



DENTRO LA SCATOLA

Rubrica a cura di

Fabio A. Schreiber

Dopo aver affrontato negli scorsi anni due argomenti fondanti dell'Informatica – il modo di codificare l'informazione digitale e la concreta possibilità di risolvere problemi mediante gli elaboratori elettronici – con questa terza serie andiamo ad esplorare "Come parlano i calcolatori". La teoria dei linguaggi e la creazione di linguaggi di programmazione hanno accompagnato di pari passo l'evolversi delle architetture di calcolo e di gestione dei dati, permettendo lo sviluppo di applicazioni sempre più complesse, svincolando il programmatore dall'architettura dei sistemi e consentendogli quindi di concentrarsi sull'essenza del problema da risolvere.

Lo sviluppo dell'Informatica distribuita ha comportato la nascita, accanto ai linguaggi per l'interazione tra programmatore e calcolatore, anche di linguaggi per far parlare i calcolatori tra di loro – i protocolli di comunicazione. Inoltre, la necessità di garantire la sicurezza e la privacy delle comunicazioni, ha spinto allo sviluppo di tecniche per "non farsi capire" da terzi, di qui l'applicazione diffusa della crittografia.

Di questo e di altro parleranno le monografie quest'anno, come sempre affidate alla penna (dovrei dire tastiera!) di autori che uniscono una grande autorevolezza scientifica e professionale ad una notevole capacità divulgativa.

I protocolli di comunicazione

Giorgio Ventre

1. INTRODUZIONE

Che questa sia sempre di più l'era dell'informazione è ormai evidente ai limiti del lapa-lissiano. Ed è anche evidente sempre di più che ciò che ha reso l'informazione così centrale rispetto alla nostra attuale società è stata la possibilità di distribuirla e condividerla sempre più liberamente ed efficientemente. Il salto evolutivo non è stato innescato quindi dalla disponibilità dell'informazione per se, ma dagli enormi progressi fatti nella capacità di acquisire, elaborare, memorizzare e comunicare dati nei formati e nelle tipologie più disparate: numeri, testi, immagini, suoni, filmati.

Ovviamente siamo ancora lontani dall'idea di un mercato nel quale la gran parte delle transazioni commerciali saranno relative all'accesso a pagamento a informazioni ed esperienze virtuali¹. Tuttavia, è senz'altro vero che la crescita dell'economia è più rapida e robusta proprio

dove c'è una maggiore diffusione delle tecnologie dell'informazione e della comunicazione². È impressionante vedere come oggi diamo per scontata la velocità e la qualità di interazione tra le persone e le organizzazioni che fino a pochi anni fa sembrava semplicemente impossibile. Le aziende si scambiano complessi documenti nel giro di pochi secondi, le persone comunicano agevolmente in maniera diretta o testuale ovunque si trovino, le merci vengono seguite e rintracciate nei loro spostamenti, gli studenti delle scuole e delle università possono accedere a quantità di informazioni che molto difficilmente potrebbero essere contenute in una sola biblioteca.

Velocità e qualità della comunicazione sono quindi le due parole chiave e anche i due parametri "fisici" con i quali oggi è possibile misurare questo progresso. Velocità, ossia la capacità di connettersi rapidamente e agevolmente con chiunque, ovunque esso sia, scambiando elevate quantità di

¹ Jeremy Rifkin, *The Age of Access: The New Culture of Hypercapitalism*, Tarcher.

² International Telecommunication Union, *Key ICT Indicators*, <http://www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx>

dati. E qualità, ossia la capacità di fornire un contenuto informativo ricco e composito, in grado di dare un'informazione completa, attraverso differenti media, trasmessi rispettandone le differenti proprietà e caratteristiche semantiche.

Tali risultati sono stati ottenuti attraverso un rapido sviluppo tecnologico che ha interessato principalmente due fattori: da un lato i mezzi fisici di comunicazione, ossia i "conduttori" dell'informazione, che sono diventati nel tempo sempre più capienti e affidabili; dall'altro i protocolli di comunicazione, ossia il software che gestisce e controlla la trasmissione sui mezzi fisici e ne garantisce la consegna attraverso complesse infrastrutture.

Se l'evoluzione dei mezzi fisici ha seguito un approccio in fondo prevedibile nella crescita della capacità di trasporto dei dati e nella contemporanea diminuzione degli effetti distorsivi introdotti dai canali fisici (etere, rame, fibra ottica), l'evoluzione dei protocolli ha seguito invece un percorso più complesso, utilizzando approcci spesso lontani da quelle che potevano apparire le soluzioni più ovvie al problema di fondo: come rendere più facile la comunicazione.

