiavi software normalmente utilizzate per il loro funzionamento, di una chiave ulteriore - custodita dalle Autorità pubbliche - che permetta di decifrare i messaggi ai fini di intercettazioni autorizzate. Va infine ricordato che alcune tecnologie usate per rendere sicuro lo scambio di informazioni (crittografia) sono considerate dall'Amministrazione degli Stati Uniti - Paese dove è realizzata la maggior parte di queste tecnologie - come strategiche per cui una diffusione al suo esterno comporterebbe dei rischi per la sicurezza nazionale; esse sono quindi soggette a restrizioni per l'esportazione. Si ha quindi un salto tra le "piattaforme di sicurezza" adottate negli Stati Uniti e quelle degli altri paesi, che rappresenta un freno allo sviluppo del commercio elettronico su scala internazionale. Il bilanciamento tra queste esigenze, sulle quali si registrano posizioni divergenti tra i Paesi industrializzati, è oggetto di dibattito in sede OCSE. L'esame di questi aspetti sarà ripreso nel successivo paragrafo 4.7.

3. Minacce e contromisure

3.1 Le minacce

Lo scenario degli attacchi e delle minacce perpetrabili nei confronti di un sistema di elaborazione e di trasmissione dati è molto ampio, soprattutto in un'architettura distribuita con condivisione delle risorse come nel caso della rete Internet.

Una possibile classificazione degli attacchi comprende due categorie:

- *attacchi accidentali*, caratterizzati dal fatto che non esiste la volontà di violare la sicurezza (ad esempio software difettoso o errori operazionali);
- *attacchi intenzionali*, quando sono operati con l'esplicita volontà di violare il sistema (ad esempio la violazione dei diritti di accesso o l'abuso dei privilegi).

A loro volta, gli attacchi intenzionali possono essere suddivisi in:

- *attacchi passivi*, rivolti essenzialmente a conoscere le informazioni;
- *attacchi attivi*, effettuati con l'intento di modificare le informazioni memorizzate.

All'interno di questa classificazione sono riconducibili le minacce più comuni, descritte nel seguito.

Un esempio di minaccia assai nota è quella attuata dai *virus*, ossia da quei programmi che hanno la capacità di autoreplicarsi e propagarsi rapidamente all'interno di un sistema, in questo caso di una rete, attraverso lo scambio di software e documenti contenenti macro (come quelli scritti con Word o Excel). È possibile classificare i virus secondo diverse tipologie che si differenziano per il tipo di attacco che effettuano: alcuni hanno solo l'obiettivo di disturbo e di rallentare l'attività del sistema; altri invece hanno fini distruttivi e perseguono lo scopo di cancellare o di danneggiare le informazioni sensibili che incontrano.

Nel filone dei virus troviamo anche le *bombe logiche* che sono programmi con capacità di replica paragonabili a quelle viste in precedenza, ma con la particolarità di attivarsi e quindi di perpetrare l'attacco quando si verificano particolari eventi: una data, una sequenza di operazioni, l'azzeramento di un timer.

Un altro esempio di minaccia assimilabile alle precedenti per finalità, ma perseguita in modo leggermente diverso, è quella portata dal *cavallo di Troia;* la particolarità dei cavalli di Troia è quella di insinuarsi in un sistema sotto false spoglie, generalmente una utility, giochi o programmi con funzioni apparentemente innocue, ed effettuare danni come la cancellazione o l'alterazione di informazioni, la formattazione dei dischi di sistema, il cambiamento dei diritti di accesso agli archivi elettronici *(file).* Questo tipo di minaccia è molto più subdola rispetto a quella dei virus perché mentre per questi ultimi esistono alcune tecniche di esame del software per verificare se è infetto oppure no (a patto che si tratti di virus noti) nel caso dei cavalli di Troia, dal momento che investono l'aspetto funzionale del programma, diventa molto difficoltoso scoprire se dietro una banale operazione quale potrebbe essere la pressione di un tasto o il salvataggio del proprio lavoro, si nasconda una situazione pericolosa. Questa minaccia è sempre in agguato su Internet perché uno degli utilizzi della rete è proprio la diffusione e lo scambio di programmi e sulla rete si trova oggi software di ogni genere, affidabile e inaffidabile.

Un'altra minaccia è lo *sniffing*, ovvero l'ascolto passivo delle comunicazioni che avvengono sulla rete; questo è un attacco facilmente attuabile, infatti non richiede grossi investimenti ed è praticabile con analizzatori di traffico e di protocollo interamente software, quindi di basso costo. La struttura dei protocolli classici di Internet quali ftp, telnet, http, agevola questo tipo di attacco perché prevedono la trasmissione in chiaro dei dati, ed anche delle main password di accesso ai servizi.

La cattura delle password necessarie ad accedere alle macchine *(host)* connesse alla rete costituisce un altro tipico esempio di attacco. Abbiamo già visto che lo sniffing può consentire di recuperare le password che transitano in chiaro sulla rete; quando questo approccio non porta però a risultati - perché ad esempio si stanno usando opportune contromisure - allora entra in gioco il *password cracking.* Con questo termine si intende la metodologia di attacco che mira a scoprire le password attraverso ripetuti tentativi: ad esempio esistono gli attacchi chiamati di tipo dizionario, che partendo dal considerare che la maggior parte degli utenti sceglie password tra le parole di uso comune, avviano i tentativi proprio a partire dalle parole tipiche di una lingua. Statisticamente, attacchi di questo tipo hanno una percentuale di successo di circa il 30 per cento. Su Internet sono disponibili programmi di password cracking gratuiti.

Nell'ambito delle minacce e quindi delle modalità di attacco esiste poi la tecnica del *masquerade.* Questa tecnica prevede che una terza entità, illecita, si spacci per un attore noto al sistema e a causa di questo cambiamento (mascheramento) di identità possa entrare e acquisire informazioni ed eventualmente svolgere azioni ed operazioni che altrimenti sarebbero ad essa impedite.

Un altro modo per eseguire un attacco è quello di alterare il contenuto dei messaggi trasmessi *(message*

LE MINACCE ALLA SICUREZZA

- **Un ambiente distribuito e aperto quale Internet si presta ad una vasta serie di attacchi e di minacce perpetrabili ai danni dei sistemi di elaborazione e di comunicazione collegati. Volendo fare una classificazione di massima dei possibili attacchi, essi possono essere distinti a seconda che si voglia o no, da parte di chi li esercita, violare il sistema in oggetto: nel primo caso si hanno attacchi di tipo intenzionale (del tipo ad esempio violazione dei diritti di accesso), nel secondo caso di tipo accidentale (legati ad esempio a errori nella scrittura del software). Un'altra possibile classificazione distingue gli attacchi passivi da quelli attivi: i primi sono effettuati con lo scopo di conoscere determinate informazioni; quelli attivi mirano invece a modificare le informazioni di cui si entra in possesso.**

- **All'interno di questi macro filoni trovano collocazione le diverse possibili minacce tra cui si ricordano i virus, ovvero programmi in grado di riprodursi e di propagarsi in rete tramite lo scambio di software e di documenti: mentre alcune tipologie di virus hanno il solo obiettivo di rallentare o comunque disturbare il sistema, altre sono ben più pericolose in quanto hanno fini distruttivi. Altra minaccia diffusa, nota con il nome di cavallo di Troia, consiste nell'intrusione, in un sistema di elaborazione, di un programma che si maschera per una procedura di utilità, con funzioni apparentemente innocue, e che invece effettua gravi danni come la cancellazione di informazioni.**

- **Un attacco facilmente praticabile in reti in cui il traffico viaggia in chiaro è rappresentato dallo *sniffing* che consiste nel porsi in ascolto sulla rete per spiare le comunicazioni; esistono analizzatori di traffico e di protocollo, facilmente reperibili in rete, in grado di attuarlo. Oltre a questa possibilità di intercettazione, alcuni attacchi mirano a modificare il contenuto dei messaggi per indurre ad esempio un sistema a comportarsi in modo diverso da quello atteso o per scopi fraudolenti.**

- **Altri tipi di attacchi consistono nel ridurre la disponibilità dei servizi offerti in rete generando traffico fittizio o cancellando messaggi provenienti da una determinata macchina *(denial of service)* o ancora inviando più volte uno stesso messaggio (attacco noto come *replay).* Va infine ricordato che anche gli errori di programmazione possono essere una causa di debolezza del sistema, ancor più grave in quanto essi sono spesso non noti e quindi sono ignorati.**

modification), in modo che abbiano comunque un senso nel contesto in cui sono generati, e che quindi possano indurre il sistema a comportarsi in modo diverso da quello atteso.

Un ultimo tipo di minaccia, non meno significativa e pericolosa di quelle finora descritte, è rappresentato dal *denial of service* (negazione del servizio), consistente nella generazione di traffico fittizio diretto verso i sistemi che forniscono il servizio preso di mira, o nella cancellazione sistematica dei messaggi provenienti da una determinata macchina o dominio della rete. Con metodologie analoghe, ma con finalità differenti, troviamo la minaccia del *replay* (reiterazione) che consiste nel rinviare più volte ad una stessa entità un intero messaggio o parte di esso: nel caso di informazioni non significative l'effetto dell'attacco è riconducibile al caso precedente; se il messaggio contiene invece informazioni importanti, (si pensi al caso di mandati di pagamento o cartelle esattoriali), il danno può diventare assai elevato.

Questa breve elencazione delle minacce e delle modalità di attacco non può però prescindere dal ricordare che esiste un altro aspetto che, se trascurato, può essere una fonte indiretta di minaccia; esso è relativo alla perizia con cui è scritto il software sia di tipo applicativo sia dei protocolli, per cui può capitare che errori di programmazione o il semplice fatto di non aver previsto nel progetto del software particolari situazioni possano introdurre debolezze e quindi possano costituire una minaccia assai pericolosa in quanto ignota e ignorata.

Il modo più semplice ed efficace per garantire alcuni aspetti di sicurezza della comunicazione sulla rete Internet, come in altri contesti, è ricorrere ai servizi e alle funzionalità della crittografia. La crittografia non rappresenta tuttavia la risposta unica a tutte le possibili minacce: possono essere infatti condotti attacchi contro cui è necessario adottare differenti meccanismi di protezione.

3.2 La crittografia

Le tecniche crittografiche, o di cifratura, consistono nell'applicare alle informazioni da comunicare o

da memorizzare una procedura (algoritmo) che rende incomprensibile il messaggio originale, ma che può ricostruirlo mediante l'impiego di un processo inverso. In generale, la trasformazione che un algoritmo di cifratura applica al messaggio originale tiene conto di un ulteriore elemento, la cosiddetta "chiave crittografica"[1], la cui conoscenza è pertanto necessaria per ricostruire in maniera corretta il messaggio originale. La robustezza di un algoritmo di cifratura è, infatti, data dalla difficoltà di ricostruire il messaggio originale senza disporre della chiave; questa difficoltà

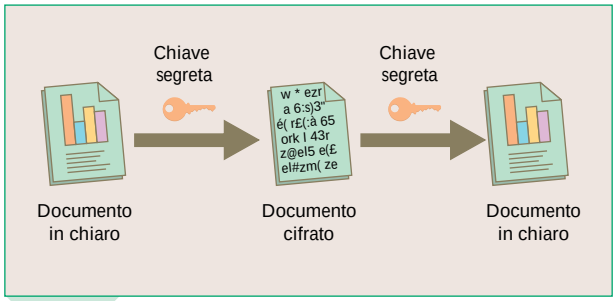


Figura 1 *Schema crittografico simmetrico.*

cresce con il volume di elaborazioni necessarie per compiere questa effrazione.

Di seguito sono descritte le tipologie di algoritmi crittografici esistenti e le loro caratteristiche più rilevanti. Una trattazione tecnica di maggior dettaglio, con i riferimenti bibliografici dei singoli standard tecnologici, è riportata in [2].

Sono oggi disponibili due classi principali di tecniche crittografiche:

- *crittografia a chiave privata*, detta anche simmetrica, in cui una stessa chiave crittografica è utilizzata per cifrare e decifrare le informazioni (figura 1). In questo caso occorre che le due parti interessate alla comunicazione conoscano la chiave crittografica utilizzata (il mittente per cifrare e il destinatario per decifrare). La segretezza di questa chiave è naturalmente un requisito fondamentale in quanto su di essa si basa la sicurezza del sistema: la chiave deve quindi essere scambiata secondo modalità e canali sicuri, di solito diversi da quelli poi usati per la comunicazione cifrata.
  Quest'approccio comporta la sensibile crescita del numero di chiavi da gestire, una diversa per ogni coppia di interlocutori, e porta rapidamente all'esplosione del sistema (per permettere a *n* persone di comunicare tra loro sono, infatti, necessarie $n*(n-1)/2$ chiavi).
  Esempi di algoritmi crittografici simmetrici sono: DES, 3-DES, RC2, RC4, IDEA.
- *Crittografia a chiave pubblica*, detta anche asimmetrica: essa è basata sull'impiego di una coppia di chiavi, legate da una relazione matematica, una privata da mantenere segreta e una pubblica da distribuire a tutti i possibili interlocutori.
  Gli algoritmi asimmetrici presentano la caratteristica di permettere la decodifica del messaggio con una chiave solo quando questo è stato codificato con l'altra chiave della coppia (figura 2). In questo modo, utilizzando la propria chiave segreta per cifrare un messaggio, chiunque sia in possesso della corrispondente chiave pubblica potrà decifrarlo e verificarne l'origine (questo è l'uso alla base della firma digitale); cifrando invece con la chiave pubblica di un destinatario, solo questo sarà in grado di decifrarne il contenuto in quanto è in possesso della corrispondente chiave privata (in questo modo si garantisce la confidenzialità della comunicazione).
  In questo schema il numero di chiavi coinvolte è sensibilmente inferiore rispetto al caso precedente perché è sufficiente una coppia di queste chiavi per ogni interlocutore; se *n* persone devono perciò comunicare tra loro, ognuna in modo sicuro, è sufficiente gestire solo *n* chiavi, ognuna delle quali è la parte pubblica della coppia di chiavi di ciascun interlocutore.
  Esempi di algoritmi crittografici asimmetrici sono: RSA, DSA, Diffie-Helmann, EC (curve ellittiche).

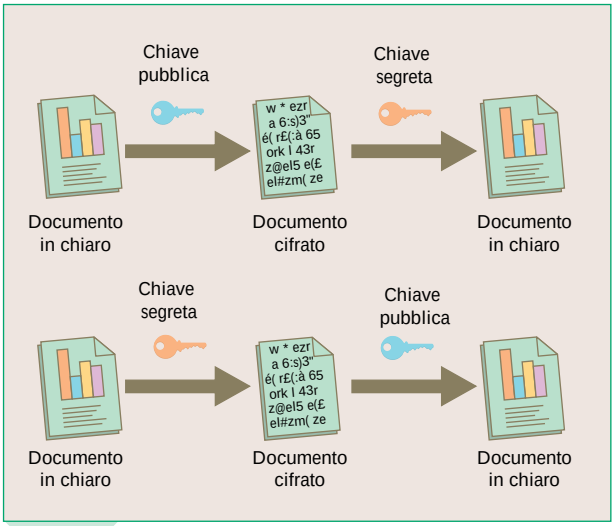


Figura 2 *Schema crittografico asimmetrico.*

In entrambi i casi presentati, la robustezza del metodo dipende anche dalla lunghezza delle chiavi: più esse sono lunghe, maggiore è la complessità dell'elaborazione necessaria per violarlo.

L'applicazione degli schemi crittografici a chiave pubblica si basa sull'esistenza di un'*AC* (*Autorità di Certificazione*), ovvero di una terza parte fidata che è il garante dell'autenticità delle chiavi pubbliche. Occorre infatti assicurare l'appartenenza di una chiave pubblica ad un determinato soggetto, sia esso persona fisica, giuridica o un elaboratore. Questo aspetto è realizzato mediante il *certificato elettronico*,

(1) *In questo contesto con chiave crittografica si intende una stringa di bit.*

un documento informatico rilasciato dall'AC che contiene una serie di informazioni tra cui: i dati personali del soggetto certificato, la sua chiave pubblica, il periodo di validità, dati inerenti l'AC emittente, informazioni legate al possibile utilizzo da parte del singolo soggetto (ad esempio nel servizio di posta elettronica), identificativo dell'algoritmo utilizzato per generare la firma e la firma della AC. La raccomandazione ITU-T X.509 descrive il tipo ed il formato di queste informazioni e prevede una struttura di certificazione di tipo gerarchico.

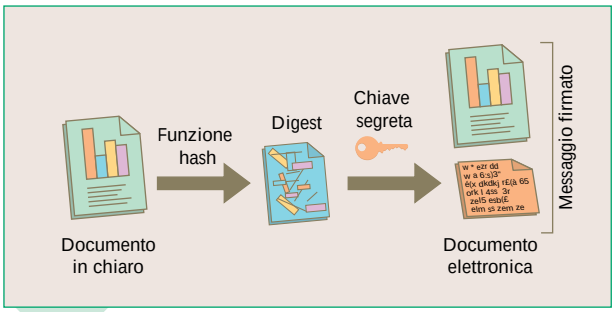


Figura 3 *Firma elettronica in ingresso.*

La tecnica di cifratura consente di proteggere i dati trasmessi, garantendo la *riservatezza* di una comunicazione e quindi la possibilità di instaurare un canale sicuro di comunicazione con un interlocutore, in modo da poter scambiare informazioni private. Entrambi gli schemi - simmetrici o asimmetrici - consentono di cifrare un messaggio; lo schema simmetrico è tuttavia preferito nei casi in cui sia necessaria una certa velocità di esecuzione della cifratura, in quanto gli algoritmi di cifratura/decifratura a chiave pubblica sono più complessi e hanno quindi tempi di elaborazione più lunghi.

La cifratura rappresenta il metodo più efficace per evitare lo sniffing, attacco inteso al solo ascolto dei messaggi presenti nella rete.

Un meccanismo utile per assicurare l'autenticità delle informazioni trasmesse è la *firma elettronica.* Con questo termine si identifica una particolare procedura, basata sulla crittografia a chiave pubblica, tramite la quale è possibile generare una stringa di bit che, associata a un messaggio in chiaro, consente di verificare l'*autenticità* del mittente (ovvero di accertare la provenienza delle informazioni) e l'*integrità* (cioè la conformità delle informazioni ricevute rispetto a quelle inviate). Per calcolare una firma elettronica occorre applicare il procedimento qui di seguito descritto.

Il messaggio in chiaro è inviato all'ingresso di un sistema che calcola su di esso una funzione matematica detta *funzione hash a una via*[2]; il risultato del calcolo è una stringa di bit di lunghezza fissa, denominata *digest* (riassunto). Questo tipo di funzione gode della proprietà per cui a partire dal risultato è molto difficile risalire al messaggio in ingresso e che, dato un messaggio in chiaro, è molto difficile individuare un altro messaggio che abbia lo stesso digest. Il digest è successivamente cifrato con la chiave privata del mittente; il risultato costituisce la firma elettronica da allegare al messaggio in chiaro (figura 3). Il ricevente, esaminando la firma elettronica, ha la possibilità di verificare l'integrità e l'autenticità del messaggio ricevuto: utilizzando la chiave pubblica del mittente decodifica la firma elettronica, ottenendo così il digest del messaggio; applicando la stessa funzione hash[3] utilizzata dal mittente, ricalcola il digest e confronta poi i due digest, quello allegato al messaggio e quello ricalcolato (figura 4). Nel caso in cui essi coincidano il sistema decide che il messaggio non ha subìto alcuna alterazione durante la trasmissione; se invece i due digest sono differenti, proprio per le proprietà matematiche di cui gode la funzione hash, il sistema stabilisce che è stato alterato il messaggio o la firma. Si ha così anche la garanzia sull'identità del mittente, in quanto dovrebbe essere l'unico possessore della chiave privata utilizzata per generare la firma.

La firma elettronica si presta quindi come una tecnica abilitante ai servizi di integrità dei dati (contromisura all'attacco noto come message modification, inteso come modifica del contenuto di una trasmissione) e di non-rifiuto (contromisura alla frode di una parte che avendo partecipato ad una transazione neghi successivamente di averla svolta).

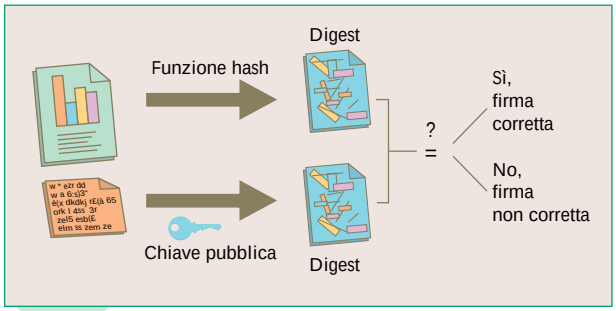


Figura 4 *Verifica di una firma elettronica in ricezione.*

Un'importante evoluzione della firma elettronica, utilizzata ad esempio in applicazioni di moneta elettronica per garantire l'anonimato dell'utente che spende questo tipo di moneta (questo tema sarà ripreso nel paragrafo 5.2), è la cosiddetta *firma cieca (blind signature):* questa tecnica, sfruttando le proprietà della crittografia a chiave asimmetrica, permette di codificare un messaggio, 'mascherato' con una sequenza casuale di bit, con la chiave privata di un utente, e di eliminare successivamente la sequenza

(2) *Il termine "hash" significa in inglese* impasto, *ed è utilizzato in ambito informatico per dare l'idea di una funzione che "trita e reimpasta" cioè rielabora i dati.*

(3) *Le funzioni hash da utilizzare nelle applicazioni della firma elettronica sono indicate dallo standard ITU-T X.509; in particolare la normativa italiana, al fine della validità legale delle firme elettroniche, prescrive l'uso delle funzioni RIPEMD-160 e SHA-1 (come specificato nel paragrafo 4.6.3).*

casuale mantenendo la firma sul messaggio. In questo modo l'originatore del messaggio può dimostrare che il messaggio è stato validato dal firmatario; peraltro il firmatario, che ha ricevuto il messaggio mascherato con una sequenza casuale aggiunta ad esso dall'originatore, non ne conosce il contenuto.

Un notevole miglioramento nella sicurezza si ottiene facendo eseguire le elaborazioni crittografiche da una *smart card.*

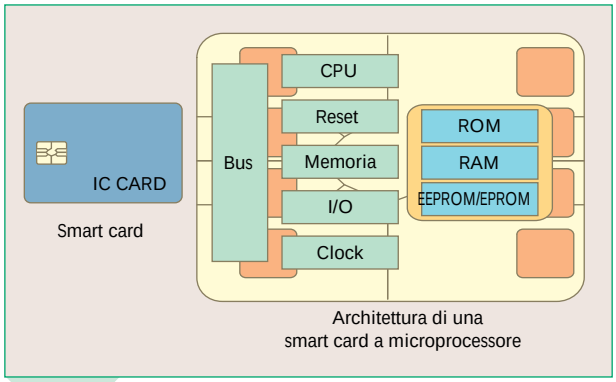


Figura 5 *Smart card per le elaborazioni crittografiche.*

La smart card è costituita da un supporto plastico analogo a quello di una carta di credito, che contiene all'interno un chip in grado di eseguire un insieme di funzioni e di comunicare con il mondo esterno tramite un connettore o un'interfaccia a radio frequenza (figura 5). Sono disponibili smart card in grado di eseguire algoritmi crittografici sia di tipo simmetrico sia asimmetrico. La maggiore sicurezza deriva dal fatto che la smart card è un dispositivo *tamper proof,* (cioè a prova di manomissione) che consente di memorizzare le chiavi crittografiche e di eseguire gli algoritmi che le utilizzano. È possibile proteggere alcune aree di memoria della smart card in modo da impedirne la lettura e da consentire l'accesso solo dopo la corretta introduzione di un *PIN (Personal Identification Number).* La smart card consente inoltre all'utilizzatore di portare con sé le proprie informazioni riservate e identificative, e di svincolarsi così dalla particolare macchina su cui altrimenti occorrerebbe memorizzarle.

3.3 Controllo degli accessi

Il controllo degli accessi è realizzato mediante un meccanismo per identificare gli utenti ed i diritti a loro assegnati in modo da regolare la lettura, la modifica e la cancellazione di dati e programmi. Può essere ad esempio necessario discriminare l'accesso alle diverse pagine di un server Web oppure controllare chi accede, con il telnet[4], a una macchina in rete. Se un'entità tenta di accedere ad una risorsa alla quale non è autorizzata oppure qualora utilizzi una risorsa alla quale è autorizzata ma con modalità impropria, il meccanismo di controllo di accesso deve intercettare e bloccare il tentativo, e possibilmente registrare il tentativo.

Sono impiegati diversi metodi per l'identificazione. Il più noto è quello basato su *user name* e *password:* il primo (user name) è l'identificativo associato a un determinato utente mentre la password è il codice di autenticazione, associato al corrispondente user name, che deve essere fornito dall'utente per far validare dal sistema la propria identità.

Questo meccanismo di controllo non è molto affidabile; da alcune prove effettuate è stato rilevato che statisticamente la maggior parte degli utenti sceglie password più o meno facilmente intuibili. Sono disponibili programmi in grado di perpetrare attacchi di tipo *password cracking,* basati sulla ricerca sistematica delle password; questi attacchi sono ancora più semplici se l'attaccante può accedere al sistema come utente o se può reperire il file delle password[5]. Per vanificare questo attacco, una possibile soluzione è rappresentata dalle *one-time-password* in cui la password è di volta in volta variata e così ha validità per una sola sessione di lavoro (esistono ad esempio dei particolari dispositivi, detti *token,* in grado di generare password dinamiche sulla base di particolari criteri definiti in precedenza tra l'unità server di autenticazione e l'entità da identificare).

Un meccanismo di autenticazione più sicuro è quello basato sul *certificato elettronico:* quando un'entità presenta ad un sistema il proprio certificato, per verificarne la legittima appartenenza, il sistema lancia una sfida ovvero invia una stringa casuale all'entità remota che deve restituirla firmata con la propria chiave privata. Il sistema la verifica utilizzando la chiave pubblica contenuta nel certificato e, se il certificato è valido e la verifica ha esito positivo, attesta la corretta identità del soggetto.

Una volta identificato il soggetto occorre verificarne i diritti di accesso. Alcuni meccanismi sono basati sull'uso di basi di dati in cui sono registrati tutti i diritti di accesso delle diverse entità (ad esempio le Access Control List). Altri sono basati sul possesso e sulla presentazione di *informazioni di autenticazione* che forniscono l'autorizzazione all'entità (ad esempio password e ticket[6] in un sistema Kerberos, oppure un certificato e un messaggio firmato).

Gli accessi ad una rete locale possono essere regolati anche mediante i *firewall*[7]. Si tratta di un sottosistema in grado di controllare la connessione tra due reti in base a determinati parametri di sicurezza. Rispetto alle soluzioni esaminate in precedenza, il firewall consente di realizzare un meccanismo di protezione di

(4) Protocollo di emulazione di terminale.

(5) Nelle prime versioni del sistema Unix, ad esempio, l'archivio dati contenente le associazioni username-password (cifrate) era accessibile agli utenti del sistema. Sebbene le password siano cifrate, disporre dell'accesso all'archivio offre all'attaccante vantaggi nell'esecuzione di una ricerca sistematica delle stesse.

(6) Un ticket è in questo contesto un documento elettronico che attesta di poter godere di un diritto: un "titolo di ammissione".

(7) Muri tagliafuoco, secondo un'analogia con il campo dell'edilizia.

livello più basso: la funzione tipica di protezione è svolta mediante il filtraggio dei pacchetti dati in ingresso e in uscita dalla rete che si intende proteggere, in modo da bloccare il traffico non consentito. Esso consente anche un'azione di controllo e di auditing del traffico e dei tentativi di connessione illecita, segnalando tempestivamente il verificarsi di situazioni anomale. La riservatezza di una comunicazione può essere realizzata facendo cifrare tutto il canale a livello di rete, da due firewall posti alle due estremità.

3.4 Protocolli sicuri

Sono disponibili alcuni protocolli in grado di garantire l'autenticazione e la riservatezza della comunicazione: un esempio è costituito dal *SSL (Secure Sockets Layer)*, che è un protocollo a livello di trasporto sviluppato dalla Netscape e inserito nella maggior parte dei prodotti Web, sia server che browser, oggi presenti in commercio. Si tratta di un protocollo, posto sopra il *TCP/IP (Transmission Control Protocol/ Internet Protocol)*, che è stato progettato per trasportare diversi protocolli applicativi. Esso è principalmente utilizzato per sessioni sicure con *HTTP (HyperText Transfer Protocol)*, richiamate con il protocollo HTTPS. La prima fase del protocollo, detta *handshake*, prevede un'autenticazione delle parti coinvolte; successivamente è stabilita una chiave di sessione, utilizzata per cifrare tutto il canale mediante un algoritmo crittografico simmetrico.

Un altro protocollo che garantisce la sicurezza è *S-HTTP (Secure HTTP)*, ideato originariamente da

LE CONTROMISURE

- **Uno dei modi più semplici ed efficaci per garantire alcuni requisiti di sicurezza della comunicazione su Internet è l'uso della crittografia. Si tratta di un meccanismo, basato su principi matematici, che consiste nel manipolare un messaggio in modo da renderlo leggibile solo se si è in possesso di un'informazione detta chiave di decifratura. Esistono oggi due tipologie di algoritmi crittografici: i simmetrici (detti anche a chiave privata) e gli asimmetrici (o a chiave pubblica). I primi utilizzano una stessa chiave crittografica per cifrare e decifrare i messaggi (in questa categoria si collocano gli algoritmi DES, 3-DES, IDEA); i secondi si basano invece sull'uso di una coppia di chiavi - una pubblica e una privata - legate tra loro da una relazione matematica per cui tutto ciò che si cifra con una chiave è decifrabile solo utilizzando l'altra componente della coppia e viceversa (appartengono a questa tipologia gli algoritmi RSA, DSA). Cifrando i messaggi trasmessi si garantisce la riservatezza della comunicazione e si ha la possibilità di instaurare un canale sicuro per lo scambio di informazioni private.**

- **Per garantire l'autenticità e l'integrità delle informazioni trasmesse è utilizzabile la firma digitale, basata sulla crittografia asimmetrica. Per generare questa firma da allegare a un messaggio in chiaro, occorre applicare prima una funzione matematica (detta *hash)* al messaggio in modo da ottenerne un riassunto (solitamente chiamato *digest):* il riassunto è successivamente cifrato con la chiave privata del mittente e il risultato costituisce la firma elettronica da allegare al messaggio di partenza. Il ricevente, per verificare la firma digitale, deve conoscere la chiave pubblica del mittente. Solitamente questa chiave è contenuta in un documento elettronico detto certificato elettronico. Le elaborazioni crittografiche si possono far eseguire da una smart card, accrescendo i livelli di sicurezza del sistema in quanto è possibile fare in modo che sia la carta stessa a generare la chiave crittografica privata ed essere l'unica entità che la conosca. Per proteggere l'accesso alle risorse informatiche in rete occorre attuare un'attenta politica di controllo degli accessi. Molti metodi sono basati sull'uso delle password; sono numerosi e in via di diffusione tuttavia altri meccanismi che prevedono l'autenticazione mediante firma digitale, più sicuri dei precedenti in quanto per poter accedere a risorse protette non solo si deve conoscere una password (con cui si accede alla chiave privata) ma si deve anche essere in possesso di un'informazione riservata (la stessa chiave privata con cui si genera la firma).**

- **La sola crittografia non è tuttavia sufficiente per prevenire gli attacchi attuabili; è necessario affiancarla con una costante e attenta politica di controllo di tutte le vulnerabilità dei sistemi (azione di *scanning),* così pure è importante attuare un processo di audit, che consenta di ricostruire tutti gli eventi verificatisi e la relativa sequenza, in modo da poter analizzare e controllare la presenza di anomalie.**

Enterprise Integration Technologies e sviluppato successivamente da Terisa Systems. A differenza di SSL che - operando a livello di trasporto è indipendente dalle applicazioni - S-HTTP è un protocollo di comunicazione sicuro orientato ai messaggi e progettato come estensione dell'HTTP.

I due protocolli adottano diversi criteri per quanto riguarda la cifratura: SSL cifra tutto il canale di comunicazione e quindi instaura un vero e proprio canale cifrato; S-HTTP cifra invece singoli messaggi. Inoltre S-HTTP consente di firmare ogni messaggio, diversamente da SSL che prevede invece la firma di messaggi solo durante la fase iniziale di autenticazione.

Infine *PCT (Private Communication Technology)*, sviluppato da Microsoft e da Visa International per rendere sicura la comunicazione su Internet, è molto simile a SSL. Anche il formato dei messaggi è analogo, e di conseguenza un server riesce a interagire sia con utilizzatori che impiegano SSL che con utilizzatori che impiegano PCT. Questo protocollo è stato ideato per migliorare alcuni punti deboli di SSL (ad esempio esso consente una maggiore scelta per la negoziazione degli algoritmi e per il formato dati; l'autenticazione dei messaggi e la cifratura sono poi eseguite con chiavi diverse).

3.5 Scanning, Audit Trail e Controlli Procedurali

I meccanismi visti in precedenza non sono sufficienti per prevenire numerosi altri tipi di attacco, quali ad esempio l'utilizzo di comportamenti erronei o imprevisti *(bug)* nel software di alcune versioni di programmi per la posta elettronica o delle funzioni di base di alcuni server Web, che consentono l'ingresso fraudolento nel sistema e l'acquisizione di informazioni e di dati (ad esempio archivi delle password, parametri di configurazione di apparati e servizi), si rende quindi necessario attuare una strategia orientata al costante controllo di tutte le vulnerabilità del sistema di elaborazione; questa azione, svolta automaticamente o manualmente, è detta *scanning* (scansione).

Uno scanner è uno strumento software che, configurato opportunamente, consente di semplificare l'operazione di *scanning*, automatizzando le operazioni ripetitive e organizzando i risultati ottenuti secondo criteri precisi. Uno scanner automatizza quindi le azioni di un ipotetico attaccante che intenda compromettere il funzionamento del sistema in esame. Si indica come *scanning interno* quello nel quale i controlli sono eseguiti per la stessa macchina o sistema su cui è eseguita la scansione. Lo *scanning esterno* è effettuato invece da remoto: in questo caso si accede, attraverso la rete, ai soli servizi che la macchina fornisce, tentando di sfruttarne i malfunzionamenti per portarne alla luce le vulnerabilità. Un buon prodotto di *scanning* non è solo in grado di mettere in evidenza le vulnerabilità di un sistema ma anche di dare informazioni sulle contro misure da adottare (quali ad esempio patch software o parametri di riconfigurazione).

Un altro metodo per controllare e mantenere l'integrità e l'affidabilità di un sistema di elaborazione e di trasmissione dell'informazione è il processo di *audit*. Questo processo permette di ricostruire in sequenza tutte le azioni, le trasmissioni e gli interventi che hanno interessato il sistema in modo da poterle analizzare e controllare per verificare la presenza di possibili anomalie. Principio base di questo meccanismo è quello per cui nessuno dovrebbe essere in grado di accedere a qualsiasi elemento del sistema distribuito senza che ogni azione da esso svolta venga contemporaneamente registrata.

I *controlli procedurali* consentono infine di controllare l'intero sistema mediante verifiche automatiche e sistematiche. I principali controlli attuabili consistono nel monitorare costantemente lo stato della rete - in modo da notificarne tempestivamente i malfunzionamenti - e, allo stesso tempo, di controllare periodicamente gli archivi dati di registrazione degli accessi e dell'attività del sistema per verificarne l'integrità complessiva.

4. Nuove regole

La consistenza della sicurezza su Internet richiede interventi non solo tecnologici, ma anche regolamentari. Il problema delle regole da stabilire su Internet è particolarmente critico, anzitutto per lo sviluppo esplosivo che essa ha avuto, in secondo luogo per il ruolo centrale che Internet gioca, come prototipo della *Global Information Infrastructure*, l'infrastruttura tecnologica della Società dell'Informazione e, infine, per la complessità da essa presentata, essendo un mezzo di comunicazione innovativo, privo dei tradizionali vincoli di tipo geografico, e uno strumento interattivo ed estremamente flessibile, in quanto è in grado di gestire svariati modelli di comunicazione, dalla pubblicazione diffusiva alla comunicazione personale.

Assegnare regole su Internet non è semplice, in quanto la Rete è stata caratterizzata fin dalla sua nascita da un carattere fortemente libertario e alternativo rispetto ai sistemi di comunicazione tradizionali, e anche per le modalità *bottom-up* di progettazione e sviluppo, per l'amministrazione e gestione estremamente decentrata, per la facilità di espressione, di comunicazione, di interconnessione a livello globale, e per l'esteso numero di utilizzatori, favorito dai bassi costi di impiego finale.

Su Internet però non è agevole localizzare chi fa che cosa e dove lo fa, è difficile attribuire le responsabilità e la giurisdizione territoriale, e infine può essere problematica l'applicazione delle leggi, concepite per i tradizionali contesti di comunicazione.

Questo contesto ha condotto negli anni scorsi a posizioni estreme, che sostenevano che Internet è un "territorio" nel quale non valgono le leggi ordinarie, ma dove vige una sorta di diritto virtuale *(cyber-law)*. Questa posizione sarebbe inadeguata, dal momento che Internet è un territorio in cui si possono avere contenuti o comportamenti illegali, come la violazione della proprietà intellettuale e della riservatezza, il coinvolgimento dei minori nella produzione e diffusione di materiale pornografico, o attività di truffa o di terrorismo. Negli ultimi anni si sono perciò moltiplicate, in ambito nazionale, comunitario e internazionale, le iniziative per

costituire un assetto di regole per Internet.

Una trattazione organica di questa materia, che è oggetto di consultazioni internazionali ed essendo estremamente fluida lascia aperte molte questioni, può essere trovata in due documenti pubblicati di recente [3], [4]. In questa sezione sono solo focalizzate le iniziative di regolamentazione più attinenti ad alcuni aspetti di sicurezza informatica.

4.1 Le regole comunitarie sull'uso sicuro di Internet

La Commissione europea si è pronunciata sul processo di regolamentazione di Internet con due documenti di rilievo, predisposti dalla Direzione Generale XIII - competente per le Telecomunicazioni, il Mercato dell'Informazione e la Ricerca - e pubblicati nell'ottobre 1996: la Comunicazione sui contenuti dannosi e illegali su Internet e il Libro Verde sulla Protezione dei Minori e della Dignità umana nei servizi audiovisivi e informativi (i documenti sono reperibili sul sito Internet http://www2.echo.lu/legal).

I concetti delineati qui di seguito sono stati sviluppati nella Dichiarazione Ministeriale di Bonn (luglio 1997) e nel piano di azione, per promuovere l'uso sicuro di Internet, che la Commissione ha recentemente proposto [5].

Punti fondamentali della posizione comunitaria sono:

- Gli stati membri sono tenuti all'applicazione della legge anche su Internet. Ciò che è illegale nel mondo offline resta illegale anche online.
- Si promuove la cooperazione tra gli Stati nazionali per l'armonizzazione e l'applicazione delle legislazioni su Internet.
- Si consiglia l'adozione di sistemi di classificazione e filtraggio dei contenuti, accompagnati ad una azione di creazione di consapevolezza sulle risorse e le potenzialità di Internet, rivolta particolarmente all'infanzia, ai genitori e agli insegnanti.
- Si raccomanda agli operatori privati coinvolti, un processo di autoregolamentazione, che includa l'adozione di codici di comportamento e la definizione di numeri telefonici di emergenza per la segnalazione di eventuali contenuti illegali.

4.2 La regolamentazione di Internet in Italia

L'Italia è stato il primo Paese europeo a recepire le indicazioni della Commissione e del Consiglio Europeo in merito all'autoregolamentazione di Internet: già nel giugno 1997 è stato infatti presentato al Ministero delle Poste e delle Telecomunicazioni un Codice di autoregolamentazione per i servizi Internet, che costituiva il risultato di un gruppo di lavoro formato da esperti di *AIIP (Associazione Italiana Internet Provider), ANEE (Associazione Nazionale Editoria Elettronica),* Telecom Italia e Olivetti. Il codice, che può essere esaminato su Internet presso il sito http://www .aiip.it/codice.htm, fissa i principi di:

- *identificazione degli utenti:* tutti i soggetti di Internet devono essere identificabili, in particolare devono consentire di acquisire i propri dati personali a chi fornisce loro accesso e/o hosting. I fornitori di servizi, a loro volta, sono tenuti a registrare questi dati per renderli disponibili all'autorità giudiziaria nei termini previsti dalla legge;
- *anonimato protetto:* qualsiasi soggetto, una volta identificato dal proprio fornitore di accesso, ha diritto a mantenere l'anonimato nell'utilizzo della Rete al fine della tutela della propria sfera privata. Questo potrà essere realizzato mediante un identificativo diverso dal nome (pseudonimo), fornito dal fornitore di accesso o di hosting, utilizzato per operare in Rete;
- *responsabilità:* il fornitore dei contenuti è responsabile delle informazioni che mette a disposizione del pubblico (il fornitore di accesso è perciò sollevato dalle responsabilità sui contenuti trasportati).

Il codice tutela le libertà fondamentali di espressione e di accesso alle informazioni, e garantisce la protezione della vita privata e la tutela dei dati personali. La posta elettronica è equiparata alla normale corrispondenza, per quanto riguarda il diritto al segreto epistolare. Il codice poi garantisce la tutela dei consumatori nelle attività di commercio elettronico e tutela i diritti di proprietà intellettuale e industriale; vincola i fornitori di contenuti ad autoclassificare i contenuti da essi offerti e a rendere facilmente accessibili le informazioni funzionali e tecniche sull'utilizzo dei programmi di filtraggio. Infine, regola le attività commerciali e professionali, in particolare la pubblicità.

Il codice sarà applicato da un Comitato attuativo e da un Giurì di autotutela. Al Comitato attuativo spetta la definizione delle modalità per l'autoclassificazione e il filtraggio, tenendo in considerazione lo stato dell'arte tecnologico, la diffusione dei sistemi in ambito internazionale e la coerenza con le scelte effettuate dagli altri Stati membri dell'Unione Europea. Le procedure attuative prevedono la segnalazione di infrazione attraverso una istanza, contenente la descrizione dell'infrazione e il riferimento dell'indirizzo Internet interessato, che l'utilizzatore di Internet potrà inviare per posta elettronica, fac-simile o con la posta tradizionale. Al Giurì spetta di procedere all'istruttoria in merito, adottando i necessari provvedimenti, che potranno variare dalla chiusura del sito, in caso di pronunciamento negativo, alla diffida o alla formale ammonizione del soggetto di Internet interessato. In caso di contenuti o comportamenti che, oltre a infrangere il codice di autoregolamentazione, fossero anche illeciti, il Giurì dovrà provvedere alla segnalazione all'Autorità giudiziaria, garantendo la massima collaborazione per il seguito delle indagini.

4.3 La piattaforma per la selezione dei contenuti di Internet (PICS)

Per la classificazione e il filtraggio dei contenuti, oggi si sta affermando il sistema *PICS (Platform for Internet Contents Selection),* un insieme di standard aperti sviluppato dal World Wide Web Consortium, conforme con le linee guida comunitarie e largamente riconosciuto sia dall'industria, sia dal mondo accademico (per approfondire questo argomento può essere consultato, su Internet, il sito http://www.w3.org/PICS e possono essere esaminati i lavori fondamentali [6] e [7], da cui

sono state tratte le figure 6 e 7.

PICS definisce le specifiche su come creare etichette di classificazione *(rating labels)* per i contenuti su Internet, ma non specifica il vocabolario delle etichette, né chi è preposto a controllarle. Per fare un paragone con il mondo fisico, PICS specifica dove le etichette devono essere collocate su un pacco, e con quale carattere debbono essere scritte, ma non il contenuto di esse. Il principio di funzionamento di PICS è che "non tutti i contenuti sono adatti a ogni

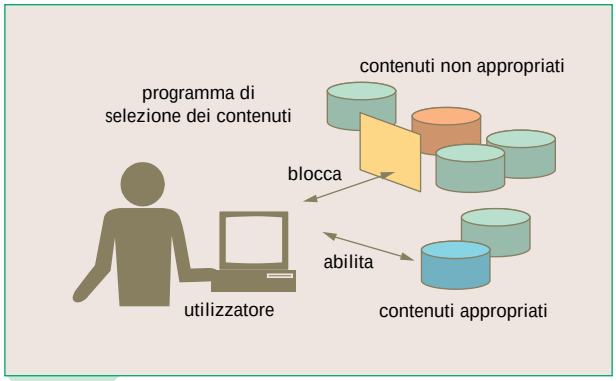


Figura 6 *Schema di riferimento per i contenuti di Internet (PICS).*

tipo di audience". D'altra parte, non tutti hanno la necessità di bloccare gli stessi contenuti. I genitori possono desiderare di non esporre i propri figli ad immagini di sesso o di violenza. Negli ambienti di lavoro, può essere opportuno impedire agli impiegati di accedere a siti di intrattenimento. I governi nazionali possono avere l'obiettivo di impedire l'accesso a contenuti che sono illegali rispetto al proprio ordinamento legislativo e giuridico. È necessaria pertanto una soluzione flessibile, che tenga conto di almeno tre fattori:

- *il supervisore:* gli stili educativi, o le politiche di direzione e governo, che possono essere diverse;
- *il destinatario:* i contenuti appropriati possono dipendere dall'età, o dalla sensibilità dei destinatari;
- *il contesto:* un'applicazione di intrattenimento, o una chat room, possono essere appropriate in ambiente domestico, ma non in quello professionale o scolastico.

La piattaforma PICS consente di realizzare i controlli di accesso in base a questi tre fattori. L'idea base, illustrata in figura 6, consiste nell'interporre tra il destinatario e i contenuti in linea un programma di filtraggio. Il programma controlla le etichette per decidere se consentire l'accesso a determinati contenuti, in maniera flessibile, ad esempio in base al destinatario o all'orario.

Prima dello sviluppo di questo tipo di piattaforma, non era disponibile un formato standard per le etichette, per cui gli utilizzatori che intendevano esercitare un controllo sugli accessi dovevano sviluppare sia il software, sia le etichette. PICS fornisce un formato comune per le etichette, riconoscibile dai programmi conformi a questo standard. Un singolo sito o un documento può essere classificato in base a diverse tipologie di etichette, fornite da diversi servizi di classificazione *(rating services).* Gli utenti hanno la facoltà di scegliere indipendentemente il software di filtraggio e, in base ai criteri determinati dai loro orientamenti *(policy),* possono individuare i servizi di classificazione più appropriati (figura 7).

Questa separazione funzionale ha consentito lo sviluppo di due mercati, uno più tecnologico, orientato alla realizzazione di programmi di filtraggio (che non entrano in merito sui contenuti), e quello dei servizi di classificazione, che è invece indipendente dalla tecnologia.

Le etichette possono riguardare aspetti specifici dei contenuti, quali i livelli di linguaggio offensivo, sesso, violenza. A loro volta i servizi di classificazione, forniti dallo stesso Web publisher *(self-rating)* o da una organizzazione indipendente *(third-party rating),* assegnano i valori alle etichette. Il software di filtraggio ha le funzioni di leggere le etichette e di bloccare automaticamente i contenuti che non soddisfano i criteri specificati dall'utente Internet.

La flessibilità di questo standard consente a un singolo sito Web di disporre di etichette multiple, applicate da diversi sistemi di rating. Gli utenti (ad esempio i genitori) sono liberi di selezionare i servizi di classificazione più appropriati in base ai loro valori. Essi possono scegliere anche se bloccare l'accesso dei loro figli ai contenuti che non hanno etichette, o se condizionare il blocco a una visione del materiale.

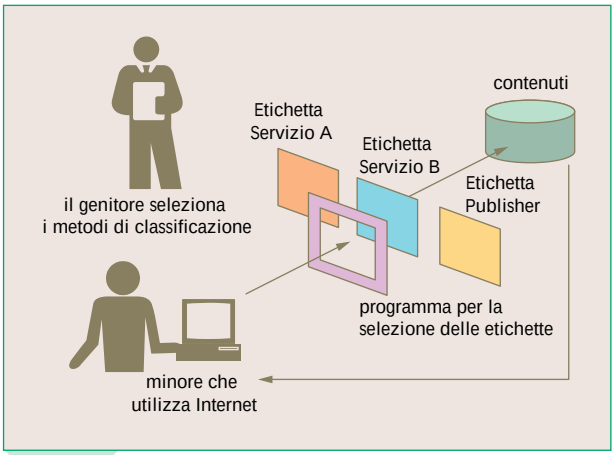


Figura 7 *Selezione delle etichette.*

L'offerta di prodotti conformi a standard PICS è oggi piuttosto ampia. Il Web browser Microsoft Internet Explorer integra un programma di filtraggio. Servizi di classificazione conformi a PICS, che entrano pertanto in merito ai contenuti, sono adesso forniti da *RSACI (Recreational Software Advisory Council on the Internet,* si veda il sito http:// www .rsac.org/), SafeSurf (si veda http://www .safe surf.com/), CyberPatrol (si veda http://www. cyberpatrol.com). Al crescere dell'uso di Internet e delle conseguenti necessità di filtraggio dei contenuti, è presumibile che cresceranno domanda e offerta di questo tipo di soluzioni.

4.4 Progetti di ricerca e sviluppo sui servizi sicuri

L'impegno della Direzione Generale XIII sulla ricerca e sviluppo riguarda anche la promozione dei servizi sicuri, oggi in corso nei programmi *ETS (European Trusted Services,* si veda http://www.cordis.lu/infosec/src/ets.htm) e Telematics (si veda http://www2.echo.lu/telematics/research). Una breve descrizione dei progetti più significativi può dare l'idea della grande varietà delle applicazioni di ricerca e di business.

4.4.1 ETS I

La prima fase di ETS, avviata nel 1997, ha riguardato il finanziamento di progetti pilota relativi a servizi di base e a diversi settori applicativi.

