IPv6, la nuova versione del protocollo Internet

FRANCESCO IUSO

"Internet sta diventando vittima del suo successo". Questa è l'espressione ricorrente con cui gli addetti ai lavori cercano di sintetizzare la fase che sta attraversando Internet. Il possibile esaurimento degli indirizzi, la necessità di adeguare l'organizzazione dell'instradamento alla dimensione planetaria della rete, le esigenze di qualità e di sicurezza conseguenti all'impiego commerciale di Internet, stanno alla base della definizione della nuova versione del protocollo IP (Internet Protocol), denominata IPv6 (Internet Protocol version 6). La nuova versione del protocollo non stravolge i criteri generali su cui si basa Internet, ma mantiene una eredità molto importante: la semplicità. Essa costituisce una razionalizzazione delle funzionalità già sviluppate, una loro "traslazione" in base alle nuove e mutate esigenze.

In questo articolo sono illustrate le motivazioni che hanno spinto verso la definizione e lo sviluppo di una nuova versione dei protocolli della famiglia TCP (Transmission Control Protocol)/IP e quindi sono descritte le caratteristiche principali della nuova versione del protocollo IP.

1. Perché IPv6

I tassi di sviluppo della rete Internet registrati negli ultimi tempi portano a far prevedere che fra poco più di una decina di anni il numero di utenze della rete potrebbe raggiungere quello dell'intera popolazione sulla terra. Tale scenario viene ipotizzato considerando che una medesima persona potrà avere più di un accesso e che alla rete saranno collegati non solo computer, ma anche nuovi dispositivi, nati dall'integrazione degli elaboratori palmari con le tecnologie cellulari, o addirittura apparecchi domestici come il televisore o i sistemi di riproduzione in alta fedeltà. È previsto dunque un impiego della rete Internet per tutte le necessità di telecomunicazione, compreso il telecontrollo di ogni tipo di dispositivo.

Lo spazio di indirizzamento previsto dall'attuale versione del protocollo IP - indicata con *IPv4 (Internet Protocol version 4)* - è a 32 bit e potrebbe rivelarsi non adeguato per soddisfare le esigenze ipotizzate tenendo conto della limitata efficienza nell'impiego degli indirizzi, come messo in luce nello studio di Huitema [1].

Sono presenti tuttavia altri fattori da considerare: IPv4 offre un servizio best effort e gli aspetti di sicurezza sono curati da funzionalità di differente livello protocollare, quali, ad esempio, i firewall, la crittografia a livello applicativo. Queste caratteristiche, che sono state finora i punti di forza del protocollo perché alla base della sua semplicità, si stanno trasformando in serie limitazioni per l'impiego in un contesto pubblico.

L'impiego commerciale di Internet richiede che vengano attuate nuove e sofisticate politiche amministrative, di controllo e di sicurezza, sia nell'accesso alla rete, sia nel trasporto dell'informazione. Il modello di servizio deve includere la qualità come elemento fondamentale per poter esigere un corrispettivo economico; d'altra parte gli aspetti di sicurezza sono indispensabili per le transazioni commerciali in rete.

Non possono essere poi trascurati gli aspetti di mobilità, specie se si pensa di voler consentire non solo la mobilità personale e dei terminali ma anche di installare reti Internet su mezzi quali ad esempio le navi, gli aerei, le stazioni spaziali. I problemi di instradamento che ne conseguono si preannunciano piuttosto complessi in quanto devono essere gestiti cambiamenti dinamici, anche profondi, nella topologia della rete.

Alla luce di questi scenari, il gruppo *IETF (Internet Engineering Task Force)*, che si occupa di specificare gli aspetti tecnici di Internet, ha definito i criteri per il nuovo protocollo IP fin dal 1992, arrivando nel 1994 alla definizione della cosiddetta "versione 6" di IP - IPv6 [2]. Da allora sono state prodotte numerose specifiche tecniche e il lavoro di specifica è tuttora in corso. È stata inoltre realizzata una rete sperimentale IPv6, sovrapposta a Internet e denominata "6bone", per verificare l'interoperabilità delle nuove realizzazioni e gli aspetti tecnici della nuova tecnologia.

2. Caratteristiche del protocollo IPv6

La nuova versione del protocollo non si discosta sostanzialmente da quella precedente, ma riorganizza e razionalizza le funzionalità in essa presenti, operando così una "traslazione" delle funzionalità piuttosto che una revisione radicale.

Gli specificatori hanno infatti riconosciuto che il successo di Internet deve essere attribuito anche al protocollo IP e, in particolare, ad una sua caratteristica peculiare: la semplicità.

Essi hanno quindi preferito mantenere la vecchia struttura di IPv4, ampliare lo spazio di indirizzamento e procedere con una operazione di miglioramento generale in base alle esperienze maturate sul campo, piuttosto che cercare di recepire tutte le esigenze manifestate dagli utenti della rete e riscrivere un nuovo protocollo a scapito della sua semplicità.

IPv6 offre un servizio di trasferimento a pacchetto senza connessione, in modo indipendente dal mezzo fisico e le sue principali novità rispetto a IPv4 possono essere così elencate:

- struttura dell'intestazione dei pacchetti più semplice e flessibile;
- spazio di indirizzamento più esteso;
- meccanismi per la gestione del traffico in tempo reale;
- meccanismi per garantire la sicurezza.

Il formato dell'intestazione del pacchetto ha una lunghezza doppia (40 byte senza opzioni) rispetto a IPv4, e contiene campi per gli indirizzi sorgente e destinazione quattro volte più lunghi: si passa infatti da 32 a 128 bit per indirizzo. Il formato del pacchetto è mostrato in figura 1.

In essa sono riportate le tre parti principali [3] che costituiscono il pacchetto:

- una intestazione di 40 byte contenente gli indirizzi sorgente e destinazione, l'identificatore del flusso dati, la lunghezza del pacchetto, l'indicazione di altre intestazioni opzionali e il numero di nodi attraversati;
- una o più intestazioni opzionali *(Extension Header)* per le funzionalità opzionali, quali ad esempio l'autenticazione, la crittografia, la frammentazione, l'instradamento determinato dalla sorgente *(source routing);*
- il campo Dati Utente *(Payload),* contenente i dati dell'utente.

CARATTERISTICHE PRINCIPALI DI IPv6

Scalabilità

IPv6 prevede indirizzi di lunghezza 128 bit, quattro volte maggiore di quello della versione attuale.

Ottimizzazione

La struttura del protocollo IPv6 è semplice e flessibile, in quanto sono eliminati gli aspetti minori e obsoleti di IPv4: l'intestazione dei pacchetti ha un formato fisso; è rimosso il controllo d'errore sull'intestazione *(header checksum)* ed è rimossa la procedura di segmentazione a rimbalzo da un router al successivo. La struttura dell'intestazione del pacchetto è ottimizzata per essere elaborata dalle macchine di nuova generazione e la lunghezza dell'intestazione del pacchetto è doppia rispetto alla versione precedente, pur contenendo indirizzi quattro volte più lunghi. Il meccanismo delle funzionalità opzionali è stato completamente rivisto ed è stato studiato nell'ottica di ottimizzare l'elaborazione dei pacchetti.