2. PIÙ VELOCI O PIÙ INTELLIGENTI?

La comunicazione moderna nasce con la scoperta della possibilità di modulare un segnale elettrico su di un mezzo fisico. Dapprima segnali molto semplici, poi informazioni complesse quali segnali telegrafici multipli e la voce, non appena fu risolto il non semplice problema di come tradurre un segnale sonoro in un segnale elettrico variabile e viceversa. La telefo-

nia è in origine una comunicazione punto-punto su connessioni dirette e solo in un secondo momento si arriva al concetto di rete, ossia di una infrastruttura che consenta la comunicazione tra una molteplicità di utenti non più connessi direttamente tra loro. Nasce una rete quando vengono creati dei nodi di commutazione, ovvero dei sistemi manuali o automatici che consentono di realizzare una momentanea interconnessione esclusiva tra i circuiti che partono da due estremi della rete, secondo un meccanismo definito appunto "commutazione di circuito" (circuit switching). La configurazione dei circuiti oggi avviene automaticamente attraverso l'uso di segnali. Questi segnali rappresentano un esempio di meccanismo di controllo di un sistema di comunicazione: sono il protocollo per controllare la commutazione.

Un protocollo di comunicazione è principalmente l'insieme delle regole che stabiliscono i formati dei dati da scambiare, le procedure di scambio e, se necessario, i meccanismi per attivare, monitorare e terminare l'interazione tra le entità che comunicano. Nella figura 1, è riportato un automa a stati finiti semplificato relativo alle azioni legate alla creazione di una connessione telefonica così come visto dalla centrale del chiamante. Gli automi sono un eccellente strumento per la definizione e lo studio dei protocolli: in questo esempio sono riportati gli stati dello switch e, in **grassetto**, le azioni effettuate dalla rete mentre in *corsivo sottolineato* sono riportate le azioni effettuate dagli utenti (chiamante e ricevente).

La nascita dei primi calcolatori digitali ha portato ovviamente ad una radicale trasformazione delle architetture di comunicazione. In primo luogo, perché ha visto la nascita di una nuova tipologia di "utenti" della comunicazione, ossia gli stessi computer e le relative applicazioni. In secondo luogo, perché ha introdotto una nuova famiglia di tecnologie che ha modificato fortemente il modo stesso di progettare e realizzare le reti ed i relativi elementi.

Per quanto riguarda il primo aspetto, ossia la nascita di una nuova tipologia di servizi ed utenti, è evidente che una cosa è progettare una rete per trasmettere la voce, ed un'altra è progettare per la trasmissione dati tra calcolatori. I calcolatori non comunicano come gli esseri umani: le loro applicazioni prevedono, o meglio prevedevano in origine, una comunicazione asincrona di dati atomici quali numeri, informazioni testuali, o file.

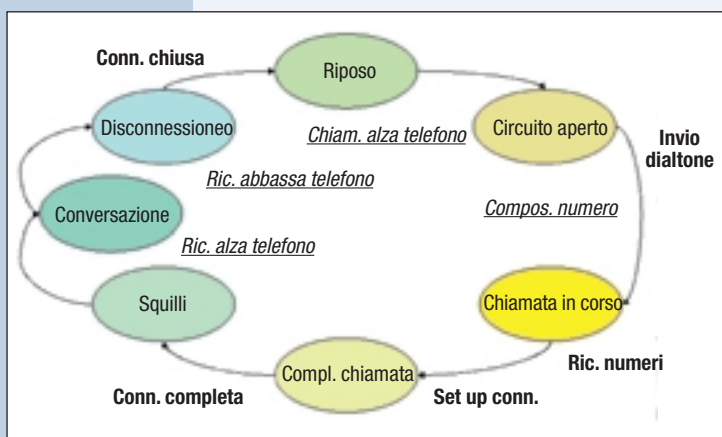


FIGURA 1

Automa a stati finiti semplificato di una conversazione telefonica

Una comunicazione in genere direttamente controllata da un utente umano, che procedeva secondo un meccanismo ripetitivo del tipo: richiesta, attesa della risposta, sua interpretazione, ulteriore richiesta ecc.. Il tutto con tempi molto differenti da quelli classici che caratterizzano il comportamento di due utenti umani a telefono. Questo approccio alla comunicazione è quindi caratterizzato dall'uso discontinuo della infrastruttura di comunicazione, ed è stato naturale quindi, nel cercare differenti meccanismi di comunicazione per progettare le basi delle reti adatte a tali nuove tipologie di servizi, fare riferimento ad un meccanismo di comunicazione asincrono ben noto: quello della Posta.