Tra i progetti sui servizi di base di *Trusted Third Party* sono di particolare rilievo *Oparate* e *Eurotrust.* Il progetto Oparate cura aspetti organizzativi e di gestione, l'interoperabilità di servizi eterogenei e la possibile evoluzione di una rete di Trusted Third Party verso servizi di garanzia della riservatezza e di ricostruzione delle chiavi. Il progetto Eurotrust persegue l'obiettivo di realizzare un servizio di Trusted Third Party pilota, mediante il quale i partner del progetto possano distribuire e gestire chiavi digitali e certificati da utilizzare per posta elettronica sicura, EDI, trasferimento di archivi dati e servizi di messaggistica e pagamento elettronico.

Tra i diversi progetti sviluppati per particolari applicazioni, può essere ricordato il progetto *Oscar,* per il mercato interno europeo (certificazione di business e servizi di messaggistica sicura), e il progetto *Krisis,* per la definizione di un sistema di ricostruzione delle chiavi, che sia accettato dal settore commerciale e possa essere utilizzato da agenzie governative per l'intercettazione controllata. Infine i progetti *Mandate, Aequitas* e *Euromed-ETS* riguardano rispettivamente applicazioni finanziarie, giuridiche (per avvocati, giudici, pubblici ministeri) e per la telemedicina.

4.4.2 ETS II

Per la seconda fase di ETS è stato indetto nel 1998 un bando di gara con l'obiettivo di sviluppare una architettura per una infrastruttura a chiave pubblica e firma elettronica, comprendente un quadro di riferimento per la verifica della qualità dei servizi di sicurezza, modelli dei costi, promozione del mercato, servizi di validazione temporale, sicurezza del World Wide Web.

4.4.3 ICE-TEL

Nell'ambito del programma *Telematics,* è stato avviato il progetto *ICE-TEL (Interworking Public Key Certification Infrastructure for Europe),* che ha l'obiettivo di aumentare l'affidabilità di Internet, negli utilizzi di ricerca industriale e universitaria. Il progetto, a cui collabora il Politecnico di Torino, comprende un'infrastruttura di sicurezza ed una piattaforma applicativa per adattare e per integrare gli strumenti necessari ad inserire un sistema di sicurezza basato su chiavi pubbliche in applicazioni di tipo Web, di posta elettronica, di banche dati elettroniche e di conferenze multimediali. L'applicabilità e la possibilità di impiego degli strumenti sarà validata in diversi contesti: la comunicazione sicura tra gli Enti amministrativi, le reti nazionali *CERT (Computer Emergency Response Teams)* e la realizzazione di servizi di indirizzari elettronici *(Directory).*

4.5 Normative europee per l'Autorità di Certificazione

La Direzione Generale XIII è il punto di riferimento in ambito europeo anche per la definizione degli aspetti normativi per l'Autorità di Certificazione. I documenti fondamentali da essa redatti sono la Comunicazione "Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche: verso la definizione di un quadro europeo in materia di firme digitali e di cifratura" (ottobre 1997, può essere consultata sul sito Internet http://www.ispo.cec.be/eif/policy/) e una proposta di Direttiva, ora in corso di esame presso il Parlamento Europeo e il Consiglio dell'Unione Europea, presentata in una azione congiunta con la Direzione Generale XV sul Mercato Unico (maggio 1998, consultabile sul sito Internet http://europa.eu.int/comm/dg15/en/media/infso/sign.htm).

4.5.1 La Comunicazione sulla firma digitale

La Comunicazione persegue l'obiettivo di sviluppare una politica europea, destinata a creare un quadro comune per le firme digitali che garantisca il funzionamento del mercato interno di servizi e di prodotti per la crittografia, dia impulso a un'industria europea di riferimento e stimoli gli utilizzatori in tutti i settori economici a trarre beneficio dalle opportunità della Società dell'informazione globale. Per quanto riguarda il calendario di attuazione, la Commissione considera che le misure opportune dovranno essere messe in opera entro il Duemila e si impegna a completare i progetti di ricerca e sviluppo in corso nel campo della firma elettronica e della cifratura (già trattati nel paragrafo 4.4) - nell'ambito del Quarto Programma-quadro (1994-1998) - ed a promuovere nuovi progetti nell'ambito del Quinto Programma-quadro (1998-2002).

Il documento affronta anche il delicato problema del riconoscimento reciproco dei certificati rilasciati dalle Autorità di Certificazione di Paesi differenti. Per realizzare questo obiettivo, le strutture operanti a livello nazionale potrebbero essere affiancate da un meccanismo di coordinamento a livello europeo. Questa concezione è in linea con la strategia di negoziazione istituita dalla Comunità in materia di riconoscimento reciproco e dovrebbe incoraggiare lo sviluppo di servizi di certificazione in Europa, anche perché accordi con Paesi terzi saranno più facili da concludere e saranno più interessanti sul piano economico, se basati su un regime comune a livello comunitario.

4.5.2 La proposta di Direttiva sulla firma digitale

La proposta di Direttiva si propone di dare concretezza legale a questo regime comune, assicurando che

la firma digitale (il termine usato è *electronic signature),* introdotta nelle singole legislazioni nazionali e applicata in reti aperte, è legalmente riconosciuta nell'Unione Europea, sulla base dei principi del Mercato Unico sul libero movimento dei servizi.

La proposta fa riferimento ad un quadro tecnologico neutrale, che prevede dispositivi di creazione e di verifica della firma *(signature creation device* e *signature verification device),* ma non fa alcun riferimento alle modalità tecnologiche.

Il testo pone requisiti molto stringenti ai certificatori, ai quali non si richiede un'autorizzazione preventiva, ma si precisa che essi sono tenuti alla rispondenza a requisiti essenziali, quali l'affidabilità del personale, l'uso di sistemi sicuri e il divieto di mantenere le chiavi private di firma. I Paesi membri sono liberi di definire schemi di accreditamento aggiuntivi per i certificatori, in modo da garantire livelli qualificati di sicurezza. In ogni caso, quei certificatori che intendano fornire ai propri utenti il riconoscimento legale dei certificati dovranno soddisfare requisiti aggiuntivi.

I certificatori sono responsabili dell'accuratezza del contenuto dei certificati (a meno che il certificatore non dichiari esplicitamente il contrario, questo requisito è comunque più stringente di quanto oggi prescritto dalla regolamentazione italiana, come sarà chiarito nel successivo paragrafo 4.6) e devono assicurarsi della corrispondenza tra il titolare del certificato e i dispositivi di creazione e di verifica della firma. Per quanto riguarda la validità legale, è prescritto che la firma digitale non dovrebbe essere discriminata per il fatto di essere disponibile in forma elettronica. Per facilitare il commercio elettronico a livello globale, la

IL QUADRO NORMATIVO ITALIANO

- **In Italia il valore legale dei documenti elettronici, della firma elettronica e dell'Autorità di Certificazione è riconosciuto dall'impianto legislativo, secondo uno schema articolato in una struttura gerarchica a tre livelli, che ha consentito al legislatore una azione più snella per adeguare l'applicazione del diritto alla rapida evoluzione tecnologica: una legge (nota come Bassanini 1) che fissa i principi generali; un regolamento attuativo, che definisce gli aspetti regolatori; un allegato di norme tecniche - ancora non approvato - che dovrà essere formalizzato con un Decreto del Presidente del Consiglio dei Ministri. Il regolamento e le norme tecniche sono stati predisposti dall'*AIPA (Autorità per l'Informatica nella Pubblica Amministrazione).***

- **La legge 15 marzo 1997 n. 59 (nota come "legge Bassanini 1") dispone che atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge.**

- **Il regolamento attuativo, emesso con Decreto del Presidente della Repubblica del 10 novembre 1997 n. 513 (Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'articolo 15, comma 2, della legge 15 marzo 1997 n° 59), introduce nella legislazione italiana i concetti tecnologici di documento informatico, firma digitale, indirizzo elettronico, certificazione e validazione temporale. I certificatori riconosciuti dalla legge, per cui il regolamento determina competenze e obblighi, devono essere registrati presso l'AIPA.**

- **Le norme tecniche sono contenute in un allegato al regolamento (Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513) che dovrà essere reso operativo con un Decreto del Presidente del Consiglio. L'allegato tecnico adotta gli standard RSA e DSA per la firma digitale, la raccomandazione ITU-T X.509 per il formato dei certificati, gli algoritmi Dedicated Hash-Function 1 (RIPEMD-160) e Dedicated Hash-Function 3 (SHA-1) per le funzioni di hash. La lunghezza minima della chiave è fissata in 1024 bit. Si prevede la possibilità di accordi tra certificatori diversi, in modo da ammettere certificazioni incrociate (cross-certification) e gerarchie di certificatori. Le Pubbliche Amministrazioni potranno istituire e gestire servizi di certificazione, avvalendosi di servizi offerti dai certificatori riconosciuti dall'AIPA, nel rispetto delle norme vigenti per l'aggiudicazione delle pubbliche forniture.**

proposta prevede meccanismi per la cooperazione con Paesi terzi, sul mutuo riconoscimento dei certificati sulla base di accordi bilaterali o multilaterali.

La Direttiva (in particolare la totale indipendenza dalle tecnologie e la elevata responsabilizzazione dei certificatori) è ora in corso di esame nel Consiglio dell'Unione Europea, e si prevede l'emanazione di una norma entro la prima metà del 1999.

4.6 La regolazione della certificazione e della firma digitale in Italia

In Italia, come in altri Paesi (tra cui la Danimarca, la Francia, il Belgio, la Gran Bretagna, gli Stati Uniti, il Canada e il Giappone) è riconosciuto il valore legale dei documenti elettronici, della firma elettronica e dell'Autorità di Certificazione. Il quadro normativo è articolato in una struttura gerarchica a tre livelli: una legge (nota come *Bassanini 1)* che fissa i principi generali; un regolamento attuativo (definito nel DPR del 10.11.97 n. 513); un allegato di norme tecniche, ancora non esecutivo, che dovrà essere approvato mediante un Decreto del Presidente del Consiglio dei Ministri. Una volta entrate in vigore, le norme tecniche dovranno essere riaggiornate con cadenza almeno biennale, in modo da essere in linea con l'evoluzione tecnologica. Questa struttura articolata, in cui l'*AIPA (Autorità per l'Informatica nella Pubblica Amministrazione)* ha avuto il compito di predisporre il regolamento e le regole tecniche, ha consentito al legislatore un'azione più snella per adeguare l'applicazione del diritto alla rapida evoluzione tecnologica.

4.6.1 La legge (Bassanini 1)

La legge del 15 marzo 1997 n. 59 (nota come "legge Bassanini 1") prescrive all'articolo 15 che sono validi e rilevanti a tutti gli effetti di legge atti, dati e documenti predisposti dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici. Lo stesso articolo fa riferimento a specifici regolamenti che stabiliscono, per la Pubblica Amministrazione e per i privati, i criteri e le modalità di applicazione di quanto affermato.

4.6.2 Il regolamento (DPR del 10 novembre 1997, n. 513)

Il primo regolamento è stato emesso con Decreto del Presidente della Repubblica del 10 novembre 1997 n. 513 (Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici a norma dell'art. 15, comma 2, della legge 15 marzo 1997 n° 59), con l'obiettivo di definire gli aspetti regolatori relativi alla firma digitale. Questo regolamento introduce nella legislazione italiana i concetti tecnologici di documento informatico, di firma digitale (con i concetti collaterali di sistema di validazione e di chiavi asimmetriche), chiave biometrica, indirizzo elettronico, certificazione - con i concetti collaterali di revoca, sospensione e validità del certificato - e infine di validazione temporale.

Il servizio di validazione temporale è definito come il risultato della procedura informatica, con cui si attribuiscono ad uno o a più documenti informatici una data e un orario opponibili a terzi, cioè presentabili come prova nel caso di contestazioni. Questo servizio, che in generale serve per attribuire certezza ad un documento circa il momento in cui esso è stato redatto ed è divenuto valido, dovrebbe svolgere un ruolo fondamentale nel processo di certificazione riconosciuto valido, in quanto consentirebbe di indicare i momenti critici della vita del certificato (emissione, sospensione e revoca) e quindi di evitare la retroattività in caso di revoca dei certificati per la compromissione della chiave segreta.

Il regolamento fissa gli obblighi dei certificatori, precisa i requisiti di legge a cui essi debbono sottostare (tra cui solidità finanziaria, possesso dei requisiti di onorabilità richiesti ai soggetti bancari, affidabilità, qualità dei processi e dei prodotti informatici). I certificatori poi dovranno essere inclusi in un apposito elenco pubblico predisposto, mantenuto e aggiornato a cura dell'AIPA. Inoltre, le pubbliche amministrazioni provvederanno autonomamente alle funzioni di generazione, certificazione e utilizzo delle chiavi pubbliche di competenza.

Il regolamento fissa anche le condizioni per la validità legale della firma digitale e dei contratti stipulati con strumenti informatici o per via telematica. Altresì, sancisce la segretezza della corrispondenza trasmessa per via telematica, precisando che gli addetti alle operazioni di trasmissione telematica non possono prendere cognizione dei contenuti, duplicarli o cederli a terzi. Il regolamento infine prescrive le condizioni di validità della firma digitale autenticata, che integra e sostituisce la tradizionale firma autenticata.

Il regolamento ammette il deposito in forma segreta della chiave privata presso un notaio o presso un altro archivio pubblico autorizzato (ma non presso il certificatore). La chiave privata deve essere consegnata chiusa in un involucro sigillato in modo che le informazioni non possano essere lette, conosciute o estratte da terzi senza l'effrazione del contenitore.

Il regolamento non precisa le responsabilità legali dell'utente per la perdita della chiave privata (non specifica ad esempio la differenza tra i casi di negligenza, di furto o di abuso di fiducia da parte di un impiegato), dell'Autorità di Registrazione - nelle attività di verifica relative all'identità del proprietario di un certificato - dell'Autorità di Certificazione - per il controllo della firma digitale, o nei casi di interruzione del servizio, guasto del dispositivo di firma, compromissione della chiave privata.

4.6.3 Le regole tecniche (allegato tecnico dell'AIPA)

Le regole tecniche sono contenute nell'apposito allegato di un Decreto del Presidente del Consiglio, che è in attesa di approvazione (Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513).

L'allegato tecnico, dopo l'introduzione di alcune

regole generali, definisce regole di dettaglio sulla certificazione, sulla validazione temporale e sulla conservazione dei documenti, e infine sull'uso dei certificati da parte delle Pubbliche Amministrazioni.

Regole generali

Le regole definiscono tre tipi di chiavi, precisando che una chiave non potrà essere utilizzata per fini diversi da quelli per cui è stata generata (questa indicazione implica che le chiavi di sottoscrizione non possono essere utilizzate per la cifratura):

- chiavi di sottoscrizione (per la generazione e la verifica delle firme apposte o associate ai documenti);
- chiavi di certificazione (per la generazione e la verifica delle firme apposte ai certificati e alle liste di revoca o sospensione);
- chiavi di marcatura temporale (per la generazione e la verifica delle marche temporali).

È stato anche introdotto il concetto di dispositivo di firma, che consiste in un apparato elettronico dedicato facente parte del sistema di validazione e in grado di conservare in modo protetto le chiavi private e di generare al proprio interno le firme digitali. È stato prescritto che gli strumenti e le procedure utilizzate per la generazione, l'apposizione e la verifica delle firme digitali debbono presentare al sottoscrittore, con chiarezza e senza ambiguità, i dati a cui la firma si riferisce. In questo senso, la firma digitale è una manifestazione di volontà dell'utente e non un processo automatico che egli subisce.

Né il dispositivo né le chiavi in esso contenuto possono essere duplicati. Il titolare delle chiavi (che è unico, per una data coppia di chiavi) è tenuto a conservare con la massima diligenza il dispositivo di firma ed a mantenere le informazioni di abilitazione all'uso della chiave privata (tipicamente, un PIN) in luogo diverso dal dispositivo contenente la chiave. Nel caso di smarrimento o difetto, l'utente è tenuto a richiedere immediatamente la revoca della certificazione della chiave.

La coppia di chiavi è generata in un sistema (per il quale si richiede la rispondenza al livello di valutazione ITSEC[8] E3, o superiore, e al livello HIGH, per la robustezza dei meccanismi) che deve garantire l'equiprobabilità di tutte le coppie possibili e l'identificazione del soggetto che attiva la procedura di generazione. Se la generazione avviene su un sistema diverso dal dispositivo di firma, devono essere assicurate l'immediata distruzione di qualsiasi informazione prodotta durante il processo di generazione e non più necessaria, e il trasferimento sicuro nel dispositivo di firma.

Il dispositivo di firma e l'intero processo di generazione della firma devono essere conformi ai livelli E3 high di ITSEC, mentre il processo di verifica deve essere conforme ai livelli E2 high.

Il certificato può contenere i dati anagrafici dell'utente o uno pseudonimo. In questo caso, il certificatore è tenuto però a conoscere l'effettiva identità del titolare ed a conservare le informazioni relative per almeno dieci anni dopo la scadenza del certificato.

Per quanto riguarda le specifiche tecnologiche, sono stati adottati per la firma elettronica gli standard RSA e DSA ([8] e [9], già indicati nel paragrafo 3.1), mentre per l'algoritmo di hash, da applicare nel processo di firma elettronica (anch'esso chiarito nel paragrafo 3.1) sono adottate le funzioni Dedicated Hash-Function 1 (RIPEMD-160) e Dedicated Hash-Function 3 (SHA-1), definite mediante la norma ISO/IEC 10118-3:1998. La lunghezza minima delle chiavi è stabilita in 1024 bit. Per i certificati, sono riconosciute la validità della Raccomandazione ITU-T X.509 edizione 1995 (variante 1) e le specifiche pubbliche PKCS#6 e PKCS#9[9]. L'accesso al registro pubblico dei certificati mantenuto dal singolo certificatore avviene con una modalità compatibile con il protocollo LDAP definito nella specifica pubblica RFC 1777. Sui dispositivi di firma (che potranno essere sistemi hardware dedicati, come una smart card) non sono definiti requisiti tecnici più precisi, oltre alla conformità alla valutazione secondo ITSEC.

Regole per la certificazione delle chiavi

Il certificatore, la cui domanda di iscrizione sia stata accettata (sulla base delle modalità definite nel Regolamento) deve predisporre con l'AIPA un sistema di comunicazione sicuro e deve fornire le proprie informazioni da inserire nell'elenco pubblico mantenuto dall'AIPA, tra cui i certificati relativi alle proprie chiavi di certificazione (generati sottoscrivendo con la chiave privata della coppia cui il certificato si riferisce). Inoltre il certificatore deve generare un proprio certificato per ciascuna delle chiavi di firma dell'AIPA e provvedere a pubblicarlo nel proprio registro dei certificati.

È consentito l'accordo di certificazione tra certificatori diversi, con cui uno di essi emette a favore di un altro un certificato relativo a ciascuna chiave di certificazione che è riconosciuta nel proprio ambito. Sono così ammesse le certificazioni incrociate *(cross-certification).*

Regole per la validazione temporale

In questo ambito, si prescrive che qualunque evidenza informatica può essere soggetta a validazione temporale generando per essa una marca temporale. Le marche temporali sono generate da un apposito sistema elettronico sicuro in grado di:

- mantenere la data e l'ora con sufficiente precisione. A questo proposito si fa riferimento alla scala di tempo *UTC (Tempo Universale Coordinato),* mantenuta dall'*IEN (Istituto Elettrotecnico Nazionale)* Galileo Ferraris, di Torino (consultabile nel sito Internet http//www.ien.it/), rispetto alla quale l'orologio del servizio non può variare

(8) Per la valutazione di sicurezza di un sistema o prodotto ITSEC, si veda il riquadro di pagina 55.

(9) I PKCS (Public-Key Cryptography Standards) *sono un insieme di standard (sviluppati presso* RSA Laboratories *a partire dal 1991) che definiscono le modalità tecniche di realizzazione e interoperabilità per la crittografia a chiave pubblica. In particolare, gli standard 6 e 9 definiscono rispettivamente la sintassi per un'estensione del certificato X.509 e i tipi degli attributi che possono essere inclusi nel certificato esteso.*

LA VALUTAZIONE DELLA SICUREZZA

- **I criteri *ITSEC (Information Technology Security Evaluation Criteria)* sono l'insieme dei principi, adottati dall'Unione Europea, per la valutazione della sicurezza di un sistema o prodotto informatico (si veda anche il sito Internet http://www.cordis.lu/infosec/src/crit.htm). In generale, la valutazione della sicurezza comprende un esame ed un collaudo particolareggiato del prodotto o sistema, in modo da assicurarsi che esso operi in maniera corretta ed efficace, senza presentare vulnerabilità logiche. Il rigore delle verifiche è misurato da un livello di valutazione dichiarato (assurance level). ITSEC è il risultato dell'armonizzazione dei criteri nazionali prodotti, nel corso degli anni Ottanta, dai gruppi di studio costituiti in Gran Bretagna, Germania, Francia e Olanda. L'attuale versione (1.2) è stata pubblicata dalla Commissione Europea nel giugno 1991. In base ad un accordo sottoscritto nel dicembre 1997, i certificati ITSEC hanno validità in tutti i Paesi membri dell'Unione Europea. I criteri sono accompagnati da un manuale operativo, redatto nel settembre del 1993, e chiamato *ITSEM (IT Security Evaluation Manual)*.**
- **I livelli di valutazione di ITSEC sono misurati da una scala di rigore crescente, da E0 a E6. Senza entrare nei dettagli, il livello E0 rappresenta una valutazione inadeguata, mentre quello massimo E6 richiede che le funzioni di sicurezza e il disegno architetturale siano specificati in stile formale, coerente con un modello di policy di sicurezza specificato. Per quanto riguarda i livelli intermedi, richiesti dalle regole tecniche per la firma digitale, il livello E2 richiede la produzione di un progetto informale particolareggiato e di documentazione delle prove, la separazione dei componenti di sicurezza nell'architettura del sistema, l'esecuzione di prove di vulnerabilità, una verifica del controllo della configurazione e della sicurezza dello sviluppo, infine un tracciamento delle funzioni di auditing. Il livello E3 richiede, oltre ai requisiti del livello precedente, la produzione del progetto del codice sorgente e di hardware, la corrispondenza tra il codice sorgente e il progetto particolareggiato, l'adozione di procedure di accettazione e di standard nei linguaggi di sviluppo, la ripetizione del collaudo dopo la correzione degli errori.**
- **Per quanto riguarda l'efficacia dei sistemi, ITSEC definisce tre livelli di forza dei meccanismi di sicurezza: basic, se il meccanismo è adeguato per attacchi accidentali; medium, se il meccanismo è adeguato per la protezione da attacchi intenzionali da parte di impostori con risorse e opportunità limitate; high (il livello richiesto dalle regole tecniche per la firma digitale), se il meccanismo può essere neutralizzato solo da un impostore che possiede elevati livelli di competenze, opportunità e risorse.**

più di un secondo;
- generare una determinata struttura di dati (comprendente le informazioni rilevanti, la data e l'orario, il digest dell'evidenza informatica);
- firmare in maniera digitale questa struttura di dati.

Per il sistema di validazione temporale, si richiede la verifica della conformità ai livelli E2 high di ITSEC, mentre per la parte destinata alla sottoscrizione delle marche temporali sono richiesti i livelli E3 high. Il servizio di validazione deve garantire un tempo di risposta - misurato come differenza tra l'ora in cui la richiesta è ricevuta dal servizio e l'ora riportata nella marca temporale - non superiore al minuto primo. Il servizio deve provvedere a mantenere in un apposito archivio le marche temporali emesse.

Regole per la Pubblica Amministrazione

Le Pubbliche amministrazioni possono istituire e gestire autonomamente servizi di certificazione, per le firme digitali utilizzate nell'ambito della organizzazione interna dei propri uffici. Devono però avvalersi di servizi offerti dai certificatori riconosciuti dall'AIPA, nel rispetto delle norme vigenti per l'aggiudicazione delle pubbliche forniture.

4.7 Aspetti normativi e legali per la crittografia

Nella progettazione di sistemi che utilizzano tecnologie crittografiche, uno dei problemi di maggior rilievo riguarda la diversa regolamentazione vigente nei diversi Paesi, per utilizzo, importazione ed esportazione degli algoritmi crittografici. Il panorama mondiale si presenta oggi in maniera assai differenziata.

Dal punto di vista dell'esportazione, generalmente il controllo è mirato al trasferimento dei prodotti crittografici usati per la protezione dei dati. Alcune nazioni hanno leggi specifiche al riguardo. Per l'offerta tecnologica, di particolare importanza è la situazione degli

Stati Uniti, da cui è vietata l'esportazione di algoritmi crittografici, considerati alla stregua di armi, senza la specifica approvazione del Dipartimento del Commercio. Fino a tempi recenti non era consentita l'esportazione di algoritmi crittografici simmetrici con chiavi più lunghe di 40 bit. Questi vincoli si sono progressivamente ridotti e da quest'anno il Governo Federale degli Stati Uniti consente la libera esportazione sia di prodotti di cifratura simmetrica (DES, RC2, RC4, RC5, CAST) con chiavi fino a 56 bit, sia di prodotti per lo scambio di chiavi, contenenti algoritmi simmetrici con chiavi fino a 112 bit, o algoritmi asimmetrici con chiavi fino a 1024 bit.

Per quanto riguarda l'importazione di prodotti crittografici, la maggior parte dei Paesi, con l'esclusione significativa della Francia, non ha limitazioni; la Francia però, proprio in questo ultimo periodo sta rivedendo la sua posizione in merito alle limitazioni d'uso ed importazione di prodotti crittografici, è stata infatti annunciata (19 gennaio 1999) direttamente dal primo ministro Jospin, la decisione di abbandonare molti degli aspetti contenuti nella legge sulla crittografia del 1996 ed arrivare rapidamente ad una liberalizzazione del settore.

Negli Stati Uniti, il Governo ha intrapreso l'iniziativa di istituire infrastrutture dedicate alla gestione delle chiavi, con funzioni sia di certificazione, sia di affidamento *(key escrow):* l'affidamento delle chiavi ha lo scopo di consentire alle Autorità preposte all'ordine pubblico, di intercettare e di decifrare le comunicazioni, una volta che siano in possesso di un'autorizzazione della magistratura. L'iniziativa del Governo americano persegue l'obiettivo di subordinare alle esigenze della sicurezza nazionale il diritto personale alla riservatezza delle comunicazioni, e ha suscitato un animato dibattito nel Paese. La posizione che si sta delineando è di permettere ai singoli utilizzatori, nel caso di uso privato della crittografia, sia di scegliere l'algoritmo di cifratura, sia di aderire a sistemi con agenzie di affidamento delle chiavi.

Nei Paesi europei non sono oggi in vigore norme che limitino la lunghezza delle chiavi relative ad algoritmi simmetrici ed asimmetrici, sempre se incluse in prodotti europei. La stessa Comunicazione (indicata nel paragrafo 4.5) promuove l'utilizzo della cifratura per proteggere lo scambio di informazione confidenziale, e benché lasci piena facoltà alle singole legislazioni nazionali di formulare una propria legge sulla cifratura, evita di imporre limitazioni interne al Mercato europeo, all'esportazione di strumenti di cifratura forte.

In Italia l'uso della crittografia è regolato per quel che riguarda il suo impiego solo nella tutela del Segreto di Stato. Per altri impieghi, privati o pubblici, l'uso della crittografia non è vietato né controllato.

Un'importante iniziativa per definire una politica comune sull'utilizzo della crittografia è stata avviata dall'*OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico),* che ha definito nel marzo 1997 un documento di linee guida sulle politiche crittografiche *(Cryptography policy: the guidelines and the issues*, si veda http://www.oecd.org/dsti/sti/it /secur/index.htm). Esse sono il frutto di un bilanciamento, certamente non semplice, di principi e di interessi diversi, e spesso in conflitto tra loro, sostenuti dai differenti governi nazionali. Basti pensare alla differenza tra la posizione del Governo degli Stati Uniti, caratterizzata dai vincoli all'esportazione e dal controllo delle autorità sulla cifratura, e quella dei Paesi Scandinavi, estremamente sensibili alla protezione della riservatezza delle comunicazioni dei singoli utilizzatori. I principi espressi dalla posizione dell'OCSE riguardano la libertà di scelta del metodo crittografico impiegato dall'utente finale, lo sviluppo di standard tecnologici, il rispetto della riservatezza, e infine la possibilità per le legislazioni nazionali di autorizzare l'accesso legale ai dati cifrati, per motivi di ordine pubblico o di sicurezza nazionale. Il documento promuove il libero mercato dei prodotti crittografici, auspicando la cooperazione dei governi per coordinare le politiche crittografiche. Il documento prescrive infine che la responsabilità degli individui o delle entità che offrono servizi crittografici o che conservano chiavi crittografiche deve essere espressamente dichiarata.

5. I servizi sicuri

Grazie alla sua capillarità e crescente diffusione, la rete Internet è utilizzata per offrire una serie di nuovi servizi, in aggiunta a quelli tradizionalmente disponibili. In questo capitolo sono trattati tre dei più promettenti servizi su Internet, per i quali è d'obbligo prestare una particolare attenzione alle problematiche di sicurezza: il servizio di Autorità di Certificazione, il commercio elettronico e l'home banking.

5.1 L'Autorità di Certificazione

I contesti che richiedono relazioni fidate sono molteplici: un'azienda ad esempio ha l'esigenza di identificare con sicurezza i propri dipendenti, i collaboratori esterni, i fornitori e discriminarne i diritti d'accesso alle risorse aziendali. Per offrire un servizio di home-banking, la banca deve identificare i propri clienti e assicurare che essi percepiscano come affidabile il sito bancario. Considerazioni analoghe valgono per un servizio di vendita in rete.

Per consentire l'identificazione dei soggetti che operano in rete entra in gioco l'*AC (Autorità di Certificazione)*[10], la terza parte fidata che certifica l'identità attraverso l'assegnazione di un documento elettronico, il certificato. La fiducia riposta nell'AC è alla base dell'infrastruttura di certificazione elettronica, che è il presupposto necessario per l'adozione di uno schema crittografico a chiave pubblica.

Il ruolo della AC è affiancato da quello dell'*AR (Autorità di Registrazione)*, la cui funzione è quella di identificare l'entità che ha richiesto un certificato, di verificarne il diritto e quindi di approvarne o no l'emissione; l'AR ha inoltre il compito di approvare le

(10) Come già chiarito al precedente paragrafo 3.2, questo termine non indica un'istituzione pubblica, bensì un ruolo funzionale che può essere svolto, con modalità commerciali, da diversi soggetti.

richieste di revoca dei certificati. L'AR opera per conto di una Autorità di Certificazione e deve perciò seguire le regole ed i criteri stabiliti da questa seconda Autorità nell'accettazione delle richieste di un certificato.

Per ottenere un certificato, un'entità deve inoltrare la sua richiesta all'AC (solitamente attraverso un'interfaccia Web o il servizio di posta elettronica). Le richieste pervenute sono prima elaborate dalla AR per accertare l'identità dei soggetti: a questo scopo si possono adottare diversi criteri. Ad esempio, si può richiedere la presentazione di un documento di identità valido, oppure l'iscrizione e l'appartenenza a ordini professionali o a organizzazioni riconosciute (quali Camera di Commercio e ordine dei notai). Dopo l'approvazione da parte dell'AR, la richiesta è trasferita alla AC che rilascia il certificato, firmandolo con la propria chiave privata.

Le disposizioni applicate dalla AC sono contenute in un documento chiamato *CPS (Certification Practice Statement).* Esse devono essere rese pubbliche in modo da poter essere consultate dai sottoscrittori del servizio. Deve in particolare essere descritto il servizio di certificazione offerto, le procedure che regolano il ciclo di vita dei certificati e la loro gestione, le regole poste alla base della conduzione dell'infrastruttura di erogazione per assicurarne la sicurezza e le disposizioni da seguire per l'attuazione di esse.

Il ruolo della AC è di estremo rilievo e delicatezza e, quindi, richiede un'infrastruttura complessa non tanto dal punto di vista tecnologico, quanto piuttosto operativa per il tipo di dati elaborati.

In molti Paesi operano diversi fornitori di tecnologia e di servizi di certificazione, e tra questi i più noti sono Verisign, COST, Xcert Software Inc, Entrust Technologies e GTE CyberTrust.

Anche Telecom Italia sta entrando nel mercato dei servizi di certificazione con un'offerta, denominata VillageTrust, basata su tecnologia GTE e destinata a coloro che hanno l'esigenza di offrire ai propri clienti o ai propri collaboratori il servizio senza però sobbarcarsi il costo ingente che la realizzazione di una infrastruttura di questo tipo richiede.

L'offerta di Telecom Italia sarà quella di un servizio di certificazione in outsourcing, in cui il cliente assumerà il ruolo di certificatore esponendo il proprio marchio e ricoprirà direttamente il ruolo di Autorità di Registrazione.

Il servizio consentirà ampie possibilità di personalizzazione da parte del cliente e comprenderà , tra l'altro, politiche di sicurezza, procedure operative, personale fidato e specializzato, ridondanza delle risorse, protezione dei locali, misure di controllo e di auditing.

5.2 Commercio elettronico e home banking

Durante una transazione commerciale che si svolge su Internet devono essere tenuti in conto diversi aspetti che riguardano la sicurezza.

Il primo riguarda l'*autenticità* delle parti: occorre un meccanismo che assicuri l'utente circa la reale identità e legittimità del venditore e che, d'altra parte, assicuri quest'ultimo dell'identità del compratore. Un secondo aspetto riguarda la garanzia del *non rifiuto* di una transazione da entrambe le parti: occorre avere la prova che l'ordine di acquisto sia partito proprio da un determinato utente per impedirgli di poter affermare in seguito di non averlo inoltrato; occorre allo stesso tempo che il commerciante non abbia modo di sostenere di non aver ricevuto l'ordine di acquisto o altre informazioni di rilievo.

Un altro risvolto cruciale riguarda la fase di elaborazione del pagamento. Sono impiegati diversi *meccanismi di pagamento elettronico*, e quello oggi più utilizzato è basato sull'uso della carta di credito. Inserire il numero della propria carta di credito in rete è causa di molte perplessità da parte di utenti timorosi che possa essere intercettato e che poi sia utilizzato per scopi fraudolenti. L'*anonimato* rappresenta un'altra questione di rilievo: il compratore potrebbe infatti non gradire di dover comunicare al venditore la propria identità o altri dati personali.

Sono oggi disponibili soluzioni tecnologiche in grado di risolvere, almeno in parte, questi aspetti. A tutela dell'identificazione e autenticità delle parti coinvolte in un processo di acquisizione elettronica di beni, è adottabile il meccanismo della certificazione elettronica. La presentazione del proprio certificato e la dimostrazione di possedere la chiave privata ad esso relativa, costituisce un metodo sicuro per accertare la propria identità. Per garantire la riservatezza delle informazioni private trasmesse in rete - quale appunto il numero della carta di credito - è possibile cifrare le informazioni trasmesse in modo che solo le parti abilitate riescano a decifrarne il contenuto.

La fase di pagamento costituisce l'aspetto più critico in termini di sicurezza: le soluzioni disponibili sono realizzate a imitazione dei diversi metodi di pagamento legati al commercio tradizionale. Sono stati messi a punto meccanismi di moneta elettronica - basati sull'uso di *digital coin* - ovvero informazioni elettroniche che hanno un valore monetario utilizzabile in rete, rilasciati da intermediari quali le banche o istituti finanziari (ad esempio NetCash, Ecash). Altri metodi di pagamento sono invece ispirati al modello degli assegni cartacei (quelli, ad esempio, di BankNet e NetCheque). La maggior parte delle attuali transazioni commerciali sono oggi concluse mediante la carta di credito: in questo ambito lo standard de facto è *SET (Secure Electronic Transaction)* che è un protocollo sviluppato congiuntamente dalla VISA e dalla MasterCard insieme ad altre aziende. SET prevede un'infrastruttura di certificazione a chiave pubblica per il rilascio di certificati elettronici da utilizzare per l'autenticazione delle parti coinvolte. È inoltre assicurata la riservatezza delle informazioni scambiate utilizzando meccanismi di cifratura in modo tale che i dati di pagamento siano decifrabili solo dagli istituti finanziari e non dai commercianti, mentre al contrario il dettaglio degli ordini di acquisto sia decifrabile solo dal commerciante. Alcuni produttori, tra cui Verifone e IBM, hanno già realizzato piattaforme di commercio elettronico che consentono di concludere transazioni mediante questo protocollo.

Esiste inoltre un settore del commercio elettronico relativo a transazioni caratterizzate da notevole frequenza e da bassi importi. Esso è relativo ad esempio all'acquisto di informazioni elettroniche - quali

potrebbero essere le pagine Web - oppure di piccole applicazioni software, tipo applet Java, o ancora di immagini o di piccole registrazioni video. Per queste transazioni sono stati studiati alcuni protocolli adatti ai piccoli importi: i *micropagamenti.* L'obiettivo è quello di concludere la fase di pagamento nel modo più efficiente possibile, sia in termini di tempo (il fatto che una pagina Web sia a pagamento non deve comportare ulteriori ritardi) sia di costi aggiuntivi (è improponibile pagare un importo di poche centinaia di lire con la carta di credito in quanto il costo per concludere la transazione supererebbe l'importo da pagare). In questo contesto non è ancora stato raggiunto uno standard: sono oggi state approntate diverse soluzioni, alcune nate nell'ambito universitario (ad esempio PayWord) altre realizzate in quello commerciale (quali Millicent della Digital e MiniPay[11] di IBM).

Per quanto riguarda il requisito di anonimato del compratore, esso non può essere rispettato quando il metodo di pagamento è la carta di credito. Sono disponibili tuttavia sistemi basati sulla moneta elettronica, in grado di rispettare questo requisito. Uno di questi è *Ecash,* sviluppato dalla DigiCash. In questo modello, utilizzando la tecnica della firma cieca (si veda il paragrafo 3.2), si riesce a fare in modo che la banca convalidi le monete elettroniche senza conoscere l'identità del possessore. Per una migliore comprensione di questo modello di moneta si consideri che, con qualche approssimazione, il cliente scelga il "numero di serie" della banconota elettronica che vuole emettere e che lo invii alla banca mascherato con una sequenza casuale di bit. La banca appone una firma cieca sul numero di serie, rendendo valida la nuova banconota, e ne addebita l'importo sul conto del cliente. Quando, successivamente, un venditore presenterà alla banca la moneta elettronica ricevuta dal cliente, per accreditarla sul proprio conto, la banca verifica che il numero di serie è validato con la propria firma ma non è in grado di ricollegarlo al numero di serie firmato con una mascheratura.

Sebbene la crittografia rappresenti la soluzione di molteplici problemi di sicurezza legati alla comunicazione su Internet, sembra opportuno segnalare che la versione internazionale dei prodotti Web commerciali - per i limiti all'esportazione dagli USA di materiale crittografico - consente solo chiavi di cifratura lunghe 40 bit, non sufficienti per poter essere considerate sicure.

Le problematiche indicate per il commercio elettronico circa l'*autenticità,* la *confidenzialità* e il *non rifiuto* sono presenti anche per i servizi dell'*home banking* con i quali la banca trasferisce i propri sportelli sulla rete Internet, e permette ai clienti di effettuare molte operazioni bancarie tradizionali dal personal computer di casa o dell'ufficio.

Per quanto riguarda l'Italia, già oggi diverse banche hanno realizzato siti Web attraverso i quali i clienti possono, ad esempio, avere informazioni circa il saldo del conto corrente, gli ultimi movimenti effettuati, la situazione del portafoglio titoli, il risparmio gestito ed i tipi di finanziamento. Inoltre, sottoscrivendo un apposito contratto, è concessa anche la facoltà di effettuare bonifici e operazioni di giroconto preautorizzati. Il controllo d'accesso è d'altra parte effettuato con un meccanismo di bassa affidabilità, quale l'impiego di *username* e *password.*

Un maggiore sviluppo dei servizi di home banking sarà possibile con l'introduzione dell'autenticazione del cliente tramite certificato e firma digitale, realizzata con sistemi di crittografia di tipo forte, e con la creazione di canali di comunicazione altrettanto affidabili. Alcune banche si avvalgono ad esempio di un livello di crittografia "custom", da aggiungere a quello standard, che consente di utilizzare l'algoritmo RSA a 1024 bit, durante lo scambio di tutti i dati personali tra cliente e sito bancario.

La soluzione di Telecom Italia come ausilio alla banca elettronica è Finance-Net. L'offerta prevede tre tipi di servizi:

- *Home banking,* per l'utenza residenziale, che consente un'ampia gamma di servizi finanziari online suddivisi in due aree: gestione dei conti correnti e area finanza.
- *Corporate banking,* sviluppato per le aziende mediograndi che, oltre ai servizi bancari di base, hanno ulteriori esigenze quali la gestione del portafoglio commerciale e di pratiche verso l'estero. In questo caso le comunicazioni fra la banca e l'azienda avvengono secondo lo standard per il *CBI (Corporate Banking Interbancario),* definito dall'ABI.
- *Redazione virtuale,* è uno strumento di supporto ai processi di pubblicazione dei documenti in un sito Web, fornito in un ambiente che consente di preparare le informazioni usando i propri strumenti di Office Automation in modo da sottoporle in un secondo tempo ad un ciclo automatico di approvazione. Le informazioni validate sono poi trasformate automaticamente in documenti secondo i formati predefiniti dalla Banca, e sono quindi pubblicati e resi disponibili ai clienti.

La sicurezza a livello applicativa di Finance-Net comprende aspetti relativi all'autenticazione della banca, mediante certificato elettronico, e degli utenti (per questi il meccanismo può essere quello della password oppure del certificato), e altri riguardanti la riservatezza dei dati trasmessi - tramite un algoritmo misto con crittografia simmetrica e asimmetrica - e l'integrità, mediante funzione hash per la generazione del message digest dei dati.

6. Considerazioni finali

La chiave di successo dei servizi sicuri per facilitare lo sviluppo di Internet, e di conseguenza della Società dell'Informazione, si può individuare nella capillare diffusione dei servizi: una distribuzione di massa dei certificati digitali può infatti dare un impulso alle applicazioni della Pubblica Amministrazione e del commercio elettronico. Questo contesto apre perciò importanti opportunità per gli operatori di servizi infrastrutturali, quali i gestori dei servizi di telecomunicazione, che sono molto attivi nella

(11) Da non confondere con il servizio MiniPay italiano, il borsellino elettronico sviluppato dalla SSB (Società per i Servizi interBancari).

progettazione e nella fornitura di nuovi servizi specifici. Significativo è il caso dei servizi di outsourcing verso soggetti operanti come Autorità di Certificazione, offerti da numerosi gestori delle reti di telecomunicazione, tra i quali sono compresi Telecom Italia (con VillageTrust) e Deutsche Telekom.

Un secondo elemento di successo nel mercato dei servizi sicuri è l'integrazione trasparente delle funzioni di sicurezza nel contesto applicativo, ottenuta offrendo una interfaccia *user-friendly*, in modo che il cliente possa trarre beneficio dal servizio senza subire i sovraccarichi procedurali e prestazionali che le funzioni di sicurezza possono causare. Da questo punto di vista, la tecnologia smart card, con le sue più recenti evoluzioni (tra cui l'inclusione di tecnologia Java e la capacità di fornire più applicazioni) si presenta come una delle più promettenti in termini di facilità d'uso, anche grazie all'enorme diffusione e familiarità che questo dispositivo ha avuto nel mondo consumer, negli ambiti del GSM e della *pay-TV*. La progettazione delle soluzioni di sicurezza è quindi oggi focalizzata nell'attenta analisi delle offerte tecnologiche basate sulla smart card.

La disponibilità di leggi e di normative sulla sicurezza, se da un lato è un fattore abilitante del commercio elettronico su Internet - in quanto *regolarizza* il contesto legale, amministrativo e commerciale - d'altra parte costituisce un importante elemento di sfida per i fornitori di servizi sicuri, per i vincoli più o meno stringenti che la normativa può dettare alle modalità di servizio e l'impiego delle tecnologie. Il presidio delle attività in corso di regolazione o di auto-regolazione, necessarie per allineare la soluzione tecnologica e, se possibile, per alimentare il processo di regolamentazione tecnica, è dunque un importante obiettivo che debbono perseguire gli operatori di servizi sicuri.

Un ultimo elemento di riflessione per gli operatori dei servizi sicuri riguarda la necessità di sviluppare soluzioni aperte e interoperabili. Questa esigenza è particolarmente sentita per dare concretezza ai servizi di certificazione incrociata *(Cross-Certification)* che, come si è visto, sono entrati nelle prescrizioni anche dalla normativa europea e di quella italiana. Lo sviluppo di piattaforme di interoperabilità è promosso a diversi livelli, nei progetti a finanziamento europeo, su un piano di ricerca e sviluppo (come chiarito al paragrafo 4.4), e nell'ambito di Forum dedicati, costituiti da fornitori di servizi di rete a valore aggiunto, tra cui *MSAF (Multimedia Services Affiliate Forum,* disponibile sul sito http://www.msaf.org), per la definizione di piattaforme tecniche e procedurali, in un contesto precompetitivo.

In conclusione, si può ritenere che il livello di avanzamento delle tecnologie e della normativa sia già tale da consentire lo sviluppo e la diffusione di servizi sicuri sulla rete Internet, e che in considerazione del forte interesse al suo utilizzo commerciale come infrastruttura di comunicazione, e quindi dell'impegno di molti soggetti in questo senso, vi saranno ulteriori miglioramenti nelle tecnologie di protezione delle informazioni e, soprattutto, una progressiva armonizzazione del quadro normativo e legale nei diversi Paesi.

Abbreviazioni

3-DES	Triple DES
ABI	Associazione Bancaria Italiana
AC	Autorità di Certificazione
AIIP	Associazione Italiana Internet Provider
AIPA	Autorità per l'Informatica nella Pubblica Amministrazione
ANEE	Associazione Nazionale Editoria Elettronica
AR	Autorità di Registrazione
CAST	Encryption Algorithm
CBI	Corporate Banking Interbancario
CERT	Computer Emergency Response Team
CPS	Certification Practice Statement
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EC	Elliptic Curve
EDI	Electronic Data Interchange
ETS	European Trusted Services
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICE-TEL	Interworking Public Key Certification Infrastructure for Europe
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
ITSEC	Information Techonology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
LDAP	Lightweight Directory Access Protocol
MSAF	Multimedia Service Affiliate Forum
OCSE	Organizzazione per la Cooperazione e lo Sviluppo Economico
PCT	Private Communications Technology
PICS	Platform for Internet Contents Selection
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
RC2	Rivest's Code #2
RC4	Rivest's Code #4
RIPEMD-160	Privacy Enhanced Mail D-160
RSA	Algoritmo crittografico a chiave pubblica sviluppato da Ron Rivest, Adi Shamir e Len Adelman
RSACI	Recreational Software Advisory Council on the Internet
SET	Secure Electronic Transaction
SHA-1	Secure Hash Algorithm #1
S-HTTP	Secure HTTP
SSB	Società per i Servizi interBancari
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
UTC	Tempo Universale Coordinato

Bibliografia

[1] Dècina, M.: *Internet e l'Infrastruttura Globale dell'Informazione.* «Notiziario Tecnico Telecom Italia», Anno 6, n. 2, ottobre 1997.

[2] Schneier, B.: *Applied cryptography.* John Wiley & Sons Inc., 1996.

[3] Hance, O.: *Internet e la legge.* McGraw-Hill, giugno 1997.

[4] Torrani, O.; Parise, S.: *Internet e diritto.* Il Sole 24 ore, aprile 1998.

[5] *Action Plan on promoting safe use of the Internet.* Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions 26 November 1997 COM (97) 582 OJ C48 of 13/02/98, p. 8.

[6] Resnick, P.: *Filtering Information on the Internet.* Scientific American, March 1997, pp. 106-108.

[7] Resnick, P.; Miller, J.: *PICS: Internet Access Controls Without Censorship.* Communications of the ACM, 1996, vol. 39(10), pp. 87-93.

[8] Rivest, R.L.; Shamir, A.; Adleman, L.: A *Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM, 1978, vol. 21, n. 2, pp. 120-126.

[9] *Digital Signature Standard (DSS).* National Bureau Of Standards, Federal Information Processing Standard, U.S. Department of Commerce, FIPS PUB 186, Washington, DC, 1994.

Stefano Brusotti si è laureato in Scienze dell'Informazione presso l'Università di Torino nel febbraio del 1994 con una tesi di ricerca nell'ambito della programmazione logica induttiva (ILP) e apprendimento automatico. Ricercatore CSELT a partire dal 1996, oggi presso l'unità di ricerca Architetture e Servizi di Sicurezza nella Linea Servizi Internet della Direzione Cliente Finale; ha conseguito nel 1997, un diploma di Master COREP in Telecomunicazioni con una tesi sui servizi e sulle opportunità di utilizzo delle smart card senza contatti. Impegnato in problematiche di sicurezza fin dal suo ingresso in azienda, si è occupato di sistemi di commercio elettronico, posta sicura, certificazione digitale a standard X509 e in particolare di smart card e sistemi di moneta elettronica. Nel 1998 è stato coinvolto nel progetto ACTS SCARAB (Smart Card and Agent enabled Reliable Access) finalizzato allo studio e alla realizzazione di una architettura aperta basata sulla tecnologia degli agenti mobili e delle Java smart card e in quello Telematics, denominato DISTINCT Deployment and Integration of Smartcard Technology and Information Networks for Cross-sector Telematics) che ha come obiettivo l'integrazione di tecnologie telematiche e la definizione di una comune architettura per l'erogazione di servizi basati su smart card.

Roberta D'Amico si è laureata in Scienze dell'Informazione nel 1994 presso l'Università degli Studi di Torino. Nello stesso anno ha iniziato un'attività di collaborazione con CSELT dove è stata assunta nel 1995. Per conto di CSELT ha frequentato il Master in Telecomunicazioni, organizzato dal COREP di Torino, conseguendone il diploma nel luglio 1996 con una tesi sui sistemi di pagamento elettronico connessi al commercio elettronico su Internet. Sempre in relazione ai sistemi di pagamento elettronici sicuri, ha partecipato ad un progetto in ambito Eurescom. Dal 1996 opera nell'Unità di Ricerca Servizi e Architetture di Sicurezza, presso la linea Servizi Internet della Direzione Cliente Finale, dove si occupa di aspetti di sicurezza a livello applicativo, di infrastrutture di certificazione a chiave pubblica e di smart card. Ha collaborato con Telecom Italia per la realizzazione del servizio di certificazione elettronica per gli utenti TIN e alla definizione della policy del servizio VillageTrust. Attualmente è anche coinvolta nel progetto di introduzione della carta a chip nella telefonia pubblica, occupandosi in particolare degli aspetti di sicurezza del sistema di pagamento. A questo proposito ha partecipato all'attività di standardizzazione in ambito ETSI per definire uno schema di interoperabilità fra carte telefoniche a chip di diversi Paesi.