Qualità

Il protocollo offre un miglior supporto per il trattamento del traffico in tempo reale e per il conseguimento della qualità, in quanto prevede nell'intestazione un campo specifico per l'identificazione del flusso a cui appartiene il pacchetto. In questo modo i router della rete possono riconoscere agevolmente a quale flusso appartiene ciascun pacchetto.

Sicurezza

IPv6 include funzioni per la sicurezza nella specifica di base: prevede l'autenticazione del mittente e la crittografia dei pacchetti.

Plug & Play

Sono previsti meccanismi di autoconfigurazione, mediante i quali le macchine possono ad esempio determinare il proprio indirizzo IP.

Routing

Si introduce la gerarchia quale garanzia per la scalabilità e sono predisposti meccanismi relativi all'instradamento determinato dalla sorgente *(source routing)* e alla mobilità.

Dalla figura 1 si osserva che nell'intestazione non è presente alcuna forma di controllo di errore del pacchetto. Questa scelta non pregiudica lo scambio di informazioni tra sorgente e destinazione: se necessario l'architettura di rete prevede infatti nei terminali meccanismi sufficientemente robusti da recuperare eventuali errori casuali che possono presentarsi nel trasferimento delle informazioni attraverso la rete. Questi errori sporadici non possono causare situazioni critiche.

Viceversa malfunzioni a livello fisico o di collegamento, che sono causa di errori sistematici nel trasferimento delle informazioni attraverso la rete, sono rilevati di solito dai sistemi di gestione o sono fronteggiati da specifici protocolli dei livelli inferiori ad IP. Non è stato perciò ritenuto necessario appesantire il protocollo IP con ulteriori verifiche di integrità dei dati a livello di pacchetto.

2.1 Il concetto di flusso

In IPv6 è stato esplicitamente introdotto il concetto di flusso, inteso come sequenza di pacchetti che hanno parametri in comune, quali ad esempio gli indirizzi sorgente e destinazione, le caratteristiche di autorizzazione e accounting o quelle della qualità richiesta.

L'appartenenza di un pacchetto ad uno specifico flusso può essere facilmente indicata per mezzo di una apposita etichetta - il campo Etichetta di Flusso *(Flow Label)* - presente nell'intestazione. Una volta che i pacchetti sono riconosciuti appartenenti ad uno specifico flusso, questi possono essere opportunamente trattati nei nodi della rete, ad esempio con un sistema di code a priorità in accordo con quanto indicato nel campo priorità. La definizione delle classi con la relativa codifica del campo Priorità *(Priority)* e la definizione delle modalità di impiego del campo Etichetta di Flusso all'interno di una architettura di rete capace di erogare servizi con qualità è tuttora oggetto di discussione.

2.2 Lunghezza dei pacchetti

La lunghezza dei dati di utente trasportati è indicata nel campo Lunghezza dei Dati di Utente *(Payload Length)* di 16 bit e l'unità di misura è il byte. La lunghezza massima dei dati utente indicata nell'intestazione del pacchetto è dunque pari a 64 kbyte, ma la effettiva lunghezza massima del pacchetto è limitata dalla capacità di trasporto della rete fisica (ad esempio nelle reti Ethernet essa è di 1500 byte).

Sono previsti nel protocollo meccanismi opzionali che consentono di indicare dimensioni superiori a 64 kbyte. Questi meccanismi sono necessari per il trasferimento di pacchetti di dimensioni eccezionali, denominati Jumbogram [7], scambiati ad esempio dai "supercomputer" interconnessi da particolari reti ad alta velocità. Una delle applicazioni tipiche di queste infrastrutture è il supercalcolo distribuito.

2.3 Diametro della rete

Il campo Massimo Numero di Salti *(Hop Limit)* contiene il numero massimo di router che il pacchetto può attraversare prima di giungere a destinazione.

Esso è stato introdotto principalmente per motivi di robustezza e affidabilità, in quanto evita che in caso di loop accidentali nell'instradamento i pacchetti permangano in rete indefinitamente.

Sono possibili altri impieghi: nelle trasmissioni multicast, la limitazione del numero di router attraversabili significa definire la regione della rete all'interno della quale possono essere allocati i ricevitori del traffico multicast. In questi casi il campo Hop Limit definisce il diametro della rete.

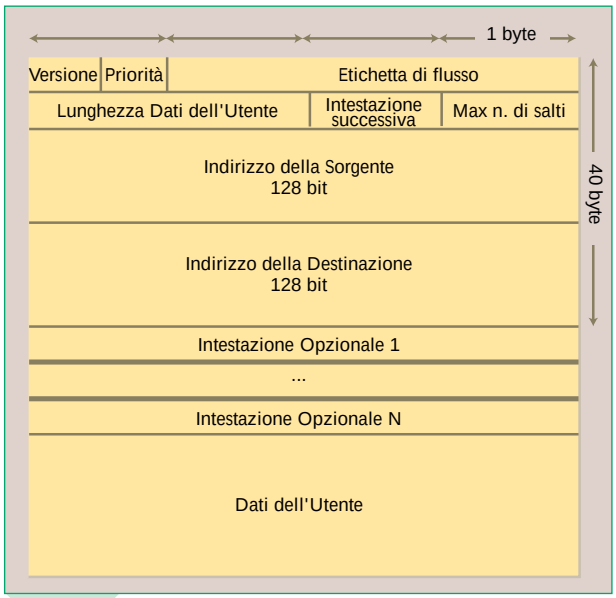

Figura 1 *Formato del pacchetto IPv6.*

2.4 Funzionalità opzionali

La struttura dell'intestazione del pacchetto risulta molto semplificata: sono state infatti mantenute solo le funzionalità ritenute essenziali mentre sono state eliminate o rese opzionali le altre.

In IPv6 le funzionalità opzionali sono espresse in intestazioni separate [3], denominate Intestazioni Opzionali *(Extension Header)*: la lunghezza di queste intestazioni è multipla di 8 byte e la loro presenza è opzionale come le funzionalità che abilitano. Questa circostanza consente di ottimizzare l'elaborazione dei pacchetti nei router in quanto l'elaborazione delle Intestazioni Opzionali in essi avviene solo quando essa è necessaria; se non è richiesto diversamente il router può svolgere le funzionalità di inoltro dei pacchetti senza tenere alcun conto delle Intestazioni Opzionali. La maggior parte delle Intestazioni Opzionali è esaminata solo dalla destinazione finale.