In un sistema postale, l'infrastruttura di comunicazione (uffici postali, mezzi di trasporto e consegna, intelligenza di smistamento) è condivisa da tutti i dati che vengono inoltrati attraverso di essa in un determinato istante di tempo su un itinerario comune. Presupposto per questa condivisione è ovviamente la possibilità di identificare i vari atomi di informazione attraverso il destinatario (in modo da non confondere le informazioni destinate a utenti differenti) e la possibilità di eseguire su ogni dato una azione di instradamento differenziato.

Nel mondo della comunicazione "digitale", al posto di lettere si inviano quanti di informazione, definibili "pacchetti", e siamo quindi di fronte ad una rete dove nei nodi non si creano circuiti, ma si effettua una **commutazione di pacchetto** (packet switching). La condizione tecnologica necessaria per poter seguire questo approccio è quella di poter avere nei nodi la possibilità di immagazzinare i dati di passaggio, al fine di poter procedere ad una loro lettura per decidere il corretto inoltramento ad un successivo elemento della rete, fino alla consegna finale. Un nodo di rete deve quindi accodare i dati in ingresso dalle connessioni per decidere sulla base dell'indirizzo di destinazione su quali connessioni in uscita inviarla, secondo un meccanismo definito "store and forward".

È quindi chiaro che stiamo parlando di reti i cui nodi non sono più degli "incroci" di connessioni ma sono macchine in grado di memorizzare i dati, eseguire su di essi delle operazioni di analisi ed elaborazione, e di inoltrarli secondo strategie definite in maniera dinamica tra i nodi stessi della rete. Stiamo quindi parlando di moderni calcolatori, ed in effetti uno dei primi nodi

di commutazione di pacchetti fu un minicomputer Honeywell DDP-516 modificato per la sua installazione sul prototipo di rete ARPANET.

Un aspetto sorprendente è il fatto che, nella commutazione di circuito, l'informazione viaggia ad una velocità prossima a quella della luce, mentre nella commutazione di pacchetto, l'informazione viene elaborata, immagazzinata in ogni nodo di commutazione e quindi rallentata nel suo flusso dal mittente al destinatario. Tuttavia la modellistica matematica ci ha aiutato a capire che sistemi di questo tipo sono estremamente efficienti³ e in grado di garantire la possibilità di adattarsi alle differenti esigenze del traffico trasportato e alle condizioni della rete. In poche parole, nell'evoluzione delle reti di comunicazione, si è barattata la velocità con l'intelligenza, a tutto vantaggio della flessibilità.

Il passaggio dalla semplice configurazione dei circuiti all'inoltramento differenziato e coordinato dei pacchetti impone però un costo: lo sviluppo di meccanismi di controllo e di cooperazione (tra i nodi di rete e tra questi e i terminali) ben più complessi di quelli richiesti dalle reti a commutazione di circuito. Occorre cioè sviluppare protocolli più complessi, caratterizzati da funzioni differenti: come la comunicazione affidabile tra un nodo e un nodo vicino, o come la gestione dell'instradamento dei dati attraverso l'intera rete, oppure come la definizione di un meccanismo globale di indirizzamento.

Per esempio, il protocollo IP che è alla base del funzionamento di internet ha il compito di gestire l'inoltramento dei dati da un terminale trasmittente a uno o più terminali destinazione, passando attraverso i nodi e le connessioni della rete. Per fare questo, il protocollo definisce un meccanismo di indirizzamento dei nodi e dei terminali, una politica di servizio dei pacchetti da parte dei nodi e un formato del pacchetto. Il formato prevede che ogni pacchetto sia diviso in una parte contenente informazioni di servizio (dati di identificazione, meccanismi di verifica di eventuale corruzioni in questa parte, informazioni per la frammentazione dei dati in blocchi di dimensione più piccola) e una parte che contiene il carico utile o *payload*. IP si occupa del trasporto dei pacchetti, ma è supportato da una famiglia di protocolli "ancillari" per lo

³ L. Kleinrock, *Queueing Systems*, Wiley Interscience, New York, 1975.