Francesco Marconi si è laureato in Fisica nel 1984, con lode, presso l'Università di Pisa, dove ha collaborato alla progettazione del sistema di controllo di un laboratorio di spettroscopia applicata. Nel Gruppo Finsiel (Tecsiel, 1987/1996) si è occupato di sviluppi software in area OSI, e ha progettato soluzioni di messaggistica elettronica e applicazioni di carte a microprocessore. In Telecom Italia dal 1996, ha operato per Telecom Italia Net e successivamente nell'Area Tecnologie e Architetture Informatiche, partecipando alla definizione di soluzioni per la sicurezza informatica in ambito Internet e Intranet. Supervisiona progetti di ricerca applicata (CSELT) e partecipa a diversi Forum di operatori di rete (ETNO, MSAF).

Stefano Montesi si è laureato nel 1985 in Scienze dell'Informazione presso l'Università degli Studi di Pisa. Dopo un'esperienza come analista software presso una società di consulenza, nel 1989 è entrato a far parte della Linea Ricerca e Sviluppo di SIP (oggi Telecom Italia) operando fino al 1995 nel settore di Commutazione.
In questo ambito ha svolto attività di analisi di tecnologie per i servizi di telecomunicazione e delle loro applicazioni in Telecom Italia, seguendo tra l'altro le attività preliminari all'avvio del progetto di Rete Intelligente, la prototipazione di applicativi multimediali su reti broadband e le sperimentazioni sul riconoscimento del parlato per mezzo di reti neurali.
Dal 1990 ha partecipato attivamente alle iniziative internazionali finalizzate a promuovere la convergenza tra tecnologie informatiche e di telecomunicazione, cooperando nel 1992 alla costituzione del Consorzio TINA e successivamente operando nel Team tecnico del Consorzio presso Bellcore.
Dal 1995 ha operato nell'ambito dell'Architettura di Rete, seguendo in particolare l'evoluzione dei sistemi di gestione collegata con l'introduzione in rete di tecnologie a larga banda. In questo ambito ha inoltre esaminato aspetti di sicurezza nei servizi su ATM e su IP.
Attualmente opera nell'Area Architettura e Ingegneria di Rete della Direzione Rete, presso la Linea Architetture e Standard Internazionali, dove collabora al disegno delle soluzioni di rete per la fornitura di nuovi servizi.

xDSL

Soluzioni di rete per l'offerta di servizi interattivi su sistemi ADSL

FERRUCCIO ANTONELLI
LAMBERTO PETRINI

La tecnica trasmissiva ADSL ha ormai raggiunto una maturità tecnologica tale da essere riconosciuta come una delle soluzioni più promettenti per la realizzazione di reti d'accesso a larga banda su cavi a coppie simmetriche in rame. L'attenzione dei costruttori e dei gestori di rete si sta oggi perciò concentrando sulla definizione di sistemi e di soluzioni in grado di valorizzare appieno le notevoli potenzialità offerte dal modem ADSL e capaci di offrire una vasta gamma di servizi sia alla clientela residenziale sia alla clientela affari e piccolo affari. In quest'ambito le caratteristiche e le potenzialità del sistema ADSL sono da inquadrare in un contesto più ampio di realizzazione di nuove reti di servizi.

1. Introduzione

Le notevoli potenzialità offerte dai sistemi di linea xDSL stanno trovando larghi campi di applicabilità presso tutti i principali gestori di reti di telecomunicazioni [1]. Mentre i sistemi *HDSL (High bit-rate Digital Subscriber Line)* sono utilizzati per la realizzazione di circuiti diretti a 2,048 Mbit/s, i sistemi *ADSL (Asymmetric Digital Subscriber Line), SDSL (Symmetric Digital Subscriber Line)* e *VDSL (Very high bit-rate Digital Subscriber Line)* sono proposti all'interno di soluzioni di rete per la fornitura di servizi a larga banda, sia per la clientela affari sia per quella residenziale. Queste soluzioni consentono di offrire servizi interattivi, servizi di video numerico commutati *SDVB (Switched Digital Video Broadcasting)* e *VOD (Video On Demand)*, servizi di accesso veloce a reti per dati ed in particolare a Internet e di realizzare reti private virtuali.

Inizialmente il sistema ADSL è stato utilizzato in diverse sperimentazioni con configurazioni che prevedevano il trasporto di flussi plesiocroni (1,544 o 2,048 Mbit/s) fra l'unità di centrale e l'unità remota con modalità sostanzialmente monodirezionale nel verso dalla rete al terminale del cliente. La crescente diffusione di servizi basati su reti *ATM (Asynchronous Transfer Mode)* e su reti *IP (Internet Protocol)* [1] ha reso però necessario definire un modello di servizio in grado da un lato di accogliere relazioni di traffico bidirezionale - seppure in alcuni casi sbilanciato - e dall'altro le modalità di trasporto di celle e di pacchetti dati sul sistema di linea ADSL [2].

Nell'offerta di servizi interattivi e di accesso a Internet il segmento di trasporto delle informazioni nella rete di accesso mediante linee ADSL è integrato nell'ambito della catena di servizio completa, che presenta caratteristiche notevolmente diverse dai modelli di servizio tradizionali basati su linee dedicate o su accessi tramite la rete commutata (PSTN, ISDN).

In questo articolo sono mostrate le caratteristiche principali delle soluzioni di rete basate sulle reti di accesso ADSL per l'offerta di servizi interattivi. In particolare l'approccio illustrato prevede dapprima la descrizione del modello di business preso come riferimento e nel quale sono elencati i ruoli svolti dai diversi attori coinvolti. In questo modo è possibile meglio definire le interfacce logiche del servizio e allo stesso tempo identificare i diversi domini di competenza: in questo contesto l'utilizzo della tecnologia ADSL rappresenta il tassello con cui il fornitore dei servizi di accesso è in grado di offrire connettività con la rete all'utilizzatore finale.

Nell'articolo sono poi esposti gli aspetti tecnici e tecnologici della rete di accesso, identificando le caratteristiche del multiplatore ADSL *(MuxADSL)* come elemento di multiplazione e di flessibilità della rete. Sono infine presentate le differenti soluzioni di rete che possono essere realizzate in accordo con il modello di business impiegato come riferimento e che sono centrate sull'utilizzo del multiplatore ADSL.

Le soluzioni di rete riportate in questo testo sono suddivise in due gruppi secondo le caratteristiche del servizio di trasporto offerto dalla rete d'accesso: il primo prevede soluzioni che consentono di realizzare servizi di trasporto di livello due, in particolare ATM, il secondo invece riguarda soluzioni che permettono di gestire il livello tre, in particolare IP. In questo

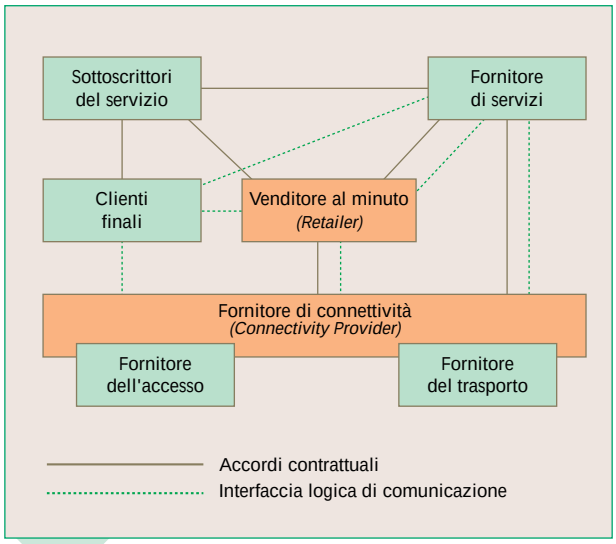


Figura 1 *Modello di servizio.*

secondo caso, al multiplatore ADSL come tecnologia di base si affianca un elemento di controllo e gestione del servizio, *NAS (Network Access Server)*, in grado di garantire accessi multipli ai servizi e di realizzare applicazioni di rete privata virtuale.

2. Modello di business per l'offerta di servizi interattivi su tecnologia ADSL

Il modello di servizio riportato in figura 1 propone uno schema generale per l'identificazione dei diversi ruoli nell'offerta di servizi di telecomunicazioni.

Nell'offerta di servizi interattivi su ADSL, il fornitore di connettività *(Connectivity Provider)*, l'entità cioè che offre i servizi di accesso e di connettività al fornitore di servizio *SP (Service Provider)*, è responsabile dello sviluppo, dell'esercizio e della manutenzione delle reti di sua pertinenza nonché del rispetto dei livelli di qualità stabiliti con i clienti. In generale, il ruolo del fornitore di connettività si articola in due sottoruoli: il fornitore dell'accesso *AP (Access Provider)* ed il fornitore del trasporto *TP (Transport Provider)*, anche se spesso questi ruoli sono svolti da una stessa entità, in genere dal gestore della rete di telecomunicazioni.

In particolare, la rete di accesso basata su tecnologia ADSL è governata dal fornitore dell'accesso.

Il fornitore di connettività offre il servizio di accesso ai fornitori di servizio (SP), le entità cioè che offrono servizi a valore aggiunto ai sottoscrittori del servizio, *SS (Service Subscriber)* sulla base di un contratto. L'SP è responsabile della ideazione, fornitura e gestione del servizio offerto agli utenti finali; può dotarsi di propri ambienti di esecuzione (server) o può utilizzare i servizi forniti da un fornitore di connettività o da altri.

In genere, la rivendita del servizio di accesso da parte del fornitore di connettività avviene in quantità (all'ingrosso). In questo caso è possibile individuare una funzione di rivendita al minuto svolta dal dettagliante *(Retailer)* sia verso i fornitori di servizio stessi sia verso i sottoscrittori del servizio.

In questo caso gli SP sono in genere quelli di Servizi Internet *ISP (Internet Service Provider)*, di reti d'azienda e quelli di contenuti *CP (Content Provide)*.

Gli SP offrono servizi ai sottoscrittori del servizio e, in pratica, alle singole entità (singola persona o società) che stipulano il contratto di sottoscrizione per la fornitura del servizio con l'SP. Il sottoscrittore del servizio è anche responsabile del completo rispetto degli obblighi contrattuali (ad esempio la fatturazione del servizio e la riscossione delle bollette) derivanti dall'utilizzo del servizio da parte dei clienti finali - indicati come *SU (Service User)* - e quindi della persona fisica che effettivamente impiega il servizio. L'infrastruttura di rete del cliente finale è denominata rete del cliente *(User Network)*: essa comprende generalmente più terminali *(host)* facenti parte della stessa rete locale LAN, ma può anche essere costituita da un unico terminale quale un personal computer.

Il fornitore dell'accesso utilizza tecnologie trasmissive di accesso di tipo ADSL la cui struttura fisica prevede una terminazione di rete *NT ADSL (Network Termination ADSL)* presso la sede del cliente e un multiplatore di accesso ADSL (MuxADSL) lato fornitore di servizio secondo quanto riportato nella figura 2.

Il paradigma di offerta risulta quindi quello secondo il quale il cliente finale sottoscrive il servizio dal SP, che svolge tutte le funzioni di tipo commer-

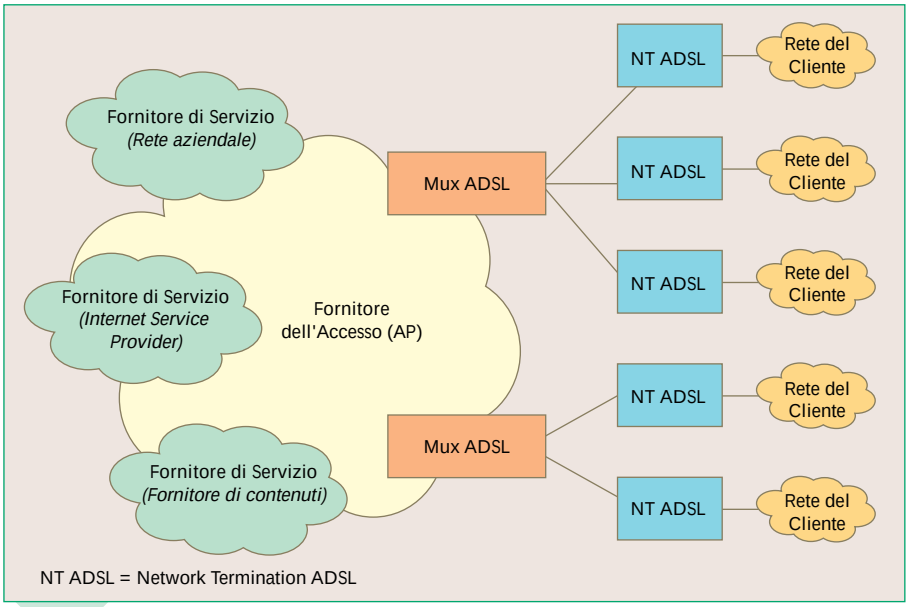


Figura 2 *Scenario relativo ad un ambiente multi service provider per isole ADSL.*

PROTOCOLLO PPP – POINT-TO-POINT PROTOCOL

Il protocollo PPP è stato definito per consentire il trasporto di pacchetti IP su circuiti punto-punto (connessioni commutate, linee dedicate, connessioni via satellite, connessioni SDH). Il suo progetto risolve anche altre problematiche quali l'autenticazione, l'assegnazione e la gestione degli indirizzi IP, l'incapsulamento sia asincrono *(start/stop)* che sincrono, la multiplazione del protocollo di rete, la configurazione del circuito, le prove sulla qualità della linea, la rilevazione di errori, la negoziazione della compressione (opzionale). Oltre ad IP, PPP consente il trasporto anche di altri protocolli quali *IPX* e *DECnet* utilizzati per le reti di computer.

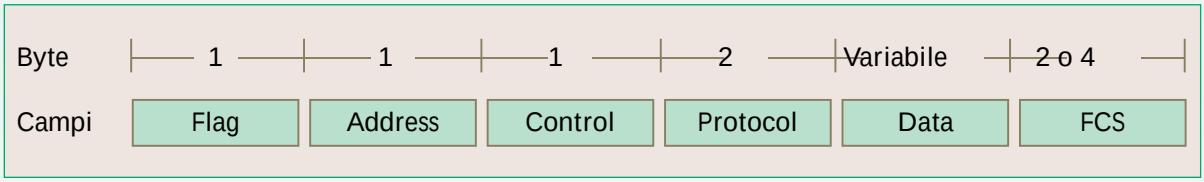
PPP è costituito da tre parti principali:

- **un metodo per l'incapsulamento di datagrammi su linee seriali. In particolare PPP usa *HDLC (High-Level Data Link Control)*;**
- **un protocollo di controllo del collegamento *LCP (Link Control Protocol)* per stabilire, configurare e provare la connessione di dati;**
- **una famiglia di protocolli di controllo del livello di rete *NCP (Network Control Protocol)* per stabilire e configurare differenti protocolli di livello di rete. PPP consente, infatti, l'uso simultaneo di più protocolli di rete.**

Per stabilire una connessione su un circuito punto-punto, il sistema che costituisce il PPP invia trame LCP per configurare e, in via opzionale, per provare la linea dati. Dopo che la linea è stata costituita da LCP, l'invio di trame NCP consente di indicare e configurare uno o più protocolli di rete che devono essere trasportati sulla connessione PPP. Quando un particolare protocollo di rete è stato configurato (ad esempio per la lunghezza massima e per quella media di trama, per il livello di diagnostica e correzione di errore), pacchetti di quel protocollo specifico di rete sono trasmessi sulla connessione.

La connessione rimane attiva finché le singole trame LCP o NCP concludono la sessione, ovvero nei casi in cui qualche evento esterno ne determini la conclusione (ad esempio scade una temporizzazione a seguito di un lungo periodo di inattività della connessione).

Il formato della trama PPP è riportato qui di seguito:



I campi sopra riportati hanno il seguente significato:

- ***Flag:* indica l'inizio della trama. Consiste nella sequenza 01111110.**
- ***Address:* contiene la sequenza binaria 11111111 e rappresenta l'indirizzo di tipo diffusivo (broadcast) standard in quanto PPP non sceglie le stazioni individualmente (la connessione è del tipo punto-punto).**
- ***Control:* contiene la sequenza 00000011 e rappresenta la trasmissione di dati d'utente in una trama non numerata.**
- ***Protocol:* questi due byte identificano il protocollo trasportato nel campo dati della trama.**
- ***Data:* in questo caso i byte da zero a 1500 contengono il datagramma d'utente. È possibile allargare ancora il numero di byte.**
- ***Frame Check Sequence:* consente il controllo e l'eventuale correzione di errori di trama con un meccanismo di *FEC (Forward Error Correction).***

ciale (vendita, assistenza e fatturazione). Il fornitore di servizio a sua volta acquista dal fornitore di connettività o dal dettagliante il servizio di accesso. I rapporti tra il fornitore di servizio e il fornitore d'accesso sono regolati da un contratto nel quale sono specificati in particolare procedure e tempi di fornitura, manutenzione e contabilizzazione dei consumi, livelli di qualità minimi da garantire.

3. Il multiplatore di accesso ADSL (MuxADSL)

Il modello di servizio illustrato in precedenza prevede che il fornitore dell'accesso raccolga il traffico degli utilizzatori finali tramite l'impiego di uno o più sistemi di multiplazione e che trasporti questo traffico aggregandolo sulla propria rete, per consegnarlo poi al fornitore di servizio. Le relazioni di traffico sono bidirezionali e le informazioni fluiscono quindi in entrambi i versi sebbene questi, nel caso di servizi interattivi, possano essere di differente capacità.

Il multiplatore di linee *ADSL (Mux ADSL)* è l'apparato nel quale sono poste le terminazioni ADSL di rete e dove sono gestiti i flussi di dati ed i segnali telefonici da e verso i clienti. Il segnale telefonico è estratto mediante l'impiego di un filtro passivo *(POTS splitter)* che separa, nella parte terminale del doppino del cliente, la banda telefonica da quella impiegata per la trasmissione dati [2]. Il segnale telefonico è instradato verso l'autocommutatore telefonico locale, mentre i segnali dati sono inviati verso la terminazione di linea ADSL.

Sono possibili diverse modalità di trasporto di informazioni dati su ADSL [4], [5] e [6]. Tra queste differenti possibilità la soluzione che utilizza la tecnica *ATM (Asynchronous Transfer Mode)* [7] e [8] consente una gestione delle risorse di rete maggiormente flessibile in termini sia di banda e di qualità di servizio sia di riconfigurazione delle stesse connessioni. Inoltre la soluzione con MuxADSL di tipo ATM consente, rispetto ai sistemi tradizionali di multiplazione a pacchetto, una maggiore modularità del sistema permettendo anche di aggregare più di cinquecento linee ADSL su un unico multiplatore.

Nel seguito sono riportate le caratteristiche principali del sistema MuxADSL e delle modalità di trasporto con tecnica di tipo ATM su ADSL.

3.1 Caratteristiche del MuxADSL

La tecnica ATM permette di usufruire di una notevole flessibilità, in quanto consente il trasporto di una grande varietà di applicazioni con diversi profili di traffico e garantisce i parametri di qualità del servizio richiesti da ciascuna applicazione. Essa permette inoltre una rapida integrazione con la rete di trasporto dove la tecnica ATM è già utilizzata in diversi nodi di rete.

Nel caso di trasporto di celle ATM la canalizzazione dei diversi flussi informativi è realizzata utilizzando le potenzialità della tecnica ATM di multiplare su un unico flusso differenti connessioni virtuali di tipo *VP (Virtual Path)* e/o *VC (Virtual Circuit)*; la normativa internazionale [4] [5] prevede, infatti, che il trasporto di ATM su ADSL sia realizzato impiegando un solo canale, l'AS0[1], in direzione downstream ed un solo canale, l'LS0 (configurato in modalità *simplex),* in direzione *upstream* [1][2].

La modalità di trasporto di celle ATM su modem ADSL permette di impostare in maniera indipendente la velocità di cifra nelle due direzioni di trasmissione, a passi di 32 kbit/s fino alla massima velocità permessa sul particolare rilegamento di utente. La velocità massima permessa dai sistemi ADSL è fino a 10 Mbit/s in direzione *downstream* e fino a 1 Mbit/s in direzione *upstream.*

Le soluzioni sistemistiche basate sulla tecnica ATM prevedono un apparato di centrale, denominato Nodo di Accesso *(Access Node),* ma chiamato anche MuxADSL o *DSLAM (Digital Subscriber Line Access Multiplexer):* esso è costituito da diversi modem ADSL (fino ad alcune centinaia); al Nodo di Accesso (figura 3) sono interconnesse, tramite i doppini della rete di distribuzione, le terminazioni di rete *NT (Network Termination)* ADSL presso le sedi dei clienti. Al cliente possono essere fornite una o più connessioni ATM permanenti di tipo VP o VC.

Il Nodo di Accesso svolge le funzioni di adattamento fra la rete di transito ATM e la rete di accesso[3]. Le principali funzioni in esso effettuate sono qui di seguito illustrate:

- l'interconnessione con la rete di transito *(Core Network Interface)* tramite interfacce standard, generalmente a 155 Mbit/s (STM-1) od a 34 Mbit/s (E3), svolgendo le funzionalità di livello ATM e di livello fisico;
- la terminazione di linea dei sistemi trasmissivi ADSL utilizzati nella rete di distribuzione;
- la demultiplazione, in direzione downstream, delle celle ATM provenienti dalla rete di transito ed il loro instradamento verso le unità *ATU-C (ADSL Termination Unit – Central office);*
- la multiplazione, in direzione upstream, delle celle ATM provenienti dalle unità ATU-C verso la rete di transito;
- l'eventuale realizzazione di funzionalità ATM di *policing, traffic shaping e congestion control* [8];
- la fornitura di funzionalità per la gestione della rete di accesso.

---

(1) La specifica ANSI T1.413 sui sistemi ADSL indica le caratteristiche di multiplazione e di trasporto sul modem ADSL di alcuni sottocanali elementari nei due versi di trasmissione: essa più precisamente definisce il trasporto di quattro sottocanali simplex AS0, AS1, AS2 e AS3 (nella direzione dalla rete verso il cliente), di tre sottocanali duplex LS0, LS1 e LS2 e di un sottocanale di esercizio O&M [2].

(2) Nel caso in cui il modem ADSL sia stato progettato per operare con una struttura di trama a "doppio ritardo" (dual latency) è possibile utilizzare i canali AS1 e LS1 per la fornitura di una seconda connessione. Non sono state tuttavia finora realizzate soluzioni capaci di gestire contemporaneamente connessioni con un basso e un alto ritardo.

(3) Il Nodo di Accesso può essere costituito anche da una terminazione ottica ONU (Optical Network Unit) in configurazioni di reti ottiche passive PON (Passive Optical Network).

Le funzioni di multi/demultiplazione dei VC fra la rete di transito e gli ATU-C sono svolte dal blocco *"Traslazione VPI/VCI e funzioni di ordine superiore"* che provvede eventualmente anche a cambiare gli identificativi dei circuiti virtuali (VPI e/o VCI) [7] da e verso le unità ATU-C[4]. Nel Nodo di Accesso possono essere allocate, oltre alle schede ADSL, anche quelle HDSL, SDSL e VDSL.

Le terminazioni di rete NT ADSL installate presso la sede del cliente sono connesse al Nodo di Accesso tramite la rete di distribuzione in rame. L'NT termina, lato rete, tutte le funzioni di livello trasmissivo originate nel corrispondente modem ADSL di centrale. La NT ADSL può includere al suo interno anche funzionalità di traslazione di identificativi VCI e VPI. La terminazione di rete NT ADSL permette l'interconnessione con gli apparati del cliente (Set Top Box, PC, router) tramite interfacce standard; le interfacce oggi più diffuse sulla terminazione di rete NT ADSL sono l'interfaccia ATM a 25 Mbit/s (ATM25) [10] e quella Ethernet 10BaseT. Nel caso di connessione verso un'interfaccia 10BaseT, la terminazione di rete NT ADSL deve includere, oltre alle funzionalità già viste, anche quelle di terminazione di celle ATM e di incapsulamento su celle ATM delle trame Ethernet provenienti dall'interfaccia 10BaseT. Il nodo di accesso permette la connessione del cliente ADSL con il fornitore di servizi (SP) impiegando, a questo scopo, una o più connessioni sulla rete di transito. Le possibili soluzioni per l'interconnessione sono illustrate nel paragrafo successivo.

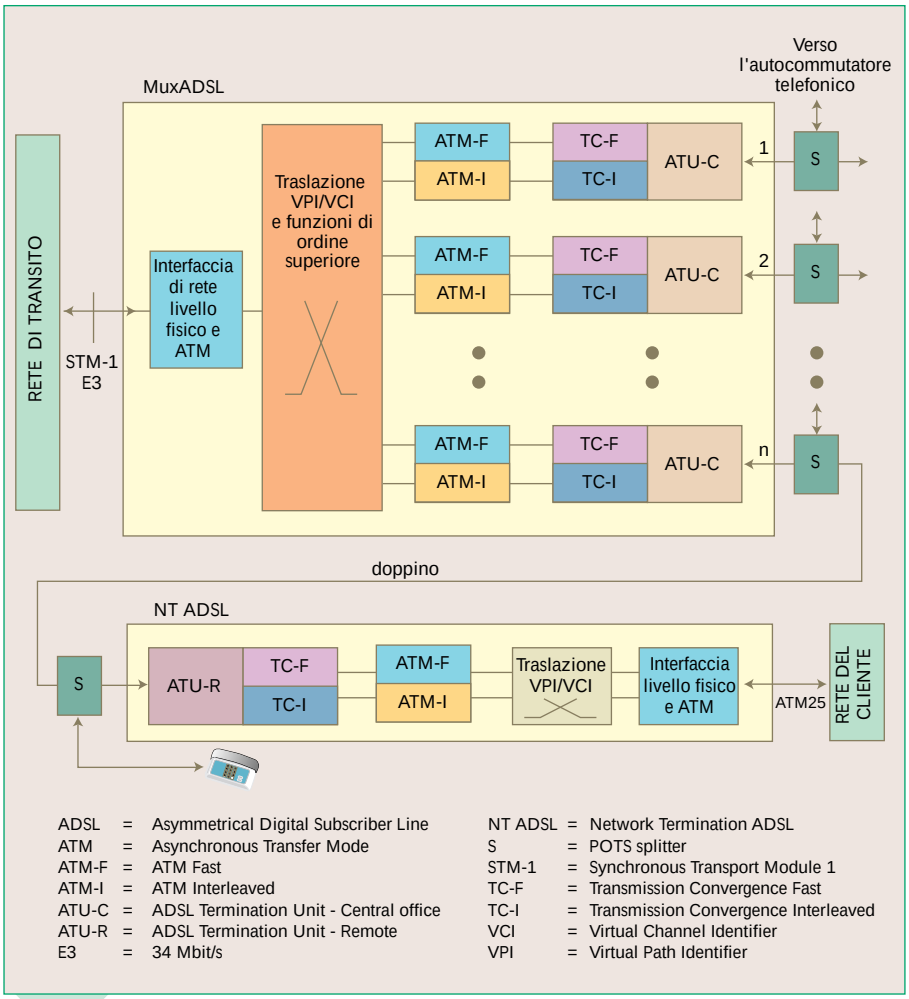


Figura 3 *Esempio dello schema di riferimento relativo alla rete di accesso ADSL per il trasporto di celle ATM.*

4. Soluzioni di rete per ADSL

I sistemi ADSL permettono di realizzare diverse modalità di interconnessione, e quindi differenti soluzioni di rete, tra i sistemi del cliente finale e le reti di servizio. A seconda del tipo di servizio di trasporto di dati realizzato sulla rete di accesso ADSL è possibile individuare soluzioni completamente basate su ATM, che offrono un trasporto di livello due, ovvero altre soluzioni basate sul protocollo IP che offrono un trasporto di livello tre, e che sono maggiormente indicate per l'accesso a Internet.

Nei paragrafi successivi sono illustrate le soluzioni di rete globali per consentire il traffico di dati dalla rete del cliente a quella di servizio.

4.1 Soluzione di rete completamente ATM

La soluzione di rete "completamente ATM" è caratterizzata dalla presenza di una o più connessioni ATM permanenti (PVC o PVP) fra il cliente e la rete di servizio (servizio del tipo *Always On).*

I Mux ADSL sono connessi alla rete di accesso ATM, mediante l'interfaccia E3 o STM1, come mostrato in figura 4; alla stessa rete ATM è connesso pure il nodo della rete di servizio, *PoP (Point of Presence)*, del fornitore di servizio mediante interfacce ATM E1, E3 o STM1 (è anche possibile l'in-

(4) Nel caso in cui il sistema di linea ADSL sia in grado di gestire contemporaneamente i canali a doppio ritardo (Fast e Interleaved) devono essere previste nel blocco "Traslazione VPI/VCI e funzioni di ordine superiore" due funzioni di livello ATM distinte per ciascuna linea ADSL. Come è stato ricordato in precedenza la gestione contemporanea di canali "Fast" e "Interleaved" non è stata finora realizzata.

terconnessione tra la rete ATM e quella Frame Relay in modo da collegare i POP all'ingresso della rete Frame Relay).

Sul MuxADSL sono configurate connessioni ATM, di tipo PVP o PVC, che sono terminate, da un lato, sul modem *ATU-R (ADSL Termination Unit – Remote)* presso il cliente e dall'altro sul nodo della rete del fornitore di servizio; queste connessioni transitano sulla rete ATM di accesso fra MuxADSL e nodo di servizio e possono essere di tipo simmetrico o asimmetrico. In funzione poi del tipo di tecnologia ADSL e ATM impiegata è possibile configurare modalità differenti di trasporto ATM (CBR, UBR, VBR, ABR) [7] [8].

Nel caso in cui il cliente sia dotato di un modem ADSL con interfaccia ATM25 la connessione fra cliente e fornitore di servizio è interamente realizzata a livello ATM.

Quando la rete del cliente è invece collegata tramite interfaccia Ethernet, occorre realizzare delle funzioni aggiuntive all'interno della terminazione di rete ATU-R che permettano il trasporto delle trame Ethernet imbustate in celle ATM secondo lo schema riportato nella norma IETF RFC1483 [10]: in questo caso lo schema di interconnessione è basato sulla modalità *transparent bridging* con la quale la rete d'accesso trasporta in modo trasparente, tra la rete del fornitore di servizio e la rete del cliente, le trame Ethernet che si presentano a una delle due terminazione della connessione ATM.

La soluzione "completamente ATM" presenta il vantaggio di essere relativamente semplice, di poter essere già realizzata - in quanto sono disponibili gli apparati - e di costituire una naturale evoluzione dei collegamenti diretti numerici, in quanto consente una facile migrazione delle soluzioni già impiegate. Essa presenta invece l'inconveniente di richiedere una configurazione manuale delle connessioni ATM con un appesantimento della gestione e dell'esercizio della rete e di essere poco modulare in quanto richiede, per interconnettere a maglia completa un numero n di sedi, di predisporre un numero n(n-1)/2 di collegamenti ATM.

Per quanto riguarda la rete di servizio del fornitore di servizi, essa può essere basata su diverse soluzioni:

- *ATM* – in questo caso le soluzioni sono caratterizzate da una connettività ATM da estremo ad estremo *(end-to-end);*
- *IP* - le connessioni ATM sono terminate su un router nella rete di servizio ed il traffico IP, recuperato all'interno delle trame Ethernet, è trasportato secondo modalità classiche IP [11];
- *Frame Relay* – in questo caso l'interconnessione avviene attraverso opportune unità di interconnessione tra la rete ATM e quella Frame Relay poste all'interno della rete di accesso ATM.

È anche previsto che le soluzioni completamente ATM potranno evolvere consentendo di poter realizzare connessioni ATM di tipo commutato *SVC (Switched Virtual Circuit)*, in grado di semplificare gli aspetti di gestione e di modularità realizzando in modo automatico, su richiesta del cliente finale, la costituzione ed il rilascio delle connessioni ATM; devono invece essere introdotte alcune funzioni aggiuntive negli apparati ADSL per permettere la gestione della segnalazione ATM.

4.2 Soluzione di rete IP

Nel caso in cui l'applicazione del cliente sia basata sul trasporto di pacchetti IP (quali, ad esempio, accesso a Internet, applicazioni per reti private aziendali, videoconferenza su IP) sono possibili alcune specializzazioni e miglioramenti rispetto alla soluzione "completamente ATM", che comportano però una maggiore complessità della rete. L'elemento principale in questo caso è un meccanismo di controllo della sessione d'utente *(Virtual Dial Up)* che funziona in modo analogo a quanto realizzato per le soluzioni di accesso basate su rete commutata *(Dial Up)*, telefonica o ISDN. In particolare il cliente finale accede alla rete indicando, all'interno della maschera di connessione, l'indirizzo IP o, in modo equivalente, il nome simbolico del dominio (invece del numero telefonico) a cui intende collegarsi per ricevere servizio, il proprio identificativo d'utente *(username)*, la propria parola d'ordine *(password)*. Al termine della sessione di lavoro, si disconnette rilasciando le risorse di rete impegnate.

L'introduzione di questo meccanismo permette una maggiore flessibilità per l'accesso alla rete di servizio, consentendo al cliente finale di scegliere i servizi ed i profili di accesso desiderati e, ai Service Provider, il controllo dinamico dell'accesso alle reti ed ai servizi offerti, con la possibilità di personalizzarne le caratteri-

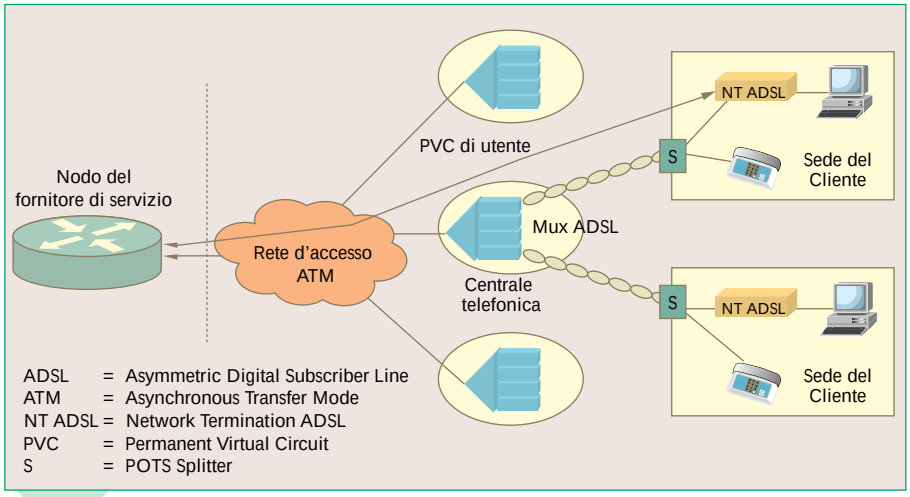


Figura 4 *Soluzione di rete con interconnessione diretta di SP (Service Provider) alla rete.*

stiche (rete privata virtuale, Intranet, Extranet, commercio elettronico) e di differenziarne la tariffazione (a volume, a tempo, forfettaria, per transazione, per fasce orarie).

Il meccanismo *Virtual Dial Up* prevede di inserire all'interno della catena di servizio una funzione denominata Server di Accesso alla Rete, conosciuta anche come *NAS (Network Access Server).* Questa funzione è, in genere, realizzata all'interno di un apparato o di un sistema indipendente; in alcuni casi, essa è invece realizzata come funzione aggiuntiva di apparati già presenti in rete.

Il NAS è un dispositivo collocato in rete di accesso tra i Mux ADSL e i router del fornitore di servizi e costituisce il punto di flessibilità dell'architettura di rete all'interno del quale è possibile attuare la selezione dei servizi e trattare efficacemente le connessioni per il trasporto dei dati.

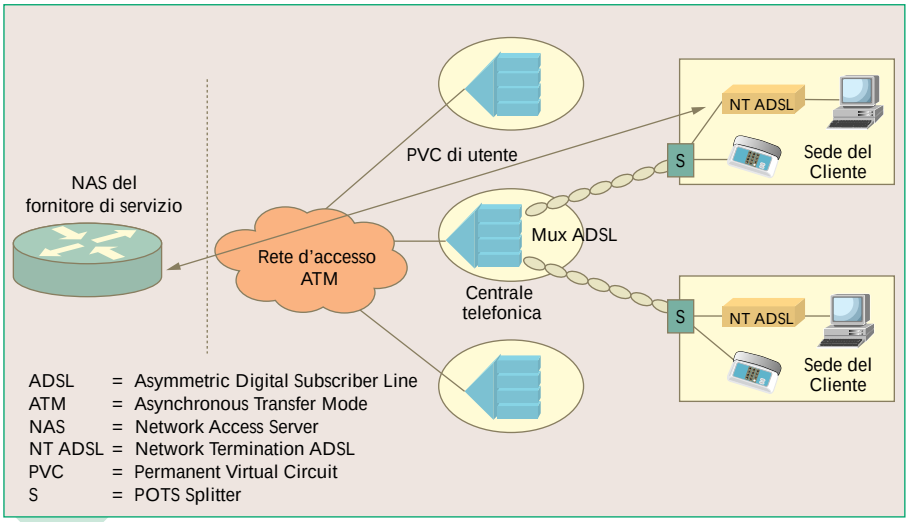


Figura 5 *Interconnesione mediante NAS (Network Access Server) posto nel dominio del fornitore di servizi.*

I NAS rappresentano una specializzazione dei router IP e consentono in particolare di svolgere alcune funzioni quali:

- la terminazione dei PVC ATM provenienti dai clienti e la concentrazione di essi in un numero più ridotto di connessioni verso ciascun fornitore di servizi;
- l'interconnessione alla rete di trasporto con interfacce di servizio di vario tipo (ad esempio ATM, Frame Relay, linee dedicate);
- la gestione degli utenti ADSL, per attuare i profili di servizio e per realizzare le funzioni di autenticazione, autorizzazione e tariffazione *AAA (Authentication, Authorization, Accounting)* secondo modalità che saranno illustrate nel seguito (paragrafi 4.2.1 e 4.2.2);
- la realizzazione di soluzioni di reti private virtuali *VPN (Virtual Private Network),* con configurazione di gruppi chiusi di utente e accesso protetto (ad esempio mediante canali virtuali denominati *tunnel),* a reti private ovvero *corporate.*

L'apparato NAS è inoltre in grado di terminare le numerose connessioni PVC ATM (con banda relativamente modesta) tra il sistema del cliente e la rete di servizio; questa funzione spesso non è gestita dagli apparati router tradizionali che sono maggiormente specializzati nella terminazione di poche connessioni ATM di grossa capacità.

Il sistema NAS può essere posizionato sia nel dominio del fornitore di servizio che in quello del fornitore di accesso.

4.2.1 NAS posizionato nel dominio del fornitore di servizi

Nel caso in cui il NAS sia posizionato nel dominio del fornitore di servizi (figura 5), il servizio gestito dal fornitore di accesso coincide in pratica con una soluzione "completamente ATM" in cui le connessioni ATM dalla rete d'utente sono terminate sul NAS.

Con il segnale inviato su queste connessioni, il cliente finale può comunicare al NAS l'intenzione di accedere a servizi specifici fornendo le proprie credenziali di accesso *(username* e *password, chip card,* firma elettronica). Il NAS valuta la richiesta del cliente e, in base ai dati di profilo posseduti, stabilisce la possibilità del singolo cliente di accedere ai servizi richiesti. Le proposte più interessanti per la realizzazione di questi tipi di servizio prevedono che [12] la richiesta di accesso ai servizi avvenga attraverso l'instaurazione di una sessione *PPP (Point to Point Protocol;* si veda riquadro di pagina 63), in analogia con la modalità tipica dell'accesso mediante la rete telefonica o ISDN, che prevede al suo interno i meccanismi richiesti di autenticazione, autorizzazione e tariffazione.

La connessione PPP trasportata sulla connessione ATM predefinita [13] è terminata in genere nel NAS. Dal NAS in poi il traffico IP è trasferito con le modalità classiche delle reti Internet. In alcuni casi particolari, quali quelli relativi all'accesso remoto a reti aziendali, la connessione PPP potrebbe essere prolungata nella rete di servizio fino a terminare su un server remoto, consentendo così di mantenere le caratteristiche tipiche del PPP anche nella rete di servizio.

4.2.2 NAS posizionato nel dominio del fornitore di accesso

Nel caso in cui il NAS sia posizionato nel dominio del fornitore di accesso, le funzionalità del servizio sono le stesse riportate nel caso precedente; in questo caso varia il servizio offerto dal fornitore di accesso a quello di servizio. Questa configurazione (figura 6) prevede infatti che la rete d'accesso trasporti non solo celle, ma anche pacchetti dati PPP ovvero IP (trasporto di livello 3) e che in essa siano

L2TP: Layer 2 Tunnelling Protocol

L2TP è un'estensione del protocollo PPP ed è impiegato per la realizzazione di reti private virtuali su IP. Esso consente di costituire connessioni virtuali *(tunnel)* per il trasporto di diversi tipi di protocolli (PPP, IP, IPX, Appletalk) idonei per differenti tecniche di trasporto (IP, ATM, Frame Relay, X.25, SDH ma anche Ethernet, Fast Ethernet, FDDI). Consente anche di multiplare più protocolli all'interno dello stesso tunnel e permette di gestire sofisticati meccanismi di sicurezza e di garantire una prefissata qualità di servizio.

L'architettura di funzionamento di L2TP prevede due componenti:

- ***L2TP Access Concentrator (LAC):* riceve le connessioni d'utente (PPP) e le multipla verso L2TP Network Server avviando le funzioni di sicurezza, qualità di servizio, gestione di rete e di servizio relative alla connessione d'utente. Nel caso specifico di ADSL esso si identifica con il NAS e le funzioni di sicurezza sono svolte per procura (proxy) dal NAS in relazione con L2TP Network Server;**
- ***L2TP Network Server (LNS):* termina le connessioni L2TP provenienti da LAC e attiva i meccanismi di sicurezza e di controllo della qualità di servizio. Esso è in genere presente nella rete del fornitore di servizio (o della rete aziendale nel caso di soluzioni Intranet).**

collocate le funzioni di controllo della sessione quali l'autenticazione, l'autorizzazione, la sicurezza e l'assegnazione dinamica delle risorse IP, definite in base sia al profilo d'utente sia ai servizi che possono essere da esso richiesti.

Con questa modalità di funzionamento il NAS del fornitore di rete termina le connessioni ATM (PVC) dei clienti ed esercita le funzioni di autenticazione, autorizzazione e tariffazione *AAA (Authentication Authorisation Accounting)* indicate in precedenza sulle sessioni PPP. Sulla rete di trasporto il NAS del fornitore di rete è connesso ai nodi dei fornitori di servizio mediante due possibili alternative:

- *tunnel L2TP (Layer 2 Tunnelling Protocol)* [14] su ATM, Frame Relay o IP - la sessione PPP è prolungata oltre il NAS ed è trasferita fino al nodo del fornitore di servizio; il NAS può effettuare le funzioni di autenticazione, autorizzazione e tariffazione (AAA) per conto del fornitore di servizi (funzionalità *Proxy*). Il protocollo L2TP permette di definire una connessione virtuale (tunnel L2TP) tra il NAS ed il nodo del fornitore di servizio su cui sono multiplate più sessioni PPP di clienti diversi, dirette verso uno stesso fornitore di servizio, con la stessa qualità del servizio. Il tunnel L2TP può essere definito su una rete IP o su una connessione virtuale ATM o Frame Relay. Il nodo del fornitore di servizio *PoP (Point of Presence)* deve essere in grado di eseguire le funzioni di L2TP Network Server; deve permettere cioè di terminare un tunnel L2TP per ciascun NAS presente nella rete.
- *rete IP* – in questo caso tutte le funzioni di autenticazione, autorizzazione e tariffazione (AAA) sono svolte esclusivamente dal NAS di rete che termina

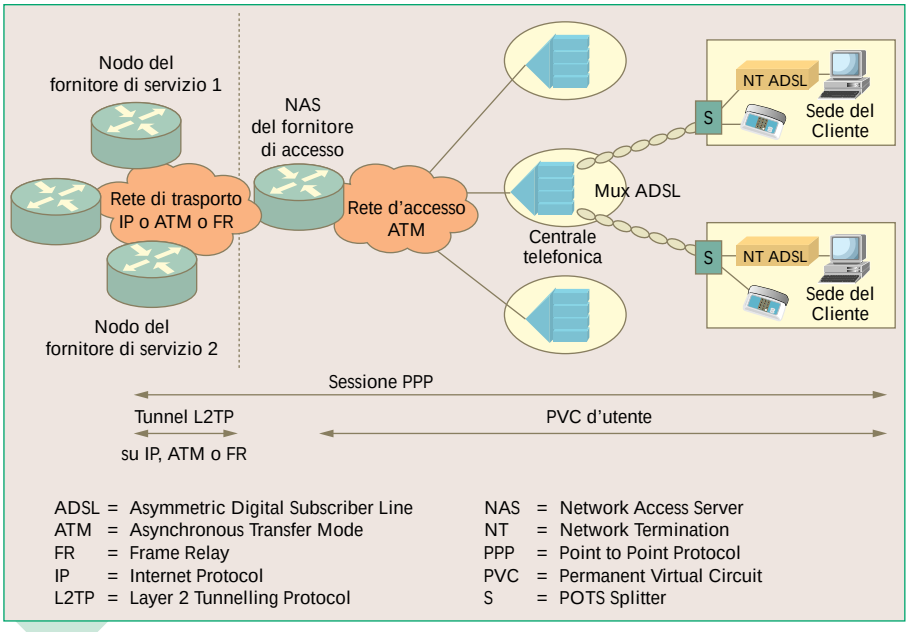


Figura 6 *Interconnesione mediante NAS (Network Access Server) posto nel dominio del fornitore di accesso.*

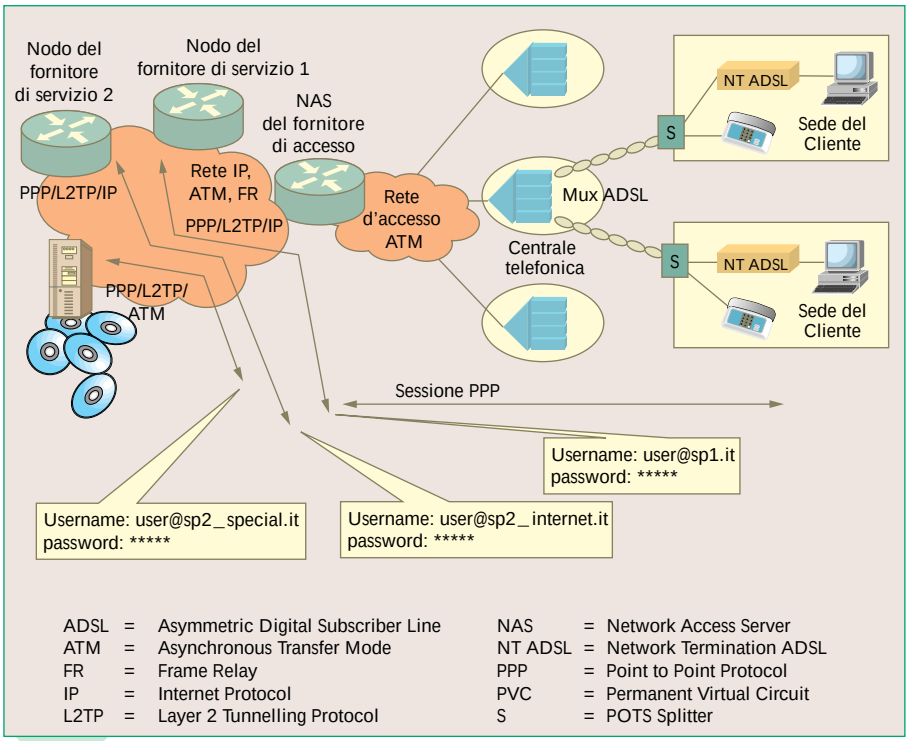


Figura 7 *Selezione dinamica del fornitore di servizio.*

le sessioni PPP sulla terminazione ATM del cliente finale e che instrada il traffico IP nella rete di trasporto.

Nel caso di ambiente in cui siano presenti una pluralità di fornitori di servizi, la soluzione con il NAS nel dominio del fornitore dell'accesso consente al cliente finale del fornitore di servizio (o dei relativi servizi) una selezione dinamica, così come mostrato nella figura 7. In particolare il campo *username* della sessione PPP è impiegato dall'utilizzatore finale nel corso dell'avvio della sessione di lavoro per indicare il fornitore di servizio o il servizio richiesto concatenandolo al proprio codice identificativo di accesso al servizio con il simbolo @.

Il NAS, ricevuti i campi *username* e *password* digitati dall'utilizzatore, interpreta il campo presente dopo il simbolo @ e provvede, nel caso di tunnel L2TP, a incapsulare la connessione PPP sul tunnel L2TP del fornitore di servizio designato ovvero, nel caso di rete IP, a terminare la sessione PPP ed a richiedere al fornitore di servizio prescelto l'autenticazione e l'autorizzazione a connettere il cliente che ha effettuato la richiesta di collegamento.

5. Conclusioni

L'utilizzo di soluzioni di trasmissione dati basate sulla tecnologia ADSL rappresenta un passaggio molto importante per valorizzare gli impianti in rame esistenti nella rete di accesso dei gestori tradizionali di telecomunicazioni. In questo articolo sono state descritte le soluzioni di rete adottabili per la fornitura di servizi interattivi fra i due estremi *(end-to-end)* costituiti dall'utilizzatore finale e dal fornitore di servizi, cercando anche di indicare gli aspetti di maggior rilevanza e di criticità di ciascuna soluzione individuata.