In figura 2 è mostrato un pacchetto IP con alcune Intestazioni Opzionali [5, 6]. Nella figura è evidenziata la struttura generale delle intestazioni opzionali, che prevede la presenza di un puntatore alla intestazione successiva nel campo intestazione successiva, l'indicazione della lunghezza della intestazione nel campo lunghezza (ad eccezione della intestazione per la frammentazione, la cui lunghezza non è variabile) e

i dati richiesti dalle funzionalità abilitate.

Diverse sono le funzionalità previste e la loro presenza, opzionale, nel pacchetto deve rispettare un certo ordine, che è stato seguito nel riportare la descrizione delle funzionalità:

- *Hop-by-hop Option header* è impiegato per trasportare informazioni opzionali che devono essere esaminate da tutti i nodi attraversati lungo il cammino verso la destinazione finale. L'esempio più significativo è il *Jumbo Payload* [7]: la sorgente può inviare pacchetti di lunghezza superiore a 64 kbyte indicando l'effettiva lunghezza del pacchetto nell'intestazione opzionale. La capacità di trasporto della rete, indicata con il nome di *MTU (Maximum Transfer Unit)*, deve naturalmente permetterlo;
- *Routing header* contiene informazioni sul percorso che il pacchetto dovrà effettuare per raggiungere la destinazione finale (ad esempio *Source Routing);*
- *Fragmentation header* è impiegato dalle sorgenti per inviare pacchetti di dimensione superiore alla capacità di trasporto della rete. In questi casi la sorgente deve suddividere il pacchetto in segmenti di lunghezza adeguata alla MTU della rete [8]. Per la corretta ricostruzione del pacchetto quando giunge a destinazione sono necessarie informazioni come l'ordine di sequenza e la fine della sequenza dei segmenti. Queste informazioni sono inserite dalla sorgente nell'intestazione opzionale. La segmentazione e la ricostruzione dei pacchetti sono gestite esclusivamente dalla sorgente e dalla destinazione, ma non dai router;
- *Authentication header* consente alla destinazione di verificare l'autenticità dell'indirizzo sorgente e la non alterazione del pacchetto lungo il percorso;
- *Encrypted security payload header* consente di garantire riservatezza nello scambio di informazioni mediante l'impiego della crittografia. Sono previsti meccanismi per il trasporto sia di un intero pacchetto IP crittografato sia dei soli dati utente crittografati. I meccanismi di gestione delle chiavi e la definizione degli algoritmi di crittografia sono ancora oggetto di studio da parte della IETF;
- *Destination options header* serve per il trasporto di informazioni opzionali che devono essere elaborate solo dal nodo di destinazione.

Il meccanismo delle intestazioni opzionali garantisce, come evidenziato in [6], la flessibilità di aggiungere ulteriori funzionalità al protocollo attraverso la definizione di nuove intestazioni opzionali.

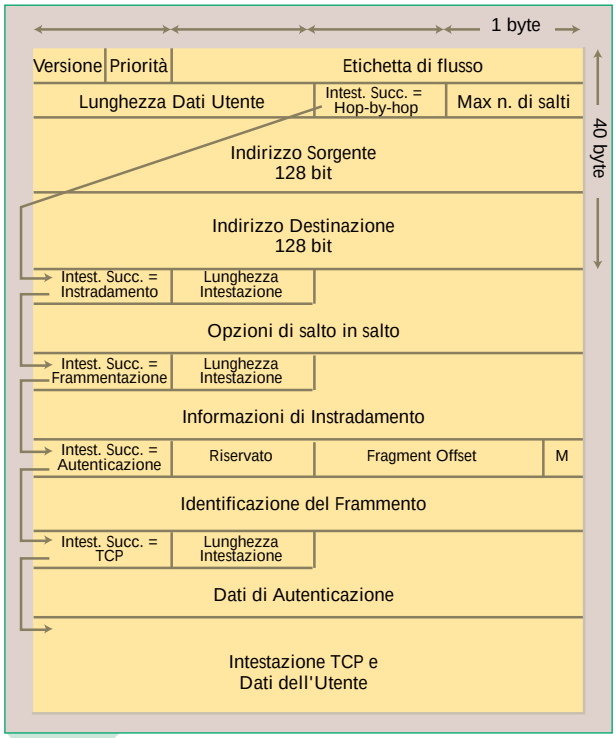

Figura 2 *Le Intestazioni Opzionali nel pacchetto IP.*

3. Indirizzamento e instradamento in IPv6

Lo schema di indirizzamento rappresenta il principale elemento di differenziazione rispetto alla versione precedente del protocollo e la ridefinizione di esso ha voluto perseguire l'obiettivo principale della scalabilità, inteso non solamente come capacità di indirizzamento, ma anche come efficienza dell'instradamento.

Il nuovo schema di indirizzamento IPv6 prevede infatti l'impiego di indirizzi di 128 bit, in modo da non creare in futuro problemi di esaurimento degli indirizzi IP.

Gli indirizzi IPv6 sono di tre tipi differenti [4]:

- *unicast:* identifica una singola interfaccia;
- *multicast:* identifica un insieme di interfacce;
- *anycast:* identifica un insieme di potenziali interfacce, ma a differenza del caso precedente la rete consegna il pacchetto solo a quella più vicina.

L'indirizzo *anycast* è impiegato ad esempio quando una macchina richiede una informazione che ciascun router di un insieme di router può fornire: la macchina invia il pacchetto all'indirizzo *anycast* che identifica l'insieme di router, ma la rete consegna il pacchetto al router più vicino, che provvede a rispondere alla richiesta.

Gli indirizzi IPv6 hanno una struttura gerarchica in modo da garantire una efficiente realizzazione dell'instradamento in rete. Lo spazio di indirizzamento IPv6 è suddiviso in sottoinsiemi, attraverso l'impiego di prefissi [4, 9]. I prefissi di rete costituiscono l'informazione di base per instradare i pacchetti.

L'instradamento dei pacchetti è infatti realizzato in base al prefisso della rete di destinazione, in analogia a IPv4, ma con alcune differenze significative, come descritto in [6]. In IPv4 lo scambio di traffico tra reti di servizio IP differenti, cioè tra sottoreti IP differenti, può avvenire solo attraverso un router, anche se queste reti di servizio sono configurate sulla stessa infrastruttura di rete. In IPv6 perde di importanza la rete logica di servizio e assume un ruolo centrale la rete fisica a cui le macchine terminali sono attestate: se le reti di servizio sono configurate sulla stessa infrastruttura di rete fisica, allora è consentito lo scambio diretto di traffico tra esse.

ALLOCAZIONE DEGLI INDIRIZZI IN IPv6

Lo spazio di indirizzamento di IPv6 risulta suddiviso in sottoinsiemi ciascuno identificato da un prefisso differente. Per ora essi sono stati assegnati come mostrato nella tabella riportata qui a fianco.