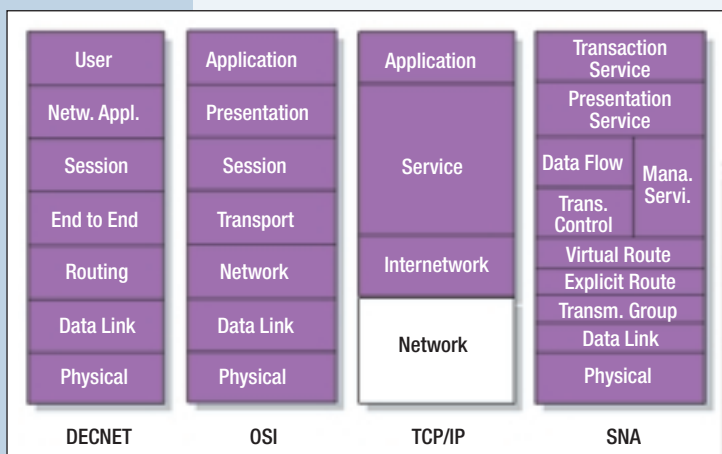


FIGURA 2
 Protocolli per reti
 a commutazione
 di pacchetto

svolgimento di azioni di supporto e gestione quali il controllo dell'instradamento dei pacchetti e la verifica dello stato dei nodi di rete.

Nella figura 2 sono riportate differenti architetture protocollari per reti a commutazione di pacchetto sviluppate nel corso degli anni. A soluzioni proprietarie (SNA proposta da parte di IBM, DECNET dalla Digital Equipment Corp.) si sono affiancate nel tempo architetture di rete definite per favorire l'interoperabilità, seguendo schemi di standardizzazione "de iure" (architettura OSI) o "de facto" (architettura TCP/IP).

Da questa figura emergono evidenti le forti similitudini tra le differenti proposte: innanzitutto la strutturazione a livelli delle architetture, con attribuzione di specifiche funzioni ad ogni livello e con la possibilità di implementare tali funzioni all'interno di ogni livello in maniera indipendente dalle implementazioni negli altri livelli. Tale struttura garantisce estrema flessibilità nello sviluppo, ma impone la definizione di interfacce standardizzate tra i livelli adiacenti. Un esempio di tale filosofia di progettazione può essere trovato proprio nell'architettura IP che addirittura non prevede gli strati responsabili per la gestione della comunicazione fisica (livello fisico) e per la connessione diretta tra i nodi di rete (livello data-link) e si limita semplicemente alla definizione di una interfaccia verso altre architetture di rete in grado di offrire tali strati.

3. DALLA CONNETTIVITÀ ALLA QUALITÀ DEL SERVIZIO

Al di là delle differenze tra le singole implementazioni, le architetture nella figura 1 sono accomunate dal fatto di essere state progettate per l'i-

noltro efficiente di "messaggi", rendendole quindi poco idonee all'inoltro di dati "continui" ossia di sequenze sincrone di dati, specialmente quando queste sequenze devono essere trasmesse rispettando precisi requisiti di qualità quali limiti nei ritardi di comunicazione o nella perdita di pacchetti. Infatti, se al fine di aumentare la flessibilità e la robustezza di una rete, si ammette che un nodo di commutazione di pacchetti possa gestire in maniera differente pacchetti che in realtà hanno le stesse caratteristiche (origine, destinazione e tipologia di dato), corro il rischio che i dati vengano consegnati alla destinazione con livelli di qualità differenti, in termini di ritardo, di sua variazione, e di percentuale di perdite. Occorre tuttavia chiarire che in realtà, la maggiore disponibilità su internet di reti a banda media e larga rende oggi già possibile la trasmissione di semplici dati isocroni (audio, video a bassa risoluzione) a qualità medio-bassa.

Pertanto, per la trasmissione di dati strutturati su flussi quali suoni o video, occorre aggiungere a queste architetture la possibilità di identificare tali flussi e di differenziarne il trattamento in funzione delle caratteristiche dei media trasportati quali per esempio la banda media o di picco, facendo in modo che i dati appartenenti allo stesso flusso siano trattati dalla rete in maniera analoga e predeterminata. Ciò richiede però che all'interno dei nodi di rete sia possibile discriminare il trattamento dei dati attraverso l'uso di schemi di schedulazione preferenziale del traffico e attraverso la conservazione di informazioni sullo stato di questi flussi. Inoltre richiede che i nodi siano in grado di sviluppare algoritmi di instradamento più complessi, con obiettivi di ottimizzazione di tipo multidimensionale sui parametri di misura della qualità.