Il punto di maggior pregio è costituito dal modello *Virtual Dial Up* che consente, pur nel rispetto della trasmissione dati *connection-less* tipica di Internet, di conservare il concetto di sessione, riprendendolo dall'accesso tipico di rete commutata. La criticità più importante di questa soluzione è costituita dalla mancanza, in sede di standardizzazione internazionale, di un modello di protocollo di collegamento tra il terminale del cliente e la terminazione di rete NT ADSL nel caso di accesso dell'utilizzatore alla rete attraverso interfaccia di tipo Ethernet.

Tra gli aspetti evolutivi di maggior rilievo sembra opportuno infine segnalare lo sviluppo di soluzioni ADSL splitterless atteso per la seconda metà del 1999, la cui normativa è stata ratificata in ITU-T alla fine del 1998 [15]. I sistemi ADSL Splitterless - in grado quindi di essere installati facilmente dall'utilizzatore finale senza modifiche dell'impianto telefonico preesistente [2] e [3] anche se particolarmente lungo (fino a 5 Km), ma con limitazione sulla massima velocità di cifra (1,5 Mbit/s *downstream*, 128 kbit/s *upstream)* - dovrebbero nel medio periodo affiancare e gradualmente sostituire i sistemi di accesso classici basati su modem telefonici necessari per accedere ai servizi Internet. La descrizione e le modalità di utilizzo di questi sistemi formeranno l'oggetto di un articolo successivo.

Abbreviazioni

AAA	Authentication Authorisation Accounting
ABR	Available Bit Rate
ADSL	Asymmetric Digital Subscriber Line
AP	Access Provider
ATM	Asynchronous Transfer Mode
ATM-F	ATM Fast
ATM-I	ATM Interleaved
ATU-C	ADSL Termination Unit – Central office
ATU-R	ADSL Termination Unit - Remote
CBR	Constant Bit Rate

CP	Content Provider
HDSL	High bit-rate Digital Subscriber Line
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
L2TP	Layer 2 Tunnelling Protocol
LNS	L2TP Network Server
MuxADSL	Multiplexer ADSL
NAS	Network Access Server
NT	Network Termination
ONU	Optical Network Unit
PON	Passive Optical Network
PoP	Point of Presence
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
SDSL	Symmetric Digital Subscriber Line
SDVB	Switched Digital Video Broadcasting
SP	Service Provider
SS	Service Subscriber
STM-1	Synchronous Transport Module 1
SU	Service User
SVC	Switched Virtual Circuit
TC-F	Transmission Convergence Fast
TC-I	Transmission Convergence Interleaved
TP	Transport Provider
UBR	Unspecified Bit Rate
VBR	Variable Bit Rate
VC	Virtual Circuit
VCI	Virtual Circuit Identifier
VDSL	Very high bit-rate Digital Subscriber Line
VOD	Video On Demand
VP	Virtual Path
VPI	Virtual Path Identifier
VPN	Virtual Private Network

Bibliografia

[1] Pietroiusti, R.; Volpe, M.: *Internet e le evoluzioni delle reti di telecomunicazioni*. «Notiziario Tecnico Telecom Italia», Anno 7, n. 1, aprile 1998.

[2] Magnone, L.; Petrini, L.: *Sistemi xDSL per l'accesso ad alta velocità su coppie simmetriche in rame*. «Notiziario Tecnico Telecom Italia», Anno 7, n. 2, ottobre 1998.

[3] Di Biase, V.C.; Petrini, L.: *Aspetti impiantistici dei sistemi ADSL*. Su questo stesso numero del «Notiziario tecnico Telecom Italia».

[4] *Draft Standard on Asymmetric Digital Subscriber Line (ADSL) Metallic Interface*. T1E1.4/97-007R2, Issue 2, settembre 1997.

[5] *ATM over ADSL Recommendations*. ADSL Forum, Technical Report 002, marzo 1997.

[6] *Framing and Encapsulation Standards for ADSL: Packet Mode*. ADSL Forum, Technical Report 003, luglio 1997.

[7] Garetti, E.; Pietroiusti, R.; Renon, F.M.: *ATM: modelli dei protocolli e funzioni di rete*. «Notiziario tecnico Telecom Italia», Anno 5, n. 2, settembre 1996.

[8] Castelli, P.; De Giovanni, L.; Vittori, P.: *Controllo del traffico e della congestione nella rete B-ISDN: contratto di traffico e classi di trasporto ATM*. «Notiziario Tecnico Telecom Italia», Anno 6, n. 1, luglio 1997.

[9] *Physical interface specification for 25.6 Mb/s over Twisted Pair Cable*. The ATM Forum Technical Committee, novembre 1995.

[10] Heinanen, J.: *Multiprotocol Encapsulation over ATM Adaptation Layer 5*. IETF RFC1483, July 1993.

[11] Antonelli, F.; Carissimi, M.; Iuso, F.; Pugliese, F.: *I protocolli TCP ed IP*. «Notiziario Tecnico Telecom Italia», Anno 4, n. 1, luglio 1995.

[12] *An End-To-End Packet Mode Architecture With Tunneling And Service Selection*. ADSL Forum Technical Report TR-011 June 1998.

[13] Gross, G.; Kaycee, M.; Li, A.; Malis, A.; Stephens, J.: *PPP Over AAL5*. IETF RFC2364 – July 1998.

[14] Valencia, A. et alii: *Layer Two Tunneling Protocol - L2TP*. IETF Draft, October 1998.

[15] *Splitterless Asymmetric Digital Subscriber Line (ADSL) Transceivers*. ITU-T G.992.2, Transmission Systems and media, Draft Recommendation.

La biografia di Lamberto Petrini è riportata a pagina 80.

Ferruccio Antonelli si è laureato in Ingegneria Elettronica nel 1989 presso l'Università di Roma "La Sapienza" ed ha conseguito il Master of Science in Electrical Engineering dal Polytechnic University di New York nel 1990. Ha seguito in passato le tematiche relative ai servizi e alle tecnologie di trasmissione dati (Frame Relay, SMDS, IP/Internet, ADSL) partecipando ai maggiori Organismi di standardizzazione internazionale (ETSI, ESIG, Frame Relay Forum) e contribuendo ad alcune iniziative Telecom Italia per lo sviluppo di servizi IP (Interbusiness, Telecom on Line, SIRIUS, Prisma). È oggi responsabile della ingegnerizzazione dei sistemi di networking all'interno della linea Ingegneria di Reti Dati e Multimediali della Direzione Rete, Telecom Italia dove si occupa della identificazione e della industrializzazione delle soluzioni di rete per la gestione di servizi interattivi e di accesso ad Internet.

xDSL

Realizzazione di reti di accesso con sistemi ADSL

VALERIO CLAUDIO DI BIASE
LAMBERTO PETRINI

L'introduzione in rete di sistemi ADSL implica una notevole attività impiantistica sia presso la centrale sia presso il cliente. Soprattutto gli aspetti relativi alla definizione dell'impianto presso il cliente costituiscono uno dei punti cruciali nella realizzazione della piattaforma a larga banda sia perché essi possono influenzare in misura non trascurabile il costo per linea della soluzione di rete complessiva sia perché il cablaggio presso il cliente può influenzare fortemente il grado di accettabilità del servizio. Nel presente articolo saranno descritte le soluzioni scelte per la realizzazione degli impianti sia lato centrale sia lato cliente, concentrando maggiormente l'attenzione sull'ambiente residenziale, in quanto quelli dei clienti affari pongono vincoli meno stringenti per l'installazione.

1. Introduzione

Il sistema ADSL consente di fornire servizi dati a larga banda sullo stesso doppino impiegato per il servizio telefonico tradizionale *POTS (Plain Old Telephone Service)*, permettendo al cliente di fruire contemporaneamente dei due servizi. La combinazione di questi due servizi su un unico portante è realizzata con la tecnica a divisione di frequenza *FDM (Frequency Division Multiplexing)*, utilizzando una coppia di filtri passivi *(POTS Splitter)*, da collocare rispettivamente presso la centrale e presso il cliente che assicurano il corretto trasporto del segnale telefonico e di quello dati. La trasparenza del canale in banda base assicura il funzionamento, oltre che degli apparecchi telefonici, di tutti i dispositivi che utilizzano la banda fonica, quali, ad esempio, terminali fax, modem in banda fonica, centralini privati analogici *PABX (Private Automatic Branch Exchange)* in banda fonica. La caratteristica di trasferimento dei filtri è tale da permettere anche il passaggio degli impulsi di teleconteggio (tono a 12 kHz) eventualmente presenti sul rilegamento del cliente. Gli splitter garantiscono il funzionamento del canale telefonico, e dell'eventuale segnale di teleconteggio a 12 kHz, anche in particolari condizioni operative quali:

- guasto dell'unità ATU-C;
- guasto dell'unità ATU-R;
- mancanza di alimentazione dell'unità ATU-C;
- mancanza di alimentazione dell'unità ATU-R;
- presenza, sul rilegamento di utente, della sola unità ATU-C e POTS Splitter di centrale;
- presenza, sul rilegamento di utente, della sola unità ATU-R e POTS Splitter remoto.

È inoltre garantita, in qualsiasi condizione operativa, la telealimentazione del terminale telefonico.

In alternativa al canale telefonico analogico è possibile il trasporto, in banda base, del segnale relativo all'accesso base *ISDN-BRA (ISDN Basic Rate Access)*. Questa soluzione, denominata *"ADSL over ISDN"*, è stata standardizzata dal gruppo di lavoro internazionale ETSI TM6. Qualora sulla stessa coppia si intendesse fornire al cliente, mediante l'ausilio di un "ISDN splitter", sia una connessione ISDN-BRA sia una connessione ADSL, si avrebbe una penalizzazione sulle prestazioni del sistema ADSL. Il trasporto del segnale ISDN-BRA sulla stessa coppia costringe, infatti, ad allocare l'estremo inferiore dello spettro ADSL sopra i 100 kHz, invece che sopra i 26 kHz, frequenza quest'ultima che rappresenta il limite inferiore dello spettro ADSL nel caso di trasporto di segnale fonico. La mancata utilizzazione della porzione bassa dello spettro, che tipicamente presenta una minore attenuazione trasmissiva e migliori prestazioni di diafonia, può comportare rispetto al sistema ADSL con POTS Splitter una riduzione sulla portata anche del 20 per cento.

Nel presente articolo si pone l'accento sulle problematiche connesse all'introduzione in rete di sistemi ADSL.

Gli aspetti impiantistici - soprattutto quelli relativi alla sede del cliente - rivestono un ruolo molto importante nella realizzazione di piattaforme di rete a larga banda che impiegano sistemi *ADSL (Asymmetric*

Digital Subscriber Line), in quanto l'introduzione in rete di questi sistemi comporta la necessità di svolgere una serie di attività ai due estremi del collegamento. In figura 1 è mostrata la configurazione di riferimento per sistemi ADSL: essi sono costituiti da un'unità di centrale *ATU-C (ADSL Termination Unit - Central office)* posta tra il permutatore e l'attacco telefonico del cliente, e da un'unità remota installata presso il cliente *ATU-R (ADSL Termination Unit - Remote)* posta all'interno della terminazione di rete *NT (Network Termination)* [1].

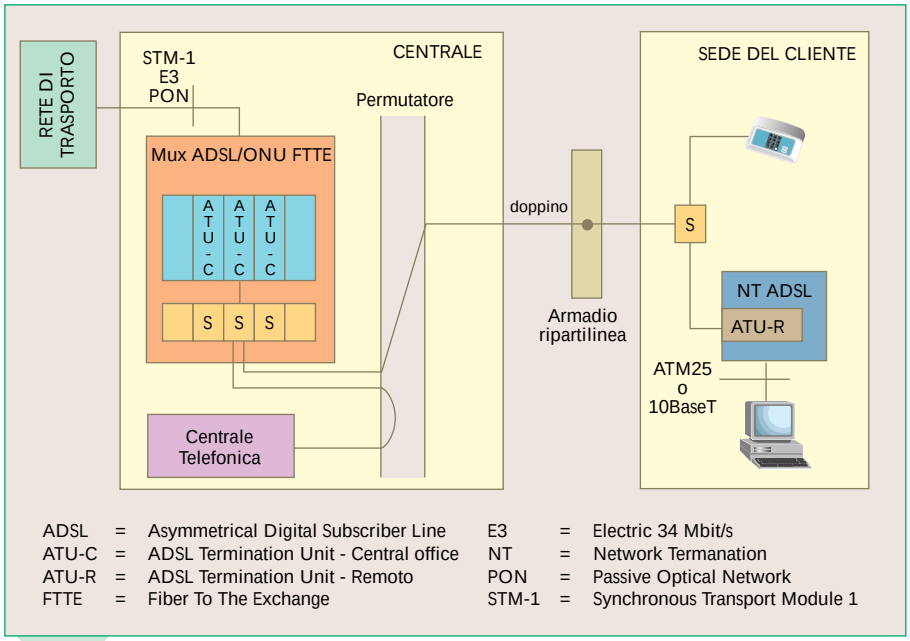


Figura 1 *Configurazione tipica dei sistemi ADSL.*

Le due unità ADSL sono connesse tramite una generica coppia simmetrica in rame della rete di distribuzione. Le unità ATU-C possono essere contenute in schede poste all'interno di un Multiplex ADSL (MuxADSL) o, nel caso di soluzioni che prevedono l'impiego di reti ottiche passive *PON (Passive Optical Network)*, in schede poste all'interno di un elemento di rete ottica in centrale. L'unità ATU-R può essere realizzata come unità *stand-alone (NT ADSL)* oppure può essere integrata in una scheda da porre all'interno di un terminale del cliente. Per realizzare correttamente il collegamento è necessario che il doppino che connette l'unità ATU-R a quella ATU-C sia dedicato esclusivamente al cliente che ha richiesto il servizio; non è perciò possibile offrire servizi a larga banda su ADSL a clienti attestati su multiplatori di rete quali, ad esempio, i multiplex d'abbonato simmetrici e asimmetrici, o le terminazioni per quattro clienti MT4.

2. Impianto in centrale

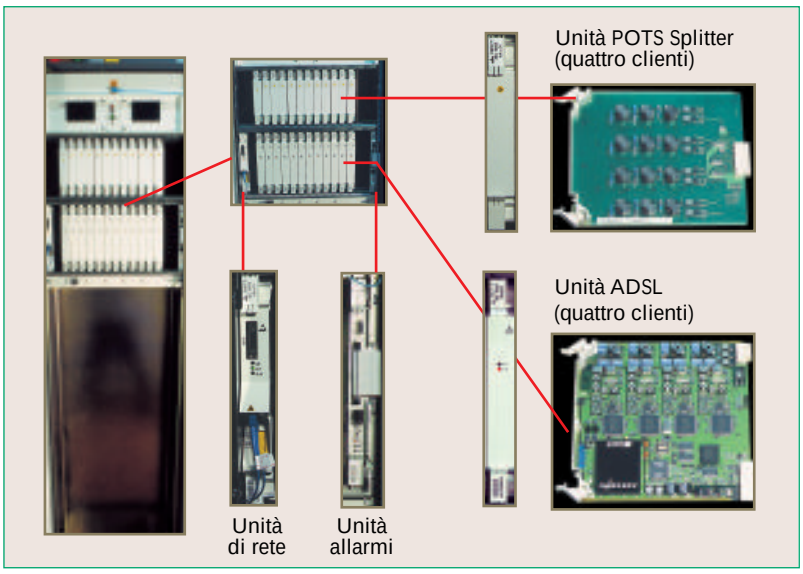
La configurazione di rete ADSL prevede che le unità ATU-C di centrale siano poste nella centrale sede dell'autocommutatore telefonico al quale è collegato il cliente. L'inserimento del flusso dati a larga banda è realizzato tramite un filtro di inserimento connesso al doppino proveniente dall'attacco del cliente prima dell'uscita verso la rete[1]. Per semplificare le operazioni di inserimento del filtro e per garantire un'elevata disponibilità del servizio telefonico, si utilizza un filtro passivo caratterizzato da un elevato livello di affidabilità; un filtro attivo potrebbe infatti garantire migliori prestazioni di separazione tra i segnali, ma comporterebbe una maggiore complessità circuitale, costi aggiuntivi e una riduzione dell'affidabilità complessiva del sistema.

Il filtro passivo può essere collocato in differenti posizioni. Finora Telecom Italia non ha definito particolari requisiti per l'allocazione dei singoli POTS Splitter; questa scelta è infatti affettuata dal fornitore del sistema in modo che ottimizzi l'impiego dei telai in funzione di dove essi sono inseriti. Mentre è ormai generalmente accettato di impiegare, presso il cliente, splitter esterni all'unità ADSL remota, sono invece possibili scelte differenti per quanto riguarda gli splitter di centrale: alcune realizzazioni integrano il POTS Splitter nella scheda ADSL; altre, quali ad esempio quelle adottate nella sperimentazione Endeavour[2], raggruppano i POTS Splitter in schede poste all'interno di un sub-telaio separato da quello contenente le unità ADSL. Questa seconda soluzione rende più flessibile la gestione tra le due schede in quanto non è rigida l'associazione tra la scheda ADSL e quella POTS Splitter. Sarebbe auspicabile, in relazione alle esigenze dei gestori e alle risposte dei costruttori, poter disporre in futuro di un sub-telaio suddiviso in due parti: una contenente le schede ADSL, l'altra i corrispondenti POTS Splitter.

Nel seguito sono riportate le attività da svolgere in centrale per installarvi i sistemi ADSL con gli apparati oggi disponibili; queste soluzioni sono generalmente applicabili anche agli sviluppi futuri dei sistemi ADSL.

(1) Per alcuni segmenti di clientela affari potrebbe non risultare conveniente l'impiego di una sola coppia per la fornitura congiunta del servizio telefonico e di quello a larga banda. In questi casi il sistema ADSL può essere trasportato su una coppia separata che collega direttamente il cliente con l'unità ADSL di centrale senza passare nel POTS Splitter.

(2) Si tratta di una sperimentazione condotta in ambito nazionale di servizi IP ad alta velocità su differenti piattaforme di rete di accesso (ADSL e Cable Data Modem).



Il sistema ADSL installato in centrale.

Lo schema logico di riferimento del collegamento fra telaio ADSL e permutatore urbano è illustrato in figura 2; in essa è mostrata l'unità di un subtelaio contenente le schede ADSL e POTS Splitter. I telai MuxADSL o gli elementi di rete ottica[3], *ONU (Optical Network Unit)*, contenenti le unità ATU-C ed i POTS Splitter sono collocati all'interno della centrale trasmissiva *AF (Alta Frequenza)*. Gli ingressi e le uscite del subtelaio impiegano connettori multipli di subtelaio.

Il segnale telefonico proveniente dal sistema di commutazione (cavo rosso) deve essere connesso al POTS Splitter per essere poi combinato con il segnale numerico proveniente dal modem ADSL. Il segnale complessivo così formato (cavo blu) è inviato nuovamente verso il permutatore ed è terminato su strisce di attestazione dedicate al servizio a larga banda. È previsto un sezionamento nella centrale trasmissiva in alta frequenza per semplificare le operazioni di manutenzione da parte del personale di esercizio. Una volta realizzato questo cablaggio, il cliente è connesso al servizio effettuando la connessione nel permutatore urbano e rimuovendo, al contempo, la connessione diretta preesistente tra l'autocommutatore locale e la terminazione orizzontale sul permutatore urbano alla quale era attestata la coppia del generico cliente.

Per eliminare l'effetto di interferenze reciproche tra i segnali utili è opportuno utilizzare cavi distinti per il cablaggio del telaio ADSL con il permutatore urbano. Sono perciò distinti i cavi con le coppie che trasportano i segnali telefonici provenienti dall'autocommutatore, da quelli che trasportano verso la rete i segnali multiplati (telefonia assieme al segnale numerico).

La potenzialità dei cavi da utilizzare per il cablaggio fra subtelaio ADSL e permutatore è legata alla modularità degli apparati MuxADSL o ONU FTTE: se il subtelaio si presenta, ad esempio, verso l'esterno con un connettore multiplo da ventiquattro coppie (per servire altrettanti clienti) è conveniente adottare un cavo con una potenzialità uguale o superiore. I cavi utilizzati devono presentare, naturalmente, caratteristiche trasmissive e di schermatura idonee al trasporto dei segnali a larga banda.

La quantità di telai necessari dipende dalla modularità prevista dalla tecnologia utilizzata: ad esempio per la soluzione MuxADSL, adottata nella fase di avvio della sperimentazione tecnico-commerciale, in ogni sub-telaio trovano posto dodici schede contenenti ciascuna quattro ADSL (quattro clienti a scheda), e un telaio, realizzato secondo lo standard ETSI, contiene tre subtelai; esso ha quindi una potenzialità complessiva di centoquarantaquattro clienti.

Di seguito sono riepilogate le attività da svolgere in centrale:

- installazione del telaio MuxADSL o ONU FTTE

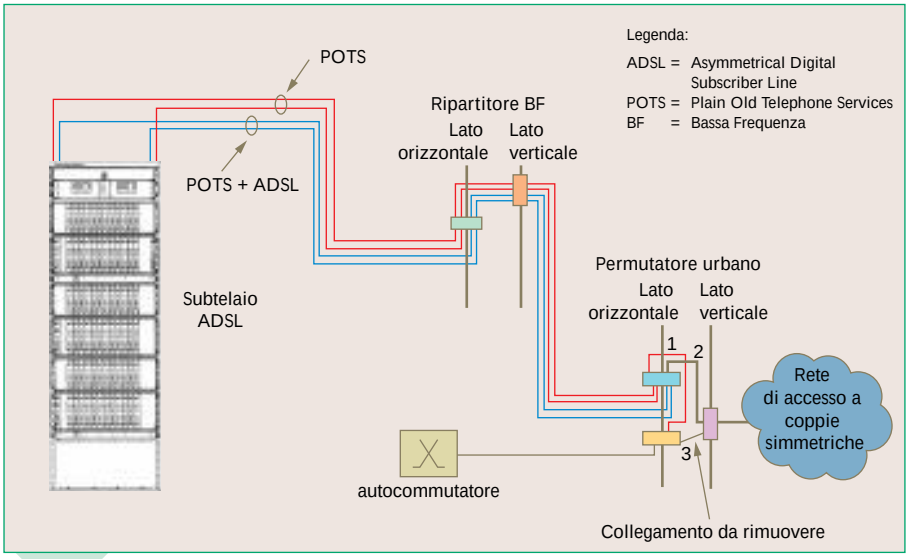
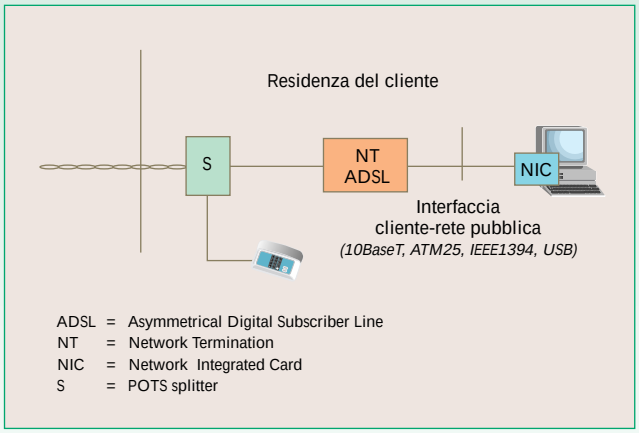


Figura 2 *Schema logico delle connessioni fra telaio ADSL e permutatore.*

(3) *Nel caso in cui la terminazione di rete ottica è posta in centrale, la configurazione di rete è del tipo* FTTE (Fiber To The Exchange) *e la terminazione di rete ottica prende il nome di* ONU FTTE.

CONFIGURAZIONE CON TERMINAZIONE DI RETE NT ATTIVA

- **La soluzione con terminazione di rete (NT) attiva prevede che essa faccia parte della rete di accesso e presenti verso la porzione interna della rete interfacce di tipo standard, quali ad esempio 10 BaseT e ATM25.**
- **La NT attiva è realizzata come un'unità remota; essa è di proprietà del gestore pubblico e costituisce il punto di confine tra la rete pubblica e quella privata. Questa scelta facilita la possibilità di garantire una prefissata qualità del servizio in quanto il sistema ADSL non utilizza un cablaggio interno alla sede del cliente e quindi non controllato; sono poi migliori le possibilità di gestire il rilegamento del cliente in quanto è facilitata l'individuazione di guasti e la suddivisione di competenze su questa parte della rete mediante controlli con prove di chiusura in loop remoto sulla NT ADSL.**



Schema di impianto con NT attiva.

- **La terminazione di rete NT attiva consente di disaccoppiare i sistemi utilizzati nella rete di accesso da quelli impiegati presso i clienti e permette l'evoluzione della rete di accesso senza avere conseguenze sui terminali del cliente e sul cablaggio da essi utilizzato. L'approccio con NT attiva è oggi perseguito dai più importanti gestori di rete europei.**

e dei sub-telai relativi alle unità ATU-C, POTS Splitter;
- realizzazione del cablaggio per l'alimentazione e per l'estrazione degli allarmi di telaio;
- installazione delle strisce di attestazione sia al ripartitore in bassa frequenza della sala trasmissiva sia al permutatore urbano;
- realizzazione del cablaggio tra il singolo subtelaio e il permutatore urbano.

La pre-cablatura dei subtelai consente, una volta ricevuta la richiesta di attivazione di una linea ADSL, un'esecuzione rapida delle operazioni rimanenti da effettuare in centrale prima di recarsi dal cliente per installare l'unità ADSL remota.

Queste attività riguardano:
- inserimento eventuale della scheda ATU-C e POTS Splitter;
- attivazione della scheda ATU-C;
- realizzazione della permuta fra il punto di attestazione dell'attacco di utente telefonico e la striscia di attestazione dedicata al servizio a larga banda (connessione 1 di figura 2);
- realizzazione della connessione tra la striscia di attestazione dedicata al servizio a larga banda e il punto di attestazione del doppino del cliente (connessione 2 di figura 2);
- rimozione della connessione preesistente del cliente (connessione 3 di figura 2).

L'interruzione del servizio telefonico sulla linea del cliente che ha chiesto il servizio ADSL è quindi limitata al periodo necessario per la realizzazione delle connessioni al permutatore urbano e dura solo qualche minuto. Il corretto funzionamento della fonia è infatti garantito anche nel caso in cui sia presente, sul rilegamento in oggetto, soltanto l'unità ADSL di centrale con il relativo POTS Splitter: si garantisce così la continuità del servizio telefonico nel periodo di tempo che intercorre fra la realizzazione dei collegamenti di centrale e l'ultimazione dell'impianto presso il generico cliente.

3. Impianto presso il cliente

3.1 Configurazioni possibili per l'impianto presso il cliente

La realizzazione dell'impianto domestico comporta la risoluzione dei problemi connessi con il posizionamento ed il cablaggio del POTS Splitter, della terminazione di rete NT-ADSL e dei terminali del cliente. Il posizionamento di tali elementi è sensibilmente condizionato anche da aspetti regolatori e normativi relativi al limite di demarcazione fra la rete pubblica e quella privata in quanto dovrà essere chiarito se la terminazione di rete NT ADSL sia di proprietà del gestore della rete di telecomunicazioni o del cliente finale. La scelta ha, naturalmente, conseguenze sull'esercizio dell'NT-ADSL e sul cablaggio interno alla

sede del cliente. Quest'ultimo aspetto riveste quindi un ruolo molto rilevante poiché ha un elevato impatto sul modello di servizio e sulle competenze degli attori in gioco. Le soluzioni proposte si basano su due configurazioni principali: configurazione con NT attiva (vedi riquadro a pagina 74) e configurazione con NT passiva (vedi riquadro a pagina 76).

Le soluzioni di rete promosse dai gestori di rete europei sono indirizzate verso l'impiego di una terminazione di rete NT di tipo attivo; l'approccio oggi proposto in Europa per la fornitura di servizi a larga banda su sistemi ADSL è infatti molto simile a quello praticato nell'offerta del servizio ISDN, per il quale la terminazione di rete NT1 è di proprietà del gestore di rete. In questo modo si può controllare più facilmente la qualità del servizio fornito al cliente finale e risulta semplificata l'identificazione dei guasti e dei malfunzionamenti discriminando fra le competenze del gestore della rete pubblica e quella del cliente finale.

Nel seguito l'attenzione sarà posta sulle soluzioni impiantistiche presso il cliente che prevedono NT attiva. Le soluzioni proposte sono valide non solo nel caso di terminazioni di rete NT ADSL, ma anche per le terminazioni *NT VDSL (Very high bit-rate Digital Subscriber Line)* e, più in generale, per tutte le terminazioni di rete NT del tipo xDSL che consentano il trasporto del segnale fonico in bassa frequenza.

Non esistono oggi norme di riferimento a livello internazionale riguardanti la realizzazione dell'impianto domestico basato su soluzioni ADSL anche se alcuni comitati di standardizzazione hanno allo studio questa tematica (FSAN, ATM Forum, ADSL Forum, IEC). Le uniche prescrizioni applicabili agli edifici adibiti ad uso residenziale sono le norme che definiscono i cablaggi dedicati ad un impiego specifico (telefonia di base, ISDN). Per gli edifici adibiti ad un uso commerciale (o ad uffici) sono disponibili oggi invece normative consolidate di tipo nazionale ed internazionale (EIA/TIA-568) [2], relativi ad un cablaggio per uso generale, anche se molto orientato alla realizzazione di reti locali di computer (LAN).

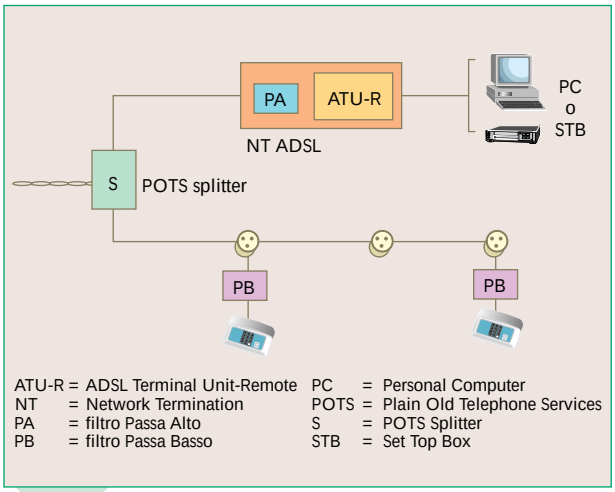


Figura 3 *Impianto realizzato presso il cliente con POTS Splitter concentrato e separato dalla NT ADSL.*

La separazione del segnale telefonico da quelli numerici avviene mediante l'impiego del POTS Splitter, le cui caratteristiche realizzative hanno un elevato impatto sull'impianto realizzato presso il cliente. Sono oggi disponibili almeno tre diverse soluzioni di impiego del POTS Splitter: a splitter concentrato, a splitter distribuito [3] e splitterless.

Postazione realizzata presso la residenza di un cliente.

3.1.1 Configurazione con POTS Splitter concentrato ed esterno all'unità NT ADSL

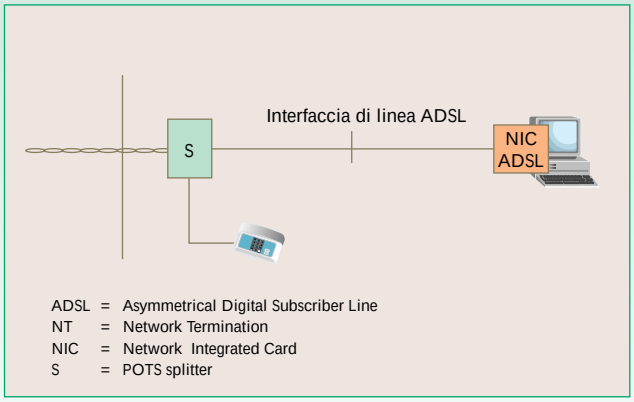
Lo schema di principio dell'impianto domestico con POTS Splitter concentrato ed esterno all'unità NT ADSL è riportato in figura 3: il POTS Splitter è posto in prossimità dell'ingresso della linea telefonica, mentre la terminazione di rete NT ADSL è sistemata nei pressi del terminale che usufruisce del servizio a larga banda (ad esempio un PC o un Set Top Box). La terminazione di rete NT ADSL comprende l'unità ATU-R e un filtro *Passa-Alto (PA)* che blocca le componenti dello spettro con frequenza sotto il limite inferiore di quello ADSL.

Questa configurazione permette di ottenere diversi vantaggi tra i quali, ad esempio, quelli di seguito elencati:

- il collegamento tra POTS Splitter e la terminazione di rete NT ADSL non rappresenta che l'ultima tratta dell'intero collegamento fra ATU-C e ATU-R, tipicamente lunga anche qualche decina di metri, e si avvale perciò di tutte le potenzialità del sistema di linea ADSL in termini di robustezza della modulazione trasmissiva e di caratteristiche di protezione adottate contro gli errori; il cavo che si deve utilizzare fra POTS Splitter e NT ADSL deve essere del tipo *twisted* (a coppie intrecciate) e deve presentare buone caratteristiche di bilanciamento, quali, ad esempio, quelle offerte dal cavo UTP di categoria 3 (nel seguito

CONFIGURAZIONE CON TERMINAZIONE DI RETE NT PASSIVA

- **Nella soluzione con terminazione di rete (NT) passiva il gestore di rete offre al cliente finale l'interfaccia di linea ADSL; la terminazione di rete passiva NT è quindi solo un punto - passivo - di connessione alla rete pubblica al quale il cliente collega l'unità ADSL remota di sua proprietà. L'unità ADSL può essere realizzata come unità a sé stante oppure può essere integrata in una scheda all'interno di un apparato del cliente (PC, workstation, router).**



Schema di impianto con NT passiva.

- **La soluzione con NT passiva presenta un minor costo per linea per il gestore pubblico della rete, in quanto l'unità ADSL remota è del cliente. Le soluzioni di rete con NT passiva sono incoraggiate dai gestori delle reti pubbliche degli Stati Uniti.**

indicato con UTP3) o UTP di categoria 5 (indicato più avanti con UTP5);
- la connessione tra l'NT ADSL e il terminale del cliente è ridotta a meno di due metri e può generalmente essere realizzata mediante un cavo di raccordo in modo da evitare un ulteriore cablaggio;
- la connessione dedicata tra POTS Splitter e NT ADSL rende la qualità della trasmissione ADSL indipendente da eventuali imperfezioni dell'impianto telefonico installato all'interno della residenza del cliente;
- il posizionamento della NT ADSL in prossimità del terminale del cliente rende assai probabile la disponibilità nelle immediate vicinanze di una presa di rete elettrica pubblica necessaria per la sua alimentazione.

I sistemi ADSL realizzati finora non permettono, tuttavia, l'interconnessione di POTS Splitter con NT ADSL di costruttori diversi per cui, finché non sarà disponibile l'interoperabilità completa del sistema, occorrerà installare POTS Splitter e NT ADSL provenienti da uno stesso fornitore. Una sensibile semplificazione nell'installazione si ha nel caso di una configurazione con POTS Splitter distribuito; questa riduce l'intervento di personale tecnico presso il cliente e quindi comporta una riduzione sia dei costi diretti, legati ai tempi di trasferimento del personale verso la sede del cliente, sia di quelli latenti quali quelli legati alla non risoluzione degli appuntamenti con il cliente per l'installazione e all'eventuale revisione degli impianti.

3.1.2 Configurazione con POTS Splitter distribuito

Nella figura 4 è mostrato lo schema di principio dell'impianto domestico nel caso di impiego di POTS Splitter distribuiti: su tutte le prese telefoniche presenti all'interno dell'appartamento sulle quali è connesso un apparato tradizionale (telefono, terminali in facsimile, modem dati) deve essere inserito un POTS Splitter (PB); il filtro *PA (Passa Alto)* è invece integrato nella terminazione di rete NT ADSL.

Questa soluzione presenta il vantaggio che la NT ADSL può essere installata su una qualsiasi delle prese telefoniche dell'appartamento (o su una presa già utilizzata dotandola di un adattatore quale quello impiegato con i modem) mentre il modulo POTS Splitter è connesso ad altre prese. La realizzazione dell'impianto domestico è così notevolmente semplificata rispetto al caso precedente in quanto permette di evitare un nuovo cablaggio fra POTS Splitter e NT ADSL; in questo modo lo stesso cliente potrebbe provvedere a installare e ad attivare la NT ADSL, con evidenti risparmi dal punto di vista economico.

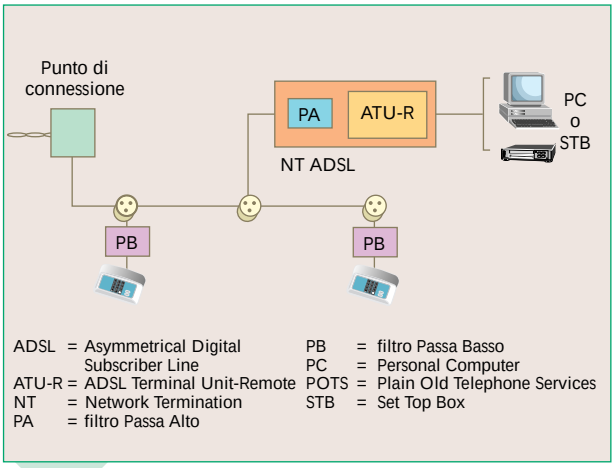


Figura 4 *Impianto posto presso il cliente con POTS Splitter distribuito.*

Questa soluzione è oggi in fase di esame, ma la sua adozione comporta alcune conseguenze di rilievo quali, ad esempio:

- i collegamenti interni verso l'unità ADSL sono realizzati sull'impianto telefonico esistente, sulla cui corretta realizzazione e sulla cui qualità il cliente non è in grado di fornire alcuna garanzia;
- le prestazioni del collegamento possono essere ridotte dal 10 al 40 per cento in funzione della qualità dell'impianto interno. Questa aleatorietà delle caratteristiche dell'impianto domestico rende molto variabile, e non definibile a priori, la velocità di cifra *(bit-rate)* fornibile al singolo cliente finale: la fornitura del servizio è quindi del tipo *Best Effort;*
- il costo del POTS Splitter è ad oggi ancora elevato. Il costo va poi moltiplicato per il numero di apparecchi telefonici presenti presso il cliente;
- il terminale del cliente non è sempre collocato in prossimità di prese telefoniche. Secondo recenti rilevazioni statistiche la distanza tipica è di circa 12 m; occorrerebbe perciò realizzare un cablaggio fra la presa telefonica e la postazione del cliente.

3.2 Realizzazione dell'impianto del cliente con POTS Splitter di tipo concentrato

La realizzazione con POTS Splitter concentrato, posto fuori della terminazione di rete NT ADSL, è la soluzione che oggi Telecom Italia adotta per l'impianto eseguito presso il cliente. Questa soluzione sarà utilizzata anche per la fornitura di servizi effettuati con Mux ADSL e, nella prima fase di offerta dei servizi SDVB, su una rete con fibra ottica e con la parte terminale realizzata con cavi a coppie simmetriche in rame. In questo modo è possibile garantire le prestazioni per tutte le tipologie di servizio (anche per quelli SDVB) controllando al contempo la qualità dell'esecuzione dei lavori da eseguire presso il cliente. In figura 5 è presentato lo schema dei collegamenti tra gli elementi posti presso il cliente.

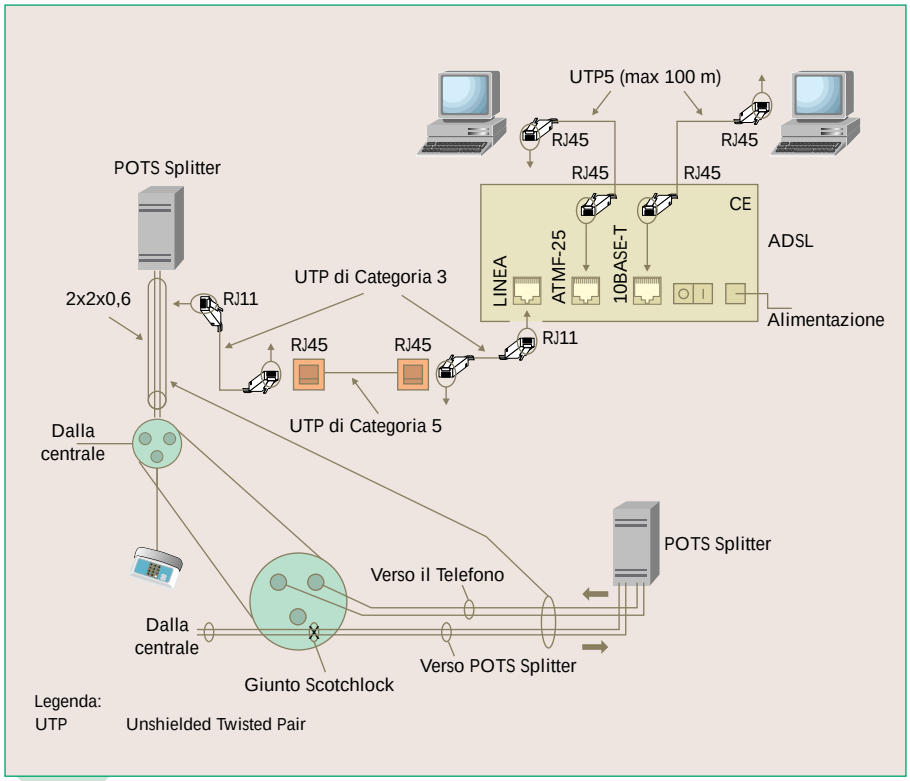


Figura 5 *Schema delle connessioni realizzate presso la residenza del cliente.*

3.1.3 Configurazione Splitterless (senza filtro di separazione)

La soluzione *splitterless* (o G.lite) consente di inserire un modem ADSL - senza l'adozione di filtri di separazione - direttamente a una qualsiasi delle prese telefoniche disponibile all'interno dell'appartamento. La soluzione splitterless è idonea per i profili di servizio del tipo *best effort* a più bassa velocità di cifra (fino a 1,5 Mbit/s). Non è possibile invece impiegarla nel caso di fornitura di servizi di video numerico commutato quali *SDVB (Switched Digital Video Broadcast).*

L'impossibilità di garantire una qualità determinata del servizio può rendere poi la soluzione splitterless difficilmente estensibile al caso di clientela affari.

La soluzione *splitterless* risulta idonea nell'ambito di un'architettura di rete e di un'offerta commerciale che preveda una NT passiva, una completa compatibilità trasversale tra prodotti di costruttori diversi e l'installazione effettuata direttamente dal cliente. Queste tematiche sono in corso di esame e di definizione all'interno dei Gruppi UAWG e ITU-T SG 15.

Nel caso di POTS Splitter realizzato su un'unità esterna alla NT ADSL, esso deve essere posto in un punto subito a monte della borchia telefonica principale; in questo modo è possibile separare l'impianto a larga banda da tutto l'impianto telefonico.

Il POTS Splitter presenta le seguenti porte di accesso:

- *linea:* a quest'ingresso, con connessione a vite, arriva dalla linea il segnale multiplato;
- *telefono:* da questa uscita è estratto il segnale telefonico verso la borchia telefonica principale e quindi verso il resto dell'impianto telefonico interno: la connessione è a vite. Per attestare la

linea telefonica al POTS Splitter e l'uscita telefonica del POTS Splitter alla borchia telefonica principale è necessario accedere alla coppia proveniente dalla rete pubblica ed effettuare un giunto di tipo Scotchlock[4];

- *ADSL:* questa uscita, per collegare il POTS Splitter all'ADSL, è realizzata con una presa RJ11. Il collegamento è effettuato con cavo di categoria 3 o superiore[5].

Entrambe le interfacce 10BaseT e ATM25 utilizzano lo stesso tipo di cavo UTP5 e lo stesso tipo di connettore RJ45.

L'utilizzo del cavo di tipo UTP5 per la porzione più lunga del cablaggio assicura una buona qualità trasmissiva ed una sufficiente immunità ai disturbi. La realizzazione del cablaggio UTP5 richiede tuttavia attenzioni particolari poiché la normativa prevede che siano seguite alcune regole nell'installazione (quali ad esempio il tipo dei cavi, la massima curvatura dei cavi, le connessioni) e non dipende solamente dalla qualità dei componenti utilizzati.

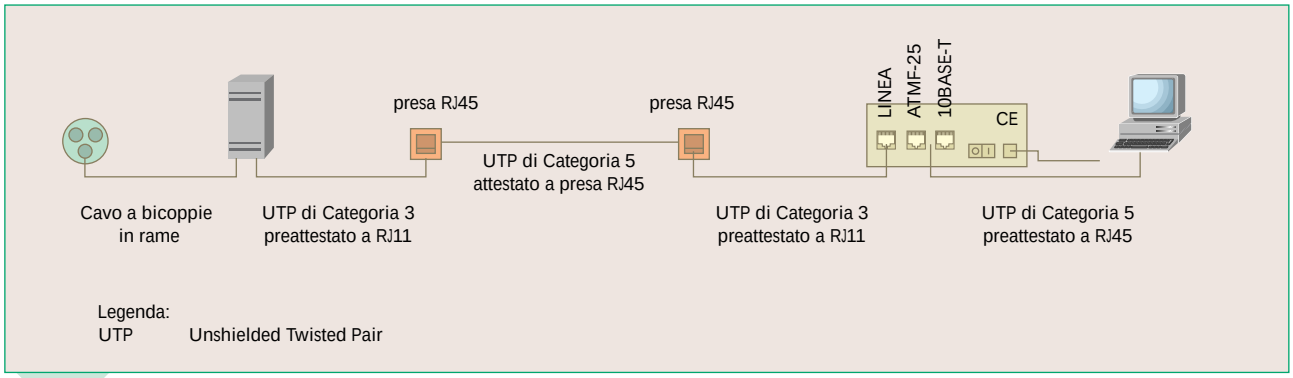


Figura 6 *Sviluppo di un impianto ADSL installato presso clienti piccoli affari SOHO (Small Office Home Office).*

Per installare il POTS Splitter è necessario far effettuare dal personale tecnico alcune operazioni sulla borchia telefonica principale.

La NT ADSL presenta invece i seguenti punti di accesso:

- alimentazione a 12V in continua;
- *linea:* a questo ingresso arriva il segnale proveniente dal POTS Splitter. La presa può essere di tipo RJ11 o RJ45[6];
- *ATMF25:* uscita verso il *CPE (Customer Premises Equipment)* con interfaccia ATM25. La presa è di tipo RJ45;
- *10BaseT:* uscita verso il CPE con interfaccia Ethernet 10BaseT. La presa è di tipo RJ45.

I collegamenti dal POTS Splitter alla NT ADSL e dalla NT ADSL ai terminali non sono già predisposti presso il cliente e devono quindi essere realizzati ex-novo. Per questi cablaggi sono adottati rispettivamente i cavi prima menzionati UTP3 e UTP5. Nel caso di clienti residenziali o di clienti piccolo affari, *SOHO (Small Office Home Office)* nella quale la borchia telefonica principale è posta in genere all'ingresso dell'appartamento e il terminale in un punto qualsiasi dello stesso, lo sviluppo dell'impianto è mostrato nella figura 6.

Una volta effettuate, nella borchia telefonica principale le operazioni di connessione della coppia proveniente dalla rete pubblica e dopo aver eseguito le attestazioni sul POTS Splitter, occorre realizzare un collegamento con cavo UTP5 fino al punto dove il cavo è terminato con una presa RJ45. Il resto dell'installazione è effettuato con raccordi preattestati come riportato in figura 6. L'uso del cavo UTP5 per la realizzazione dell'impianto interno consente di ottenere una certa flessibilità nel posizionamento dell'ADSL che può essere posto indifferentemente o nei pressi del POTS Splitter oppure vicino al CPE.

Altre interfacce che potrebbero in futuro trovare una larga diffusione nei terminali posti presso i clienti - e che di conseguenza potrebbero essere poste all'interno della NT ADSL - sono l'interfaccia *USB (Universal Serial Bus)* e l'interfaccia *IEEE1394* (descritte ai successivi paragrafi 4.3 e 4.4).

È allo studio la possibilità di rendere più rapide le operazioni di esecuzione dell'impianto, limitando al contempo impatti di tipo estetico presso il cliente, inserendo il POTS Splitter all'interno della preesistente borchia telefonica principale. L'installazione del filtro consisterebbe così nella semplice sostituzione della borchia telefonica principale già presente presso il cliente con una nuova.

(4) Connettore di tipo stagno a spostamento di isolante; garantisce una connessione stabile, è di facile impiego e presenta un ingombro assai modesto che consente di sistemarlo all'interno della borchia telefonica principale.

(5) La categoria del cavo fa riferimento all'insieme di caratteristiche trasmissive (attenuazione, diafonia,..) che identifica il campo di utilizzo di esso. I cavi di categoria 3 sono utilizzabili per frequenze fino a 16 MHz mentre quelli di categoria 5 sono utilizzabili fino a 100 MHz. I cavi sono multicoppia (due coppie per la categoria 3 e quattro coppie per quella 5) e sono intrecciati singolarmente. Il cavo può essere inoltre non schermato, o UTP (Unshielded Twisted Pair) *o schermato, o* STP (Shielded Twisted Pair).

(6) Tipo di presa e di spina definita in ambito EIA/TIA a quattro, a sei fili (RJ11) od a otto fili (RJ45).

4. Interfacce fra NT ADSL e il terminale del cliente

Come già anticipato nei paragrafi precedenti le interfacce tra il cliente e la rete pubblica oggi preferite sono quella 10BaseT e quella ATM25. Altri tipi di interfacce, quali l'USB e la IEEE1394, potrebbero in un prossimo futuro essere impiegate diffusamente nei terminali del cliente, soprattutto nell'ambito dei clienti residenziali, e trovare quindi applicazione nel collegamento verso la NT ADSL.

4.1 Interfaccia 10BaseT

L'interfaccia Ethernet su UTP ha raggiunto una larga diffusione nelle reti locali di calcolatori ed è disponibile ad un costo ridotto. Potrebbe però risultare interessante l'impiego anche per applicazioni nella rete domestica per collegare ad esempio un PC alla ATU-R permettendo il trasporto di servizi di tipo Internet. L'interfaccia Ethernet su UTP è definita nello standard IEEE802.3 ed è identificata dalla sigla 10BaseT, dove la cifra 10 indica la velocità aggregata massima consentita dalla rete (10 Mbit/s) e la T indica il mezzo fisico utilizzato (Twisted Pair: coppia simmetrica). I trasduttori 10BaseT sono in grado di trasmettere e ricevere segnali su coppie simmetriche di classe superiore alla 3 su collegamenti di lunghezza fino a 100 m, come previsto dagli standard per il cablaggio strutturato.