ALLOCAZIONE	PREFISSO	FRAZIONE DELLO SPAZIO DI INDIRIZZI
Riservato	0000 0000	1/256
Non assegnato	0000 0001	1/256
Riservato per NSAP	0000 001	1/128
Riservato per IPX	0000 010	1/128
Non assegnato	0000 011	1/128
Non assegnato	0000 1	1/32
Non assegnato	0001	1/16
Non assegnato	001	1/8
Indirizzi unicast su base Fornitore di servizio	010	1/8
Non assegnato	011	1/8
Indirizzi unicast su base geografica	100	1/8
Non assegnato	101	1/8
Non assegnato	110	1/8
Non assegnato	1110	1/16
Non assegnato	1111 0	1/32
Non assegnato	1111 10	1/64
Non assegnato	1111 110	1/128
Non assegnato	1111 1110 0	1/512
Indirizzi locali al Collegamento	1111 1110 10	1/1024
Indirizzi locali al Sito	1111 1110 11	1/1024
Indirizzi Multicast	1111 1111	1/256

Questo cambiamento architetturale dovrebbe favorire l'integrazione di IP con alcune tecnologie di rete come ad esempio la tecnologia *ATM (Asynchronous Transfer Mode)*.

In figura 3 è messa in evidenza la differenza nello scambio di traffico tra terminali attestati a reti di servizio differenti nel caso IPv4 e in quello IPv6 [10].

La rete fisica, sia essa una rete locale o una rete geografica o un collegamento punto-punto, è indicata con il nome di *collegamento* (in inglese "link").

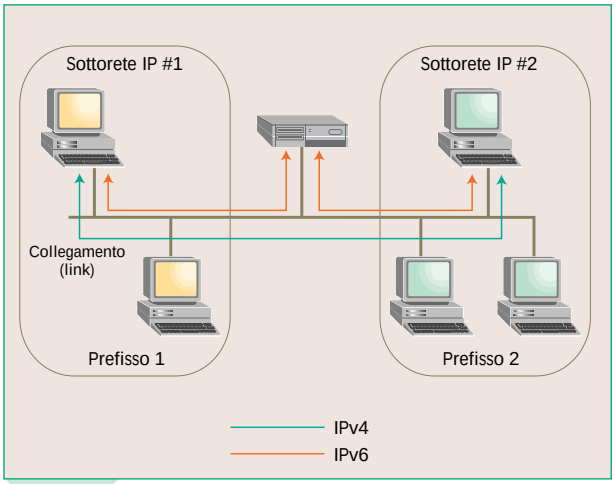

Figura 3 *Differenze tra le architetture IPv4 e IPv6.*

Le macchine attestate al medesimo collegamento sono indicate come vicine (neighbor) e l'insieme di collegamenti controllati dalla stessa autorità amministrativa è chiamata sito *(site)*. I siti sono poi interconnessi ai fornitori di servizio *(provider)*.

L'organizzazione in Internet dei collegamenti, dei siti e dei fornitori di servizio introduce in rete una gerarchia, che si riflette sia nella assegnazione degli indirizzi, sia nella organizzazione dell'instradamento.

La struttura gerarchica non ha quindi solo risvolti tecnici, legati alla efficienza dell'instradamento. All'astrazione della gerarchia deve corrispondere una precisa organizzazione topologica della rete; sono perciò prevedibili conseguenze sulla riorganizzazione amministrativa di Internet e, in particolare, sulla definizione degli ambiti su cui questa gerarchia deve fondarsi.

3.1 Esempi di strutture di indirizzi IPv6

Il primo esempio di organizzazione gerarchica applicata agli indirizzi IPv6 è dato dalla cosiddetta struttura basata sul fornitore di servizio *(Provider Based)* [4, 9, 11, 12], mostrata in figura 4: la struttura rispecchia una organizzazione gerarchica della rete corrispondente ai fornitori del servizio.

Gli indirizzi basati sul fornitore di servizio sono identificati dal prefisso "010" e sono costituiti da cinque componenti [12]: i primi N bit dopo il prefisso identificano il registro nel quale è riportato il Gestore di rete. I successivi M bit identificano il Gestore,

mentre P ulteriori bit identificano il cliente del gestore. Seguono poi Q bit che identificano per ciascun cliente una rete di servizio e i restanti bit identificano una particolare interfaccia in quella rete.

La struttura basata sul fornitore di servizio implica che se il fornitore cambia, allora il cliente deve provvedere ad effettuare una rinumerazione a causa di questo cambiamento. D'altra parte la struttura mal si adatta alla interconnessione contemporanea a più di un fornitore di servizio.

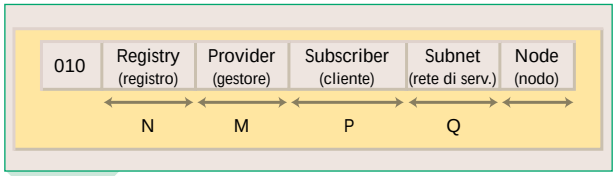

Figura 4 *Struttura degli indirizzi basata sui fornitori di servizio.*

Per superare queste limitazioni è stato proposto un nuovo formato di indirizzo unicast, *Aggregatable Global Unicast*, che suddivide l'indirizzo IPv6 in due porzioni di lunghezza nota: la prima riguarda l'organizzazione della rete pubblica, la seconda è relativa alla rete di utente [13]. La struttura degli indirizzi è mostrata in figura 5. Nella struttura di rete pubblica sono identificabili due macro livelli gerarchici, individuati dai prefissi *TLA (Top Level Aggregator)*, aggregatore di livello superiore, e *NLA (Next Level Aggregator)*, aggregatore di livello successivo.

A livello gerarchico superiore si ipotizza dunque di collocare le organizzazioni responsabili del transito del traffico Ipv6. Un esempio è rappresentato dai punti di interscambio, dove le reti dei differenti operatori si interconnettono tra loro. A queste organizzazioni sono assegnati blocchi di numeri IP identificati dallo specifico prefisso TLA. A livello gerarchico successivo sono collocati i fornitori di servizio o le grandi reti aziendali. Ciascuna organizzazione di livello TLA è responsabile della assegnazione dei prefissi NLA alle organizzazioni gerarchicamente dipendenti.

I successivi 80 bit dell'indirizzo IPv6 riflettono la struttura di rete di utente e sono indipendenti dalla struttura di rete pubblica.

Gli indirizzi Aggregatable Global Unicast non sono stati ancora approvati definitivamente, e questo spiega perché il prefisso "001" è ufficialmente riservato, ma la struttura di essi sembra la più promettente per il futuro in quanto coniuga i vantaggi dello schema di indirizzamento basato sui fornitori di servizio con i vantaggi dello schema basato sulla dislocazione geografica. È stato infatti deciso di impiegare questi indirizzi nella rete sperimentale 6bone [14], realizzata in modo sovrapposto alla Internet per sperimentare la tecnologia IPv6.