Occorre quindi passare dai meccanismi di commutazione di pacchetto a meccanismi di **commutazione di flusso**, nei quali alla rete è affidato il compito di gestire le risorse disponibili (capacità dei link, memoria e potenza di schedulazione dei nodi) e di attribuirle ai differenti flussi sulla base delle loro esigenze e della definizione di specifici livelli di servizio. La rete diventa così in grado di offrire diverse tipologie di trasporto alle differenti tipologie di applicazioni, quali servizi isocroni per la telefonia, servizi di comunicazione real-time per applicazioni multimediali o di tele-controllo, servizi ad alta affidabilità per applicazioni di tipo transazionale; imponendo però

un incremento elevatissimo della complessità e del corrispondente costo per l'intera architettura di rete: nodi, terminali, software.

Il secondo approccio potrebbe essere definito di "forza bruta" ed è basato sulla considerazione che il problema della gestione a qualità garantita di flussi di dati può essere risolto semplicemente attraverso il **sovradimensionamento** (*overprovisioning*) delle infrastrutture di rete, sfruttando la sempre maggiore diffusione delle fibre ottiche e la loro elevatissima capacità di trasporto. Purtroppo, la storia delle tecnologie dell'informazione ci insegna che un tale approccio sia vincente solo su un orizzonte temporale breve e comunque a fronte di costi e di inefficienze molto elevati. Inoltre la crescita della domanda di connettività legata a servizi a larga banda quali l'**IPTV** (ossia il broadcasting televisivo su protocollo IP) e i limiti di capacità di trasporto presenti nelle tecnologie di rete di accesso, ossia quelle che consentono la copertura dell'ultimo tratto di rete verso il terminale dell'utente, rendono comunque necessaria l'adozione di strategie di gestione efficiente ed ottimizzata delle risorse.

4. LA CREAZIONE DINAMICA DEI SERVIZI

Quale è lo sviluppo ipotizzabile per le reti di comunicazione e in particolare per i protocolli che le controllano? Anche se risulta difficile azzardare ipotesi in uno scenario che si è dimostrato essere estremamente variabile e incerto, si possono qui identificare dei trend che dovrebbero continuare a contraddistinguere l'evoluzione delle architetture e dei servizi di rete.

Un primo fattore caratterizzante è certamente lo spostamento di alcuni servizi dagli estremi di una rete (terminali e server) al suo interno. Negli ultimi anni sono emerse infatti numerose tipologie di servizi che sono stati sviluppati per essere localizzati su nodi della rete. Esempi di questo approccio sono tutti i servizi legati alla sicurezza delle reti, quali i firewall e i sistemi di prevenzione e di rilevamento delle intrusioni informatiche. In questo caso il posizionamento all'interno della rete piuttosto che ai suoi margini rafforza la capacità di azione e di controllo di questi sistemi.

Un altro esempio di questo tipo è rappresentato dai sistemi di *web-caching* e di *content delivery*, che sono sistemi che tendono a replicare il contenuto informativo di servizi web o multimediali su

architetture distribuite di archiviazione, al fine di consentire da un lato il decongestionamento dei server principali e dall'altro una maggiore vicinanza dell'informazione al terminale dell'utente. Purtroppo lo sviluppo di servizi ispirati a tale filosofia è avvenuto in maniera incontrollata, senza cioè la definizione di standard condivisi e senza una corretta analisi delle conseguenze che tale approccio avrebbe potuto avere sul classico modello di internet, dove al contrario l'ipotesi di fondo è di avere una rete tendenzialmente agnostica rispetto ai servizi che vengono su di essa ospitati. È quindi evidente che le future architetture protocollari dovranno prendere atto di tale tendenza e dovranno renderla compatibile con un disegno organico delle funzionalità di rete e della loro localizzazione.