4.2 Interfaccia ATM25

Per collegare i terminali del cliente alla NT ADSL un'altra proposta interessante, in grado di garantire il trasporto di celle ATM, è quella di utilizzare l'interfaccia a 25,6 Mbit/s (ATM25) definita in ambito ATM Forum. L'impiego di un'interfaccia ATM verso il terminale del cliente consente di connettere in ATM la sede del fornitore di servizi alla terminazione del cliente finale. L'interfaccia ATM25 è in genere disponibile in forma di scheda da inserire in una workstation, in un router o in un PC. Presso il cliente l'interfaccia ATM25 è proposta per il collegamento fra NT ADSL ed il Set Top Box per la fornitura di servizi video a larga banda commutati (SDVB e Video On Demand).

L'interfaccia ATM25 è un'interfaccia del tipo punto-punto per cavi a coppie simmetriche (una per ciascuna direzione di trasmissione) di classe almeno pari alla 3. La trasmissione è in formato *NRZ (Non Return to Zero)* con codifica 4B/5B e permette di operare su collegamenti di lunghezza fino a 100 m.

4.3 Interfaccia USB

L'interfaccia *USB (Universal Serial Bus)* definisce un bus a velocità fino a 12 Mbit/s per il collegamento di PC con dispositivi periferici quali, ad esempio, stampanti o scanner. Questa interfaccia potrebbe essere impiegata per connettere l'unità NT ADSL con il PC. In questo modo potrebbe non essere più necessario inserire all'interno di un PC la scheda ATM25 o quella 10BaseT (l'interfaccia USB comincia d'altra parte ad essere già presente nei PC). L'impiego dell'interfaccia USB presenta una limitazione dovuta ad una velocità di cifra sul bus non interamente disponibile per il traffico transitante sulla linea ADSL quando sul bus sono impiegati altri dispositivi; questa limitazione potrebbe rendere difficoltosa la possibilità di garantire una qualità di servizio sui dati ADSL. Un'altra limitazione causata da questa interfaccia riguarda la portata: essa infatti consente di coprire con velocità di cifra di 12 Mbit/s distanze inferiori a 5 m.

4.4 Interfaccia IEEE1394

Lo standard IEEE1394 Serial Bus, chiamato anche dai suoi ideatori alla Apple Computer, *FireWire*, definisce una tecnica di interconnessione ad alta velocità (fino a 400 Mbit/s) a basso costo, e adatta al collegamento di unità periferiche o di apparecchiature elettroniche non professionali.

Il collegamento fra due apparecchiature differenti può essere realizzato mediante più tratte fino ad un massimo di sedici; ciascuna delle tratte copre una distanza di 4,5 m.

La principale limitazione dell'interfaccia IEEE1394 risiede nella portata, che è solo di qualche metro (4,5 m) e ne compromette quindi l'efficacia per l'impiego nel cablaggio domestico (l'interfaccia IEEE1394 è nata per connettere direttamente apparecchi *consumer* quali telecamere, ricevitori televisivi, videoregistratori). Per superare questa limitazione è oggi in corso di definizione una nuova versione dello standard, denominata lunga portata *(Long Reach)*, che dovrebbe incrementare la distanza massima dei collegamenti fra apparecchiature diverse fino a 100 m utilizzando cavi a coppie simmetriche UTP5.

5. Conclusioni

Gli aspetti impiantistici rivestono un ruolo di primo piano nell'introduzione in rete dei sistemi ADSL, richiedendo la soluzione di numerosi problemi che si presentano nella realizzazione dell'impianto di centrale e di quello domestico. Soprattutto su quest'ultimo aspetto si sta concentrando l'attenzione dei principali gestori delle reti pubbliche poiché la realizzazione dell'impianto presso il cliente può costituire una quota significativa del costo per linea nell'offerta di servizi a larga banda su sistema ADSL. Si ha anche la consapevolezza che cablaggi che presentino un forte impatto presso le terminazioni remote possono essere difficilmente proposti ed accettati da parte della clientela, specie da quella residenziale.

L'orientamento prevalente è oggi verso soluzioni con POTS Splitter concentrato, realizzato su un'unità esterna alla terminazione di rete NT ADSL. Questa soluzione comporta tuttavia un costo aggiuntivo per l'intervento di personale qualificato necessario all'installazione del POTS Splitter e al cablaggio di questo con la NT ADSL.

La soluzione ADSL senza cablaggio interno (tipo

splitterless), appena disponibile, dovrebbe eliminare la maggior parte di questo costo, in quanto permetterà di connettere l'unità ADSL remota a una qualsiasi delle prese telefoniche presenti all'interno delle residenze dei clienti. Le soluzioni *splitterless* mirano alla realizzazione di un sistema ADSL a ridotta velocità di cifra (fino a 1,5 –2 Mbit/s dalla centrale al cliente e fino a 300-400 kbit/s in senso opposto) per l'offerta di servizi con qualità non garantita e rendono di fatto difficilmente praticabile l'impiego di questi sistemi per l'offerta di servizi con una qualità elevata quali ad esempio il servizio SDVB ad alta velocità di cifra.

Il presente articolo ha indicato le linee guida preliminari relative all'installazione delle apparecchiature ADSL in centrale e presso il cliente facendo riferimento a quanto già utilizzato nella sperimentazione o in fase di prossima introduzione. Dopo una sperimentazione estesa in condizioni di esercizio, e in conseguenza della disponibilità di soluzioni re-ingegnerizzate, alcuni particolari relativi all'installazione saranno naturalmente rivisti alla luce dell'impostazione generale già definita e impiegata.

Bibliografia

[1] Magnone, L.; Petrini, L.: *Sistemi xDSL per l'accesso ad alta velocità su coppie simmetriche in rame.* «Notiziario tecnico Telecom Italia», Anno 7, n. 2, ottobre 1998.

[2] *Commercial building telecommunications cabling standard.* ANSI/TIA/EIA 568-A, ottobre 1995.

[3] *Interfaces and System Configurations for ADSL: Customer Premises.* ADSL Forum, Technical Report 007, febbraio 1998.

Abbreviazioni

ADSL	Asymmetric Digital Subscriber Line
ATU-C	ADSL Termination Unit - Central Office
ATU-R	ADSL Termination Unit - Remote
CDM	Cable Data Modem
CPE	Customer Premises Equipment
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
ETSI	European Telecommunications Standard Institute
FDM	Frequency Division Multiplexing
FSAN	Full Service Access Network
FTTE	Fiber To The Exchange
ISDN	Integrated Services Digital Network
ISDN-BRA	ISDN Basic Rate Access
ITU-T	International Telecommunications Union
LAN	Local Area Network
MuxADSL	Multiplexer ADSL
NRZ	Non Return to Zero
NT	Network Termination
ONU	Optical Network Unit
PABX	Private Automatic Branch Exchange
PC	Personal Computer
PON	Passive Optical Network
POTS	Plain Old Telephone Service
SDVB	Switched Digital Video Broadcast
SOHO	Small Office Home Office
STB	Set Top Box
UAWG	Universal ADSL Working Group
USB	Universal Serial Bus
UTP5	Unshielded Twisted Pair - Category 5
VOD	Video On Demand
VDSL	Very high bit-rate Digital Subscriber Line
xDSL	x-Digital Subscriber Line

Lamberto Petrini si è laureato in Ingegneria Elettronica presso l'Università di Pisa nel 1988 ed ha conseguito il Master of Science in Electrical Engineering dal Polytechnic University di New York nel 1991. Nel 1989 ha ricevuto una borsa di studio dalla Fondazione Ugo Bordoni su tematiche relative ai ponti radio numerici ad alta capacità. Nel 1990 è stato assunto nell'unità di Ricerca e Sviluppo di Telecom Italia (all'epoca SIP) dove ha cominciato ad occuparsi di sistemi trasmissivi numerici su coppie simmetriche in rame (HDSL, ADSL, VDSL). Ha partecipato alla definizione ed alla realizzazione delle sperimentazioni di Video On Demand e di accesso veloce a reti IP condotte da Telecom Italia. Nell'ambito della Direzione Rete, si occupa ora di tematiche relative all'integrazione e alle definizione delle prestazioni delle reti dati e multimediali. È membro dei Gruppi internazionali ETSI TM6, ADSL Forum e DAVIC.

Valerio Claudio Di Biase ha conseguito il diploma di perito tecnico in telecomunicazioni presso ITIS A.Meucci di Roma nel 1978. Opera dal 1981 nel settore di ricerca e sviluppo di sistemi trasmissivi in Telecom Italia. Inizialmente Ia sua attività ha riguardato l'introduzione in rete dei primi sistemi in fibra ottica (1983) occupandosi della conduzione delle prove eseguite su diversi impianti sperimentali. Ha successivamente avviato le prime attività in Telecom Italia sulla distribuzione di segnali televisivi sia in formato analogico sia in formato numerico (anche HDTV). Questa esperienza è stata poi utilizzata nella definizione delle specifiche della rete a larga banda SOCRATE alla quale ha partecipato anche come coordinatore di Gruppi di Lavoro specifici. Ha inoltre partecipato alla definizione e all'esecuzione pratica di diverse sperimentazioni tecnico/commerciali quali quelle relative alla rete PON (Passive Optical Network) a banda stretta, alla VOD (Video On Demand) con ADSL e al progetto europeo AMUSE. Ha preso parte anche alle attività del gruppo FSAN (Full Service Access Network), in particolare a quelle svolte nel gruppo specialistico per le tecnologie ottiche. È autore di diverse pubblicazioni sia in ambito nazionale sia internazionale e svolge attività di docenza presso la Scuola Superiore Guglielmo Reiss Romoli. Oggi si occupa delle norme per la realizzazione di sistemi multimediali nell'ambito del settore Rete Ingegneria Reti Dati e Multimediali – Sviluppo Reti Speciali Trasmissive e in questo ambito coordina anche le attività relative all'inserimento in rete di sistemi CDM (Cable Data Modem) sulla rete HFC.

SDH

Apparati e tecniche di protezione della rete di trasporto SDH di Telecom Italia

GUGLIELMO AURELI
LUIGI CUDIA

Dopo una breve descrizione dell'architettura della rete di trasporto relativa a Telecom Italia, l'articolo illustra i vari tipi di apparati SDH in essa utilizzati sia dal punto di vista funzionale sia dal punto di vista delle loro applicazioni di rete.
Sono inoltre descritti i vari tipi di protezione di apparato che i sistemi forniscono e sono passate in rassegna le varie topologie di rete possibili e le protezioni definite per ognuna di esse dalle Raccomandazioni ITU-T.
Un breve cenno è dato ai nuovi sistemi TDM a 10 Gbit/s che potrebbero trovare impiego in un prossimo futuro nella rete di trasporto e alle principali problematiche di interoperabilità tra apparati di costruttori diversi e di interconnessione con altri gestori delle reti di telecomunicazioni.

1. Introduzione

L'innovazione tecnologica degli ultimi anni, unita alla liberalizzazione dei mercati e alla conseguente entrata di nuovi gestori, sta mettendo in discussione la tradizionale concezione della rete di telecomunicazioni: una stessa piattaforma di rete può essere utilizzata per offrire una pluralità di servizi anche da parte di più gestori. In questo contesto, integrazione e apertura diventano le caratteristiche fondamentali delle reti. L'integrazione è il presupposto dello sviluppo dei nuovi servizi, l'apertura è la condizione per l'interoperabilità di reti e servizi e per l'accesso in regime di competizione da parte di una pluralità di gestori e di clienti.

La rete di telecomunicazioni del futuro deve poter far fronte alle richieste del mercato in termini di offerta di servizi personalizzati; il modello generale della rete che sta emergendo tende così a rendere autonoma la parte di puro trasporto delle informazioni, demandando alla parte di controllo e gestione della rete stessa la realizzazione dei servizi.

La componente trasmissiva delle reti si va sempre più basando sulla tecnica *SDH (Synchronous Digital Hierarchy)* che risponde all'esigenza dei gestori delle reti di telecomunicazioni di disporre di una struttura di rete interna *(core network)* che abbia un livello elevato di prestazioni e di affidabilità, assieme a caratteristiche di flessibilità e gestibilità tali da consentire di offrire ai clienti una vasta gamma di servizi.

Avere nel centro della rete una tecnologia con queste caratteristiche, per un gestore di telecomunicazioni, è critico: gli investimenti necessari sono notevoli e la tecnologia deve essere flessibile per poter consentire di offrire anche nuovi servizi non previsti al momento dell'investimento. Inoltre, guasti o malfunzionamenti nel centro della rete si ripercuotono su un numero non trascurabile di clienti.

La gerarchia SDH (in pratica equivalente a quella SONET, impiegata nella rete nordamericana) è una tecnica numerica per comunicazioni ad altissima velocità su fibra ottica; essa adotta una tecnica di multiplazione "sincrona", che permette di configurare la successione di bit nella trama in modo da consentire l'estrazione e l'inserimento *(drop-insert)* di segnali numerici a frequenza di cifra più bassa da flussi ad alta velocità (ad esempio un flusso a 2,048 Mbit/s da un multiplex a 155,520 Mbit/s) senza alterare gli altri segnali numerici trasportati con il medesimo flusso ad alta velocità. Si definisce quindi una "gerarchia" di flussi che, partendo da un flusso base a 155,520 Mbit/s, possono essere composti in flussi a velocità via via crescente.

Inoltre, l'elevata capacità addizionale riservata ai canali di servizio (overhead) permette il trasporto, all'interno del flusso trasmissivo, di una quantità di informazione per la gestione tale da fornire all'operatore della rete un controllo remoto su tutte le operazioni di configurazione dei flussi come ad esempio la sorveglianza degli allarmi e la supervisione delle prestazioni per ciascuna risorsa di rete.

A partire dal 1997, Telecom Italia ha avviato in maniera sistematica l'inserimento di apparati SDH nella rete di trasporto e sono state così poste le premesse per l'impiego generalizzato della gerarchia numerica sincrona che permetterà di compiere un notevole balzo in avanti nell'ammodernamento dell'infrastruttura di rete e di porsi così all'avan-

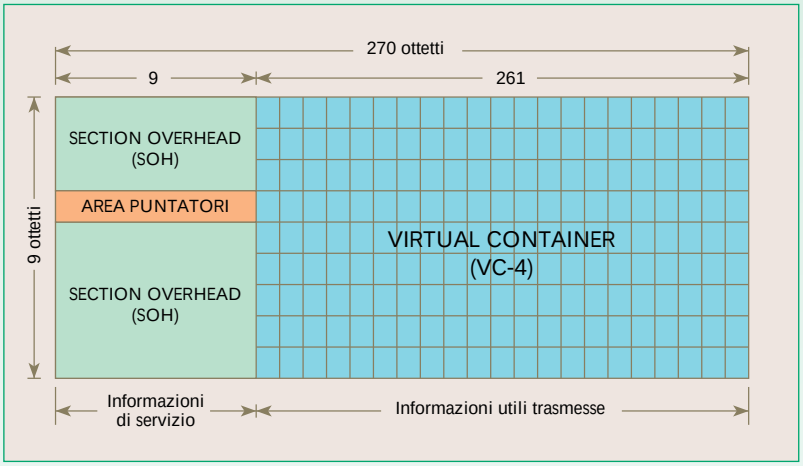
LA GERARCHIA NUMERICA SINCRONA SDH

La gerarchia sincrona dell'SDH è basata su un flusso numerico a 155,520 Mbit/s, generalmente indicato come *STM-1 (Synchronous Transport Module-level 1)*, nel quale l'informazione numerica da trasportare è strutturata in trame *(frame)* che si ripetono nel tempo con un periodo di 125 µs. Un flusso STM-1 trasporta quindi 8 mila trame al secondo.

multiple di 155,520 Mbit/s) sono multipli interi del primo livello e sono indicati come STM-N avendo indicato con N il livello gerarchico. La trasmissione di una trama STM-N avviene inviando ciclicamente un ottetto da ognuna delle trame STM-1 elementari. I livelli gerarchici finora definiti sono:

- STM-1 (155,520 Mbit/s);
- STM-4 (622,080 Mbit/s);
- STM-16 (2,488 Gbit/s);
- STM-64 (9,953 Gbit/s).

La gerarchia numerica sincrona è stata definita in modo da consentire il trasporto di differenti flussi, caratterizzati da diverse frequenze di cifra e da strutture di trama, che



Rappresentazione della struttura di trama STM-1.

La trama STM-1 è strutturata in ottetti (sequenza di 8 bit) ognuno dei quali rappresenta un elemento da trasportare. La trama, rappresentata in figura sotto forma tabellare, è composta di due parti:

- una parte, denominata *Section Overhead*, di 9 x 9 ottetti che contiene le informazioni di servizio;
- un contenitore virtuale composto da 9 x 261 ottetti *(Virtual Container VC-4)* che contiene le informazioni da trasportare.

Nel flusso STM-1 è inviata una nuova trama ogni 125 µs. La trasmissione è seriale (bit per bit) e avviene inviando gli ottetti riga per riga.

I livelli superiori della gerarchia sincrona (velocità di trasmissione

non richiedono modifiche sull'intera rete ogni volta che si introduce un nuovo segnale.

Questo obiettivo è ottenuto inserendo i diversi flussi nei cosiddetti *VC (Virtual Container)* che sono trasportati nell'STM e che sono trattati nei nodi di rete indipendentemente dal contenuto *(payload)*.

La posizione dei diversi VC nella trama è indicata in campi predefiniti della stessa trama, chiamati "puntatori". L'impiego dei puntatori facilita la multiplazione e la demultiplazione, poiché la posizione di ogni byte di un singolo tributario in una trama STM-N può essere facilmente ricavata dal valore del puntatore.

La gerarchia numerica sincrona mette anche a disposizione dei gestori della rete una serie di campi informativi di servizio necessari per realizzare le funzioni di *OAM&P (Operations, Administration, Maintenance and Provisioning)* che devono essere disponibili in una moderna rete di telecomunicazioni. Sono previsti in particolare ottetti per gli allarmi, per il controllo delle prestazioni e per la realizzazione di canali dedicati al trasporto delle informazioni di gestione.

I principali vantaggi legati all'impiego della gerarchia SDH sono:

- una grande flessibilità di gestione dei flussi trasmissivi;
- la possibilità (grazie all'impiego di tecniche di multiplazione sincrone a più stadi) di inserire e di estrarre segnali a più bassa frequenza di cifra da un flusso trasmissivo ad alta capacità senza dover scomporre e ricostruire l'intero flusso *(add-drop multiplexer)*;
- la disponibilità di interfacce ottiche ed elettriche normalizzate, in grado di consentire l'interconnessione di linea tra apparati di costruttori diversi;
- la protezione dei flussi di traffico realizzata negli apparati, che permette una riconfigurazione automatica della rete in caso di guasti *(self-healing network)*;
- l'elevata capacità trasmissiva dedicata al trasporto delle informazioni di gestione;
- la possibilità di effettuare tutte le operazioni di OAM&P da postazioni remote opportunamente dislocate sul territorio;
- la possibilità di utilizzare differenti tipologie di apparati: *ADM (Add Drop Multiplexer)*, in grado di inserire ed estrarre flussi più "lenti" da flussi più "veloci"; RED, detti anche *DXC (Digital Cross Connect)*, in grado di effettuare permutazione a più livelli dei flussi trasmissivi; terminali di linea; rigeneratori; ponti radio;
- la possibilità di connettere in molti modi gli apparati in rete secondo differenti topologie (a maglia, ad anello, ad anelli interconnessi) per poter ottenere sempre il miglior compromesso tra l'affidabilità e i costi.

guardia rispetto alle reti di altri gestori di rilievo con i quali spesso si effettuano i confronti.

Tra le motivazioni che hanno spinto Telecom Italia ad adeguare la propria rete di trasporto, possono essere elencate: la rapida crescita dell'innovazione tecnologica, le buone prospettive di sviluppo del mercato dei nuovi servizi a larga banda e la necessità di interconnessione di nuovi gestori.

In questo articolo, dopo una breve descrizione della rete di trasporto SDH di Telecom Italia, saranno analizzati i vari tipi di apparati SDH, le loro principali funzionalità e l'impiego di essi all'interno della rete. Saranno poi descritti i vari schemi di protezione resi disponibili dalla gerarchia SDH.

In due altri articoli, presenti nel numero precedente del *Notiziario Tecnico* [1, 2], sono riportate le caratteristiche dei sistemi di gestione per la rete SDH, mentre per una descrizione dello schema a blocchi generalizzato degli apparati SDH, così come riportato nelle Raccomandazioni ITU-T, si rimanda all'articolo "Apparati per la rete SDH" già pubblicato sul *Notiziario Tecnico* [3].

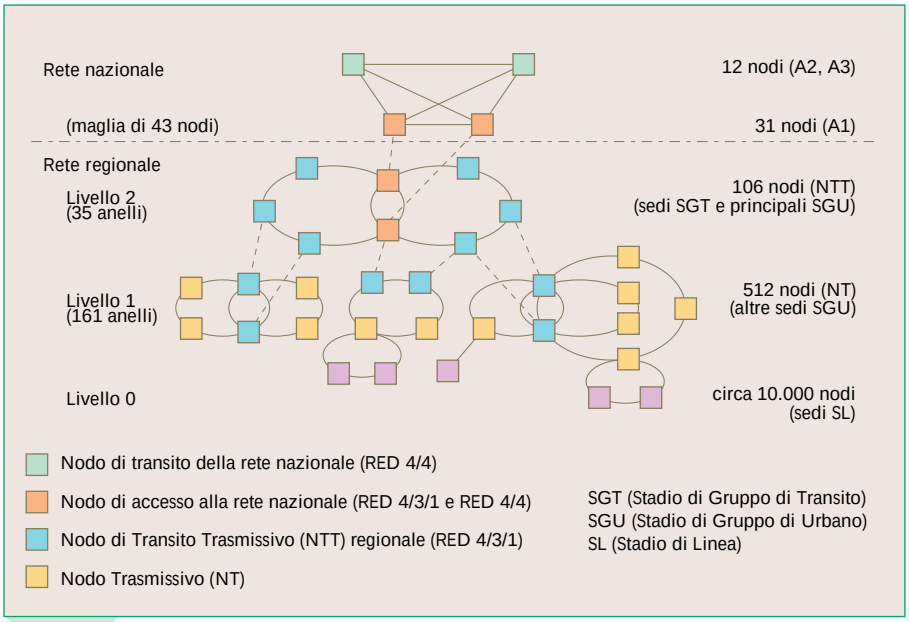


Figura 1 *Architettura di riferimento per la rete di trasporto SDH di Telecom Italia.*

2. La rete di trasporto SDH di Telecom Italia

La rete di trasporto SDH di Telecom Italia presenta una struttura gerarchica costituita da una rete nazionale e da diverse reti regionali: in particolare la rete nazionale è costituita quasi completamente dalla rete a lunga distanza della ex Iritel.

In figura 1 è riportata l'architettura di riferimento per la rete di trasporto SDH, oggi in fase di completamento.

La rete nazionale è costituita da permutatori numerici *RED 4/4 (Ripartitore Elettronico Digitale*[1] in grado di permutare flussi a 140 ed a 155,520 Mbit/s) collegati tra loro a maglia quasi completa per mezzo di sistemi di linea a 2,5 Gbit/s.

Una rete regionale è costituita da apparati *ADM (Add-Drop Multiplexer)* collegati ad anello. I diversi anelli sono organizzati su più livelli gerarchici e sono interconnessi tramite RED. In una rete regionale è possibile distinguere due tipologie di anelli: anelli di secondo livello, costituiti da *ADM-16 (Add-Drop Multiplexer* con capacità di linea STM-16 a 2,5 Gbit/s), e anelli di primo livello, costituiti da *ADM-4 (Add-Drop Multiplexer* con capacità di linea STM-4 a 622,080 Mbit/s) o *ADM-1 (Add-Drop Multiplexer* con capacità di linea STM-1 a 155,520 Mbit/s). Sono stati realizzati anche anelli di livello 0, costituiti da apparati MPX-1 (multiplatore d'utente sincrono con capacità di linea STM-1) con un ADM-1 che svolge la funzione di nodo di raccolta. Questi ultimi anelli sono considerati come parte della rete di accesso. Maggiori particolari sul funzionamento degli apparati citati sono riportati nei paragrafi successivi.

Il collegamento tra la rete nazionale e le reti regionali avviene nei Nodi A1. In ciascuno di essi sono presenti il RED 4/4 della rete nazionale, il RED 4/3/1 (Ripartitore Elettronico Digitale in grado di permutare VC-12, VC-3 e VC-4) del velo nazionale - composto da trentuno RED 4/3/1 la cui funzione è quella di interconnettere la rete regionale con quella nazionale - e un ADM-16 per ogni anello di secondo livello regionale che passa da quel nodo. Gli ADM-16 sono connessi al RED 4/3/1 che raccoglie il traffico proveniente dai vari anelli di secondo livello e lo instrada: la fonia verso gli *SGT (Stadio di Gruppo di Transito)*, il traffico di rete mobile verso l'*MSC (Mobile Switching Centre)*, il traffico dati verso la rete flessibile. Tutto il traffico uscente dalla rete regionale è instradato verso il RED 4/4 della rete nazionale. Tutti gli anelli di secondo livello passano per due Nodi A1 in modo da costituire sempre un instradamento di riserva per il collegamento tra la rete nazionale e quella regionale.

Il collegamento invece tra gli anelli di secondo livello e di primo livello della rete regionale è effettuato negli *NTT (Nodi di Transito Trasmissivo)* dove è presente un ADM-16 dell'anello di secondo livello

(1) *In questo articolo è usato il termine RED in luogo del termine DXC usato in [1] e [2].*

connesso ad un RED 4/3/1 regionale che è collegato a sua volta ad uno o più ADM-1 o ADM-4 degli anelli di primo livello. I nodi NTT sono di solito coincidenti con le sedi *SGU (Stadio di Gruppo Urbano)*. Anche in questo caso ogni anello di primo livello passa per due nodi NTT.

Infine negli *NT (Nodi Trasmissivi)* sono connessi gli anelli di primo livello con quelli di livello 0 mediante il collegamento tra un ADM-4 dell'anello di primo livello e un ADM-1 dell'anello di livello 0.

La gestione della rete di trasporto SDH è effettuata tramite un sistema unico (SG-SDH), sviluppato da Telesoft per Telecom Italia, che effettua tutte le operazioni di configurazione, sorveglianza degli allarmi e supervisione delle prestazioni dei flussi. Il sistema di gestione di rete SG-SDH dialoga con gli apparati attraverso i sistemi proprietari per la gestione di elemento realizzati dalle Società manifatturiere che hanno finora fornito gli apparati trasmissivi a Telecom Italia.

La struttura della rete di trasporto fin qui descritta è in fase di revisione e oggi si sta valutando l'opportunità di ridurre il numero dei nodi trasmissivi della rete nazionale.

3. Apparati e sistemi SDH per la rete di trasporto

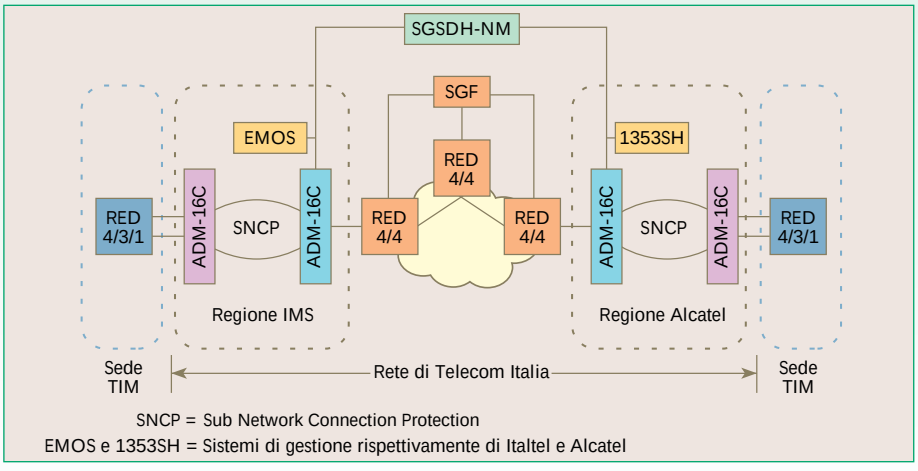
Gli apparati di trasporto SDH possono essere suddivisi in tre principali categorie: i sistemi di permutazione RED, quelli di multiplazione e Add-Drop ADM e quelli di sola multiplazione *TL (Terminale di Linea)*.

Dal punto di vista degli apparati, la rete SDH di Telecom Italia è stata suddivisa in due aree geografiche. Nel nord e nel centro-nord d'Italia sono impiegati apparati forniti dal consorzio *IMS (Italtel, Marconi Communications, Sirti)* mentre nel centro e nel sud d'Italia sono utilizzati apparati Alcatel. Più in particolare all'interno del consorzio IMS gli apparati ADM sono forniti da Italtel, mentre i RED 4/3/1 sono

REALIZZAZIONE DI COLLEGAMENTI A 155 MBIT/S PER UN DIVERSO GESTORE DI RETE

- **I problemi legati al controllo della qualità sono cresciuti di importanza da quando è iniziata l'interconnessione con altri gestori: sono stati già forniti primi flussi SDH a TIM, utilizzando strutture dedicate per portare i flussi trasmissivi dalle sedi di questo gestore alle centrali trasmissive di Telecom Italia.**
  Un esempio di collegamento con TIM è riportato nella figura in basso. Le sigle EMOS e 1353SH indicano i sistemi di gestione *EM (Element Manager)* rispettivamente dei costruttori Italtel e Alcatel [2], mentre SGSDH-NM e SGF indicano rispettivamente il sistema di gestione della rete SDH e della rete dei RED 4/4.

- **I VC-x sono generati da un apparato di TIM ed il VC-4 che li raccoglie è trasportato da un collegamento ad anello "degenere" (in quanto formato da due soli apparati) a 622 Mbit/s o a 2,5 Gbit/s verso la prima centrale di Telecom Italia. Qui il flusso è inserito nella rete nazionale dei RED 4/4 o direttamente (nel caso in cui TIM richieda VC-4 completi) o passando attraverso un RED 4/3/1 (nel caso di una richiesta di N x VC-12).**
  Nel secondo caso il RED effettua la *consolidation*, cioè affascia in un VC-4 tutti i VC-12 di diversi flussi VC-4 in ingresso che hanno la stessa destinazione. Il collegamento ad anello "degenere" è necessario perché, per proteggere il traffico del collegamento, è oggi utilizzata in via transitoria la protezione ad anello SNCP in quanto non è ancora disponibile la protezione di linea di tipo MSP che sarà utilizzabile successivamente.



Schema generale di un collegamento a 155 Mbit/s nel caso di due gestori di rete.

forniti da Marconi Communications. Il RED 4/3/1 Marconi è anche inserito nella rete del centro-sud del nostro Paese in quanto esso fa parte della rete nazionale SDH che comprende complessivamente trentuno di questi apparati.

L'aver scelto di utilizzare apparati di diversi costruttori ha reso necessario l'esame di problematiche legate alla compatibilità trasversale; la soluzione di questo problema, dal punto di vista gestionale, consiste nell'aver definito un *NM (Network Manager)* con un'interfaccia comune verso gli *EM (Element Manager)* dei diversi costruttori [1], [2].

Per quel che riguarda gli apparati, la suddivisione territoriale assicura che gli anelli regionali siano tutti dello stesso fornitore e quindi non presentino problemi legati all'interconnessione. L'unico caso di collegamento tra apparati di costruttori diversi si presenta nell'interfaccia tra rete nazionale e regionale dove i RED 4/3/1 della Marconi sono collegati ad apparati ADM sia di Alcatel sia di Italtel: in questo caso la compatibilità sia delle interfacce ottiche - assicurata dalla conformità alla Raccomandazione ITU-T G.957 [4] - sia delle interfacce elettriche - assicurata dalla Raccomandazione ITU-T G.703 [5] - permette il colloquio a livello fisico di questi apparati.

Tra le prestazioni comuni a tutti gli apparati SDH, oltre alla possibilità di permettere una gestione remota e alle protezioni di rete che è possibile introdurre, riveste un ruolo fondamentale il monitoraggio della qualità dei flussi trasmissivi: conoscere la qualità dei flussi trasportati consente, infatti, di rispondere alle esigenze dei clienti che richiedono - anche per contratto - una determinata qualità trasmissiva, e allo stesso tempo agevola notevolmente l'esercizio e la manutenzione della rete.

Gli apparati e il rilascio del sistema di gestione SG-SDH, che sono oggi in esercizio, permettono di effettuare misure di qualità, secondo i parametri prestazionali definiti dalla Raccomandazione ITU-T G.826 [6], sui VC-12, VC-3 e VC-4 generati e terminati su apparati di Telecom Italia. Questa prestazione rappresenta una limitazione soprattutto nei casi in cui Telecom Italia fornisce ad un cliente un intero flusso STM-1 ed è quindi il cliente che genera i VC-x trasportati dal flusso STM-1. La soluzione di questo problema è data dall'introduzione di funzioni di *HPOM (Higher order Path Overhead Monitoring)* e *LPOM (Lower order Path Overhead Monitoring)* che effettuano un controllo non intrusivo dell'overhead dei VC trasportati in un flusso SDH e che quindi permettono di monitorare la qualità dei VC non terminati con apparati di Telecom Italia. Mediante una correlazione tra i dati raccolti è così possibile controllare la qualità tra gli apparati terminali del VC (di tipo "end-to-end").

Per avere invece un monitoraggio completo delle prestazioni all'interno della rete gestita da Telecom Italia e senza dover effettuare correlazioni tra dati è necessaria, appena sarà disponibile sugli apparati, la prestazione di *TCM (Tandem Connection Monitoring)*. Questa prestazione comporta la realizzazione di uno pseudo-collegamento ad un livello trasmissivo sottostante al VC-x che permette di controllare una qualsiasi porzione di un percorso *(path)*.

3.1 ADM (Add-Drop Multiplexer)

L'ADM è un multiplatore in grado di estrarre flussi tributari PDH/SDH da un flusso di linea SDH, o di inserirli nel flusso.

Sono stati realizzati diversi tipi di ADM, distinti in base alla frequenza di cifra *(bit rate)* della linea SDH:

- ADM-1, con interfacce di linea STM-1 a 155,520 Mbit/s;
- ADM-4, con interfacce di linea STM-4 a 622,080 Mbit/s;
- ADM-16, con interfacce di linea STM-16 a 2,5 Gbit/s.

L'applicazione in rete tipica degli ADM è la struttura ad anello dove gli apparati consentono di fruire di numerosi vantaggi della gerarchia SDH quali:

- protezioni efficaci;
- accesso ad un qualsiasi flusso tributario senza necessità di demultiplare il flusso sincrono di linea;
- gestione centralizzata degli apparati.

Con una opportuna predisposizione degli ADM è possibile utilizzare questi sistemi come semplici terminali di linea o come rigeneratori. Lo schema a blocchi di un apparato ADM è un sottoinsieme delle caratteristiche funzionali descritte nella Raccomandazione ITU-T G.783 [7]: a seconda della frequenza di cifra di linea mancano infatti le funzionalità che consentono il trattamento dei tributari plesiocroni a 2 e a 34 Mbit/s, o la permutazione dei *path* di ordine elevato (VC-4).

Gli ADM-1 compatti sono apparati apparsi di recente sul mercato e derivati direttamente dagli ADM-1 tradizionali: essi dispongono di tutte le funzioni proprie della gerarchia sincrona, ma presentano il vantaggio di un minor ingombro, di una notevole semplicità d'installazione e di poter essere alimentati anche in corrente alternata direttamente collegati alla rete pubblica di alimentazione. Sono apparati da tavolo o installabili a muro e rappresentano una soluzione idonea (diversamente dagli apparati tradizionali ADM) per risolvere i casi in cui sia necessario dover portare un flusso STM-1 nella sede di un cliente non dotata delle strutture presenti nelle centrali telefoniche (telai, alimentazione in continua). Questi apparati hanno tuttavia alcune limitazioni quali la possibilità di un equipaggiamento con un numero ridotto di tributari, la mancanza di ridondanze e di protezioni d'apparato. Essi invece consentono di proteggere la linea nel caso sia presente un doppio instradamento.

3.2 RED (Ripartitore Elettronico Digitale)

Il RED sincrono è un apparato flessibile in grado di multiplare e demultiplare flussi, di estrarre e inserire flussi tributari dalla linea e di permutare VC-4, VC-3 e VC-12.

Sono oggi disponibili due tipi di RED sincroni:

- il RED 4/4, che permuta solo i VC-4;
- il RED 4/3/1, che permuta contenitori di qualsiasi ordine (VC-12, VC-3 e VC-4).

La principale applicazione dei RED 4/4 - che presentano una capacità di 256 porte STM-1 equivalenti - riguarda la protezione dei collegamenti trasmissivi mediante una procedura di ripristino *(restoration)*,

Glossario

RED: Apparato con capacità elevata (generalmente con 256 porte STM-1 equivalenti) in grado di effettuare multiplazione, demultiplazione, inserimento ed estrazione di flussi tributari, e permutazioni a vari livelli della gerarchia sincrona (VC-12, VC-3, VC4).

ADM: Apparato sincrono di piccola-media capacità (al più 32 porte STM-1 equivalenti per l'ADM-16) progettato per eseguire multiplazione, demultiplazione, inserimento ed estrazione di flussi tributari.

gestita in modo centralizzato; essa permette di reinstradare VC-4 da connessioni in avaria ad altre funzionanti, individuando sulla rete un instradamento disponibile. I RED 4/3/1 sono anch'essi apparati di grossa capacità (256 porte STM-1 equivalenti) e sono utilizzati nei principali nodi della rete per l'instradamento dei circuiti, per l'ottimizzazione del riempimento dei flussi trasmissivi e per le funzioni di protezione.

Oltre ai RED sincroni sopra descritti sono anche presenti in rete da diversi anni RED plesiocroni che effettuano permutazioni a livello di 2 Mbit/s (RED 3/1) o di 64 kbit/s (RED 1/0) e che sono utilizzati nella rete flessibile.

3.3 Terminale di linea a 2,5 Gbit/s

Il terminale di linea a 2,5 Gbit/s è un apparato che ha un sottoinsieme delle funzionalità di un ADM. Esso multipla o demultipla, infatti, i flussi tributari nel segnale di linea STM-16 ma non permette di inserire o di estrarre (Add-Drop) flussi con frequenza di cifra inferiore in uno in transito. Mentre fino a qualche anno fa un terminale di linea a 2,5 Gbit/s era un apparato costruito *ad hoc*, i nuovi terminali di linea a 2,5 Gbit/s oggi sono realizzati sottoequipaggiando un ADM-16.

Nella rete di Telecom Italia questi apparati sono utilizzati nei collegamenti tra i RED 4/4 della rete nazionale.

3.4 Sistemi trasmissivi a 10 Gbit/s

Sono stati finora illustrati gli apparati SDH industrializzati e inseriti nella rete di Telecom Italia. Fra breve sarà possibile disporre anche di sistemi SDH a 10 Gbit/s.

Le principali problematiche relative ai sistemi SDH a 10 Gbit/s possono essere ricondotte alle limitazioni di tipo tecnologico degli apparati e a quelle di tipo trasmissivo.

L'operazione di multiplazione elettrica dei tributari richiede circuiti integrati e memorie molto complesse. L'approccio utilizzato nella realizzazione degli apparati consiste nell'effettuare la maggior parte delle operazioni agendo su segnali trattati in forma parallela, quindi con una frequenza di cifra relativamente bassa: solo l'ultimo circuito prima del trasmettitore - in pratica un multiplatore per 8 o per 16 - deve operare con una frequenza di cifra di 10 Gbit/s.

Il segnale multiplato è poi trasferito al convertitore elettro-ottico che può essere di due tipi: il primo si basa su un diodo laser modulato direttamente tramite la corrente di iniezione, mentre il secondo prevede l'uso di un modulatore (esterno o integrato), operante su una sorgente laser in emissione continua *(Continuous Wave)*. In entrambi i casi è richiesto il controllo di temperatura del laser, l'*ATC (Automatic Temperature Control)*, ed un sistema per il controllo della potenza di emissione, l'*APC (Automatic Power Control)*.

All'aumentare della frequenza di cifra si manifestano alcune criticità per i componenti impiegati nel trasmettitore: sono critici il circuito di multiplazione per questioni di velocità e di potenza dissipata, il circuito pilota *(driver)* per il laser o per il modulatore (esterno o integrato) per analoghi motivi, lo stesso laser, nel caso di modulazione diretta, per la velocità e soprattutto per il cosiddetto "*chirp*" (allargamento dinamico dello spettro) che, assieme alla dispersione cromatica della fibra ottica, crea significative limitazioni sulla distanza tra apparati successivi.

Sul lato ricevente il segnale ottico è rivelato, cioè trasformato in una fotocorrente, e successivamente amplificato e filtrato. Con un'operazione non-lineare viene estratto dai dati un segnale alla frequenza di orologio *(clock)*, utilizzato per sincronizzare la funzione di decisione sulla presenza o no del segnale in un determinato intervallo di tempo. Ottenuti i dati in forma numerica seriale, essi sono demultiplati e da questi sono ricostruiti i tributari di partenza. Le criticità che si presentano con il crescere della frequenza di cifra sono concentrate sulla coppia fotodiodo-amplificatore, sul circuito di decisione e sul demultiplatore elettronico.

Lo stato dell'arte della tecnologia dei componenti optoelettronici ed elettronici per i trasmettitori e per i ricevitori è tale che la disponibilità commerciale di componenti per frequenze di cifra superiori a 10 Gbit/s sembra oggi avere scarse prospettive di impiego nei prossimi anni.

4. Tecniche di protezione

È possibile distinguere tra due possibili tipologie di protezione: quella di apparato e quella di rete.

4.1 La protezione di apparato

La protezione di apparato consiste sia nel raddoppio degli organi fondamentali di un apparato SDH, quali ad esempio la matrice di permutazione, l'unità di sincro-

SPERIMENTAZIONE DI UN SISTEMA A 10 GBIT/S

Con le prove eseguite nel giugno 1998 è stata portata a termine la sperimentazione in campo del sistema ottico TDM a 10 Gbit/s fornito da Alcatel (16192 SM). Obiettivi della sperimentazione sono stati:

- la verifica della possibilità di realizzare collegamenti TDM a 10 Gbit/s sui portanti fisici utilizzati nella rete di Telecom Italia (fibre ottiche G.652 e G.653);
- la verifica della possibilità di inserire in rete gli apparati SDH STM-64.

La prima fase della sperimentazione, svoltasi tra ottobre e dicembre 1997, ha permesso di rilevare la possibilità di realizzare un collegamento a 10 Gbit/s su una tratta in fibra G.653 della rete nazionale, tra le centrali di Torino-Isonzo e di Milano-Bersaglio, ma ha segnalato al contempo due punti critici:

- l'impossibilità di realizzare con il sistema sperimentato collegamenti su distanze significative su una fibra che risponde alla Raccomandazione ITU-T G.652;
- l'impossibilità di verificare l'effettiva integrabilità del sistema nella rete di Telecom Italia.

Il primo punto è attribuibile al tipo di trasmettitori con cui il sistema era equipaggiato, in quanto ottimizzati per la trasmissione su fibra in accordo con la Raccomandazione ITU-T G.653. Il secondo punto è invece legato al fatto che gli apparati provati erano destinati al mercato nordamericano e quindi conformi alla gerarchia SONET. Successivamente il costruttore ha sostituito i trasmettitori.

La fase conclusiva della sperimentazione è stata focalizzata su aspetti trasmissivi connessi all'impiego dei sistemi TDM a 10 Gbit/s, quali:

- verifica della rispondenza dei nuovi trasmettitori alle specifiche di dispersione su fibra G.652 in bobina;
- fattibilità di un collegamento di 360 km su fibra G.653 installata con tre amplificatori di linea;
- verifica della tolleranza del sistema alla non linearità della fibra trasmissiva (G.653 ed eventualmente G.652).

Le prove condotte hanno mostrato l'adeguatezza dei nuovi trasmettitori sia all'utilizzo su fibra G.653 sia su quella G.652 (almeno fino a 80 km) e la fattibilità in campo di un collegamento a 10 Gbit/s non rigenerato su 360 km di fibra G.653 installata. È stato inoltre riscontrato che l'effetto non lineare dominante nella configurazione di sistema utilizzata è la diffusione Brillouin stimolata che limita a 10 dBm la potenza ottica utilizzabile in trasmissione.

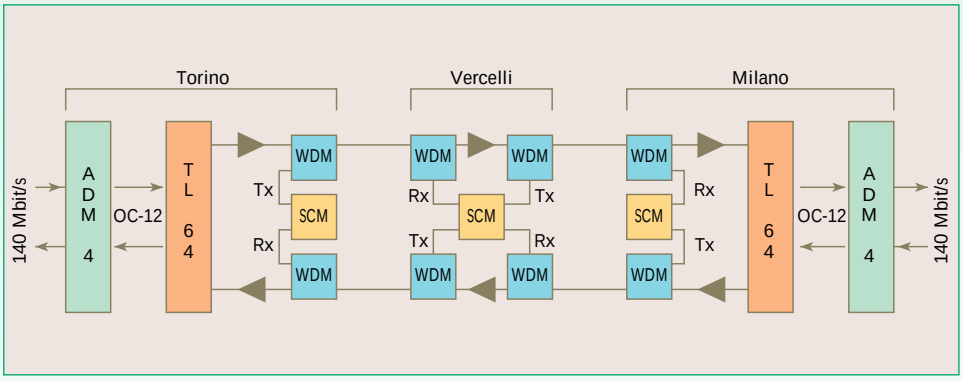
Considerando anche i risultati ottenuti nella prima fase della sperimentazione, le principali conclusioni che possono essere tratte dalle prove effettuate sono pertanto le seguenti:

- risulta possibile impiegare sistemi TDM a 10 Gbit/s su collegamenti in fibra G.653 (fino a 360 km e oltre); nelle condizioni di esercizio del sistema (potenza di lancio nominale di 10 dBm) non sono state riscontrate sensibili penalità trasmissive dovute a PMD o non linearità del portante fisico;
- è stata dimostrata la fattibilità di collegamenti in fibra G.652 fino a 80 km;
- con un passo di amplificazione di circa 90 km è possibile realizzare collegamenti a 10 Gbit/s non rigenerati su 360 km di fibra G.653;
- non sono state utilizzate tecniche per sopprimere l'effetto Brillouin; non è perciò possibile portare la potenza di lancio oltre i 10 dBm consigliati dal costruttore; questo fatto limita il budget di potenza dei collegamenti senza amplificatori di linea;
- il sistema di supervisione degli amplificatori di linea tramite il canale ottico di servizio è risultato soddisfacente, sebbene la gestione sia possibile solo localmente.

Dal lato trasmissivo, l'esito della sperimentazione è stato positivo, ha confermato che le fibre installate in rete sono compatibili con la trasmissione TDM a 10 Gbit/s.

Si può infatti prevedere, mantenendo un passo di amplificazione di circa 90 km, di spingere la portata del sistema TDM a 10 Gbit/s sperimentato oltre i 600 km, utilizzando fino a sei amplificatori di linea. La gestione di questi amplificatori risulta peraltro piuttosto agevole, anche se, per ora, soltanto a livello locale.

La portata reale del sistema è tuttavia molto condizionata dall'entità del passo di amplificazione attuabile in pratica: l'incremento del passo di amplificazione da 90 km a 120 km riduce drasticamente la distanza del collegamento non rigenerato.



Schema del collegamento a 10 Gbit/s realizzato tra Torino e Milano.

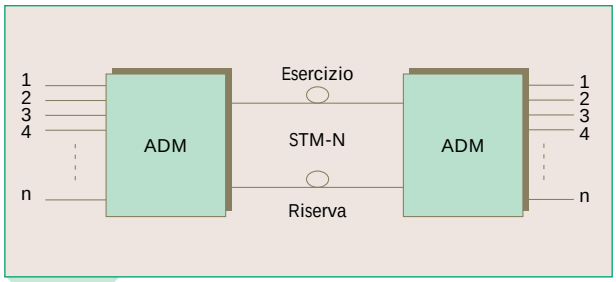


Figura 2 *Protezione MSP (Multiplex Section Protection).*

nismo, l'alimentazione, sia nella protezione delle schede di tributario.

La protezione di scheda può essere di due tipi: 1+1 e 1:N. Nel primo caso per ogni scheda da proteggere è predisposta una seconda che la sostituisce nel caso di guasto, attuando una protezione dedicata. Lo scambio tra le due schede avviene automaticamente quando l'apparato rileva il guasto.

Nel secondo caso una scheda di riserva può sostituire una delle N schede di esercizio, attuando così una protezione condivisa. Anche in questo caso lo scambio è automatico, con gli stessi tempi di intervento del caso precedente, e si attua naturalmente una protezione meno costosa che quella 1+1; questa soluzione, che non permetterebbe di far fronte al guasto contemporaneo di due o più schede, si basa sulla considerazione che risulta essere assai poco probabile l'evento di guasti contemporanei.

4.2 La protezione di rete

Per quanto riguarda la protezione di rete, sono stati definiti diversi schemi di protezione applicabili alle possibili topologie di rete. La protezione più semplice, applicata nei collegamenti lineari punto-punto, è quella della sezione di multiplazione *MSP (Multiplex Section Protection)* attuata con un sistema del tipo 1+1 (figura 2).