3.2 Indirizzamento privato

Anche per IPv6 è stato previsto un insieme di indirizzi privati, che consentono un impiego locale non connesso con il resto della rete Internet.

Vi sono due tipi di indirizzi privati: gli indirizzi locali al sito e gli indirizzi locali al collegamento.

Gli indirizzi locali al sito, identificati dal prefisso "FE:C" (in binario 1111 1110 11), sono impiegati per numerare reti IP che non intendono integrarsi con il resto della rete Internet, come ad esempio le Intranet delle aziende. L'instradamento del traffico con indirizzi locali al sito è possibile solo all'interno di queste reti IP non integrate con il resto della Internet, dove è assicurata l'unicità degli indirizzi.

Nel caso sia necessario trasformare gli indirizzi privati in indirizzi globali, è possibile adattarli alla struttura di indirizzamento gerarchica di riferimento, aggiungendo il prefisso opportuno.

Le stazioni che non sono ancora configurate né con un indirizzo pubblico né con un indirizzo privato, del tipo locale al sito, possono impiegare un indirizzo privato di tipo locale al collegamento.

Gli indirizzi locali al collegamento sono costituiti dal prefisso "FE:8" (in binario 1111 1110 10) e dall'identificativo della stazione (ad esempio l'indirizzo di livello collegamento). Questi indirizzi hanno significato solo nell'ambito del collegamento e consentono lo scambio di traffico solo tra stazioni attestate alla stessa rete fisica. Non è mai previsto che i router possano instradare pacchetti con indirizzi di questo tipo.

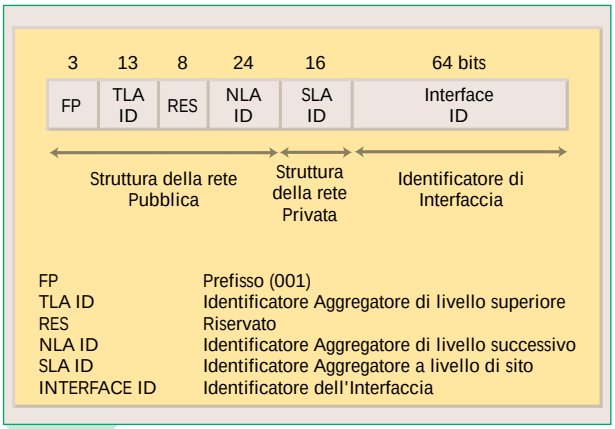

Figura 5 *Struttura degli indirizzi "Aggregatable Global Unicast".*

L'impiego degli indirizzi locali al collegamento è limitato ad applicazioni particolari, che riguardano il singolo collegamento, come ad esempio l'autoconfigurazione degli indirizzi all'avvio [1].

4. Autoconfigurazione

Per le operazioni di configurazione degli indirizzi e di rinumerazione le funzionalità di autoconfigurazione costituiscono un elemento indispensabile.

IPv6 consente differenti forme di autoconfigurazione, che permettono di interconnettere le macchine a Internet senza interventi manuali secondo il paradigma plug and play. Sono presenti diversi problemi da approfondire, tra i quali cruciale è la configurazione dell'indirizzo, in quanto senza un indirizzo non è

RAPPRESENTAZIONE DEGLI INDIRIZZI

Gli indirizzi IPv6 a 128 bit sono rappresentati per convenzione con stringhe di 8 parole da 16 bit, in notazione esadecimale. Ad esempio un indirizzo di tipo unicast è scritto nel modo seguente: 1080:0:0:0:8:800:200C:414A

Per semplificare la scrittura, una sequenza di campi nulli può essere indicata con il simbolo "::". L'indirizzo precedente può essere in maniera analoga rappresentato con la configurazione: 1080::8:800:200C:414A

Non è semplice elaborare indirizzi IPv6; sono tuttavia di grande aiuto i meccanismi di autoconfigurazione per l'assegnazione automatica degli indirizzi alle interfacce di rete e l'impiego di nomi semplici in corrispondenza degli indirizzi IP.

possibile scambiare alcun pacchetto.

Sono stati individuati due possibili approcci:

- l'approccio *stateful* prevede lo scambio di informazioni tra la macchina che deve configurare l'indirizzo e un server che provvede a passare secondo il protocollo *DHCP (Dynamic Host Configuration Protocol)* tutte le informazioni necessarie (indirizzo IP e altri parametri di configurazione). Questo server è denominato *Server DHCP;*
- l'approccio *stateless* [15] prevede che la macchina ricostruisca il proprio indirizzo da sola, senza alcun intervento manuale e senza l'interrogazione di alcun server, ma concatenando il prefisso di rete IP all'indirizzo a livello di collegamento.

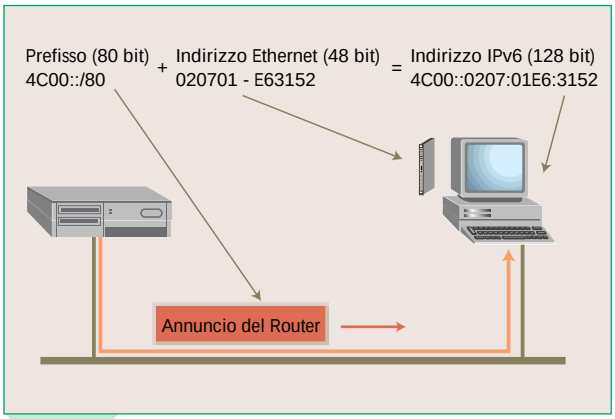

Figura 6 *Esempio di autoconfigurazione del tipo stateless: la macchina ricostruisce l'indirizzo concatenando il prefisso della rete IP con l'indirizzo a livello di collegamento.*

L'approccio di tipo stateless combina due fonti di informazione: la prima è l'indirizzo a livello di collegamento, cablato di solito sulla scheda di rete. Molte tecnologie a livello di collegamento, come ad esempio Ethernet, prevedono infatti indirizzi univoci per le interfacce. La seconda fonte di informazione è costituita dai messaggi emessi periodicamente dal router attestato al collegamento per indicare alle stazioni attestate il prefisso di rete IP. La configurazione di tipo stateless è una delle funzionalità eseguite da *ICMP (Internet Control Message Protocol)* [16].

ICMP provvede infatti a concatenare il prefisso di rete IP e l'indirizzo a livello di collegamento come mostrato nella figura 6 e permette di ricavare così un indirizzo IP univoco da assegnare alla interfaccia di rete. Il prefisso identifica la rete di servizio nella Internet, mentre l'indirizzo a livello di collegamento identifica l'interfaccia attestata al collegamento.