Un secondo fattore è l'adozione della tecnologia IP come base per lo sviluppo di architetture di rete in grado di offrire servizi di comunicazione sia dati, sia voce che TV, secondo il paradigma comunemente indicato come *triple-play*, o anche *quadruple play* nel caso di inclusione di servizi di tipo mobile. Seguendo cammini differenti, i Telecom operator sono ormai in grado di offrire ai propri clienti un portfolio completo di servizi, adottando tecnologie di rete differenti ma utilizzando i protocolli della famiglia IP come vero e proprio *middleware* di comunicazione e di controllo. Molto interessante è per esempio lo sviluppo delle tecnologie alla base della telefonia su reti IP, definite anche come tecnologie **VoIP** (*Voice over IP*). Il protocollo alla base di questo tipo di servizio è **SIP** (*Session Initiation Protocol*)⁴, definito alla fine degli anni '90 come un protocollo di segnalazione a livello applicativo per consentire il controllo di servizi di comunicazione video e audio su reti IP. Si tratta di un protocollo estremamente semplice, totalmente indipendente dalla architettura di rete sottostante e di tipo testuale. SIP è in grado di offrire funzionalità simili a quelle realizzate dai ben più complessi protocolli di segnalazione delle reti telefoniche, anche se con un approccio totalmente diverso che richiede la presenza di intelligenza distribuita sia nella rete che nei terminali.

Lo scenario evolutivo vede oggi SIP come il candidato più forte per rappresentare la base dei protocolli di segnalazione delle future reti ba-

⁴ SIP: Session Initiation Protocol, RFC 3261, reperibile su <http://tools.ietf.org/html/rfc3261>

sate sull'architettura **IMS** (*IP Multimedia Subsystem*)⁵, seguendo quindi una filosofia di progettazione che vede sempre di più le reti di comunicazione basate su architetture hardware aperte e di tipo **COTS** (*Commercial off the Shelf*), ad elevato livello di programmabilità e di riconfigurabilità, e in grado di ospitare servizi sviluppati anche da terze parti.

Non a caso l'architettura IMS prevede la presenza nella rete di differenti server, dei quali alcuni destinati alle funzioni centrali dell'architettura, altri invece destinati ad ospitare servizi ideati e attivati da terze parti per l'offerta di nuove applicazioni. L'idea è quella di rendere disponibili i servizi comuni (come ad esempio l'autenticazione, la tariffazione o il routing) a tutti i servizi a valore aggiunto che vengono resi via via disponibili da terze parti. In questo modo gli sviluppatori di nuove applicazioni potranno concentrarsi sulla logica di tali nuovi servizi, evitando di dovere re-implementare funzioni tradizionali. Si tratta quindi di una evoluzione importantissima per il mondo delle telecomunicazioni, nella quale diventa centrale non più il possesso dell'infrastruttura, ma la possibilità di creare dinamicamente nuovi "prodotti".

⁵ G. Camarillo e M.-A. García-Martín, *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*, John Wiley & Sons, 2006.

È la nascita di un mercato completamente aperto a offerte in concorrenza, dove l'infrastruttura diventa utilizzabile anche da operatori "overlay" che pur operando solo al di sopra della rete, sono in grado di usarla per vendere le loro nuove applicazioni, analogamente a quanto accade oggi in internet.

5. CONCLUSIONI

La storia delle reti di telecomunicazione appare, come spesso accade nell'ICT, una continua rincorsa tra tecnologie di trasporto fisico sempre più efficienti, processori sempre più potenti e applicazioni sempre più esigenti. I nuovi sviluppi tecnologici tuttavia sembrano avere spostato l'attenzione dalle infrastrutture di rete ai servizi che esse devono ospitare. Il possesso di connettività deve essere quindi integrato dall'esistenza di un'architettura di protocolli che consenta la creazione dinamica di nuovi servizi e la loro offerta in un mercato "rete" completamente aperto. Tuttavia, per fare ciò, è necessario che i futuri progettisti di servizi telematici siano in grado di avere sotto controllo le componenti sia hardware che software. Da un punto di vista culturale, ciò richiede sempre più la nascita di profili professionali ad ampio spettro, in grado cioè di gestire agevolmente sia le competenze tipiche dell'Informatica sia quelle caratterizzanti le Telecomunicazioni.

GIORGIO VENTRE è professore ordinario di Reti di Calcolatori presso l'Università di Napoli Federico II e presidente del Consorzio Campano di Ricerca per l'Informatica e l'Automazione Industriale. È autore di circa 200 pubblicazioni scientifiche ed è Area Editor di *Computer Networks*. Con il suo gruppo di ricerca ha partecipato a numerosi progetti di ricerca nazionali ed internazionali ed è stato tra i fondatori del Laboratorio Nazionale per l'Informatica e la Telematica Multimediali del Consorzio Interuniversitario Nazionale per l'Informatica (CINI). Le sue attività di ricerca sono relative alle architetture ed ai servizi di rete, con particolare attenzione agli aspetti di gestione della Qualità del Servizio ed alle tecnologie di Network Control e Management.
E-mail: giorgio@unina.it