Questa protezione consiste nel duplicare le interfacce trasmissive di entrambi gli apparati e il cablaggio tra essi. In trasmissione il segnale STM-N di linea è inviato su entrambi i collegamenti (uno di questi è predefinito come collegamento di esercizio mentre l'altro è di riserva); in ricezione invece è scelto, mediante un selettore, il segnale di qualità migliore (a parità di qualità è scelto il segnale sul collegamento di esercizio). Nel caso in cui il collegamento di esercizio sia danneggiato, o più in generale quando presenti una riduzione di qualità, l'apparato in ricezione rileva la mancanza o il degrado del segnale utile e, mediante il selettore, preleva il segnale dal collegamento di riserva. Queste funzioni sono svolte dal blocco funzionale MSP, definito nella Raccomandazione ITU-T G.783 [7] e presente in tutti gli apparati SDH. Il tempo di scambio è dell'ordine di qualche decina di millisecondi. La protezione può essere *"single ended"* o *"dual ended"* e, inoltre, è o no reversibile.

La protezione *"single ended"* è costituita da uno

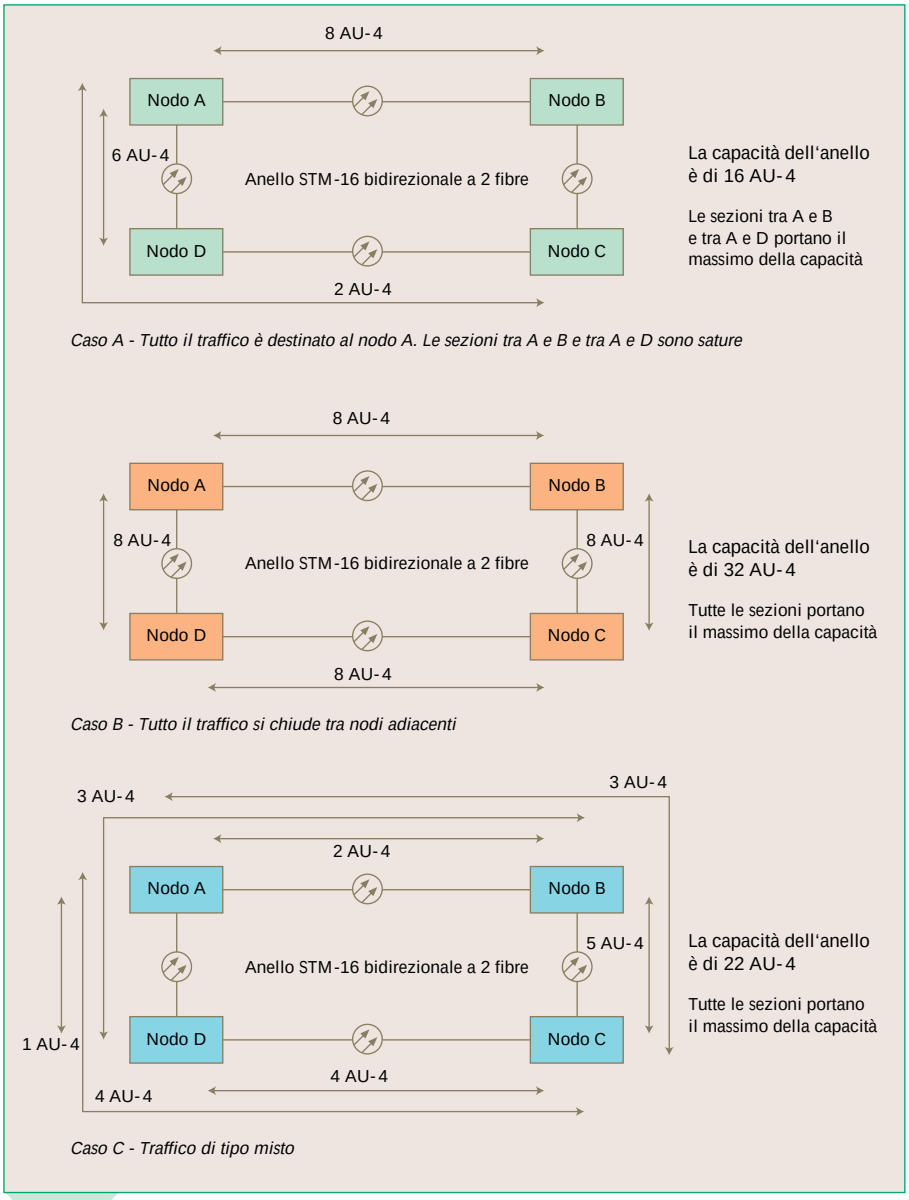


Figura 3 *Effetto della distribuzione del traffico sulla capacità di un anello bidirezionale.*

scambio sull'apparato che rileva la malfunzione indipendentemente dal comportamento dell'altro terminale e senza nessuno scambio di informazioni tra i due terminali. Nel caso di protezione *"dual ended"*, il terminale che rileva il guasto scambia sulla riserva e nello stesso tempo informa il terminale remoto - tramite i byte K1 e K2 della trama STM-N e secondo un protocollo definito nella Raccomandazione ITU-T G.841 [8] - dell'avvenuto scambio. Il terminale remoto, ricevuta l'informazione, scambia anch'esso sul collegamento di riserva.

La protezione reversibile consiste nel ritorno automatico del selettore sul collegamento di esercizio nel momento in cui la malfunzione viene eliminata; quella non reversibile non consente il ritorno automatico del selettore sul collegamento di esercizio.

capacità in tutte le sezioni dell'anello in quanto tutto il traffico in esercizio è trasportato su una sola fibra in una direzione. È quindi preferibile utilizzare l'anello unidirezionale nel caso di traffico diretto verso un unico nodo *(hub)* poiché la capacità dell'anello non può comunque superare quella di linea.

Nell'anello bidirezionale invece i VC impegnano la capacità dell'anello solo nelle sezioni che congiungono i due nodi terminali del path. Se si presentano notevoli relazioni di traffico tra i vari nodi dell'anello è quindi preferibile utilizzare l'anello bidirezionale poiché in tal caso il traffico totale smaltito dall'anello può superare la capacità di linea.

L'effetto della distribuzione del traffico sulla capacità dell'anello bidirezionale è mostrato nella figura 3, tratta dalla Raccomandazione ITU-T G.841 [8].

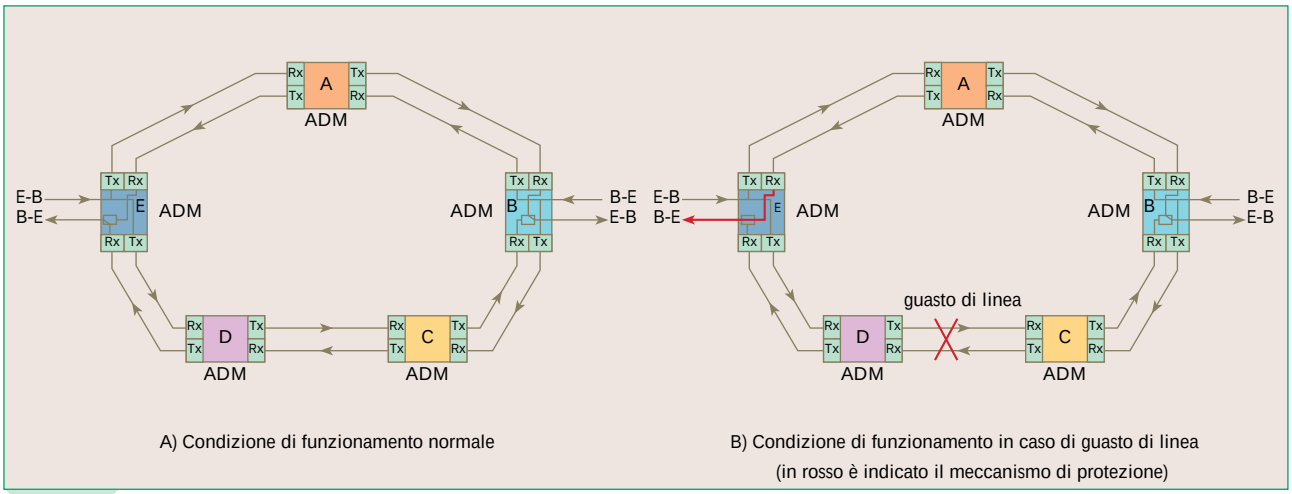


Figura 4 *Meccanismo della protezione SNCP (Sub Network Connection Protection).*

Per topologie di rete ad anello sono disponibili altri tipi di protezione: la protezione *SNCP (Sub Network Connection Protection)* e quella *MSP-Ring (Multiplex Section Protection - Ring);* prima di descrivere queste protezioni, è opportuno distinguere, tra gli anelli a due fibre, quelli unidirezionali da quelli bidirezionali.

L'anello unidirezionale è realizzato utilizzando una delle fibre come mezzo di esercizio e l'altra come riserva. Nelle condizioni normali di funzionamento il segnale è inviato da ciascun ADM dell'anello sulla fibra di esercizio ed in un senso di trasmissione prestabilito. Il volume del traffico trasportato da un anello unidirezionale è al più pari alla capacità di linea[2] degli apparati.

Nell'anello bidirezionale entrambe le fibre sono utilizzate come mezzo di esercizio e il segnale utile può essere inviato su entrambi i versi di trasmissione. Può essere comunque riservata a ognuna delle due fibre una scorta pari a metà della capacità totale dell'anello. Il volume del traffico trasportato dall'anello è quindi almeno pari alla capacità di linea degli apparati.

Nell'anello unidirezionale i VC impegnano la

La protezione di tipo SNCP può essere applicata solo negli anelli unidirezionali e agisce a livello di path; essa è quindi attivabile in maniera indipendente per ogni tipo di VC. La protezione consiste nel trasmettere il flusso contenuto in un VC che si vuol proteggere in entrambi i sensi di trasmissione dell'anello utilizzando da un lato la fibra di esercizio e dall'altro quella di riserva. L'ADM posto al termine del flusso di un VC riceve il segnale da entrambi i lati dell'anello e sceglie quello migliore. A parità di qualità del segnale ricevuto viene selezionato quello proveniente dal lato di esercizio dell'anello. In caso di guasto lungo l'anello, uno dei due versi di trasmissione si interrompe e l'ADM in ricezione si predispone sul segnale proveniente dall'altro verso di trasmissione. La protezione può essere solo del tipo *single-ended.* Il meccanismo di protezione è riportato in figura 4.

La protezione di tipo MSP-Ring è applicabile sia sugli anelli unidirezionali sia su quelli bidirezionali. Questo tipo di protezione agisce sull'intera sezione di multiplazione e non sul *path* come la SNCP. Di conseguenza la MSP-Ring non va attivata per ogni singolo VC ma una volta predisposta riguarda tutti i VC della sezione di multiplazione. In caso di guasto su una sezione dell'anello nella quale è stata attivata la MSP-Ring, gli apparati terminali della sezione in

(2) *Velocità di cifra dell'interfaccia di linea dell'apparato.*

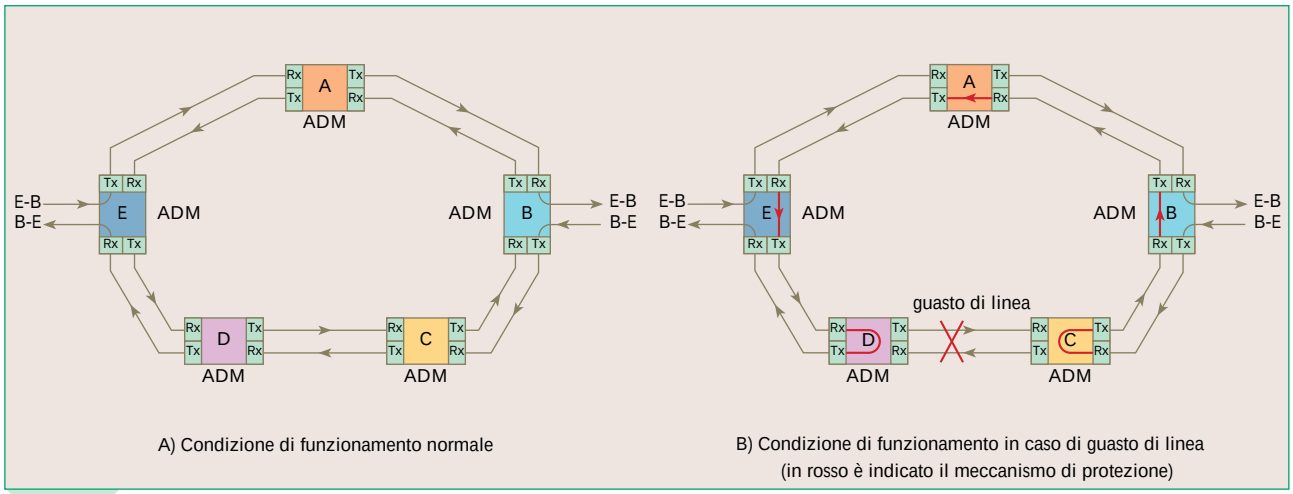


Figura 5 *Protezione MSP-Ring su un anello unidirezionale.*

avaria richiudono il traffico ricevuto sulla fibra di riserva creando dei *loop* tra il ricevitore e il trasmettitore della porta di linea sulla sezione funzionante. In questo modo tutto il traffico che sarebbe dovuto transitare sulla sezione in avaria è reinstradato sulla fibra di riserva e viaggia nel senso opposto di trasmissione. Nel caso di anello bidirezionale per il quale entrambe le fibre sono in esercizio si utilizza la capacità di riserva predisposta sulle fibre con le modalità descritte in precedenza; nel caso di anello unidirezionale si utilizza invece la fibra di riserva. Il meccanismo di intervento della protezione è riportato nelle figure 5 e 6. Nel caso di protezione MSP-Ring, la fibra di riserva sull'anello unidirezionale o la capacità di linea dedicata alla protezione sull'anello bidirezionale, possono essere utilizzate per trasportare traffico a bassa priorità, perduto quando entra in funzione la protezione.

Per entrambi i tipi di protezione degli anelli sono disponibili le modalità di funzionamento: reversibile e non reversibile.

Le protezioni impiegate oggi o pianificate per l'immediato futuro nella rete di Telecom Italia sono la MSP e la SNCP. La protezione di tipo MSP-Ring è già stata normalizzata e permette in alcuni casi un migliore utilizzo della capacità degli anelli e la possibilità di trasmettere del traffico a bassa priorità sulla capacità di riserva. Quando essa sarà disponibile su tutti gli apparati di rete sarà valutato l'impiego di questa protezione, unitamente all'utilizzo degli anelli bidirezionali.

5. Conclusioni

Gli apparati SDH sono sempre più diffusi nella rete di trasporto di Telecom Italia e oggi si sta ormai attuando il progetto di una rete SDH a livello nazionale. L'inserimento degli apparati SDH ha permesso di far crescere notevolmente la rete sia dal punto di vista dell'architettura, in quanto sono state inserite strutture ad anello non disponibili con i sistemi PDH, sia dal punto di vista dell'affidabilità grazie alle nuove

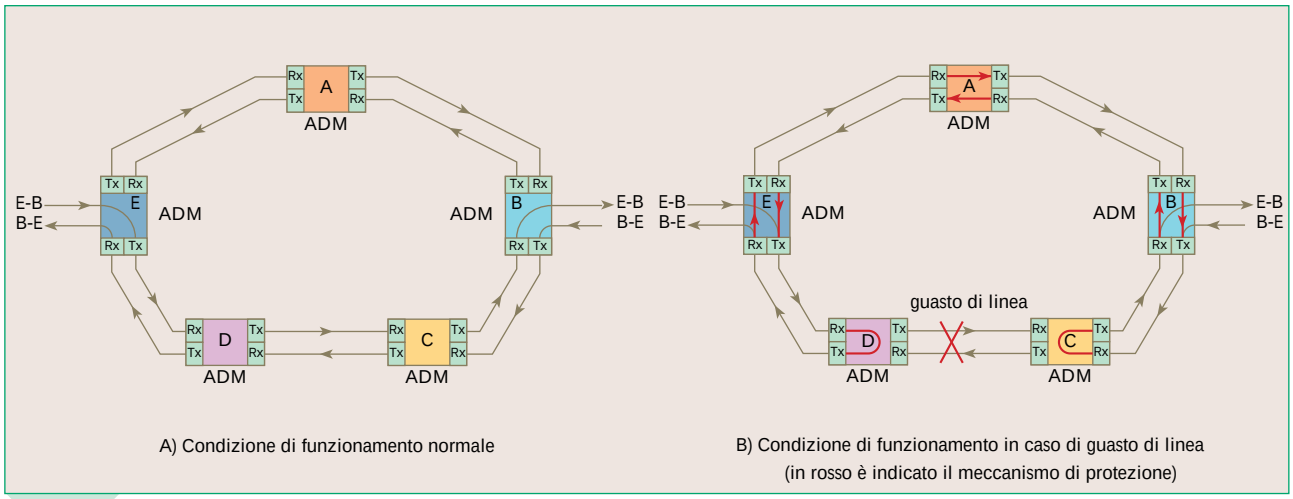


Figura 6 *Protezione MSP-Ring su un anello bidirezionale.*

modalità di protezione.

Altro impatto con una valenza tecnica di assoluto rilievo riguarda le modalità di esercizio e manutenzione, notevolmente mutate grazie alla supervisione centralizzata degli apparati: è così possibile controllare con continuità ed in maniera automatica tutti i collegamenti della rete di Telecom Italia e modificarne le configurazioni da un centro remoto e centralizzato.

Nell'articolo sono state descritte le caratteristiche principali degli apparati SDH. Sono state poi presentate le varie architetture di rete realizzabili con essi e le relative protezioni. Si è cercato così di contribuire a chiarire ai lettori del *Notiziario* concetti e definizioni di cui sentiremo parlare sempre più spesso nei prossimi mesi, durante i quali si assisterà ad una diffusione sempre più estesa della rete SDH. Si è anche voluto chiarire i motivi posti alla base della decisione di passare da una rete trasmissiva PDH ad una SDH e i vantaggi che si otterranno in termini di flessibilità e di qualità della rete.

Abbreviazioni

ADM	Add-Drop Multiplexer
APC	Automatic Power Control
ATC	Automatic Temperature Control
AU	Administrative Unit
DXC	Digital Cross Connect
EM	Element Manager
HPOM	Higher order Path Overhead Monitoring
LPOM	Lower order Path Overhead Monitoring
MPX	Multiplatore d'utente sincrono
MSC	Mobile Switching Centre
MSP	Multiplex Section Protection
MSP-Ring	Multiplex Section Protection - Ring
NM	Network Manager
NT	Nodo Trasmissivo
NTT	Nodo di Transito Trasmissivo
NZD	Non Zero Dispersion
OAM&P	Operations, Administration, Maintenance and Provisioning
PMD	Polarization Mode Dispersion
RED	Ripartitore Elettronico Digitale
SDH	Synchronous Digital Hierarchy
SGT	Stadio di Gruppo di Transito
SGU	Stadio di Gruppo Urbano
SL	Stadio di Linea
SNCP	Sub Network Connection Protection
STM	Synchronous Transport Module
TCM	Tandem Connection Monitoring
TDM	Time Division Multiplexing
VC	Virtual Container

Bibliografia

[1] Broccolini, F.; Ciminari, G.; Picciano, G.: *Gestione degli apparati SDH,* «Notiziario Tecnico Telecom Italia», Anno 7, n. 2, ottobre 1998.

[2] Broccolini, F.; Ciminari, G.; Picciano, G.: *Il sistema di gestione della rete SDH di Telecom Italia,* «Notiziario Tecnico Telecom Italia», Anno 7, n. 2, ottobre 1998.

[3] Mariconda, A.; Misul, R.; Parente, F.; Pietroiusti, R.: *Apparati per la rete SDH,* «Notiziario Tecnico Telecom Italia», Anno 2, n. 1, aprile 1993.

[4] *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*. Raccomandazione ITU-T G.957.

[5] *Physical/electrical characteristics of hierarchical digital interfaces*. Raccomandazione ITU-T G.703.

[6] *Error performance parameters and objectives for international, constant bit rate digital paths at or above the primary rate.* Raccomandazione ITU-T G.826.

[7] *Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks.* Raccomandazione ITU-T G.783.

[8] *Types and characteristics of SDH network protection architectures.* Raccomandazione ITU-T G.841.

Guglielmo Aureli si è laureato in Ingegneria Elettronica presso l'Università degli Studi di Roma "La Sapienza" nel 1989. Nello stesso anno è entrato in SIP, oggi Telecom Italia, presso la Linea Centrale Ricerca e Sviluppo dove si è occupato prevalentemente di nuove tecnologie e sistemi per la rete di accesso e di evoluzione dell'architettura di rete per servizi multimediali a larga banda. Attualmente svolge la propria attività nella Direzione Rete di Telecom Italia, nella Linea Centrale Ingegneria della Rete di Trasporto e Accesso, dove si occupa di tecnologie e industrializzazione degli apparati per la rete di trasporto, in particolare di apparati SDH e DWDM. Dal 1991 partecipa attivamente alle attività di standardizzazione in ETSI (European Telecommunications Standards Institute) dove, dal 1995, riveste la carica di Presidente del WG-TM1 (Core Networks, Fibres and Cables). È autore di diverse pubblicazioni tecniche e ha presentato memorie a Convegni e Forum nazionali e internazionali.

Luigi Cudia ha conseguito la laurea con lode in Ingegneria Elettronica presso l'Università degli Studi di Palermo nel 1994. Successivamente ha frequentato la Scuola Superiore di Specializzazione in Telecomunicazioni dell'ISCTI e nel 1996 è entrato in Telecom Italia nella Linea Centrale Ingegneria di Rete, ora Ingegneria della rete di Trasporto ed Accesso, della Direzione Rete, dove si occupa delle nuove tecnologie ottiche e dell'industrializzazione degli apparati della rete di trasporto. Nell'ambito di questa attività si interessa principalmente di sistemi SDH e DWDM. Svolge attività di docenza presso la scuola Superiore Guglielmo Reiss Romoli e partecipa, per il campo di interesse, alle attività dei principali enti internazionali di normativa e di specifica (ITU-T, ETSI).

Verso i sistemi di comunicazioni mobili di terza generazione

International Conference on Universal Personal Communications (ICUPC)

Firenze, 5-9 ottobre 1998

Valerio Palestini

"Spero, infine, che il 1998 sarà ricordato come l'anno del nuovo standard globale per i sistemi ed i servizi mobili di terza generazione, l'anno che ha reso possibile la crescita del numero di utenti mobili nel mondo dai 200 milioni del 1997 fino ad un miliardo entro il 2010".
Così Umberto de Julio, Presidente della conferenza, ha concluso il suo intervento di apertura dell'edizione 1998 della *ICUPC (International Conference on Universal Personal Communications)*, ospitata presso il "Palazzo dei Congressi e Centro Affari" di Firenze dal 5 al 9 ottobre.

L'ICUPC si è affermata negli ultimi anni come uno dei più importanti e prestigiosi convegni internazionali sui temi più attuali delle telecomunicazioni. La prima edizione della conferenza è stata tenuta nel 1992, anno in cui si tenne a Dallas, per poi essere svolta successivamente, con cadenza annuale, ad Ottawa, San Diego, Tokyo, Boston e, nuovamente, a San Diego lo scorso anno. L'edizione 1998 è quindi "approdata", per la prima volta, in Europa, ottenendo un buon successo dal punto di vista del numero dei partecipanti, che sono stati oltre quattrocento provenienti da tutti i continenti, con rappresentanze di Università, di centri di ricerca, dei principali gestori del servizio di telecomunicazioni e di società manifatturiere. Molto buona anche la qualità delle memorie presentate, visto che, dato il numero di articoli proposti (circa 280) è stato possibile operare una selezione scegliendo i 218 testi giudicati migliori dai revisori.

L'elevato numero di presentazioni ha comportato che questa edizione dell'ICUPC fosse più lunga di un giorno rispetto a quelle precedenti, occupando così un'intera settimana, anche perché la presentazione degli articoli tecnici è stata integrata da seminari e da tavole rotonde sull'evoluzione delle comunicazioni mobili terrestri e satellitari, dai sistemi oggi impiegati a quelli di futura generazione.

Il notevole interesse verso le tematiche proposte dall'ICUPC trova giustificazione nel particolare momento dell'attività internazionale. Si stanno, infatti, ponendo nei principali Organismi le basi per gli standard dei sistemi UMTS/IMT2000, la cui introduzione è prevista per i primi anni Duemila. È proprio dell'inizio di quest'anno la decisione, presa in ETSI, sulla tecnologia di accesso radio per il sistema *UMTS (Universal Mobile Telecommunications System)*, scelta come compromesso tra la tecnica CDMA a larga banda *W-CDMA (Wideband Code Division Multiple Access)*, nella porzione "simmetrica" *(paired)* della banda di frequenza assegnata all'UMTS, e una tecnica mista a divisione di tempo e di codice, chiamata *TD-CDMA, (Time Division-CDMA)* nella banda "asimmetrica" *(unpaired)*. Il sistema così definito è stato proposto in ambito ITU come uno dei possibili candidati *IMT2000 (International Mobile Telecommunications)*, da normalizzare tra le diverse scelte oggi proposte. In realtà, tra i vari sistemi la discussione sembra essere limitata all'UMTS, teso a sfruttare la *core-network* GSM, e al cdma2000, basato sempre sulla tecnica CDMA, ma compatibile con lo standard americano di seconda generazione IS-95. Lo *scontro* e la possibilità di convergenza tra il sistema europeo, sostenuto anche dal

Firenze. Ponte Vecchio.

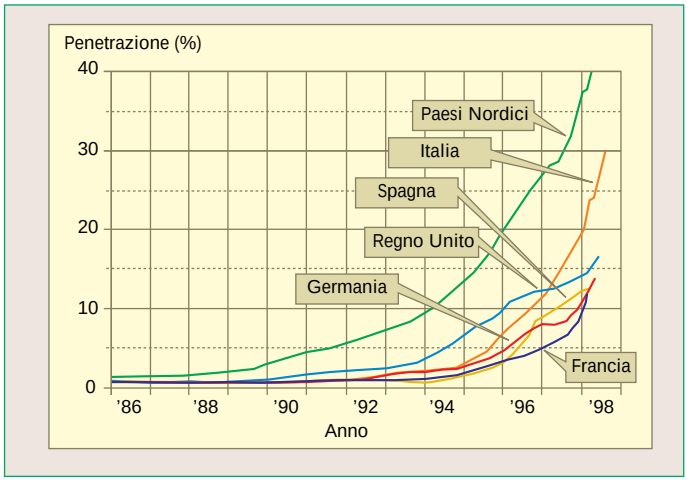
Giappone e dai gestori americani del sistema GSM, e quello americano proposto essenzialmente dalla Qualcomm, proprietaria di importanti brevetti sulla tecnica CDMA, si sono riproposti più volte nel corso della conferenza, specialmente nelle tavole rotonde e nei "tutorials".

La sessione plenaria

I lavori sono stati aperti, in sessione plenaria, da *Umberto de Julio*, Amministratore Delegato di TIM e Presidente della Conferenza, che ha sottolineato come il mondo delle telecomunicazioni stia ora attraversando un momento di rapidi cambiamenti a causa di un certo numero di fattori chiave: fra questi spiccano la deregolamentazione dei servizi, la globalizzazione e la convergenza tra Information e Communication Technology.

Umberto de Julio, Presidente della conferenza, apre i lavori. Alla sua sinistra Renzo Failli (TIM) e Nobuo Nakajima (NTT DoCoMo).

Specie in Europa il 1998 è da considerarsi un anno cruciale, in quanto esso è il primo di piena liberalizzazione del mercato per tutti i servizi di telecomunicazioni. L'oratore ha ricordato che il cambiamento di maggior rilievo è costituito dalla crescita rilevante su base mondiale della telefonia mobile; in questo campo l'Europa svolge un ruolo di leadership, con quasi 76 milioni di utenti a fine agosto 1998, e allo stesso tempo con un livello di penetrazione del 20 per cento, con punte che, nei Paesi Scandinavi, raggiungono anche il 52 per cento (Finlandia).



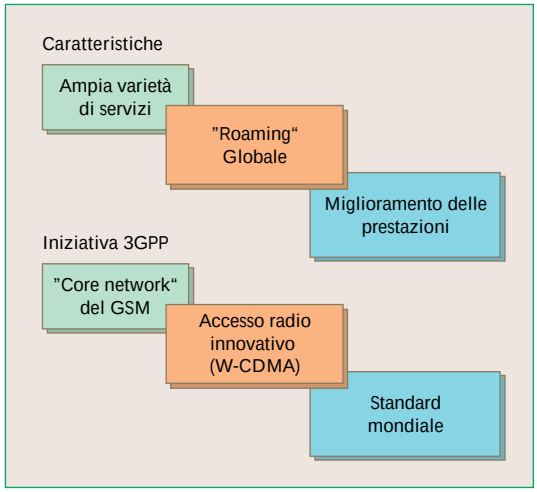
Penetrazione dei sistemi mobili in Europa nell'ultimo decennio.

Le stime per il Duemila prevedono che saranno superati i 150 milioni di utenti, e quindi che si avrà un grado di penetrazione di quattro telefoni mobili ogni dieci europei. L'incremento è assai consistente soprattutto per quanto riguarda i sistemi numerici, il cui numero di utenti è aumentato, nei primi nove mesi del 1998, del 48 per cento soprattutto grazie all'aver unificato il GSM come standard a livello europeo.

Nel discorso di apertura Umberto de Julio è poi passato a considerare la situazione italiana: 17 milioni di utenti, di cui 13 del GSM, con un incremento, per il sistema numerico, del 61 per cento nei primi nove mesi dell'anno. Uno dei fattori cui può essere attribuito questo successo è la competizione, che aiuta a migliorare la varietà dei servizi, la competitività dei prezzi e il livello di qualità offerto all'utenza. È possibile, quindi, che il grado di penetrazione continui ancora a crescere con l'avvio del servizio da parte del terzo operatore. La competizione comporta, infatti, anche un secondo fattore di successo: l'innovazione tecnica, che rende disponibili agli utenti prodotti e servizi nuovi.

Il Presidente della conferenza si è successivamente soffermato sui sistemi di terza generazione, per i quali l'Europa intende svolgere un ruolo da leader per l'ulteriore sviluppo del mercato. Il nuovo sistema è interpretato come una *rivoluzione* nelle comunicazioni mobili, dopo i successi dei sistemi analogici prima e di quelli numerici poi. Esso sarà, infatti, un sistema globale, in grado di integrare il mondo delle telecomunicazioni con quello dell'informatica, dei servizi diffusivi e multimediali (come ad esempio la videocomunicazione) l'Internet a larga banda o altre analoghe applicazioni innovative. La telefonia cellulare evolve, quindi, per diventare anche un mezzo di commercio elettronico, di telepagamento, di *mobile banking*, o, più semplicemente, una specie di *tuttofare numerico*. Per consentire questa evoluzione è necessario pervenire a uno standard comune a livello mondiale. Umberto de Julio, concludendo, ha sottolineato che l'ICUPC costituisce a suo avviso un contesto ideale per l'incontro del mondo

accademico, dei gestori, delle società manifatturiere, dei fornitori di servizi, degli utilizzatori, per discutere differenti esigenze ed esperienze nel mondo dei "sistemi mobili".
Successivamente *Renzo Failli* (TIM), Presidente del programma tecnico della conferenza, ha illustrato il programma della conferenza e il percorso che ha portato a formularlo: ha mostrato, in particolare, la suddivisione tra le diverse aree geografiche di provenienza delle memorie accettate nel Congresso; oltre il 90 per cento è stato proposto dalle tre aree più attive a livello mondiale: gli Stati Uniti (27 per cento), l'Estremo Oriente (26 per cento) e l'Europa (39 per cento, e di questo valore il 15 per cento è relativo all'Italia, Paese ospitante).
Il relatore ha anche illustrato i quattro filoni tematici nei quali sono state suddivise le memorie per garantire che le presentazioni in più sessioni parallele consentissero ai partecipanti di seguire completamente un argomento di interesse: servizi, tecniche di accesso radio, assegnazione delle risorse e pianificazione, aspetti di rete. Renzo Failli ha poi concluso augurandosi che l'attività ora in corso a livello internazionale, con particolare riferimento all'iniziativa del nuovo Gruppo *3GPP (3rd Generation Partnership Project)*, possa portare alla convergenza su un unico sistema globale basato sulla tecnica di accesso W-CDMA e sulla *core-network* GSM. Le tematiche dei sistemi di nuova generazione UMTS/IMT2000 sono state richiamate anche nei due interventi a invito che hanno chiuso la sessione plenaria, presentati rispettivamente da *Nobuo Nakajima* (NTT DoCoMo) e *Biorn Gudmundson* (Ericsson).



Definizione del sistema globale basato sul Wideband Code Division Multiple Access (W-CDMA).

L'intervento ad invito di Biorn Gudmundson (Ericsson) sui sistemi di nuova generazione UMTS/IMT2000.

Organizzazione della conferenza

Dopo la sessione di apertura, tenuta in seduta plenaria, la conferenza è stata svolta, come è stato già detto, in sessioni parallele. Il programma, in particolare, comprendeva duecentodiciotto presentazioni tecniche distribuite su cinquantacinque sessioni, nove "tutorials", (costituiti da seminari di formazione di tre ore e mezzo ciascuno) e sei tavole rotonde, che hanno visto la partecipazione di importanti personalità del mondo delle comunicazioni mobili e personali.
Significativo è stato il ruolo svolto dal Gruppo Telecom Italia nell'organizzazione della conferenza: di particolare importanza la veste attribuita a TIM, rappresentata, come si è già ricordato, dalla presenza di *Umberto de Julio*, Presidente del Congresso e di *Renzo Failli*, Presidente del Comitato Tecnico. Anche lo CSELT ha svolto una funzione di rilievo: *Federico Tosco*, Segretario della conferenza, ha seguito gli aspetti organizzativi e il processo di selezione degli articoli per la messa a punto del programma tecnico. *Giovanni Colombo* è stato scelto come responsabile dell'organizzazione delle tavole rotonde. *Valerio Palestini*, autore di questo rapporto, è stato Tutorials Vice Chair e, insieme con *Vera Kripalani* (Qualcomm, Tutorial Chair), ha selezionato i temi ed i presentatori dei tutorials. *Giuseppe Gerarduzzi*, sostituito in un secondo tempo da *Stefano Pileri* (Telecom Italia), e *Decio Ongaro* (Italtel), hanno fatto parte del Comitato Organizzatore del Congresso. Infine, *Sandro Dionisi* (Telecom Italia) era presente nel Comitato Tecnico della Conferenza.
Altri membri italiani del Comitato organizzatore sono stati: *Stefano Borghi* (Nokia), *Enrico Del Re* (Università di Firenze), *Francesco Fedi* (Fondazione Ugo Bordoni), *Massimo Gentili* (Ericsson) e *Antonio Micciarelli* (Istituto Superiore delle Comunicazioni e delle Tecnologie Informatiche). Hanno partecipato, infine, ai lavori del Comitato Tecnico: *Gabriele Falciasecca* (Fondazione Marconi), *Davide Grillo* (Fondazione Ugo Bordoni), *Franco Grimaldi* (Wind), *Aldo Roveri* (Università di Roma La Sapienza), *Francesco Vatalaro* (Università di Roma Tor Vergata) e *Valerio Zingarelli* (Omnitel).
Come si è anticipato nel punto precedente, le sessioni, pur se svolte in parallelo (quattro contemporaneamente, e in qualche caso cinque),

MEMORIE PRESENTATE DAL GRUPPO TELECOM ITALIA

[1] Donatelli G.*, Eynard C., Liggieri C., Rossi, Strocchi: *Cellular Network Strategic Planning Methods in a Service Profitability Analysis Perspective*. 4D.1. Descrive un sistema di supporto alla Pianificazione Strategica relativo alla redditività dei servizi. L'obiettivo è consentire una valutazione dell'introduzione di nuovi servizi in termini di impatto sulla rete e di conseguenza sulla redditività dell'Azienda in un periodo di pianificazione.

[2] De Pasquale A., Magnani N. P.*, Zanini P.: *Optimizing frequency planning in the GSM system*. 4D.4. Riporta alcuni risultati di simulazione, verificati da misure in campo, che mettono in evidenza come la tratta in salita del sistema GSM possa in taluni casi essere peggiore di quella in discesa. È proposta anche una metodologia per migliorare la pianificazione delle frequenze localmente, tenendo conto degli effetti della tratta in salita.

[3] Napolitano A.*, Panaioli F.: *Evolution of the GSM Platform*. 5D.2. Analizza i principali miglioramenti introdotti di recente nello standard GSM, valutandone l'impatto sull'infrastruttura attuale e considerando i possibili cammini evolutivi verso i nuovi servizi in ottica UMTS.

[4] Tomaselli W.*, Benedetto S.: *Performance analysis of two digital radiomobile systems designed for voice and data transmission on the Rayleigh fading channel*. 8B.3. Mostra le prestazioni, ottenute mediante simulazione software, di due sistemi *wireless* numerici progettati per la trasmissione della voce e dei dati su un canale selettivo nel tempo e caratterizzato da una statistica degli affievolimenti di tipo Rayleigh. Nel lavoro sono anche esposte alcune considerazioni sull'efficienza spettrale, sui ritardi di propagazione e sulla comprensibilità della voce nei due sistemi suddetti, assumendo come scenario di riferimento il sistema *wireless* GSM.

[5] Barberis S., Gaiani E.*, Melis B., Romano G.: *Performance evaluation in a large environment for the AWACS system*. 8C.3. Riporta alcuni risultati ottenuti mediante simulazione nell'ambito del progetto Europeo *ACTS/AWACS (Advance Communications Technologies and Services/ATM Wireless Communication System);* questo studio ha l'obiettivo di valutare le prestazioni del sistema AWACS in un ambiente interno di grandi dimensioni, quale, ad esempio, il corpo di una fabbrica.

[6] Chiasserini C.F., Lo Cigno R., Scarrone E., *Handovers in wireless ATM: an in-band signaling solution*. 8E.4.

[7] Demestichas P.P., Demasticha V.P., Theologou M.E., Badini F., Menolascino R.*: *Design of an ATM based access segment for third generation mobile systems*. 9C.3. È il frutto della collaborazione di due progetti ACTS entrambi coordinati dallo CSELT, cioè *Rainbow* e *Storms*. Riguarda in particolare gli aspetti dell'integrazione del sistema UMTS con la rete ISDN a larga banda (B-ISDN), e descrive il processo seguito nel progetto.

[8] Mirra D., Pascali F*., Demestichas P.P., Demasticha V.P., Theologou M.E.,: *Network performance assessment platform for third generation mobile systems*. 12D.4. Tratta di un simulatore, sviluppato per il sistema UMTS, che fornisce la possibilità di definire un modello per le varie entità di rete e per i loro ambienti; nel lavoro sono inoltre presentati una serie di risultati preliminari ottenuti attraverso il simulatore.

[9] Annunziato A.*, Sorbara D.: *Software radio link performance evaluation for the standard DECT*. 13D.3. Descrive il pacchetto software DECTSIM e, in particolare, si sofferma sulla metodologia di simulazione in termini di modelli di propagazione e di schema di ricezione adottati; presenta, infine, i risultati di simulazione ottenuti mediante il programma descritto.

** Autore che ha presentato la memoria al congresso.*

sono state organizzate seguendo filoni logici, in modo che le diverse tematiche potessero essere seguite senza sovrapposizioni.
Le tavole rotonde hanno in generale riscosso un notevole successo per quanto riguarda sia il numero di congressisti presenti, sia per la discussione che è seguita alle presentazioni introduttive dei partecipanti invitati.
Questo successo è sicuramente anche attribuibile ai coordinatori delle diverse tavole rotonde, scelti tra i migliori esperti sulle tematiche trattate nella Conferenza. In particolare *Joao da Silva* (Commissione Europea DGXIII) ha presieduto la discussione su "Ricerca e sviluppo nelle comunicazioni mobili e senza filo in Europa"; *Takeshi Hattori* (Università di Sohipa, Giappone) quella su "Trasmissione dati senza filo e tecnologia dell'informazione"; *Thomas Beijer* (Presidente dell'UMTS Forum) quella su "Accesso radio per la terza generazione, stato dell'arte per IMT2000 e UMTS"; *Aldo Roveri* (Professore presso l'Università di Roma La Sapienza e Presidente del Consiglio Superiore Tecnico delle Telecomunicazioni) ha coordinato il dibattito sul tema "Requisiti dello spettro ed aspetti di regolamentazione"; *Fred Hillebrand* (Presidente dell'ETSI SMG) quello su "Dai sistemi mobili di seconda generazione a quelli di terza generazione" e infine *Bruno Rossi* (Ericsson Italia) ha guidato il dibattito su "Sviluppi a breve termine dei servizi GSM".
Anche gli oratori invitati per i tutorials sono stati particolarmente qualificati: tra questi *Klein Gilhausen* (Qualcomm), considerato uno

dei principali artefici dello sviluppo della tecnica CDMA per i sistemi radiomobili, ha presentato i principi fondamentali del CDMA; questo argomento è stato sviluppato anche in un secondo tutorial, focalizzato sugli aspetti della progettazione della rete, presentato da *Usman Goni* e *Nandu Gopolakrishna* (LCC International). Due tutorials sono stati dedicati ai sistemi senza filo di terza generazione: il primo, riguardante gli aspetti radio, è stato presentato da *Aleksandar Gogic* (Airtouch Communications); l'altro, sugli aspetti di rete, da *Giovanni Colombo* (CSELT). Sono stati presi in esame anche i sistemi attuali: un tutorial a cura di *Kenny Niutanen* (Nokia) ha presentato le possibilità evolutive ed i miglioramenti previsti per i sistemi GSM900 e, soprattutto, per quelli GSM1800. *Mitchell Trott* (Arraycomm) ha presentato un nuovo aspetto tecnologico molto promettente per il miglioramento di qualità e capacità dei sistemi wireless, cioè le cosiddette "antenne intelligenti". Ma i tutorials non hanno avuto come relatori solo "tecnici", provenienti dal mondo dei gestori e delle società manifatturiere: tre presentazioni sono state, infatti, curate da noti esponenti del mondo accademico. *Sergio Benedetto* (Politecnico di Torino) ha trattato le tematiche legate ai "turbo codici", una tecnica di trattamento del segnale costituita da codici concatenati che promette un notevole miglioramento delle prestazioni rispetto a quelle ottenibili con i codici tradizionali. *Anthony Acampora* (University of California) ha esposto un altro argomento molto attuale: il *Wireless Local Loop* per accesso a larga banda. Infine *Vijay Bhargava* (Università di Victoria, Stati Uniti) e *Stephen Wicker* (Cornell University) hanno presentato assieme i sistemi multimediali sviluppati per la trasmissione senza filo.

Il segretario della conferenza, Federico Tosco dello CSELT, presiede la sessione sugli aspetti tecnologici dei sistemi mobili.

Il contributo italiano

Da parte italiana il contributo, come già anticipato, è stato significativo in tutte le attività della conferenza.
Per quanto riguarda le tavole rotonde, oltre al coordinamento generale svolto, come si è detto, da *Gianni Colombo* (CSELT) e alla Presidenza di *Aldo Roveri* in quello riguardante gli aspetti regolatori dello spettro radio, sembra opportuno segnalare la partecipazione di *Renzo Failli* (TIM) alla tavola rotonda intitolata "Dai sistemi mobili di seconda generazione a quelli di terza generazione". In questo caso si è assistito ad un dibattito molto animato, che ha visto ancora una volta da una parte i sostenitori del sistema proposto dalla Qualcomm e dall'altra quelli favorevoli alla proposta europea dell'UMTS.
Nella tavola rotonda sugli sviluppi a breve termine dei servizi GSM, che ha avuto come moderatore *Bruno Rossi* (Ericsson Italia), sono intervenuti *Emanuele Montegrosso* (TIM), *Valerio Zingarelli* (Omnitel), *Alessandra Bianchini* (Wind) e *Claudia Lorenzini* (Nokia). Per i tutorial, come ricordato nel punto precedente, due delle nove presentazioni sono state tenute da relatori italiani, e di queste una a cura dello CSELT.
Numerose sessioni (comprendendo tra queste anche alcune per le quali non hanno potuto partecipare i coordinatori designati per impegni sopraggiunti immediatamente prima della Conferenza) sono state presiedute da rappresentanti del nostro Paese, molti dei quali appartenenti al gruppo Telecom Italia. In particolare, *Pietro Porzio Giusto* (TIM) ha presieduto la sessione dedicata alla "valutazione delle prestazioni dei sistemi radiomobili"; *Sandro Dionisi* (Telecom Italia), la sessione dedicata ai "metodi di modellizzazione della catena di trasmissione"; *Federico Tosco* (CSELT) ha presieduto due sessioni, "sulle tecniche dei ricevitori" e sugli "aspetti tecnologici dei sistemi mobili", *Valerio Palestini* (CSELT) ha moderato la sessione sulle "tecniche di modulazione per le applicazioni senza filo"; *Carlo Eynard* (CSELT) quella sulle "tecniche avanzate di ricezione ed un'altra sui miglioramenti nel campo dei protocolli"; *Antonella Napolitano* (CSELT) ha condotto una sessione dedicata alle "tecniche di modulazione e codifica" e una relativa alle "prestazioni dei sistemi mobili".
Oltre trenta memorie hanno avuto autori o coautori italiani: di queste nove comprendevano autori dello CSELT [1÷9]. Più in particolare, due sono lavori svolti in collaborazione con TIM [1;3], due col Politecnico di Torino [4;6] e due con l'Università di Atene [7;8]. Tutte le memorie, fatta eccezione per la [6], sono state presentate al Congresso dagli autori dello CSELT. Un breve riassunto del contenuto di queste memorie è riportato nel riquadro annesso a questa nota.

Elementi emersi nel Congresso

Nel momento in cui il successo dei sistemi di comunicazione mobili numerici costituisce un vero e proprio "boom" a livello mondiale, presso i principali gruppi di normalizzazione sono già in corso di valutazione le proposte relative a sistemi di nuova generazione. L'introduzione in rete di questi ultimi sistemi comporterà una sensibile evoluzione nelle comunicazioni mobili, perché se finora le trasmissioni senza filo sono state principalmente dedicate ai servizi in fonia, la convergenza tra il mondo delle telecomunicazioni e quello informatico porterà alla richiesta di poter gestire servizi completamente innovativi, soprattutto di dati (dovrà ad esempio essere assicurato l'accesso a Internet).

I gestori, le società manifatturiere ed i fornitori di servizi del settore stanno quindi vivendo un momento cruciale per il consolidamento delle proprie strategie di innovazione per il futuro a breve ed a medio termine.

In questo contesto, una conferenza come l'ICUPC '98 ha costituito un momento utile per effettuare un confronto tra i principali attori, protagonisti del cambiamento. I partecipanti non solo hanno potuto seguire presentazioni specifiche di un buon livello, ma hanno anche avuto l'opportunità di essere parte attiva nelle numerose tavole rotonde sui temi più attuali delle comunicazioni mobili. Inoltre, per coloro che desideravano avere approfondimenti su tematiche di ampio respiro, sono stati predisposti numerosi tutorials.

Il Congresso è sembrato in accordo con l'orientamento oggi presente nel contesto internazionale: in particolare, è emerso chiaramente l'interesse verso i sistemi di comunicazioni mobili di terza generazione, con riferimenti specifici alla tecnica di accesso a divisione di codice CDMA, oggi universalmente accettata come accesso radio per i sistemi mobili che faranno parte della famiglia IMT2000. La Conferenza ha messo in luce un atteggiamento abbastanza diffuso nel mondo scientifico, vale a dire una maggiore attenzione alla definizione dell'accesso con tecnica di duplexing a divisione di frequenza *FDD (Frequency Division Duplexing)*, che prevede due bande di frequenza diverse per i due versi di trasmissione ed è quindi più adatto per la porzione di banda simmetrica *(paired)* assegnata ai sistemi di terza generazione, piuttosto che allo sviluppo della modalità *TDD (Time Division Duplexing)*, cioè a divisione di tempo, adatta per la porzione di banda asimmetrica *(unpaired)* poiché la stessa banda di frequenza è condivisa tra le due tratte. Ciò è probabilmente dovuto alla disputa molto accesa a livello internazionale, che si è riproposta più volte, anche durante la conferenza, sulla scelta tra i sistemi UMTS e cdma2000, compatibili, rispettivamente, con il nucleo centrale della rete GSM e lo standard americano di seconda generazione IS-95, entrambi definiti secondo la modalità FDD. Dall'ICUPC è stata posta in luce soprattutto l'importanza che avrebbe la definizione di un sistema unico, con benefici per le società del settore e per gli utenti; non è emersa tuttavia un'indicazione chiara, dal punto vista tecnico, sulla prevalenza di uno dei due sistemi in termini, ad esempio, di qualità o di capacità. Il dibattito è senz'altro di portata più ampia e coinvolge anche altri aspetti, come quelli legali per i brevetti sulla tecnica CDMA; è quindi presumibile che le discussioni proseguiranno negli Enti di normalizzazione incaricati di produrre le specifiche tecniche.

Firenze. Scala della torre di Palazzo Vecchio e veduta della Cattedrale. (Foto Alinari).

Sarà dunque sicuramente di pari interesse anche la prossima edizione della conferenza, che modificherà la denominazione ICUPC. L'IEEE Communication Society ha infatti deciso di espandere i contenuti in base ad un accordo con la *PCIA (Personal Communications Industry Association)*.

La prossima conferenza sarà perciò chiamata *WCNC (Wireless Communications and Networking Conference)* e sarà tenuta a New Orleans dal 21 al 25 settembre 1999.

Valerio Palestini - CSELT

"Every Call an IN Call"

Intelligent Networks '98

Madrid, 16-19 novembre 1998

Roberto Badiani, Massimo Barletta

EVERY CALL AN IN CALL

QUESTA LA PROVOCAZIONE LANCIATA DA GRAHAM COBB, DI ASCEND COMMUNICATIONS, GIÀ STRATUS COMPUTER, DURANTE LA CONFERENZA CHE HA AVUTO LUOGO A MADRID DAL 16 AL 19 NOVEMBRE, PRESSO L'HOTEL MELIA' AVENIDA AMERICA.

La conferenza, secondo incontro annuale organizzato da IIR e sponsorizzato da Telsis, da Bellcore International e da Lucent Technologies, ha presentato la situazione attuale e le tendenze sui nuovi prodotti e sui nuovi servizi di rete intelligente. L'incontro ha visto la partecipazione di circa duecento delegati di industrie manifatturiere (50 per cento), di società di consulenza (25 per cento) e di gestori di telecomunicazioni a livello internazionale (25 per cento). Per l'Italia erano presenti rappresentanti del Gruppo Telecom Italia (Telecom Italia, CSELT e TIM) e di alcune industrie manifatturiere (Ericsson, HP, IPM e Lucent Technologies).