ICMP è un protocollo separato, ma allo stesso tempo un componente essenziale per il funzionamento di IP. Oltre all'autoconfigurazione degli indirizzi IP, il protocollo consente le interazioni tra i sistemi attraverso un insieme di funzionalità note con il nome di *Neighbor Discovery* [18], di seguito descritte. Nel protocollo sono predisposte funzionalità capaci di reagire a eventuali problemi in rete con la notifica di errore mediante appositi messaggi e inoltre fornisce all'utente strumenti per gli aspetti legati all'esercizio e manutenzione della rete (è ad esempio utilizzato nei programmi *ping, traceroute).*

5. Individuazione dei vicini (Neighbor Discovery)

Una delle più importanti funzioni svolte da ICMP riguarda il Neighbor Discovery [16, 17, 18]. Le funzionalità inserite riguardano l'interazione tra macchine collegate ad un medesimo collegamento.

Oltre all'autoconfigurazione dell'indirizzo IP, Neighbor Discovery consente di localizzare i router attestati e di individuare quali prefissi di rete sono configurati sul collegamento. Inoltre questa funzione permette di individuare la duplicazione di indirizzi IP e di provvedere a far tradurre l'indirizzo IP nel corrispondente indirizzo di livello collegamento, per la trasmissione fisica del pacchetto.

Di seguito sono descritte alcune delle caratteristiche più importanti.

5.1 Risoluzione degli indirizzi (Address Resolution)

La procedura di risoluzione degli indirizzi consente di tradurre un indirizzo IP nel corrispondente indirizzo di collegamento (ad esempio indirizzo *MAC, Medium Access Control).*

In IPv4 questa funzionalità è realizzata a livello di

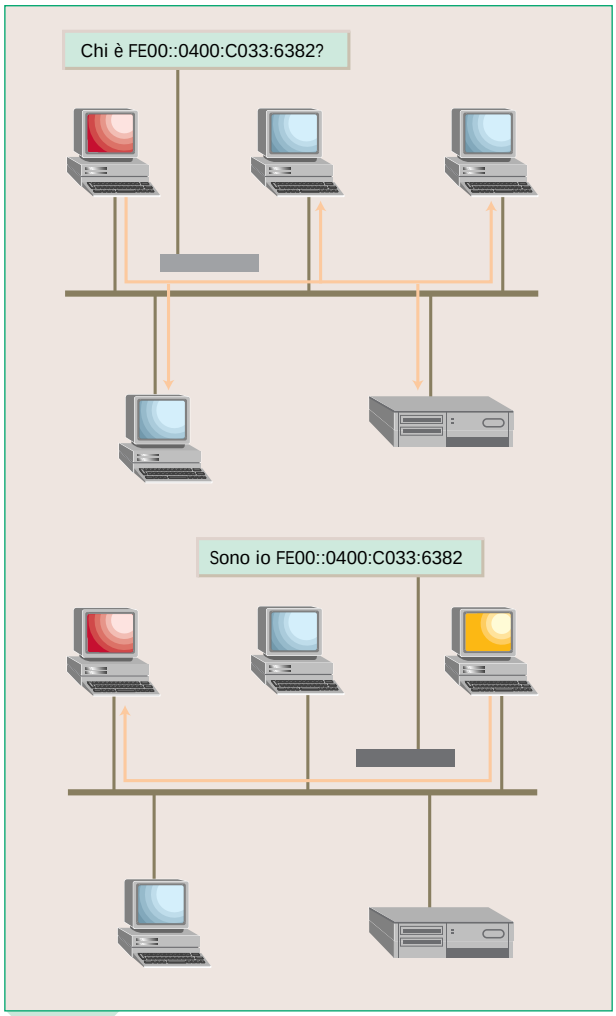

Figura 7 *Risoluzione degli indirizzi (procedura per tradurre un indirizzo IP in quello corrispondente di collegamento).*

collegamento, secondo modalità dipendenti dalla tecnologia di rete. In IPv6 la funzionalità è inserita in ICMP e quindi in modo indipendente dalle caratteristiche della interfaccia. Essa poi non è basata sulla possibilità di un trasporto broadcast delle richieste, ma sul multicast IP e quindi consente un risparmio di elaborazione, in quanto le richieste non arrivano indiscriminatamente a tutti i terminali attestati alla rete, ma ad un sottoinsieme opportunamente selezionato.

Quando una stazione deve inviare un pacchetto, ma non ha l'indirizzo fisico corrispondente all'indirizzo IP della macchina di destinazione, essa provvede a preparare una richiesta ICMP. Questa richiesta è un messaggio di *Neighbor Solicitation.*

La stazione sorgente provvede a introdurre nel messaggio il proprio indirizzo IP, il proprio indirizzo MAC e quello IP della destinazione. Invia poi il messaggio a un particolare indirizzo multicast ottenuto facendo seguire a un prefisso multicast convenzionale (prefisso FF02::1/96) gli ultimi 32 bit dell'indirizzo IP della destinazione.

Il messaggio è letto solo dalle macchine il cui indirizzo IP presenta gli stessi ultimi 32 bit rispetto a quelli impiegati nell'indirizzo multicast.

Una volta ricevuto il messaggio e dopo la verifica della corrispondenza dell'indirizzo IP ricercato con il proprio, la destinazione provvede a rispondere alla sorgente con un altro messaggio, un *Neighbor Advertisement*, in cui è inserito il proprio indirizzo MAC. In figura 7 è schematizzato lo scambio di messaggi tra sorgente e destinazione. Quando la sorgente riceve il messaggio con l'indirizzo MAC, essa è in grado di trasmettere fisicamente il pacchetto.

Se nessuna macchina presente sul collegamento ha l'indirizzo IP ricercato, allora non viene generata alcuna risposta. Allo scadere di un determinato intervallo di tempo la stazione sorgente deduce che la destinazione non è raggiungibile.

Le corrispondenze tra l'indirizzo IP e l'indirizzo MAC così determinate sono riportate in una memoria ad accesso veloce per successivi trasferimenti di pacchetti. Le informazioni contenute in questa memoria sono periodicamente cancellate in modo da garantire la coerenza delle informazioni con l'effettivo stato di attività delle macchine attestate al collegamento.