Nel corso della conferenza, nella quale è stata data più enfasi ai servizi di rete intelligente che all'architettura di rete, sono state presentate circa quaranta memorie.

Madrid: Plaza Mayor.

Riflessioni generali

Nei primi due giorni sono stati esaminati gli aspetti relativi alle opportunità e alle possibilità di sviluppo rese disponibili dall'impiego dell'intelligenza in rete, nell'ambito dell'offerta di servizi a valore aggiunto. È opinione comune che questi servizi rappresentino il vantaggio competitivo di un gestore di telecomunicazioni che opera in regime di concorrenza. Un gestore che offra un pacchetto di servizi più ricco e più orientato al cliente riuscirà più efficacemente a mantenere e ad espandere la propria quota di mercato. Questo obiettivo non potrà, comunque, essere raggiunto se non attraverso una forte riduzione del tempo di introduzione di nuovi servizi *(Time to Market)*. La riduzione non deve portare naturalmente a conseguenze sulla qualità dei servizi, in termini di prestazioni, affidabilità e sicurezza.

Ai temi trattati nei primi due giorni ha fatto seguito un ulteriore giorno di conferenza nel corso del quale è stata approfondita la fatturazione dei servizi di rete intelligente dal titolo *"Billing IN Services"*. Lo sviluppo dei sistemi di Billing e Customer Care, necessari per la commercializzazione di nuovi servizi, rappresenta oggi il maggiore ostacolo alla riduzione del *Time to Market*. Nel corso del seminario sono stati presentati i principali problemi che deve affrontare un gestore di telecomunicazioni, le soluzioni offerte da alcune industrie manifatturiere e le tendenze ipotizzate da alcune società di consulenza.

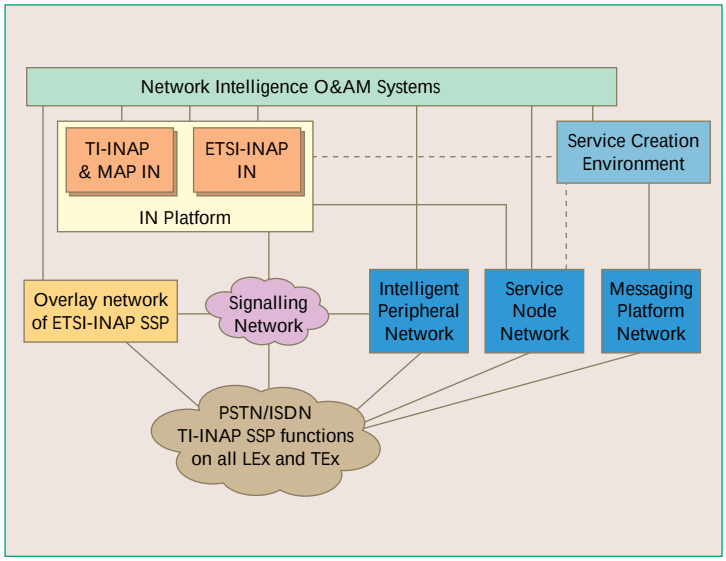
Perché investire in rete intelligente?

Sonera (in precedenza Telecom Finland), ha risposto a questo quesito sottolineando che la rete intelligente è il mezzo più efficace per realizzare nuovi servizi, disponibili in tempi brevi, di migliore qualità e disegnati sulle esigenze del cliente in un mercato fortemente competitivo come quello finlandese. La Finlandia è infatti uno dei Paesi europei, come dichiarato nel corso della presentazione da *Kimmo Matero* (Solution Development Manager della Sonera) nel quale il processo di liberalizzazione è già quasi concluso. Più di cinquanta gestori di telecomunicazioni (dei quali quarantasei locali, tre per la lunga distanza, tre per i collegamenti internazionali e tre per le reti radiomobili), dopo

essersi affrontati nel campo delle tariffe dei servizi di base, si confrontano oggi nel numero e nel tipo di servizi a valore aggiunto offerti ai clienti.
Maggiore enfasi all'importanza della rete intelligente è stata data dalla presentazione di *Graham Cobb* (Ascend Communications) che ipotizza uno scenario in cui tutte le chiamate richiedono l'intervento di rete intelligente. Motivazione trainante è la richiesta, da parte dei clienti, di disporre di nuovi servizi e di prestazioni sempre più svincolati dalla postazione fisica di rete. Per poter soddisfare quest'esigenza è necessaria una gestione centralizzata delle informazioni tipica di rete intelligente.
Marconi Communications (Società del gruppo GEC) ha anch'essa sottolineato il valore strategico dello sviluppo di servizi a valore aggiunto in un ambiente competitivo. *Geoff Dorrington*, IN Product Manager di questa Società, ha dichiarato che *now is the time for the communication revolution, where intelligent network technology will free people from the traditional work model brought about by the industrial revolution*. Questa tesi si basa sull'analisi dell'esperienza della Gran Bretagna, primo Paese europeo ad attuare la liberalizzazione del mercato delle telecomunicazioni: dal 1983 si è inizialmente sostituito, al monopolio di British Telecom, un duopolio costituito da BT e da Mercury. I due gestori, fornendo gli stessi servizi, si confrontavano sullo stesso mercato potenziale attraverso tariffe sempre più basse riducendo così i propri profitti. Oggi, con più di trecento operatori di telecomunicazioni suddivisi in gestori di lunga distanza, regionali, locali, radiomobili e rivenditori di traffico *(resellers)*, la posizione dominante di BT può essere di fatto erosa solo ampliando il mercato potenziale con una strategia basata su servizi differenziati per clientela di nicchia. Dai servizi pensati per le aziende di grandi dimensioni e per la clientela residenziale si passa a servizi personalizzati per la piccola e media impresa *(Small Medium Enterprise)*. La rete intelligente consente di realizzare questo obiettivo strategico in quanto:

- essa consente in parte di svincolare la fornitura di una prestazione o di un servizio dall'effettiva situazione di rete e non implica necessariamente interventi software sugli elementi di rete;
- le piattaforme di rete intelligente di nuova generazione sono dotate di caratteristiche avanzate di programmabilità *SCE (Service Creation Environment* ambiente di creazione dei servizi) che comportano una drastica riduzione del *Time to Market* e dei costi di sviluppo;
- le interfacce grafiche e gli strumenti di simulazione di cui è dotato un SCE forniscono uno strumento utile per la realizzazione di prototipi in modo da avere un rapido ritorno sull'interesse del potenziale cliente ad un certo servizio o per una prestazione.

Telecom Italia: intelligenza in rete.



Altro fattore chiave che ha storicamente portato all'adozione di una soluzione di rete intelligente è la necessità di fornire un servizio che sia trasparente rispetto ad infrastrutture ed a sistemi di rete *multivendor*. Questo è il caso di Microcell Connexions, gestore radiomobile canadese che fornisce sia servizi PCS sia GSM.
La presenza di un ambiente di creazione di servizi, ha aggiunto *Marilyn Poirier* (Direttore del Dipartimento di Network Systems and Services), pur con i limiti che le attuali piattaforme SCE presentano, costituisce un vantaggio ulteriore per la rapida realizzazione di servizi personalizzati.
L'esigenza di creare nuovi servizi non è espressa solo dal mercato ma, come gli esempi più recenti hanno mostrato, anche da nuove norme emanate dagli Enti Regolatori che, a fronte della liberalizzazione del mercato, impongono ai gestori la fornitura di servizi quali *Number Portability, Carrier Selection* e *Carrier Preselection*. Anche questi servizi

possono essere realizzati con la rete intelligente, come sottolineato nelle presentazioni di KPN Telecom (gestore incumbent olandese) e di Sonera.
Il processo di ingegnerizzazione di nuovi servizi incontra un grosso ostacolo nella lentezza di adeguamento dei sistemi di *Billing* e *Customer Care:* è questo il punto di vista di *James Aitken* (Logica) che propone, come possibile soluzione, l'utilizzo, da parte dell'operatore di telecomunicazioni, di strumenti di programmazione anche sui sistemi di gestione *(Total SCE).*
Teligent (fornitore svedese di applicativi per rete intelligente) ha presentato un prodotto *Total SCE* in grado di colloquiare con piattaforme di rete intelligente di diversa tecnica.

Quanto è importante da un punto di vista strategico la convergenza Fisso-Mobile?

Ascend Communications, nel corso della presentazione già citata, ha identificato una serie di motivi per cui la convergenza dovrebbe essere realizzata anzitutto su servizi a valore aggiunto:

- le aspettative del cliente sono di disporre degli stessi servizi e delle stesse prestazioni tanto sulla rete fissa quanto su quella mobile;
- in un'ottica di ottimizzazione delle risorse e di riduzione dei costi, è interesse dei gestori di rete fissa e mobile condividere, ove possibile, le stesse tecnologie e gli stessi elementi di rete;
- il gestore della rete fissa può adottare i criteri generali impiegati dalle reti mobili nelle quali la numerazione è separata dall'instradamento.

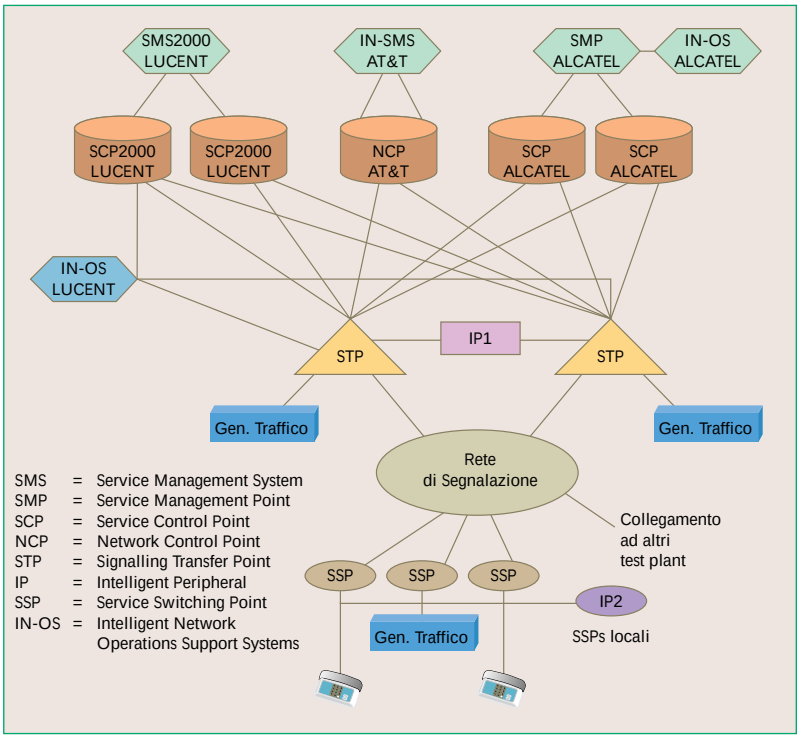
Su questo tema alcuni gestori hanno presentato proprie esperienze. Sonera, gestore dotato di ben tre piattaforme di rete intelligente sulla rete fissa e di altrettante sulla rete radiomobile, già nel 1993 ha commercializzato il suo primo servizio di rete intelligente "convergente": la carta di chiamata virtuale *(Virtual Calling Card).* Nel 1995 ha poi realizzato la prima rete privata virtuale integrata fisso-mobile (*Fixed and Mobile VPN);* a questa ha fatto seguito nel 1997 la Carta Prepagata Unica *(Prepaid Calling Card).* Il gestore finlandese ha quindi realizzato una convergenza virtuale pur mantenendo diverse piattaforme di rete intelligente.
La soluzione di TeleDanmark, gestore incumbent danese di rete fissa e mobile, rappresenta un'ulteriore evoluzione presentando un'offerta commerciale per clienti residenziali chiamata *Duet.* Le caratteristiche di questo contratto prevedono un solo numero telefonico, sia per i terminali di rete fissa che per quelli di rete mobile (GSM), una segreteria telefonica unica e una sola bolletta. Il prodotto, lanciato a settembre 1997, prevede l'utilizzo della rete intelligente per la gestione dell'instradamento e per le modifiche del profilo effettuate direttamente dal cliente *(Customer Control)* tramite un accesso via Internet o mediante una procedura telefonica.
France Telecom, che non ha ancora realizzato la convergenza fisso-mobile, ha identificato la rete privata virtuale come il servizio in cui la necessità di integrazione è più sentita.
Bell Canada ed Ericsson, nel corso di una presentazione congiunta sui servizi di messaggistica unificata *(Unified and Universal Messaging)* hanno invece messo in evidenza come l'esigenza del cliente sia quella di poter accedere a facsimili, posta elettronica, *short messages* o messaggi vocali, attraverso i diversi mezzi disponibili che utilizzano la rete fissa e radiomobile.

L'importanza del collaudo

Tra i presenti ha suscitato un grande interesse l'intervento di *Marco Bavazzano,* responsabile in *CSELT* del collaudo di servizi e sistemi di rete intelligente, che ha sottolineato l'importanza di un ambiente di collaudo in grado di contribuire a ridurre il *Time to Market.* Un collaudo mirato, che agisca in un ambiente di prova il più vicino possibile a quello di rete, è infatti la soluzione che permette di ridurre il tempo necessario per introdurre i nuovi servizi mantenendo sempre alta la qualità dei rilasci.
La memoria dello CSELT ha mostrato, in particolare, la soluzione adottata da Telecom Italia nel Test Plant di rete intelligente. Oltre ai prototipi dei sistemi di questa rete, nel Test Plant sono disponibili anche strumenti quali generatori automatici di traffico telefonico. Questi strumenti risultano di particolare importanza in fase di verifica delle prestazioni dei sistemi di rete intelligente.
Il Test Plant di questa rete è collegato con quelli delle tre tecniche di autocommutatori impiegate da Telecom Italia (Alcatel, Italtel e Ericsson) e ciò consente di ottenere, alla fine delle Prove di Verifica e Validazione (PVV), un prodotto, sistema o servizio, in grado già di

colloquiare con le diverse tecniche di centrale presenti sul territorio nazionale. Mediante le Prove di Qualificazione in Rete (PQR) si verifica successivamente la bontà del prodotto nella situazione reale di rete. Dopo aver concluso con esito positivo questo ciclo di prove, e anche le Prove di Carico Limite (PCL), il gruppo di collaudo può certificare la rispondenza del generico sistema o servizio alle specifiche.

L'acquisizione di una seconda piattaforma di rete intelligente, realizzata da Alcatel - che si affianca a quella già in servizio fornita da Lucent Technologies - ha svincolato di fatto Telecom Italia dal singolo costruttore. È stato quindi necessario verificare l'interlavoro *(interworking)* tra piattaforme di diversi costruttori. Il collaudo assume così maggiore importanza in quanto con esso si avvia il processo di interlavoro tra piattaforme *multivendor*, già realizzato in campo internazionale.



Telecom Italia: test plant di rete intelligente.

"If you can't bill it, kill it!"

Con queste parole *Peter Litzen* (Ericsson) ha precisato che non si può ipotizzare di commercializzare un nuovo servizio se non sono disponibili i sistemi gestionali che curano, in particolare, la configurazione del profilo del cliente, l'elaborazione dei dati di traffico *CDR (Call Data Records)* e l'emissione della fattura al cliente.

Nel corso del seminario *Billing IN Services* sono intervenuti alcuni rappresentanti di industrie manifatturiere e di società di consulenza, mentre Telecom Italia è stato il solo gestore a presentare la propria esperienza.

La memoria di Telecom Italia, a cura degli autori del presente articolo, ha fatto da ponte tra quanto esposto nei giorni precedenti e le riflessioni di consulenti e fornitori sul futuro non solo dei sistemi di fatturazione ma anche del concetto stesso di *IN Billing.*

Gli autori, dopo una breve presentazione della complessa struttura dell'Intelligenza nella rete di Telecom Italia e dell'altrettanto complesso insieme di sistemi di gestione presenti, suddivisi per servizi e per segmenti di mercato, hanno messo in evidenza la flessibilità del meccanismo di generazione dei CDR di rete intelligente. Il ruolo determinante di questa rete consiste nel decidere, anzitutto, se creare un CDR e successivamente nel definirne formato e contenuto informativo. La caratteristica di flessibilità propria di rete intelligente consiste nel personalizzare questi criteri di scelta, in funzione della configurazione dei dati del servizio e, in particolare, del sottoscrittore.

Gli autori hanno poi sottolineato i punti da migliorare nella presente realizzazione:

- è necessario ridurre i tempi di sviluppo dei sistemi di fatturazione *(Billing)* e di *Customer Care;* questo contenimento dei tempi potrebbe essere ottenuto mediante strumenti simili ad un *SCE (SCE-like)* sui sistemi di gestione *(Total SCE);*
- i nuovi servizi a valore aggiunto portano a un concetto di fatturazione innovativo, basato non più sull'utilizzo fisico della risorsa di rete ma sull'effettivo contenuto informativo: l'invio di un fax potrebbe essere fatturato in base al numero di pagine; l'accesso ad un servizio di informazioni, quale il "Grazie Mille", sulla base del tipo di informazione richiesto *(Billing by Content);*

- i tempi di disponibilità dei CDR dovrebbero essere ridotti mediante nuove scelte architetturali quali la generazione degli addebiti (dei "cartellini") direttamente su rete intelligente (scelta che sarà perseguita sulla piattaforma Alcatel per Telefonia Pubblica), in modo da poter fornire servizi di informazione in tempo reale sulla fatturazione *(Hot Billing)*.

Una maggiore integrazione tra i sistemi di fatturazione e quelli di rete, nuove scelte architetturali quali la generazione dei CDR su rete intelligente, tariffazione sul contenuto informativo e tariffazione su base evento sono state le soluzioni indicate dai costruttori e dagli analisti per poter raggiungere gli obiettivi di ridurre il *Time to Market* e per migliorare la flessibilità offerta dai sistemi.
Particolare interesse ha suscitato il prodotto di *TTI Telecom*, Società israeliana di sistemi di gestione per le telecomunicazioni, che propone una fatturazione basata sull'analisi dei messaggi di protocollo scambiati sul canale di segnalazione.

Conclusioni

La conferenza ha messo in evidenza come, in un ambiente di libero mercato, la competizione tra gestori di telecomunicazione avverrà sempre più sui servizi e meno sulle tariffe: un portafoglio di servizi più ampio e più orientato alle esigenze dei singoli clienti potrà permettere di contraddistinguere un gestore di successo.
In questa ottica assume una grande importanza il ruolo della rete intelligente, in quanto essa consente di realizzare servizi indipendenti dalla situazione di rete con notevole riduzione dei tempi di sviluppo. Il futuro di questa rete vedrà un coinvolgimento sempre maggiore del gestore su tutti gli elementi che intervengono nella realizzazione di un servizio *(Total SCE)*.
Questi temi formeranno l'oggetto del prossimo convegno previsto a Londra nel maggio del 1999.

Roberto Badiani, Massimo Barletta - Telecom Italia

Molto del nostro futuro dipende dalla ricerca

RICERCA E SVILUPPO NELLE TELECOMUNICAZIONI

Convegno Nazionale AEI
Napoli 13-14 novembre 1998

Daniela Fioramonti

"NELL'ATTUALE SCENARIO LA RICERCA È L'ARMA CHE PUÒ FARE LA DIFFERENZA NELLA BATTAGLIA COMPETITIVA" HA AFFERMATO *UMBERTO DE JULIO*, AMMINISTRATORE DELEGATO DELLA TIM E PRESIDENTE GENERALE DELL'AEI, APRENDO IL CONVEGNO "RICERCA E SVILUPPO NELLE TELECOMUNICAZIONI" TENUTO A NAPOLI NEI GIORNI 13 E 14 NOVEMBRE 1998; DE JULIO HA SUCCESSIVAMENTE RICORDATO CHE L'ITALIA PRESTA ALL'INNOVAZIONE MINOR ATTENZIONE RISPETTO AD ALTRI PAESI EUROPEI CHE INVESTONO SENSIBILMENTE IN RICERCA.

L'incontro, promosso dall'*AEI (Associazione Elettrotecnica ed Elettronica Italiana)* con l'adesione dell'*AIIT (Associazione Italiana Ingegneri delle Telecomunicazioni)*, ha avuto luogo a distanza di sei anni da un convegno, svoltosi a Palermo sullo stesso tema: in quell'occasione fu avviata una prima analisi sul significato e importanza di ricerca e sviluppo nel mondo delle telecomunicazioni. L'AEI ha ritenuto opportuno riproporre nuovamente questo tema per esaminare come si muove oggi a livello internazionale l'intero settore legato all'innovazione e per fornire utili suggerimenti al nostro Paese.
Le due giornate in cui si è articolata la manifestazione hanno così contribuito a presentare un quadro d'insieme della ricerca e sviluppo - dal punto di vista finanziario e delle risorse umane impegnate - ponendo particolare attenzione alla situazione presente in Europa, Stati Uniti, Giappone e Italia. Nel corso della seduta inaugurale sono intervenuti: *Alessandra Bocchino* (Assessore all'Innovazione ed Impresa della città di Napoli), *Alessandro Luciano*

(Commissario dell'Autorità per le garanzie nelle comunicazioni) e *Ovidio Mario Bucci* (Pro-Rettore dell'Università Federico II di Napoli). L'Assessore Bocchino ha in particolare ricordato che in una realtà, quale quella di una città metropolitana, si debbano ricercare, alla luce delle opportunità offerte dall'innovazione, i possibili miglioramenti da incoraggiare in ambito locale; si è poi soffermata sull'importanza che può giocare l'offerta del telelavoro. Alessandro Luciano ha sottolineato che l'attività di ricerca rappresenta il motore principale per lo sviluppo delle telecomunicazioni e che l'Authority è oggi molto sensibile al problema della crescita dell'innovazione: essa ha infatti inserito, tra gli obiettivi ritenuti prioritari, gli investimenti in ricerca avanzata da parte delle aziende di telecomunicazioni.

Napoli da Marina di Vico.
Scuola di Posillipo (1850 circa).

Ovidio M. Bucci ha manifestato il proprio apprezzamento per aver scelto Napoli quale sede del Convegno e per aver richiamato l'attenzione sulla ricerca svolta nelle Università; ha inoltre ricordato che uno studio di rilievo richiede in genere per il suo completamento circa sei anni e che quindi i rallentamenti sulla ricerca accumulati nel recente passato comporteranno ritardi o assenze sui prodotti innovativi che l'industria italiana sarà in grado di fornire ai mercati mondiali.

La *Ricerca nel contesto internazionale* è stato il tema discusso nella prima sessione, coordinata da *Alessandro Bellman* (Senior Vice President Strategic Planning and Innovation di Italtel); a questa sessione sono intervenuti, come rappresentanti di diverse situazioni internazionali: *Dave Waring* (Bellcore), *Shigehiko Suzuki* della NTT (Nippon Telegraph and Telephone Corporation) e *Kevin Fogarty* dell'Eurescom (European Institute for Research and Strategic Studies in Telecommunications GmbH). I tre relatori hanno fornito, agli oltre duecento convenuti e alla stampa accreditata, un'ampia panoramica sulla ricerca e sviluppo svolta oggi nel settore legato alle telecomunicazioni e all'Information & Communication Technology in America, in Estremo Oriente e in Europa.

Di particolare importanza è stata la presentazione di Shigehiko Suzuki che ha presentato la ricerca e sviluppo della NTT in Giappone distinguendo l'evoluzione futura nel proprio Paese in tre periodi: *Electrum Cyber Society; Megamedia; Photonic Cyber Network*. Il primo di essi si riferisce all'offerta di un servizio nel quale molte attività legate agli affari, alle famiglie o alla vita sociale potranno essere svolte sulla rete di telecomunicazioni esistente. *Megamedia* è un concetto di servizio di rete che meglio risponde alle richieste del primo periodo consentendo il trasferimento dell'informazione con un elevato standard di rete. Quando gli utilizzatori di Megamedia raggiungeranno quelli telefonici dovranno essere impiegate tecnologie di rete che permetteranno velocità di cifra dell'ordine del Terabit (10^{12} bit/s); questa esigenza dovrebbe essere soddisfatta da una rete completamente fotonica. La *Photonic Cyber Network* consentirà l'impiego di bande passanti decisamente più estese rispetto a quelle oggi disponibili per corrispondere alle richieste degli utilizzatori di impiegare comunicazioni multimediali di circa 150 Mbit/s; essa permetterà anche di ridurre drasticamente il costo della rete favorendo lo sviluppo di nuovi tipi di applicazioni basati su un ambiente con elaborazione distribuita. La NTT prevede di predisporre sistemi innovativi nella parte della rete terminale, che impiegheranno portanti ottici per soddisfare nel Duemila il 30 per cento degli utilizzatori residenziali e tutti i clienti business e di completare in Giappone intorno al 2010 la predisposizione degli accessi ottici presso le residenze dei futuri utilizzatori.

In Italia l'intero sistema legato alla ricerca è stato di recente oggetto di un processo di revisione intrapreso dalle Autorità governative, volto a rimuovere gli ostacoli che avevano reso l'intero settore dedicato alla ricerca - svolta nelle Università, nei Centri di ricerca e nel mondo industriale - inadeguato alle più recenti

esigenze dell'industria. Nel nostro Paese sono d'altra parte emersi in questi ultimi tempi problemi e limiti - sia in termini di finanziamento sia sul ridotto numero di ricercatori impegnati - che penalizzano l'Italia rispetto agli altri, aderenti all'OCSE. Secondo recenti dati dell'ISTAT, l'Italia ha speso per l'attività di ricerca - pubblica e privata - intorno ai 21 mila miliardi di lire, contro i 44 mila della Francia ed i 62 mila della Germania. Il numero di ricercatori in Italia supera di poco le 75 mila unità, mentre gli addetti francesi sono più di 150 mila e quelli tedeschi circa 230 mila. Nel 1996 la spesa per la ricerca e sviluppo nel settore delle telecomunicazioni è stata superiore ai 2 mila miliardi di lire a fronte degli 8 mila spesi in Francia, dei 10 mila in Germania ma, soprattutto, dei quasi 24 mila investiti negli Stati Uniti e dei 26 mila impiegati in Giappone.
L'Italia si trova quindi in una posizione di ritardo rispetto ad altre realtà europee.
Il quadro tracciato per la ricerca e sviluppo nel nostro Paese a livello generale presenta aspetti simili anche nel campo delle tecnologie dell'informazione e della comunicazione che - è stato sottolineato nel corso del Convegno - continuerà a essere il settore trainante dello sviluppo economico a livello globale, nonché il cuore del conflitto competitivo.
Alessandro Bellman ha mostrato un confronto sulle prospettive per il futuro delle telecomunicazioni, indicate nel precedente incontro del 1992, e la situazione odierna: Internet allora era stata quasi ignorata mentre essa oggi ha invaso con la sua presenza ogni settore; la multimedialità non ha avuto la diffusione allora ipotizzata; la tecnologia fotonica è cresciuta anche nel nostro Paese soprattutto per l'impegno di alcune industrie che hanno i propri centri di sviluppo in Italia; la mobilità si è sviluppata in misura elevata e in qualche modo non prevedibile.
L'Italia di fronte al contesto internazionale è stato il tema esaminato in maniera approfondita nel corso della seconda sessione, presieduta da Ovidio M. Bucci. In questa sessione sono state presentate relazioni da *Gianni Fabri* (Presidente del Comitato Tecnico Scientifico MURST), *Cesare Mossotto* (Direttore Generale dello CSELT), *Aldo Roveri* (Presidente del Consiglio Superiore Tecnico delle Telecomunicazioni e docente presso l'Università di Roma La Sapienza) e *Giorgio Franceschetti* (docente nell'Università di Napoli Federico II). Cesare Mossotto ha ricordato in particolare che il Gruppo Telecom ha investito nell'innovazione 700 miliardi nel 1997, operando con circa 4300 ricercatori e ha indicato le principali attività svolte nelle aziende manifatturiere e nelle società di software. Si è poi soffermato su ruolo, attività e risultati dello CSELT. Aldo Roveri ha descritto l'ambiente in cui si realizza la ricerca avanzata svolta oggi in 28 centri con 350 ricercatori. Ha poi proposto l'avvio di un piano di ricerca nazionale per il settore dell'Information & Communication Technology - come elemento essenziale per lo sviluppo anche nel nostro Paese della Società dell'Informazione - e ha suggerito, allo stesso tempo, la costituzione di un centro per la promozione, il coordinamento e la valutazione delle attività legate ai piani di ricerca.
Un panel di confronto condotto da *Maurizio Decina* (CEFRIEL) sul tema *Quale ricerca e sviluppo di fronte ai grandi cambiamenti tecnologici, di business e istituzionali* ha avuto come relatori i partecipanti alla sessione precedente ai quali si sono aggiunti *Remo Pareschi* e *Giorgio Pellegrini* (Direzione Research e Development di Telecom Italia). Quest'ultimo ha sottolineato, in particolare, che sarebbe auspicabile che l'Amministrazione statale individui i bisogni in termini di applicazioni di servizi al cittadino e che finanzi le attività tese a soddisfarli. In questo modo potrebbero essere significativamente stimolate l'attività di ricerca e sviluppo nelle telecomunicazioni in campo applicativo dell'Information & Communication Technology.
Il Ministro delle Comunicazioni, *Salvatore Cardinale*, ha concluso in maniera autorevole la prima giornata del Convegno focalizzando il suo intervento sull'importanza che le telecomunicazioni hanno per il nostro Paese e sull'attenzione che il Governo intende dare alla crescita del settore.
Il giorno successivo sono state tenute due tavole rotonde, entrambe presiedute da *Franco Vergnano* (redattore de Il Sole 24 ORE): la prima, dal titolo *Nuove prospettive per il mercato*

Un momento della tavola rotonda "Quale ricerca e sviluppo di fronte ai grandi cambiamenti tecnologici, di business e istituzionali" presieduta da Maurizio Decina (primo a sinistra).

ha raccolto pareri di autorevoli rappresentanti delle ditte manifatturiere di sistemi operanti in Italia: *Sammy Gattegno* di Alcatel Italia, *Francesco Rispoli* di Alenia Aerospazio, *Dario Cassinelli* di Compaq, *Massimo Gentili* di Ericsson Telecomunicazioni, *Alessandro Bellman* di Italtel, *Sandro Gualano* di Marconi, *Paolo Vergnano* di Pirelli e *Renzo Tani* di Siemens. Nel corso del dibattito i costruttori hanno indicato l'attività di ricerca e sviluppo promossa da ciascuno di essi in Italia in termini di impegno di risorse umane e finanziarie. È stato così delineato un quadro estremamente significativo che ha confermato che molte aziende svolgono nel nostro Paese un'attività tesa all'innovazione o alla personalizzazione dei prodotti ma che, per motivi legati alla presenza di multinazionali, buona parte degli sviluppi sono oggi svolti presso le sedi delle case madri.

I principali costruttori nazionali dibattono il tema "Nuove prospettive per il mercato".

La seconda tavola rotonda ha delineato il *Nuovo quadro competitivo degli operatori di rete*. Sono intervenuti: *Giuliano Venturi* (Albacom) *Alberto de Petris* (Infostrada) *Antonio Bernardi* (Omnitel) *Oscar Cicchetti* (Telecom Italia) *Tommaso Pompei* (Wind) e *Fulvio Zubiani* (Worldcom). Oscar Cicchetti ha in particolare sottolineato che Telecom Italia continua ad avere come obiettivo primario la "creazione di valore" e che, a suo avviso, per la difesa della propria leadership, innovare equivale ad acquisire o a conservare quote di mercato; a questo scopo l'Azienda ritiene necessario riorientare le scelte tecnologiche da essa impiegate e, in particolare, di muoversi da una situazione di centralità del trasporto della fonia a una relativa al trasferimento di dati. Essa d'altra parte, intende indirizzarsi verso un'integrazione tra i sistemi per la telefonia fissa e quelli mobili.

I nuovi gestori, che hanno preso la parola, hanno mostrato alcuni dati tra i più significativi dell'attività, da essi di recente avviata, e hanno indicato gli obiettivi di maggior rilievo perseguiti. L'annuncio da parte dell'amministratore delegato di Wind, *Tommaso Pompei*, che la propria società avvierà a marzo il servizio di telefonia cellulare "con tariffe adeguate alle aspettative del mercato" e la notizia di *Giuliano Venturi* che Albacom partirà entro fine giugno con l'offerta del servizio della telefonia fissa per le famiglie, sperimentata già su 2500 utenze private, sono alcune tra le principali anticipazioni emerse nel corso della tavola rotonda.

Il Commissario dell'Autorità per le Garanzie nelle Comunicazioni, *Giuseppe Gargani*, intervenendo in chiusura del convegno, ha affermato che lo sviluppo del settore delle comunicazioni rappresenta senza dubbio un elemento determinante per la crescita del Paese e ha ribadito l'importanza del ruolo di regolamentazione dell'Autorità necessario per lo sviluppo tecnologico nazionale.

A conclusione dei lavori è stato proposto che, per contribuire alla crescita della Società dell'Informazione, la competitività delle imprese venga sempre più spostata verso sviluppi industriali legati alle innovazioni scientifiche e tecnologiche - frutto della ricerca - e alla capacità delle stesse aziende di introdurle con tempestività e in maniera economica nei prodotti.

È stato in proposito ribadito che è difficile oggi puntare a obiettivi solo nazionali ma che occorre potenziare e coordinare a livello europeo la ricerca e sviluppo fra le realtà presenti nei diversi Paesi e che - in un mercato altamente competitivo e globale come quello presente - l'innovazione introdotta con continuità nelle reti di trasporto delle telecomunicazioni costituisce un fattore di estremo rilievo per la crescita economica.

L'evoluzione, la crescita e l'utilizzo delle nuove tecnologie d'altra parte, devono diventare sinonimo di occupazione specie per i giovani in attesa di primo impiego.

Daniela Fioramonti - AEI - Milano

"The way to go"

VIII International Telecommunication Network Planning Symposium

"Networks '98"

Sorrento, 18-23 ottobre

Marco Burgassi,
Andrea Del Pistoia,
Luigi Fammartino,
Umberto Mazzei

Locandina del Congresso

"IL MONDO IN CUI OPERIAMO STA SUBENDO UN RAPIDO CAMBIAMENTO PER L'EFFETTO DI TRE FATTORI CHIAVE: LIBERALIZZAZIONE DEI SERVIZI DI TELECOMUNICAZIONE, GLOBALIZZAZIONE, CONVERGENZA DI TLC, INFORMATION TECHNOLOGY E MEDIA. QUESTO SCENARIO COSTITUISCE UNA SFIDA DRAMMATICA PER I GESTORI DI TLC, MA OFFRE LORO L'OPPORTUNITÀ DI NUOVI BUSINESS E DI ENTRARE IN NUOVI MERCATI. IL PROCESSO DI PIANIFICAZIONE DEVE QUINDI ESSERE MAGGIORMENTE ORIENTATO AGLI ASPETTI DI "BUSINESS PLANNING" E DI REGOLAMENTAZIONE, E DEVE TENDERE A RENDERE MASSIMO IL "VALORE PER IL CLIENTE", CHE A SUA VOLTA COSTITUISCE VALORE PER I GESTORI DELLE RETI E DEI SERVIZI."

Queste parole sono tratte dal discorso con cui *Umberto Mazzei* (TIM), Chairman del Comitato Scientifico del Congresso, ha aperto l'ottava edizione dell'*International Telecommunication Network Planning Symposium (Networks '98)*, dando il benvenuto ai numerosi ospiti e introducendo il tema di base del convegno: *"the way to go"*. L'importante manifestazione si è tenuta quest'anno a Sorrento dal 18 al 23 ottobre 1998. Umberto Mazzei nel suo intervento ha anche sottolineato come proprio il 1998 costituisca un anno cruciale per le telecomunicazioni in tutto il mondo, e in Europa in particolare: il primo anno di piena liberalizzazione del mercato per tutti i servizi di telecomunicazione. La rapidissima innovazione tecnologica che ha avuto luogo nelle ultime due decadi sta ora "guidando" la crescente convergenza tra Telecomunicazioni, Information Technology e Media, testimoniata da più di quattromila operazioni di questo tipo nel mondo nel solo 1997 (per un valore di circa 200 miliardi di dollari). La globalizzazione dell'economia d'altra parte sta abbattendo le barriere geografiche tra i mercati, grazie alla maggiore libertà e velocità con cui le risorse finanziarie possono muoversi. Il processo di pianificazione delle reti è sempre stato un compito difficile, dovendo considerare una previsione per il futuro, ma ora la sua complessità è vieppiù accresciuta dallo scenario descritto. Le nuove esigenze ed i nuovi obiettivi del Network Planning, come emergerà dal presente resoconto, sono ben sintetizzati dalle parole citate. Umberto Mazzei ha concluso il suo discorso fornendo un quadro sintetico della realtà odierna in Italia della telefonia fissa e mobile.

Umberto Mazzei, Chairman del Comitato Scientifico del Congresso, apre l'ottava edizione del *Networks '98*.

Evoluzione del Convegno negli anni

"Nella key-note di apertura *Claudio Carrelli* (distaccato da Telecom Italia all'EURESCOM, dove svolge le funzioni di Direttore Generale) ha passato in rassegna l'evoluzione delle reti di telecomunicazione negli ultimi trenta anni, mettendo in rilievo come il modello "rete-centrico", fondamentalmente basato sulla spinta dell'evoluzione tecnologica, risulti ormai superato. Si è quindi soffermato sulle sempre più forti interrelazioni tra tecnologia, mercato e regolamentazione, mettendo in evidenza come queste rappresentino oggi il vero motore di sviluppo.
Con riferimento al futuro, Carrelli ha presentato un panorama di enormi potenzialità, ribadendo quanto questo venga continuamente sottostimato, a causa di atteggiamenti, troppo spesso, eccessivamente conservativi. In chiusura dell'intervento ha sottolineato l'opportunità della cooperazione tra operatori, anche nel nuovo contesto competitivo, non solo per facilitare il

processo di standardizzazione e le conseguenti economie di scala, ma anche per concorrere alla creazione di nuovi e più ampi mercati."

George Lajtha (Matáv Hungarian Telecom- munication Co., Hungary), un "decano" della manifestazione, ha presentato una retrospettiva dei vent'anni di storia del convegno, illustrandone sviluppo e cammino evolutivo. La prima edizione dell'*International Telecommunication Network Planning Symposium* è stata tenuta nel 1980 per iniziativa di alcuni pianificatori di rete europei, con l'obiettivo di confrontare da un punto di vista tecnico le differenti metodologie impiegate per ottimizzare le reti di telecomunicazioni. Nel corso degli anni Ottanta i problemi del Network Planning sono stati rivolti alla "numerizzazione" delle reti, sia trasmissiva che di commutazione; questa innovazione non ha solo portato a un cambiamento di tecnologia, ma anche dell'architettura e della struttura relativa alla rete di base. Le metodologie e gli algoritmi impiegati per la ricerca delle "condizioni di ottimo" hanno riguardato quindi problematiche quali l'instradamento del traffico, la riduzione dei costi di rete fino a raggiungere le situazioni di minimo, l'analisi ed il miglioramento della qualità del servizio.

Gli anni Novanta hanno visto un'accelerazione del cambiamento tecnologico e dell'innovazione dei servizi; questi fenomeni sono stati accompagnati e sospinti dai profondi cambiamenti nella struttura dell'industria delle telecomunicazioni, riguardanti in primo luogo la progressiva liberalizzazione dei mercati, e la convergenza tra Telecomunicazioni, Information Technology e i "Media". Le responsabilità del pianificatore di rete sono via via divenute più complesse: dalla soluzione dei problemi relativi all'ottimizzazione dello sviluppo della rete, l'attività si è spostata verso la ricerca di strumenti di analisi delle nuove opportunità di crescita dell'azienda (i nuovi "business"), tramite sia le reti esistenti sia quelle nuove.

George Lajtha presenta la storia di vent'anni del "Network Planning Symposium".

Networks '98

Il tema del convegno di Sorrento per il Network Planning, *"the way to go"*, è legato a una sfida che può essere espressa mediante le seguenti due esigenze:

- coniugare l'approccio tecnico tradizionale della pianificazione con una serie di fattori quali: la complessità; i rapidi cambiamenti presenti concernenti le alternative tecnologiche disponibili; lo scenario dei servizi, gli aspetti di mercato e di regolamentazione;
- "pianificare" l'evoluzione delle telecomunicazioni per fornire "più valore al cliente", mediante l'offerta di nuovi servizi, di nuove possibilità di "business", la costruzione di nuove reti, la presenza di nuovi gestori.

Il convegno ha visto la partecipazione di trecentocinquantaquattro delegati provenienti da trentun Paesi: centosessantotto rappresentanti dei costruttori di telecomunicazioni, centoquarantatré dei gestori di rete, quarantatré appartenenti a Università e centri di ricerca. Sono state tenute dieci "sessioni plenarie" (tra queste vi sono state due tavole rotonde rispettivamente sui temi: *Who's working on my problems* e *The truth about infrastructures)*, e diciotto "sessioni tecniche" parallele. Sono state presentate novantanove memorie: quindici di esse avevano tra gli autori tecnici del Gruppo Telecom Italia, e, in particolare, nove memorie annoveravano autori dello CSELT. Per quanto concerne i riconoscimenti, erano previste due *nomination* per il *best quality paper* e due per il *most innovative*, con un articolo premiato per ciascuna categoria: il riconoscimento per l'articolo più innovativo è stato assegnato dal Comitato Tecnico di Networks '98 alla memoria: *Common pool survivability in ATM over SDH ring networks* (autori M. Gryseels, P. Demeester – Università di Gent, Belgio; R. Clemente, M. Ravera - CSELT), preparata nell'ambito del progetto *ACTS PANEL (Protection Across NEtwork Layers)*.

Gli argomenti affrontati nelle varie sessioni riguardavano temi più tradizionali (quali: reti ottiche e a larga banda, SDH e ATM; nuovi sistemi di accesso: xDSL e "wireless"; analisi delle prestazioni di rete e dell'affidabilità; strumenti di progettazione e di "management" di rete), e temi più innovativi (accesso a Internet; aspetti regolatori e di interconnessione tra reti; "re-ingegnerizzazione" dei processi di pianificazione della rete).

Qui di seguito sono riportate alcune delle indicazioni di maggior interesse, emerse nelle presentazioni e nelle successive discussioni, anche per le caratteristiche innovative degli interventi:

- il *Network Planning* è un tema che coinvolge in misura crescente i costruttori di sistemi di telecomunicazione: i gestori di rete "nuovi entranti", infatti, molto spesso hanno un'esperienza tecnica assai limitata nelle telecomunicazioni, e richiedono

quindi sviluppi di rete chiavi in mano;
- i nuovi gestori vogliono disporre di reti flessibili e facilmente ampliabili, desiderano ridurre al minimo il rischio negli investimenti, e ottenere un rapido ritorno degli investimenti *(pay back time);*
- molti vecchi gestori *(incumbent)*, viceversa, si orientano ancora verso un'ottica di lungo periodo, dovendo considerare il patrimonio degli investimenti (che per certi aspetti può costituire un "vincolo") costituito dai costi sostenuti per realizzare la propria rete: l'approccio da essi seguito mira quindi a equilibrare l'introduzione delle nuove tecnologie con l'utilizzo della rete esistente;
- si assiste ad un generale ottimismo sullo sviluppo delle reti Internet, per applicazioni tradizionali (ad esempio per *information retrieval)* e ancor più per impieghi innovativi (quali i servizi finanziari e quelli commerciali): queste previsioni concordano sull'attesa che in anni assai prossimi (2002) il traffico dati supererà quello di fonia;
- si ritiene in generale che le "infrastrutture di rete" (tecnologie trasmissive, commutazione, OSS) costituiscano elementi necessari, ma non sufficienti, per consentire di generare le differenze e per vincere le sfide competitive. Una sempre maggiore importanza è data alla componente riguardante l'Information Technology.

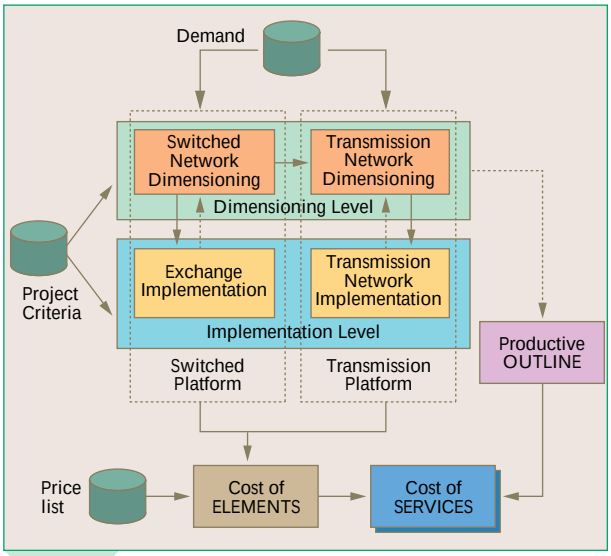


Figura 1 *Modello di valutazione dei "costi incrementali" dei servizi di rete.*

Principali indicazioni emerse

Nel convegno i gestori hanno manifestato, in generale, l'esigenza di rivedere e di adeguare il processo di pianificazione della rete, e gli strumenti di supporto a esso relativi, alle mutate condizioni di mercato e di regolamentazione; queste condizioni si traducono in:
- scarsa possibilità di prevedere i fabbisogni di risorse di rete;
- rapida fornitura dei servizi, con caratteristiche adeguate alle esigenze del cliente;
- robustezza e flessibilità della rete.

La liberalizzazione del mercato dei servizi di telecomunicazione ha infatti limitato la possibilità di impiegare metodologie per le previsioni basate su andamenti storici consolidati, e ha indotto una notevole componente di incertezza; essa ha d'altra parte introdotto nuove problematiche riguardanti l'interconnessione tra differenti gestori. Dal punto di vista tecnologico si prospettano poi in genere più soluzioni per la fornitura dello stesso tipo di servizio: queste scelte diverse, combinate con tempi di innovazione dei prodotti particolarmente contenuti, rendono difficoltosa la scelta dell'architettura di rete più appropriata.

Da diversi utilizzatori si manifesta quindi l'importanza di una pianificazione che consenta di impostare correttamente le strategie di un gestore e di valutare i relativi rischi finanziari, tramite l'elaborazione di *business case* caratterizzati da componenti sia economico-finanziari che architetturali, e mirati a un orizzonte temporale che comprenda al più quattro o cinque anni. Nel congresso alcune presentazioni hanno in proposito mostrato possibili metodologie e strumenti di supporto (ad esempio basati su modelli parametrici di tipo stocastico), in alcuni casi orientati a una visione integrata delle diverse componenti di rete. In questo contesto si collocano anche le metodologie di stima dei costi dei servizi offerti dalla rete, che possono utilizzarsi sia nei confronti dell'Autorità di regolamentazione, sia per una corretta valutazione dei prezzi da applicare ai gestori interconnessi. Un interessante esempio di modello per la valutazione dei costi dei servizi in "ottica incrementale" è illustrato in una memoria presentata dallo CSELT assieme a Telecom Italia: *A network dimensioning engineering model for calculating the incremental costs of TLC services* (figura 1).

La costruzione della rete tende a costituire un'infrastruttura il più possibile condivisa tra gli specifici fabbisogni di capacità e aperta

all'introduzione di nuovi servizi. L'orizzonte temporale per una pianificazione puntuale delle risorse infrastrutturali si riduce al minimo compatibile con le esigenze legate ai tempi di attraversamento degli interventi (al più due anni), mentre le componenti legate agli interventi dimensionali e agli aspetti di servizio sarebbero spostate a ridosso del *provisioning*. Si manifesta un notevole interesse verso sistemi che consentano di valutare il rischio legato a eventi naturali (quali terremoti e inondazioni), e alle loro conseguenze sulle infrastrutture di telecomunicazione, come elemento significativo per la pianificazione e la progettazione della rete, e per l'ottimizzazione dell'organizzazione dei centri di supervisione.

Una notevole attenzione è stata posta all'impiego di sistemi di supporto alla gestione dell'intero "flusso di lavoro" volto alla fornitura dei servizi offerti dalla rete *(Workflow Management Systems)*, come fattore abilitante per un'efficiente realizzazione del processo a livello aziendale, con l'obiettivo di ridurre il tempo necessario all'offerta sul mercato dei servizi stessi *(Time to market)*. Un esempio concreto di re-ingegnerizzazione dell'intero processo di "creazione della rete" guidata dalle esigenze di mercato è descritto in una memoria di Telecom Italia e di Andersen Consulting: *Network Creation Management: an example of market-driven reengineering:* in essa si individuano e si definiscono i tre livelli fondamentali in cui si articola il nuovo processo: *Strategic Planning, Tactical Planning, Network Construction and Project Management.*

Per quanto concerne lo scenario di accesso (*dial-up*) a Internet, è stato confermato che per diversi gestori europei l'esplosione del "fenomeno Internet", in particolare per gli utilizzatori residenziali, stia già causando alcuni problemi di congestione sulla rete telefonica commutata. Questi problemi, seppur non ancora confrontabili con quelli riscontrati negli Stati Uniti (dove si è arrivati anche al blocco delle chiamate di emergenza), inducono la maggior parte dei gestori delle reti di telecomunicazione a valutare architetture alternative per l'accesso a Internet.

L'argomento è affrontato tra l'altro in un'interessante memoria presentata da Telecom Eireann (Ireland): *Aspects of network planning for Internet access via the public network – An Operator's perspective* (figura 2). La soluzione del problema che sembra oggi più semplice, ossia quella di adeguare la rete commutata aggiungendo risorse nei punti in cui si presentano le esigenze, è ritenuta valida solo come transitoria.

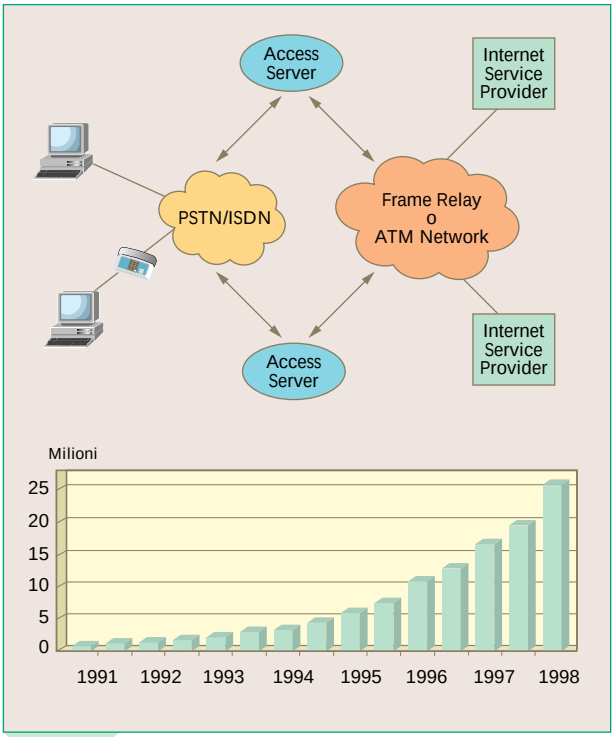


Figura 2 *Configurazione di accesso commutato a Internet e crescita degli Internet Hosts.*

D'altra parte, la fornitura di Internet tramite accessi diversi dal modem POTS/ISDN (ad esempio con terminali xDSL) è vista come soluzione valida per il medio o lungo termine. La proposta architetturale che sembra riscuotere il maggior consenso tra i gestori prevede di avvicinare il più possibile all'utente il punto in cui il segnale in ingresso è convertito in pacchetti ed è trasferito su una rete dati (IP su Frame Relay o su ATM); questa conversione è effettuata allocando l'insieme dei modem subito a valle degli autocommutatori, oppure concentrando i modem in un numero limitato di punti ma remotizzandone gli accessi su terminazioni ISDN per accessi primari *(ISDN Primary Rate Access)*.

Per quanto riguarda il futuro della rete di trasporto, è stata sottolineata la possibilità di un'evoluzione di Internet verso una piattaforma multimediale generalizzata, che comprenda la fornitura dei servizi di telefonia. Alcune presentazioni hanno quindi mostrato in particolare gli aspetti relativi alle prestazioni e alla gestione del traffico legati a questo nuovo ruolo, fornendo risultati di sperimentazioni; sono stati anche presentati i sistemi di misura.

In una prospettiva di telefonia IP, è stata tra l'altro segnalata la problematica dei ritardi; è

perciò necessario predisporre meccanismi di prenotazione della banda o di differenziazione dei pacchetti a elevata priorità. L'impiego di meccanismi di compressione della voce (per limitare il fabbisogno di risorse su IP) accresce inoltre questi ritardi e di essi dovrà essere tenuto conto in fase di progettazione della rete.

Il ruolo dell'ATM per la rete di trasporto risulta ancora controverso: sono stati infatti mostrati scenari che vanno da un impiego sulla rete ATM dei diversi tipi di reti e servizi, a quelli relativi alla realizzazione delle funzioni di commutazione di supporto ai router di Internet, all'infrastruttura per reti private virtuali *VPN (Virtual Private Network).* Sono state anche mostrate procedure e strumenti per il dimensionamento di reti ATM, sia per servizi commutati sia per la fornitura di *VP (Virtual Path)* semipermanenti, e meccanismi di reinstradamento per questo strato di rete. Altre presentazioni hanno riguardato valutazioni di architetture di rete trasmissiva SDH e WDM, il coordinamento della loro pianificazione e gestione e i problemi di tipo topologico per garantire la robustezza della rete (quali ad esempio la ricerca di percorsi ad anello). In particolare per l'SDH sono state segnalate alcune iniziative relative allo sviluppo di piattaforme di supporto alla fornitura dei percorsi seguiti dai flussi *(path),* in alcuni casi agganciate ai sistemi di gestione della rete stessa. Per la rete commutata a circuito sono stati presentati studi relativi al dimensionamento della rete in condizioni di incertezza previsionale, a guasti degli autocommutatori e agli stati di congestione della rete. Altre memorie hanno trattato invece le problematiche di accesso a fornitori di servizi *(server)* multimediali su rete Internet o ATM.

Un aspetto particolarmente interessante trattato nel congresso riguarda l'inter-lavoro tra reti di trasporto multilivello (ad esempio ATM su SDH, SDH su WDM), per quanto concerne i meccanismi di protezione e di reinstradamento dei servizi trasportati in caso di guasti, e la capacità da riservare a questi scopi. In questo ambito è compresa la memoria già citata presentata dallo CSELT e dall'Università di Gent, premiata come *most innovative paper.* Essa propone una nuova strategia di reinstradamento denominata *common pool of spare resources;* questo sistema consentirebbe di ridurre i fabbisogni di risorse richieste dai meccanismi di protezione a più livelli di rete. L'articolo presenta i potenziali vantaggi dell'applicazione proposta per una rete campione costituita da uno strato ATM sovrapposto ad anelli SDH. L'idea di base riguarda il trasporto della capacità di riserva del livello ATM come "extra-traffico" sulla rete SDH (figura 3).

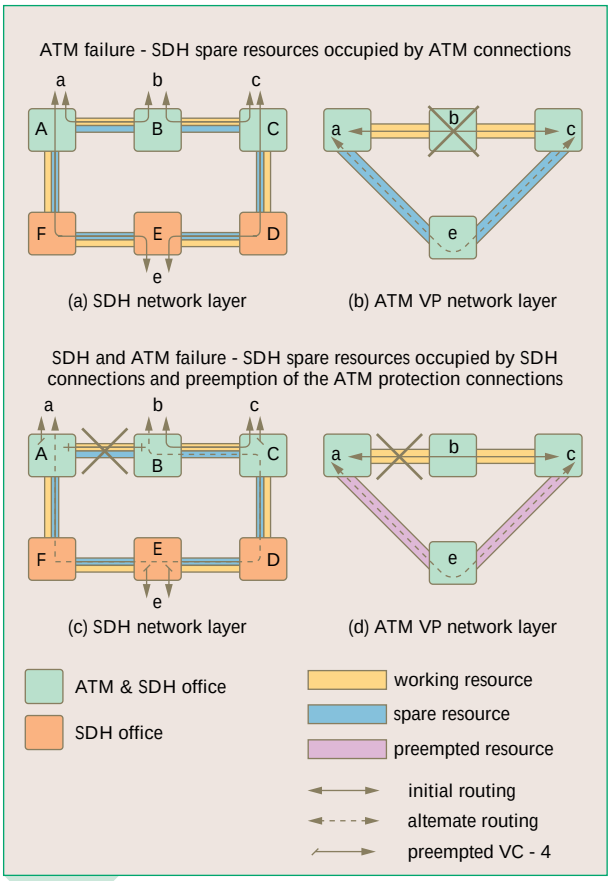


Figura 3 *Strategia di reinstradamento "Common pool survivability" per reti di trasporto multilivello.*

Nel corso della sessione sulla progettazione delle reti ATM, sono stati presentati alcuni studi relativi all'introduzione dell'ATM nella rete di transito telefonica, o più in generale all'utilizzo della tecnica ATM per il trasporto della voce. Questi studi, presentati in particolare da France Telecom e da AT&T, ma per i quali tutti i gestori presenti hanno mostrato un particolare interesse, riportavano alcune indicazioni sui benefici tecnici ed economici e sulle opportunità da un punto di vista strategico che potrebbero derivare dall'adozione di un'unica infrastruttura dorsale *(backbone)* utilizzabile anche per il trasporto del traffico di dati. In particolare France Télécom ha presentato alcuni risultati di un confronto tra architetture tradizionali e quelle basate su ATM per il trasporto della fonia: da essi risulta che con la seconda soluzione si otterrebbe un risparmio di circa l'otto per cento.

Per quanto riguarda le reti mobili, sono state discusse le problematiche relative all'impatto della fornitura di servizi evoluti su queste reti (ad esempio Internet, multimediali); questa proposta comporta la necessità di allocare nuove bande di frequenza, e di impiegare nuove tecnologie con capacità a larga banda e con nuovi standard (UMTS). I partecipanti al congresso hanno mostrato interesse per nuovi approcci e nuovi sistemi flessibili di pianificazione e di progettazione delle reti mobili e wireless, che permettano di tener conto della variabilità relativa ai numerosi parametri in gioco (di carattere ambientale, di utenza, tecnologici), delle previsioni di sviluppo e delle caratteristiche dei servizi offerti, con lo scopo di ottimizzare l'allocazione della capacità nella rete e le sue prestazioni. Un interessante esempio di questi sistemi è descritto in una memoria presentata dallo CSELT assieme a TIM: *SIRIO: a forecasting tool for strategic planning of mobile networks.* Lo strumento descritto è un ausilio per la pianificazione strategica delle reti mobili, stimando il numero e la posizione degli elementi di rete (controllori delle stazioni base, centri di commutazione mobili), la domanda dei collegamenti e il traffico offerto alla rete fissa, per un dato numero di anni di previsione (figura 4).

Sono stati anche mostrati alcuni nuovi sistemi di pianificazione delle reti basate su CDMA, e i risultati di valutazioni delle prestazioni di queste reti. Sono state affrontate infine le problematiche relative alla trasportabilità del proprio numero telefonico *(number portability).*

La convergenza delle reti fisse e mobili è considerata ormai un aspetto di importanza prioritaria sia per i gestori nuovi entranti sia per quelli già consolidati; questo aspetto è determinato, da una parte, dall'esplosione del mercato delle reti mobili, con effetto anche di "sostituzione" sulle reti fisse, e dall'altra parte dalle elevate capacità potenziali che le reti fisse tuttora mantengono. La convergenza produce benefici per i clienti delle reti (quali l'accesso uniforme ai differenti servizi, la numerazione e le forme di pagamento uniche), e nuove opportunità di competizione per i gestori ("valore aggiunto" ai servizi offerti). Una memoria presentata da Nortel (Canada) mostra alcune valutazioni secondo le quali la riduzione dei costi dei gestori fissi e mobili relativi alle proprie reti *(cost-of-ownership)* passa attraverso l'integrazione dei nodi di servizio e della gestione delle due reti.

Un momento della conferenza.

Per la rete di accesso si è dibattuto a lungo l'impiego della tecnologia VDSL possibile, in alternativa, in architetture FTTC/Cab o FTTB: le prime comportano conseguenze più contenute in termini di nuove opere civili da realizzare; le configurazioni di cablaggio della fibra considerate sono di vario tipo (ad esempio: schemi punto-punto, ad anello, PON). È stato anche segnalato l'uso di metodi di *risk analysis* per valutare l'influenza di alcuni fattori dominanti (ad esempio il numero di utenti per servizio) sulla redditività dei "progetti" per la rete di accesso.

È stato poi mostrato interesse per le soluzioni xDSL e per le loro caratteristiche di ampliabilità flessibile, in particolare per la tecnologia G-lite che consentirebbe di evitare impatti sul cablaggio di edificio; secondo Nortel la soluzione ADSL sarebbe remunerativa da un punto di vista economico già a partite da un livello di penetrazione del cinque per cento.

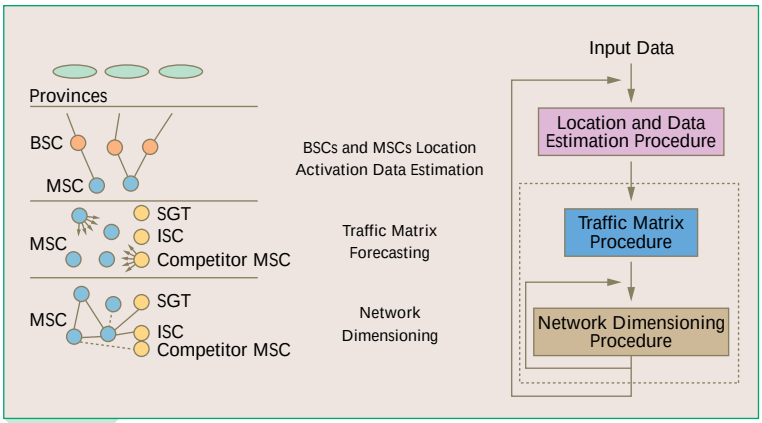


Figura 4 *Architettura del sistema SIRIO impiegato per la pianificazione di reti mobili.*

È stato anche manifestato un certo interesse per soluzioni radio in zone urbane a bassa densità e rurali, in particolare in configurazioni RTTCab per i costi più contenuti nell'installazione. È stato segnalato l'impiego della tecnologia *LMDS (Local Multipoint Distribution System)* per applicazioni a larga banda, in visibilità diretta o in configurazione *TLN (Two Layer Network)* con ripetitori radio su microcella. Per i nuovi gestori è stata infine posta in luce la problematica (già particolarmente sentita negli Stati Uniti) tesa a cercare di individuare soluzioni idonee per raggiungere gli utenti in aree in cui non si dispone di infrastrutture: in questi casi è richiesto l'affitto da terzi delle risorse necessarie (fibre, lunghezze d'onda, spazi in centrale).

Le linee evolutive seguite e le esperienze maturate verso un'infrastruttura di rete a larga banda - per la fornitura di servizi innovativi e l'integrazione di quelli tradizionali - sono illustrate in una memoria presentata da Telecom Italia: *Evolution towards the broadband network*. In essa si considerano le diverse opzioni per la rete di accesso (HFC, xDSL, FTTx, LMDS), e l'affiancamento nella rete di trasporto delle tecnologie ATM e IP a quelle tradizionali (PSTN/ISDN, *Leased Lines)*.

Il padiglione espositivo approntato dallo CSELT a margine del Congresso.

Spazio espositivo per gli strumenti di Network Planning

In occasione del convegno Newtork '98 è stato allestito uno spazio espositivo, destinato alla presentazione di strumenti per la pianificazione di rete. All'iniziativa hanno aderito una dozzina circa di costruttori e gestori (tra questi NTT, ERICSSON, SIEMENS, LUCENT, SIRTI, ALCATEL). Gli strumenti esposti e illustrati consentono di svolgere diverse fasi del processo di Network Planning: pianificazione della struttura, dimensionamento delle risorse, simulazione delle prestazioni, analisi dello stato della rete *(Network Analysis)*. I segmenti di rete interessati comprendono le reti trasmissive SDH e PDH, le reti a commutazione di circuito, le reti ATM, le reti di accesso, le reti radiomobile GSM e analogiche.

In questa occasione anche CSELT ha allestito un proprio padiglione espositivo, per presentare due strumenti sviluppati in collaborazione con Telecom Italia. Il primo, INPLAN, è un sistema di supporto usufruibile nella pianificazione dell'evoluzione di reti regionali verso piattaforme a larga banda, con lo scopo di fornire nuovi servizi ed, eventualmente, di integrare quelli tradizionali; lo strumento affronta in modo "integrato" la pianificazione dei differenti segmenti di rete (accesso, commutato, trasmissivo), e si avvale di una Base Dati (DB) territoriale concernente la struttura delle attuali reti regionali di Telecom Italia. Il secondo strumento, TITANO, è impiegato per dimensionare e ottimizzare le reti ATM, in presenza di servizi sia semipermanenti che commutati.

TITANO è utilizzabile da pianificatori e progettisti di rete che hanno la necessità di valutare diverse tipologie di struttura di rete e differenti politiche di integrazione dei servizi, con lo scopo di minimizzare i costi di realizzazione della rete.

Conclusioni

Il contesto nel quale il processo di Network Planning si trova oggi a operare è profondamente cambiato rispetto al passato (anche non troppo remoto) ed è caratterizzato da una "dinamica" crescente, sotto l'influsso di alcuni "fattori chiave": la rapidissima innovazione tecnologica; la liberalizzazione del mercato delle telecomunicazioni; la globalizzazione dell'economia; la convergenza tra Telecomunicazioni, Information Technology e Media. Di conseguenza il compito del pianificatore di rete, già difficile per tradizione (essendo strettamente legato a "previsioni sul futuro"), risulta vieppiù complicato, da una parte, per la mancanza di previsioni affidabili sullo sviluppo del proprio mercato, e dall'altra parte, per la varietà di soluzioni tecnologiche disponibili e per il dover affrontare nuovi fenomeni (ad esempio l'interconnessione tra differenti gestori, i mutamenti di regolamentazione). Ma è l'ottica stessa del *Network Planning* che ha subìto una mutazione: i nuovi obiettivi sono il business planning, la

creazione di una rete “flessibile” in termini di capacità di crescita e qualità del servizio, la ricerca del massimo valore per il cliente.
Le memorie presentate a Networks ’98 e le discussioni che ne sono scaturite hanno ben illustrato quanto si è fin qui esposto. Le presentazioni hanno mostrato sia le opzioni tecnologiche e architetturali di interesse per l’evoluzione delle reti e dei servizi, sia i nuovi approcci e strumenti necessari per permettere al pianificatore di rete di conseguire i suoi nuovi obiettivi. Sono stati messi in evidenza alcuni aspetti più rilevanti quali la re-ingegnerizzazione del processo di planning, l’esplosione del fenomeno Internet, lo sviluppo delle reti mobili. Nel complesso è stata confermata la validità del convegno che consente lo scambio tra più “attori” di esperienze e punti di vista differenti, in un campo così arduo e di importanza strategica quale il Network Planning. I fenomeni e le evoluzioni esposti saranno verosimilmente ancor più evidenti nei prossimi anni, e costituiscono motivo di crescente interesse per la prossima edizione del congresso, che si terrà a Toronto (Canada) dal 23 al 28 aprile del Duemila.

Marco Burgassi, Andrea Del Pistoia - CSELT
Luigi Fammartino - Telecom Italia
Umberto Mazzei - Telecom Italia Mobile

Abbreviazioni

ADSL	Asymmetric Digital Subscriber Line
ATM	Asynchronous Transfer Mode
DB	Data Base
FTTx	Fibre To The x: C = curb; Cab = cabinet; B = building; E = exchange
GSM	Global System for Mobile communications
HFC	Hybrid Fibre-Coaxial
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LMDS	Local Multipoint Distribution System
OSS	Operation Support System
PON	Passive Optical Network
POTS	Plain Ordinary Telephone Service
RTTCab	Radio To The Cabinet
SDH	Synchronous Digital Hierarchy
TLN	Two Layer Network
VDSL	Very high speed Digital Subscriber Line

Sorrento. La piccola Marina con la Funicolare. (Da una foto Alinari dei primi anni del Novecento).

EVOLUZIONE DELLA NORMATIVA TECNICA NELLE TELECOMUNICAZIONI

WIRELESS APPLICATION PROTOCOL

IL WAP (WIRELESS APPLICATION PROTOCOL) È UN PROTOCOLLO CHE CONSENTE L'ACCESSO AD INTERNET, E IN GENERALE A CONTENUTI WEB, ATTRAVERSO UN TELEFONO MOBILE, SENZA NECESSITÀ DI PERSONAL COMPUTER O APPARATI DI COMUNICAZIONE SEPARATI.

È derivato dall'HTTP/TCP-IP ed è semplificato allo scopo di far fronte alle caratteristiche dei servizi di trasmissione dati delle reti mobili. Impiega un linguaggio mark-up (WML, Wireless Markup Language) semplificato per consentire la realizzazione all'interno dei telefoni mobili di un browser (chiamato micro-browser) compatibile con le risorse (memoria, display, CPU) dei telefoni stessi.

È disponibile su diverse reti cellulari, che includono i sistemi GSM, CDMA IS-95, TDMA IS-136, i sistemi giapponesi PDC e PHS.

Il WAP consente l'accesso ai servizi telefonici, tipici delle reti cellulari, oltre che ad applicazioni Internet.

ACCESSO AD INTERNET TRAMITE UN "TELEFONINO"

Tra le applicazioni WAP si possono includere: servizi telefonici o di rete intelligente con interfaccia semplificata, come voice mail, unified messaging; servizi informativi, come prenotazione di taxi, ristoranti, hotel, treni, informazioni di borsa, infobanking, servizi di directory, meteo; il commercio elettronico; la posta elettronica; giochi; info-mobility.

È possibile impiegare il WAP per realizzare applicazioni corporate e verticali come ad esempio: accesso ad applicazioni aziendali; database; sistemi cooperativi; posta aziendale; despatching; monitoraggio remoto; work-force management.

Il protocollo WAP è sviluppato nell'ambito del WAP Forum, un'organizzazione fondata da Ericsson, Nokia, Motorola e Unwired Planet; di essa fanno parte (alla fine del 1998) 71 Società in rappresentanza di costruttori di apparati e di gestori di servizi mobili.

♦♦♦♦♦

COMUNICAZIONI MOBILI VIA SATELLITE

NEGLI ULTIMI ANNI I SATELLITI SI SONO RAPIDAMENTE "AVVICINATI" ALL'UTENTE FINALE. CIÒ COSTITUISCE UNA TRASFORMAZIONE RISPETTO A QUANTO AVVENUTO PER UN LUNGO PERIODO, DI CIRCA QUARANT'ANNI, DURANTE IL QUALE ESSI HANNO GIOCATO NELLE TELECOMUNICAZIONI IL RUOLO DI "PORTATORI DI INFORMAZIONE" A UN LIVELLO INTERMEDIO TRA IL FORNITORE E L'UTENTE FINALE.

Il broadcasting televisivo e la telefonia sono i due ambiti in cui è avvenuta questa trasformazione: nel primo caso il satellite, che tradizionalmente forniva la capacità di trasporto sulle dorsali intercontinentali tra centri di produzione, oggi è arrivato a casa dell'utente finale che può riceverne direttamente il segnale; nel secondo caso, esiste oggi la possibilità di fornire all'utente finale accesso diretto al segmento spaziale con terminali mobili di dimensioni contenute, mentre in precedenza il satellite realizzava solamente la funzionalità di collegamento a lunga distanza sulle tratte intercontinentali delle chiamate in fonia. L'evoluzione delle comunicazioni mobili via satellite, accelerata dal forte sviluppo ottenuto dai sistemi cellulari terrestri di seconda generazione, sta vedendo in primo luogo giungere a compimento il dispiegamento delle costellazioni LEO (Low Earth Orbit), progettate all'inizio degli anni Novanta ed a lungo considerate non realizzabili per ragioni di complessità tecnica e di costo eccessivo. Queste costellazioni tra oggi e il Duemila saranno una realtà, e rappresentano a tutti gli effetti la realizzazione della comunicazione "anytime and anywhere" a lungo cercata dal mondo delle telecomunicazioni. Le velocità di cifra in gioco, in grado di fornire poco oltre il servizio base di fonia, non sono certamente in grado di soddisfare

L'EVOLUZIONE DELLE COMUNICAZIONI MOBILI VIA SATELLITE È ACCELERATA DALLO SVILUPPO DEI SISTEMI CELLULARI TERRESTRI

tutte le esigenze di comunicazione oggi richieste. È dunque probabile che questi sistemi siano precursori di altri, che saranno progettati con funzionalità native più vicine al mondo terrestre e con potenzialità ben maggiori in termini di banda e di interlavoro con il GSM.
L'interesse verso i sistemi geostazionari per telefonia è andato contemporaneamente crescendo di pari passo e, anche se le sfide tecnologiche poste all'industria sono state meno visibili dal grande pubblico (che oggi, ad esempio, conosce Iridium), i tempi sono oggi maturi per lo sviluppo di sistemi GEO operanti su aree continentali e hanno portato all'estremo l'impostazione nata da Inmarsat negli anni Ottanta.
Nei primi anni del nuovo millennio è probabile la nascita di altri sistemi, non necessariamente solo LEO o GEO, che costituiranno una "cerniera" tra quelli di oggi ed i sistemi a banda più larga che si possono prevedere non prima del 2005-2007.

♦♦♦♦♦

Il cablaggio negli edifici

CON IL PROGREDIRE DEI SERVIZI DI TELECOMUNICAZIONE, IL CABLAGGIO CHE DEVE ESSERE PREDISPOSTO NEGLI EDIFICI E NEGLI APPARTAMENTI PER CONSENTIRE IL TRASPORTO HA ACQUISTATO UN'IMPORTANZA VIA VIA MAGGIORE. QUESTO CABLAGGIO, CHE UN TEMPO DOVEVA PORTARE ESSENZIALMENTE IL SERVIZIO TELEFONICO DI BASE, SI STA OGGI SEMPRE PIÙ INTEGRANDO CON QUELLO RELATIVO ALLA TECNOLOGIA DELL'INFORMAZIONE ED A NUOVI SERVIZI INTERATTIVI AD ALTA VELOCITÀ. LA SUA REALIZZAZIONE RAPPRESENTA OGGI UN ASPETTO CRITICO, SIA PER I CONDIZIONAMENTI CHE ESSO PUÒ COMPORTARE SULLA POSSIBILE EVOLUZIONE DEI SERVIZI, SIA PER I COSTI ASSOCIATI AD UNA SUA REALIZZAZIONE E ALLA SUA EVENTUALE MODIFICA.
Il problema ha riguardato negli anni passati soprattutto gli edifici adibiti ad usi commerciali, ma sta divenendo importante anche per gli edifici abitativi (o con piccole attività commerciali).
Le norme riguardanti il cablaggio possono essere suddivise, a seconda dell'argomento trattato, in tre differenti categorie: quelle relative al progetto, quelle sull'installazione e quelle che riguardano il collaudo o la manutenzione. Possono essere anche suddivise, in base allo scopo del cablaggio considerato, in due gruppi: norme relative a cablaggi costruiti e dimensionati per specifiche applicazioni o servizi, e norme relative a cablaggi per uso generale (o "indipendenti dalle applicazioni") che si prestano al trasporto di una vasta gamma di segnali.

La normativa per gli edifici commerciali e il crescente interesse per quelli abitativi

Altre norme sono rivolte ad argomenti specifici, quali gli aspetti di compatibilità elettromagnetica (emissione e immunità al rumore elettrico), di sicurezza (delle persone) e di protezione (degli apparati).
Nel campo della normativa sul cablaggio per uso generale in edifici commerciali si sono manifestate recentemente precise tendenze evolutive: richieste più severe per le coppie simmetriche di Categoria 5 e avvio di programmi per lo sviluppo di coppie con banda utile sino a 600 MHz; inoltre, cresce l'importanza del cablaggio in fibra ottica, soprattutto per realizzare cablaggi ad architettura centralizzata.
Nel contempo, comincia ad apparire la normativa sui cablaggi per uso generale negli edifici residenziali (mentre diminuisce di conseguenza l'interesse per quella sui cablaggi per usi specifici). Questa modifica di interesse rientra nella più generale convenienza verso lo sviluppo di reti domestiche per il trasporto di segnali di telecomunicazione, multimediali e di controllo.

Giorgio Fioretto
CSELT

LE POESIE DELLA SCIENZA

Michael Guillen

LE CINQUE EQUAZIONI CHE HANNO CAMBIATO IL MONDO

Editore: Longanesi & C.
aprile 1997
pp. 294, L. 30.000

Torniamo indietro negli anni: rivediamo il nostro professore di fisica, nel corso di una lezione, scrivere alla lavagna una nuova equazione, risultato di lunghi anni di ricerca, di tentativi e anche di errori di molti ricercatori vissuti nei secoli scorsi.
Queste espressioni matematiche apprese sui banchi di scuola hanno permesso di conoscere a noi studenti - in maniera semplice e comprensibile - le regole che governano fenomeni della natura assai complessi. Con un linguaggio universale esse, infatti, sintetizzano in una formula - di solito molto stringata - una verità altrettanto universale. Le equazioni traducono quindi, in maniera astratta ma vera, la *voce della natura* e costituiscono in qualche modo le *poesie della scienza.*
Il nostro docente del liceo associava sovente alla nuova espressione anche il nome di uno scienziato; da quel momento Ohm, Lavoisier, Carnot, Volta, Keplero erano legati a quella particolare equazione matematica che entrava a far parte del nostro bagaglio culturale. Poco o nulla però sapevamo sull'ambiente che aveva favorito questa scoperta e sulla personalità degli scienziati.
La lettura di un libro recente di *Michael Guillen* può essere un ausilio per sentire più vive - o meglio meno aride - queste equazioni e per conoscere le persone che le hanno formulate. Dopo aver insegnato per alcuni anni a Harward, l'autore si è dedicato dal 1988 alla divulgazione scientifica. Nel libro *Le cinque equazioni che hanno cambiato il mondo* Guillen sceglie altrettanti scienziati che hanno contribuito a migliorare la conoscenza delle regole, seguite dalla natura, nel governo di alcuni fenomeni che si presentano nell'universo e che, allo stesso tempo, hanno modificato la nostra visione del mondo; queste regole hanno, infatti, consentito applicazioni innovative che hanno portato a significativi cambiamenti della nostra vita quotidiana.
Per rendere il libro di più agevole lettura, Guillen ricorre ad alcune semplificazioni, che in qualche caso compromettono il rigore scientifico del testo; inquadra però le scoperte degli scienziati nell'ambiente culturale in cui essi hanno operato. L'autore del libro ci fa anche conoscere alcuni episodi della vita di questi studiosi che ci chiariscono il contesto in cui essi sono cresciuti e gli stimoli che hanno ricevuto dall'esterno.
Le formule sono in qualche modo così *umanizzate.* Una volta di più, abbiamo la conferma che potenzialità e conoscenze spesso s'intrecciano con episodi casuali vissuti da questi scienziati e - soprattutto - che la competizione rappresenta un elemento chiave per la crescita del sapere.
Il libro è suddiviso in cinque parti, una per ciascuna equazione trattata. Ogni capitolo è articolato secondo uno stesso schema: un *prologo* delinea la personalità dello scienziato attraverso alcuni episodi chiave della sua vita; tre *sezioni* successive (intitolate, rispettivamente, *Veni, Vidi, Vici)* descrivono anzitutto come lo scienziato sia venuto in contatto con il problema; passa poi a descrivere quali erano a quel tempo le difficoltà incontrate per risolvere il problema nell'ambiente in cui esso operava; chiarisce, infine, come egli sia riuscito a venirne a capo, riuscendo a sintetizzarne il risultato in un'equazione di facile lettura.
Nell'ultima sezione, *l'epilogo,* Guillen cerca di legare ogni equazione presentata nel libro alle applicazioni ed ai cambiamenti che da essa sono scaturiti negli anni più recenti: la *legge di gravitazione universale* di Isaac Newton alla discesa dell'uomo sulla luna. La *formula della pressione idrodinamica* di Daniel Bernoulli al volo aereo. L'*espressione dell'induzione elettromagnetica* di Michael Faraday ai motori elettrici. La *teoria della relatività ristretta* di Albert Einstein alla produzione di energia termonucleare.
Il *secondo principio della termodinamica* di Rudolf Clausius (l'autore la definisce "un'esperienza fallimentare") è un caso a parte. Il principio lega la crescita dell'entropia al tempo e ci invita a qualche riflessione: il principio di Clausius è forse uno dei più amari tra quelli che abbiamo appreso a scuola. Ci ricorda, infatti, che nella natura il disordine prevale sull'ordine e che il mondo procede verso un progressivo continuo deterioramento.
La legge si applica naturalmente solo al campo fisico; ma cosa accadrebbe se ad esempio volessimo applicarla a noi stessi? Mark Twain - ci ricorda Guillen - scrisse che *la nostra vita sarebbe infinitamente più felice se fossimo nati avendo ottant'anni e potessimo passo passo avvicinarci ai diciotto.* Purtroppo le leggi della natura sono diverse: avanzando negli anni, il nostro vissuto quotidiano si modifica e le nostre conoscenze continuano progressivamente ad

appannarsi. Come la vista! I processi sono irreversibili e gli oggetti viventi invecchiano e finiscono per morire.
Il secondo principio della termodinamica, meno astratto forse di come può apparire a prima vista, contiene dunque un riferimento al nostro destino: esso è come una sottile poesia velata di malinconia autunnale. Ci tornano a mente i versi *delle primavere* di Orazio (Odi I, 4): *O beate Sesti, vitae summa brevis spem nos vetat inchoare longam*... (O Sestio felice, breve è il cerchio della vita; essa non vuole che si tentino lunghe speranze) o il *Tramonto della luna* di Leopardi: *...orba la notte resta, e cantando, con mesta melodia, l'estremo albor della fuggente luce....*
Sopravvivono a questo destino solo gli Scienziati, assieme ad altri Grandi Protagonisti dell'Umanità; con Orazio potremmo infatti ripetere l'elogio a Castorino (Odi IV, 8): *...Dignum laude virum Musa vetat mori,...* (Al forte che merita la gloria, la poesia impedisce di morire).
Ci piace anche sperare che la conoscenza dell'umanità cresca via via e che la vita, in antitesi con il principio di Clausius, nell'universo migliori con il passare del tempo.
Il libro, scritto in maniera molto semplice e discorsiva, non deve essere considerato un testo scientifico ma piuttosto una piacevole occasione di completamento culturale ed un utile stimolo alla curiosità intellettuale. Esso può essere di ausilio per scoprire come sono nate alcune regole della fisica apprese sui banchi di scuola.
Il libro di Guillen in qualche modo ci fa quindi amare di più queste formule, ce le rende meno astratte e ci consente qualche nuova riflessione sulle radici e sulla evoluzione delle conoscenze dell'umanità.

r.c.

UNA GUIDA NEL DEDALO DELLE INFORMAZIONI

Enzo Pontarollo

L'INDUSTRIA DEGLI APPARATI E DEI SISTEMI PER LE TELECOMUNICAZIONI IN ITALIA

Il Sole 24 ore
ottobre 1998
pp. 335, L. 80.000

Molti di noi sono oggi sommersi dalle informazioni sul futuro prossimo delle telecomunicazioni: è tanta infatti la carta stampata che ci arriva quotidianamente dalle fonti più diverse; con cadenza ravvicinata - quasi mensile - è poi organizzato un convegno, una tavola rotonda, un seminario. Siamo a volte stanchi di sentirci ripetere durante queste presentazioni concetti che - sia pur con piccole varianti - ci sembrano sempre gli stessi: i relatori ci ricordano che siamo già nell'"era" dell'Information & Communication Technology e ci delineano gli sviluppi futuri (mobilità, Internet, larga banda,...). Al termine di questi incontri usciamo con una cartella che contiene stipate cento o più pagine, copie dei trasparenti proiettati nel corso dei convegni. Per un attimo abbiamo l'illusione di conoscere come si prospetta l'evoluzione prossima futura dell'ICT. Dopo qualche giorno però la carta è dimenticata su un tavolo o in un armadio; a noi resta una "nebulosa" sui messaggi ricevuti negli incontri e, in particolare, su come sia possibile capitalizzare nelle realtà in cui operiamo la crescita tecnologica del settore dell'ICT e su quali siano le potenzialità che oggi si offrono per espandere l'offerta dei nuovi servizi. Diventa quindi sempre più faticoso aggiornarsi e rendere fruibile nell'attività quotidiana le indicazioni - scritte o dette - ricevute dalle diverse fonti.
Il libro di Enzo Pontarollo, Professore di economia industriale presso l'Università Cattolica del Sacro Cuore di Milano, costituisce forse un'eccezione. L'autore si è avvalso, nella preparazione del testo, del "contributo di esperienza, conoscenze, informazioni e dati di mercato" fornito dall'Associazione nazionale delle telecomunicazioni dell'ANIE che di recente ha costituito un osservatorio sul mercato e sugli investimenti del comparto più legato alle telecomunicazioni. È stato così redatto un volume che presenta in maniera organica i motori del cambiamento del settore. Nel libro sono anzitutto esaminate le diverse componenti che influenzano l'evoluzione: ricerca e sviluppo, attività di produzione, richieste manifestate o latenti del mercato, servizi offerti. Il testo approfondisce successivamente le esigenze che si presentano oggi nel mercato: la richiesta di disporre di una maggiore velocità nel trasporto dell'informazione per rispondere alle richieste di trasmettere segnali a larga banda; la possibilità di disporre di servizi sempre più complessi ottenuti mediante un'accresciuta intelligenza di rete; la flessibilità nell'impiego dei mezzi di comunicazione resa possibile da sistemi di comunicazione wireless, svincolati dalla localizzazione dei terminali.
L'autore presenta poi un quadro di riferimento del mercato delle telecomunicazioni a livello mondiale, per passare poi a quello europeo e per focalizzarsi infine su quello nazionale. Esamina anche le tendenze evolutive che si sono manifestate negli anni Novanta per costruire dalle previsioni dei cambiamenti i possibili scenari futuri legati: alla crescita sensibile di Internet e della telefonia mobile; alla

convergenza del trasporto di voce, immagine e dati; al consolidamento delle alleanze tra i produttori tradizionali di sistemi di telecomunicazione e quelli del networking (dei costruttori cioè degli apparati che tradizionalmente realizzano le reti informatiche e che, a differenza dei primi, hanno di recente allargato l'offerta passando dal comparto delle reti private a quello delle reti pubbliche).
Enzo Pontarollo sottolinea anche il nuovo ruolo dei costruttori tradizionali di sistemi, che a suo avviso dovrebbe evolvere verso forme di partnering tecnico con i gestori. Con gli operatori nuovi o tradizionali devono essere infatti condivisi successi e rischi in un mercato sempre più competitivo: i tempi per la messa in servizio di nuovi sistemi debbono ridursi e, allo stesso tempo, le soluzioni debbono essere scelte anche nel caso che non diano certezze di ritorni. Dovrebbe essere perciò assunta da entrambi i partner, costruttori e gestori, una parte del rischio imprenditoriale, legato alle scelte innovative.
Un punto del libro meriterebbe forse un maggiore approfondimento: lì dove è suggerito di spostare dai gestori delle reti ai produttori di sistemi una parte delle attività tipiche dei primi; si lascia intendere nel testo che potrebbe (o che sarebbe auspicabile) trasferire ai produttori tutta o parte dell'attività di pianificazione, progettazione e, eventualmente, di gestione della rete. I costruttori di sistemi modificherebbero così il ruolo da essi svolto nella creazione di nuovo valore. Le professionalità presenti presso i gestori, unite al contatto quotidiano con i clienti, potrebbero invece, a parere dello scrivente, rendere difficile il trasferimento di queste conoscenze. Sicché prima di muoversi in tale direzione occorrerebbe valutare con attenzione quanto si guadagnerebbe, con questa decisione, ma soprattutto quanto potrebbe essere perso. Questo però è solo uno spunto per una nuova riflessione dei diversi attori che intervengono in questa attività. Il libro è completato da numerose tabelle che permettono di conoscere il mercato acquisito nei diversi settori delle telecomunicazioni dai produttori maggiori e contiene circa duecento pagine che riportano il profilo di aziende operanti in Italia in questo settore (dati di bilancio, livelli di occupazione, scomposizione del fatturato per settori, distribuzione geografica delle vendite, ...).
La raccolta dei dati è fornita in maniera organica e consente quindi agli interessati di trovare uno spaccato molto chiaro e preciso sull'industria manifatturiera che ha sedi produttive in Italia.
L'insieme di queste informazioni permette di approfondire, anche con dati obiettivi, e quindi di conoscere meglio, l'offerta di sistemi di telecomunicazione disponibile nel nostro Paese.

r.c.

OPPORTUNITÀ DI PERCORSO TRA RETE TLC E CLIENTE

Antonio Sciarappa

APPLICAZIONI PER UTENZA AFFARI

Editore: CSELT
Torino, gennaio 1999
pp. 185, L. 30.000
Distribuzione UTET Libreria

Questo libro appartiene alla Collana, curata da Silvano Giorcelli, che descrive la tecnica ATM (Asynchronous Transfer Mode) e ne identifica i possibili ambiti applicativi. Il volume affronta il tema delle soluzioni applicative per l'utenza business, il cui crescente interesse corre di pari passo con il vorticoso sviluppo tecnologico. In questo settore la crescente disponibilità di banda e di alte velocità trasmissive, insieme allo sviluppo di sistemi d'utente molto evoluti, rendono possibili sviluppi applicativi differenziati e centrati sulle reali necessità dell'utente.
L'obiettivo di questo volume è quello di fornire al lettore una visione d'insieme delle diverse opportunità disponibili, descrivendo l'intero percorso tra l'accesso alla rete e il cliente finale che utilizza e sceglie il servizio.
Al fine di illustrare in modo completo lo stato di maturità delle soluzioni possibili, il testo riporta un numero adeguato di "case study" indicando in particolare la metodologia ed il processo di sviluppo di nuove applicazioni. Queste applicazioni utilizzano un numero limitato di "servizi abilitanti", che combinati tra loro in numero e prestazioni coprono una larga fascia di esigenze applicative dell'utenza business.
L'opera contiene anche una descrizione del laboratorio di sviluppo applicazioni realizzato in CSELT e basato sul tool set denominato SABBIA (Sviluppo di Applicazioni per Broad Band su IP e ATM).
Il libro è principalmente rivolto ai gestori del mondo delle telecomunicazioni, quali tecnici, progettisti, e addetti al marketing, cui può essere di ausilio per ampliarne le conoscenze sul mercato e sulle opportunità di offerte applicative. Esso è inoltre utile ai "network manager" aziendali, ai quali permette la conoscenza della disponibilità di soluzioni basate su tecnologie innovative.
Il libro è infine utile anche in ambito universitario, per la formazione degli studenti di ingegneria delle telecomunicazioni nel settore della realizzazione di soluzioni sistemistiche ed applicative di utente.

Enzo Garetti

I seguenti sommari sono ripresi dai "Rapporti Tecnici CSELT" di ottobre 1998.

G. Argyropoulos, B. Danielsson, U. Johansson, G. Papadopoulos, I. Ruiz de Gauna, G. Salomonsen, M. Spini, T. Tjelta

Prestazioni di errore e indisponibilità di collegamenti in ponte radio in reti SDH: i risultati di un progetto di ricerca

L'articolo riporta alcune soluzioni per il miglioramento della rete *SDH (Synchronous Digital Hierarchy)* sviluppate nell'ambito del Progetto EURESCOM P513, relative alle metodologie di previsione dei valori di *SES (Severely Error Second)* e di *BBE (Background Block Error)*, con riferimento ai vari fenomeni di propagazione tipici dei collegamenti radio. La verifica della validità delle metodologie è stata effettuata tramite confronti con i dati ottenuti da misure su collegamenti SDH. Nell'ambito del progetto sono state anche definite le linee guida per la progettazione di collegamenti radio e per il loro utilizzo in reti SDH.
Alle attività di studio hanno partecipato centri di ricerca per le telecomunicazioni di Grecia, Italia, Norvegia, Spagna e Svezia, che hanno conferito all'attività un approccio squisitamente pan-europeo, con idee e risultati di misure provenienti da fonti diverse.
Queste ricerche hanno permesso di concludere che i collegamenti radio possono essere utilizzati nelle reti SDH e che i nuovi modelli di predizione presentano un notevole grado di confidenza.

Chi desiderasse ricevere copia di questi articoli può rivolgersi direttamente a: Laura CANTAMESSA
CSELT, Via Guglielmo Reiss Romoli, 274
10148 Torino
Tel: 011 - 2285366
Fax: 011 - 2285762
e-mail: laura.cantamessa@cselt.it

A. Cornaglia, E. Leonardi, R. Lo Cigno, M. Meo, F. Neri, R. Santaniello, D. Saracino

I sistemi LMDS: una soluzione possibile per reti di accesso wireless in tecnologia ATM

L'articolo illustra i risultati di uno studio sui sistemi *LMDS (Local Multipoint Distribution Services)* in uno scenario di traffico multi-servizio.
I sistemi LMDS forniscono un accesso radio a larga banda a un nodo centrale da molteplici interfacce d'utente multimediali. Sono disponibili un ampio numero di canali radio suddivisi in intervalli di tempo per l'allocazione di richieste di trasmissione da e verso le interfacce d'utente.
Lo studio suggerisce strategie di allocazione delle risorse per uno scenario di traffico multiservizio e procedure di segnalazione per le interazioni tra il nodo centrale e le interfacce d'utente. Nel lavoro è anche descritto un possibile scenario di traffico, che è stato oggetto di uno studio sulle prestazioni mediante simulazione. I risultati ottenuti provano che il sistema esaminato può servire un numero piuttosto ampio di utenti, con un grado di qualità di servizio soddisfacente.

G. Bertin, M. Mongiardo, B. Piovano, M. Sauvan, A. Verdolini, G. Zarba

Progetto a calcolatore di un trasduttore ortomodale compatto con elevate prestazioni

In questo lavoro sono presentati il progetto e la realizzazione di un trasduttore ortomodale *OMT (OrthoMode Transducer)* meccanicamente molto compatto e con elevate prestazioni elettriche, operante nella banda 17-18,5 GHz. Esso è oggi utilizzato all'interno del compact range di Aerospatiale (Cannes) per effettuare le prove di circuiti per satellite.
Il progetto è stato svolto interamente a calcolatore sviluppando un programma di analisi e di ottimizzazione dedicato. L'accuratezza dell'analisi è garantita dall'impiego congiunto di due metodi modali differenti: il primo basato sulla matrice di scattering generalizzata, il secondo sulla matrice delle ammettenze.

M. Geymonat, D. Ranasinghe

Studi ed esperimenti sulle Interfacce X della TMN per ATM

L'articolo fornisce una panoramica sull'interfaccia fra i Sistemi di Gestione (Sistemi di Supporto alle Operazioni, Operation Support Systems - OSS) appartenenti a diversi gestori e la connessione con gli studi attualmente in corso nel progetto EURESCOM P708, il cui scopo principale è la definizione di soluzioni per la gestione delle prestazioni di reti ATM multi-operatore.
Nelle Raccomandazioni ITU-T relative all'architettura di gestione TMN questa interfaccia gestionale inter-dominio è denominata Interfaccia X.
La rete da gestire è una rete ATM permutata costituita dall'insieme di varie sottoreti ATM gestite dai diversi operatori. Per la gestione di questo tipo di reti che attraversano vari domini, sono state recentemente standardizzate due specifiche da parte di ETSI, relative alle aree di *gestione della configurazione* e di *gestione dei guasti*. Sono in corso ulteriori studi in Europa per affrontare le problematiche di gestione delle aree rimanenti, quali le prestazioni, la contabilizzazione e la sicurezza.

A. Andreetto, G.P. Fici, C. Moiso

Un nuovo approccio per la creazione di servizi di Rete Intelligente

L'articolo presenta un nuovo approccio per la creazione di servizi con l'obiettivo di migliorare le soluzioni oggi realizzate, basate sui *SIB (Service Independent Building block).* Questo approccio consente di soddisfare nuovi requisiti, come la creazione integrata di servizi, la riduzione delle competenze necessarie per introdurre un servizio e delle risorse richieste per sviluppare servizi ritagliati sulle esigenze di singoli clienti. In particolare l'approccio proposto è basato su tre livelli di creazione di servizi, definendo i servizi come composizione di service features (o prestazioni di servizio), e mira a semplificare e rendere più rapida la disponibilità di nuovi servizi rispetto all'approccio basato sull'assemblaggio di SIB.

R. Minerva, C. Moiso, G. Viviani

Il Middleware come fattore chiave per l'integrazione di servizi Internet e Telecom

L'articolo descrive una nuova classe di servizi realizzabile grazie all'integrazione di funzionalità Internet e Telecom. Secondo gli autori la fornitura di questi servizi aprirà nuove opportunità di mercato per i gestori di rete e per i fornitori di servizi. I servizi Internet-Telecom devono soddisfare requisiti contrastanti: alta specializzazione per soddisfare le richieste dei clienti e necessità di riutilizzare componenti ad alta normalizzazione già sviluppate. Questi requisiti possono essere soddisfatti mediante l'introduzione e l'uso nell'infrastruttura di rete di soluzioni basate sul concetto di "Middleware".

F.L. Bellifemine, A. Bonomo, P. Civera, G. Ghigo, M. Lajolo, C. Passerone, A. Sangiovanni Vincentelli

Progettazione concorrente hardware/software per l'elaborazione delle immagini

L'articolo descrive una metodologia di progettazione di applicazioni combinate hardware/software e riporta i risultati ottenuti in un caso particolare preso in esame. Il caso considerato è un sottoinsieme sempre presente in tutti i decodificatori video basati sulla *DCT (Descriptive Cosine Transform)* inversa che comprende quantizzazione inversa, DCT inversa e compensazione del movimento. Scopo dello studio è mettere in evidenza le necessità specifiche di calcolo di algoritmi complessi (rispetto al controllo degli algoritmi dominati) e il relativo impatto sullo sviluppo della metodologia di progettazione concorrente hardware e software.

A. Ciccardi, M. Pagnottelli, P. Parise

L'introduzione di servizi a QoS differenziata nelle reti IP

L'articolo si focalizza sulle problematiche legate all'introduzione di servizi a qualità differenziata in reti *IP (Internet Protocol).* Viene presentato sia l'approccio *IETF (Internet Engineering Task Force)* che si basa sul modello *ISI (Integrated Services in Internet),* sia l'orientamento dei costruttori che propongono soluzioni adatte all'offerta di servizi in ambito geografico (quali, ad esempio, Cisco, Nortel, Newbridge). Partendo da questi concetti di base, la memoria presenta le fasi di un possibile percorso evolutivo che un *ISP (Internet Service Provider)* può intraprendere per incrementare il portafoglio di offerte aggiungendo anche la fornitura di servizi a qualità differenziata.
Sono riportati infine i risultati di una campagna di prove finalizzata alla validazione di un'offerta commerciale per SEA-BONE, il backbone Internet internazionale di Telecom Italia. Il servizio consentirà all'utente di differenziare, secondo criteri definibili dal cliente che accede al servizio, il livello di *QoS (Quality of Service)* all'accesso alla rete.

S. Dogimont, A. Finottello, M. Gandini, P. Garino, M. Gumm, M. Marchisio, F. Mombers, I. Remi

Processore MIMD per la stima del movimento e l'elaborazione di vettori in sistemi di codifica video MPEG-2 di elevata qualità

Nell'articolo è presentato il progetto di un processore *MIMD (Multiple Instruction-stream Multiple Data-stream)* che stima il movimento e effettua altri calcoli a livello di pixel per sistemi di codifica video MPEG-2 di elevata qualità. Caratteristiche peculiari del circuito integrato sono l'utilizzo di un nuovo algoritmo di stima del movimento e di speciali connessioni che permettono la codifica in cascata dei segnali video, rendendo minima così un'ampia fascia di problemi che solitamente si verificano eseguendo questa operazione.