5.2 Individuazione dei router (Router Discovery)

La funzione *Router Discovery* serve per individuare i router attestati al collegamento e i prefissi di rete su di esso configurati. In particolare nel protocollo ICMP è previsto che i router inviino in rete messaggi di Router Advertisement, come mostrato in figura 8. Questi messaggi contengono diverse informazioni e,

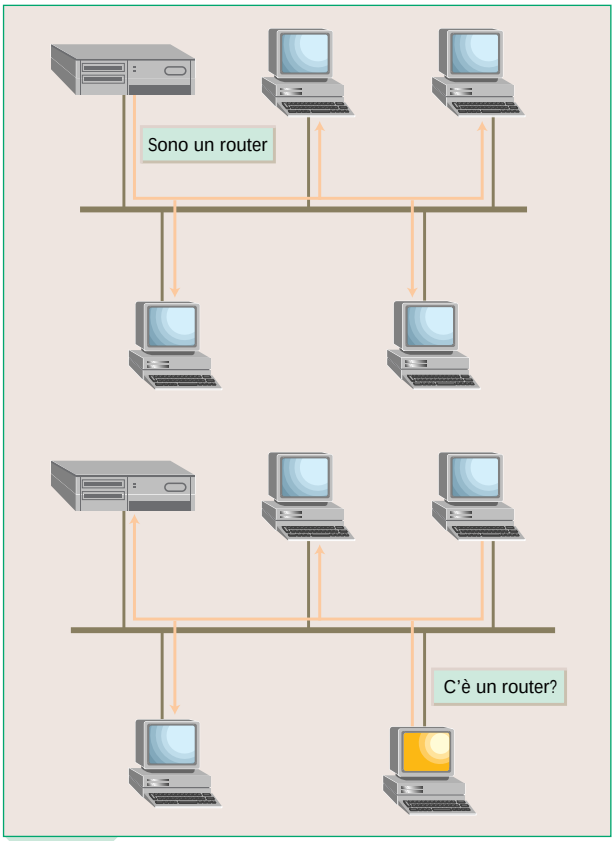

Figura 8 *Procedura per individuare i router e i prefissi sul collegamento.*

in particolare, la lista dei prefissi di rete configurati sul collegamento. Le macchine terminali possono così individuare quali destinazioni sono direttamente raggiungibili, senza l'impiego di alcun router.

Il protocollo consente anche alle macchine di stimolare i router per ottenere informazioni sui prefissi configurati. ICMP definisce a questo scopo un messaggio di Router Solicitation, con il quale una macchina può accertare se al collegamento sia attestato almeno un router.

5.3 Reinstradamento (Redirect)

Con la funzionalità del *redirect* i router possono indicare instradamenti alternativi e determinare di conseguenza il reinstradamento del traffico. Questa caratteristica è stata introdotta per ottimizzare l'impiego delle risorse di trasferimento della rete, mediante interazione tra la sorgente del traffico e il primo nodo della rete.

6. Transizione da IPv4 a IPv6

Data la grande diffusione della versione 4 del protocollo IP è prevedibile che sarà lungo il periodo transitorio in cui saranno presenti in rete entrambe le versioni del protocollo [19]. Le modalità di coesistenza e di interlavoro delle due versioni del protocollo IP passano attualmente attraverso la realizzazione della doppia pila di protocolli nelle macchine [21] e attraverso l'impiego del meccanismo del *tunnelling* [14, 19] per la realizzazione di reti IPv6 sovrapposte a Internet.

Il meccanismo del tunnelling è mostrato in figura 9 e fornisce un mezzo per trasportare pacchetti IPv6 utilizzando una infrastruttura di comunicazione di tipo IPv4. Il meccanismo funziona in abbinamento con la doppia pila di protocolli e prevede di alloggiare pacchetti IPv6 nei campi dati utente di IPv4.

Nel funzionamento della Internet con macchine a doppia pila di protocolli un ruolo è svolto anche dai *DNS (Domain Name System)*, ossia dai sistemi che fanno corrispondere ai nomi simbolici gli indirizzi IP: quando una macchina terminale richiede la traduzione di un nome, se riceve indietro un indirizzo a 128 bit, allora impiega la pila IPv6 per lo scambio di informazioni, se riceve indietro un indirizzo a 32 bit, impiega invece la pila IPv4. I DNS devono quindi essere modificati per poter memorizzare nella loro base di dati gli indirizzi a 128 bit [20].

Sono allo studio anche soluzioni di interlavoro tra le due versioni di protocollo [22], che non richiedono la doppia pila di protocolli; su queste però non è ancora consolidata una soluzione condivisa.

7. Conclusioni

La nuova versione del protocollo IP mantiene la maggior parte delle caratteristiche e delle funzionalità della versione precedente, riconoscendo a quest'ultima la validità tecnologica come elemento base del successo della rete Internet.

L'adeguamento del protocollo alle esigenze maturate dall'impiego della rete per scopi commerciali a livello mondiale non si è tradotto in un appesantimento del protocollo. Il criterio della semplicità è rimasto il principio base del progetto e, piuttosto che procedere a una riscrittura di un nuovo protocollo con il rischio di una elevata complessità, si è ritenuto più opportuno procedere alla riorganizzazione delle funzionalità, eliminando quelle superflue e aggiungendone di nuove.

IPv6 risponde in maniera organica alle esigenze di scalabilità, di qualità, di sicurezza conseguenti al grande successo della rete Internet.

L'attività di specificazione progredisce e sono già disponibili realizzazioni sia di terminali che di router. Sono inoltre avviate sperimentazioni in campo, per le quali è stata predisposta una rete sperimentale sovrapposta alla Internet, denominata *6bone*, mediante la tecnica del tunnelling.

Si ritiene tuttavia che il vero successo di *IPv6* sarà determinato non tanto dagli aspetti tecnici quanto piuttosto da fattori di natura commerciale: è infatti cruciale

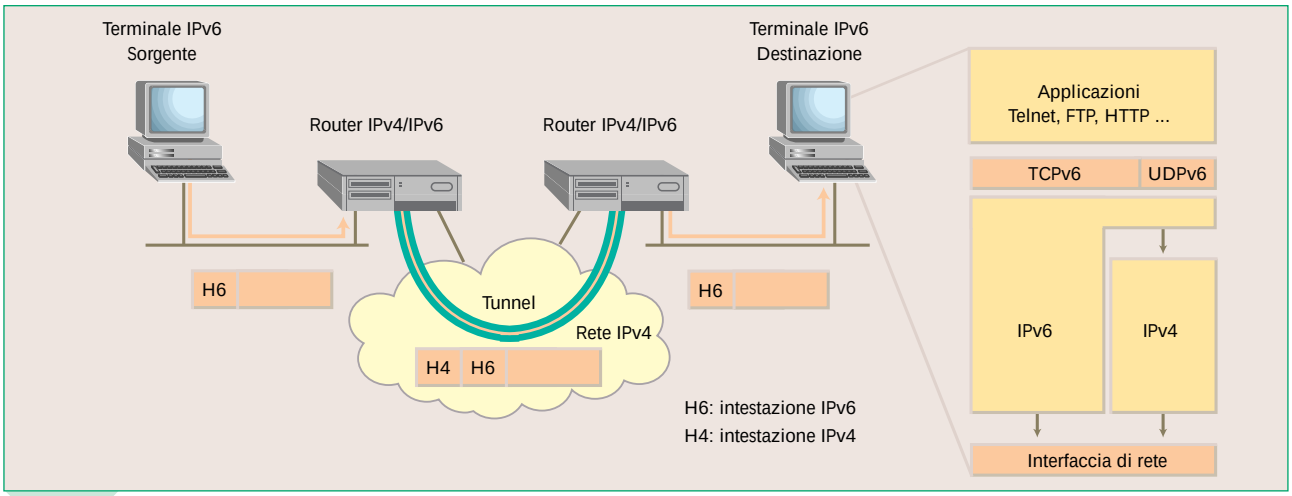

Figura 9 *Modalità per la trasmissione in rete di pacchetti IPv6 su una infrastruttura IPv4.*

il modo in cui si passerà da IPv4 a IPv6; basti pensare agli ingenti capitali investiti nella tecnologia IPv4 e alle conseguenze derivanti da una semplice sostituzione.

Deve poi essere considerata la ridefinizione di ruoli e di responsabilità nell'ambito della gerarchia di rete che si intende attuare nel prossimo futuro.

Sicuramente la flessibilità del software e del firmware saranno di aiuto per favorire nel migliore dei modi la transizione alla nuova versione del protocollo, che comunque conserva le caratteristiche di semplicità e di efficienza della tecnologia e dunque conferma la buona prospettiva di successo di IP per il futuro.

Per un maggiore approfondimento si suggeriscono i seguenti siti:

http://www.ietf.org
http://www-6bone.lbl.gov/6bone
http://playground.sun.com/pub/ipng/html/

Abbreviazioni

ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IP v4	Internet Protocol version 4
IP v6	Internet Protocol version 6
IPX	Internet Packet Exchange
MAC	Medium Access Control
MTU	Maximum Transfer Unit
NLA	Next Level Aggregator
NSAP	Network Service Access Point
SLA	Site Level Aggregator
TCP	Transmission Control Protocol
TLA	Top Level Aggregator

Francesco Iuso ha conseguito la laurea con lode in Ingegneria Elettronica presso L'Università degli studi La Sapienza di Roma nell'anno accademico 1989/90, discutendo la tesi sul riconoscimento della voce. Nel corso del 1991 ha prestato attività di consulenza presso l'Alenia Spazio di Roma sulla tematica "prodotti di intermodulazione nelle trasmissioni via satellite", dovendo ancora concludere gli obblighi di leva. Nel 1992 è stato assunto in SIP (oggi Telecom Italia) e per conto della società ha frequentato e superato con lode il master in Tecnologie dell'Informazione presso il centro "CEFRIEL", analizzando le problematiche di internetworking e di integrazione delle reti locali nell'architettura di rete integrata nei servizi a larga banda in tecnica ATM. Dal 1993 si è occupato di reti e servizi dati ad alta velocità nella Ricerca e sviluppo di SIP. Nel 1994 è stato nominato Chairman del gruppo ESIG (European SMDS Interest Group) e ha ricoperto la carica per un anno. Ha partecipato alle attività di definizione dell'interlavoro Frame Relay – ATM in ITU-T. Dal 1994 partecipa alle attività del gruppo IETF (Internet Engineering Task Force) e si occupa di problematiche di internetworking, tematica sulla quale è stato coautore di diversi articoli. Ha partecipato al progetto SIRIUS e alle sperimentazioni di Telecom Italia per lo sviluppo di servizi multimediali interattivi e ha curato la realizzazione delle soluzioni innovative di rete per i clienti della rete SIRIUS. Si è occupato di protocolli e politiche di instradamento IP, con riferimento alle problematiche di interconnessione di reti IP. Opera oggi nell'ambito della linea Ingegneria di Reti Dati e Multimediali della Direzione Rete di Telecom Italia e si occupa di internetworking.

Bibliografia

[1] Huitema, C.: *IPv6 the new Internet protocol*. Ed. Prentice Hall, 1996.
[2] Partridge, C.; Kastenholz, F.: *Technical Criteria for Choosing IP: The Next Generation (IPng)*. IETF, RFC 1726, dicembre 1994.
[3] Deering, S.; Hinden, R.: *Internet Protocol Version 6 (IPv6) Specification*. RFC 1883, Standard Track, dicembre 1995.
[4] Hinden, R.; Deering, S.: *IP Version 6 Addressing Architecture*. Rfc1884, Standard Track, dicembre 1995.
[5] Thomas, S.: *IPng and the TCP/IP Protocols2*. Ed. Wiley, 1996.
[6] Berni, S.; Fasano, P.; Guardini, I.: *Il protocollo IPv6*. Documenti tenici CSELT, DTD97.0367.
[7] Borman, D.: *TCP and UDP over IPv6 Jumbograms*. RFC 2147, Standards Track, maggio 1997.
[8] McCann, J.; Deering, S.; Mogul, J.: *Path MTU Discovery for IP version 6*. RFC 1981, Standards Track, agosto 1996.
[9] Rekhter, Y.; Li, T.: *An Architecture for IPv6 Unicast Address Allocation*. RFC 1887, Informational, dicembre 1995.
[10] Crawford, M.: *A Method for the Transmission of IPv6 Packets over Ethernet Networks*. RFC 1972, agosto 1996.
[11] Hinden,R.; Postel : *IPv6 Testing Address Allocation*. RFC 1897, Experimental, gennaio 1996.
[12] Rekhter, Y. et. al.: *An IPv6 Provider-Based Unicast Address Format*. RFC 2073, Standards Track, gennaio 1997.
[13] Documento IETF in fase di preparazione: *An IPv6 Aggregatable Global Unicast Address Format*. Draft-ietf-ipngwg-unicast-aggr-03.txt
[14] Fasano, P.; Franco, C.; Guardini, I.; Mirabelli, M.: *La sperimentazione del protocollo IPv6 in CSELT*. Documenti tecnici CSELT, DTR97, 0999.
[15] Documento IETF in fase di preparazione: *IPv6 Stateless Address Autoconfiguration*. Draft-ietf-ipngwg-addrconf-v2-02.txt.
[16] Conta, A.; Deering, S.: *Internet Control Message Protocol for IP Version 6 (IPv6)*. RFC 1885, dicembre 1995.
[17] Documento IETF in fase di preparazione: *Neighbor Discovery for IP Version 6 (IPv6)*. Draft-ietf-ipngwg-discovery-v2-02.txt.
[18] Narten, T.; Nordmark, E.; Simpson, W.: *Neighbor Discovery for IP Version 6 (IPv6)*. RFC 1970, agosto 1996.
[19] De Marco, M.; Trecordi, V.: *IP Next Generation: analisi della suite dei protocolli*. Documento CEFRIEL, 1996.
[20] Thomson, S.; Huitema, C.: *DNS Extensions to support IP Version 6*. RFC 1886, dicembre 1995.
[21] Gilligan, R.; Nordmark, E.: *Transition Mechanism for IPv6 hosts and routers*. RFC 1933, aprile 1996.
[22] Documento IETF in fase di preparazione: *Network address translation - Protocol Translation (NAT - PT)*. Draft-ietf-ngtrans-natpt-01.txt.