ISTITUTO NAZIONALE DI FISICA NUCLEARE

CNAF - Bologna

INFN/TC-98/29
30 Ottobre 1998

IPV6: INTRODUZIONE AL PROTOCOLLO E TEST EFFETTUATI AL CNAF

Andrea Chierici, Luca dell'Agnello, Antonia Ghiselli, Cristina Vistoli

SIS–Pubblicazioni
dei Laboratori Nazionali di Frascati

INFN – Istituto Nazionale Fisica Nucleare
CNAF – Bologna

INFN/TC-98/020
30 Ottobre 1998

IPV6: INTRODUZIONE AL PROTOCOLLO E TEST EFFETTUATI AL CNAF

Andrea Chierici, Luca dell'Agnello, Antonia Ghiselli, Cristina Vistoli

INFN - CNAF, v.le Berti Pichat 6/2, 40127 Bologna (Italy)

ABSTRACT

IPv6, the new version of the Internet Protocol, is under development by IETF working groups. A brief description of the protocol is presented, and analysis of the main differences from IPv4 is covered. In the second part we describe our tests of the protocol in the framework of 6BONE.

PACS.: 89.80.+h
Key words: IPv6, Internet

PREMESSA

Nei primi anni '90, un effetto paradossale del grande successo di Internet fu la paventata crisi dell'attuale versione di IP.

In effetti la crescente richiesta di indirizzi IP rendeva plausibile il loro esaurimento in breve tempo; inoltre il grande numero di reti faceva prospettare, date le caratteristiche dei router dell'epoca, la congestione delle tabelle di routing.

Questi problemi determinarono l'esigenza di una revisione del protocollo IP.

All'interno dell'IETF furono quindi costituiti gruppi di lavoro che, nel Gennaio del '95, portarono alla progettazione di una nuova versione di IP: IPv6[1].

La progettazione di IPv6 è tuttora in corso. Nel frattempo sono state introdotte modifiche, non strutturali, a IPv4 (es.: il "*classless ip*") che, insieme ad un'oculata distribuzione degli indirizzi su base geografica (così da aggregarli tenendo conto della topologia fisica della rete), hanno consentito di disinnescare la minaccia della congestione delle tabelle di routing.

Altrettanto importante e' stata ovviamente l'evoluzione della tecnologia dei router, sia in termini architetturali che di efficienza dell'hardware.

D'altra parte una piu' accorta politica nell'assegnazione delle reti e la diffusione delle Intranet (associate a meccanismi di tipo NAT), cui sono riservati gruppi di indirizzi privati cioè da non annunciare e quindi duplicabili[2], hanno contribuito ad allontanare lo "spettro" dell'esaurimento degli indirizzi. Questi due fattori hanno reso meno immediato (e meno scontato, per certi aspetti) il tramonto di IPv4.

Ma lo sviluppo di IPv6 resta importante per risolvere altre problematiche cui IPv4 non riesce a fare fronte. Per esempio, IPv4 è sostanzialmente incapace di supportare la tecnologia real-time, mentre al contrario un numero sempre maggiore di workstation è oggi equipaggiato con dispositivi multimediali.

Un altro requisito, che IPv6 è progettato soddisfare, è la sicurezza nella trasmissione dei dati criptando le connessioni già a livello di trasporto (attualmente, con meccanismi tipo *ssh*, ciò avviene a livello delle applicazioni e con metodi perciò non universalmente adottati).

In IPv6 è previsto anche il supporto per la mobilità degli host, che risponde alla crescente diffusione di PC portatili.

Anche le *intranet* in IPv6 sono gestite in modo piu` efficace: è loro assegnato un apposito tipo di indirizzi (site-local address) dai quali è immediata la conversione in indirizzi globali, qualora si decidesse il collegamento ad Internet.

Infine in IPv6 sono supportati i "jumbograms", pacchetti di dati di dimensione maggiore di 64Kbyte, pensati per ottimizzare le comunicazioni su *layer* con MTU grande.

In questa nota, dopo una breve introduzione sulle caratteristiche generali di IPv6[3], dove illustreremo le differenze più significative con IPv4, con cenni al DNS ed al routing, verranno descritte le sperimentazioni svolte al CNAF.

Sarà anche proposto un piano di assegnazione degli indirizzi IPv6 per il GARR nell'ambito di 6BONE.

In appendice riportiamo indicazioni sul software utilizzato.

---

1 RFC 1883

2 RFC 1918

3 Alcuni aspetti di IPv6 sono coperti da RFC; altri, ancora in fase evolutiva, sono descritti da draft (documenti con validità temporanea).

1. INTRODUZIONE A IPV6

IPv6 ha mantenuto le caratteristiche che hanno sancito il successo di IPv4, come la robustezza e il servizio *connectionless* di consegna dei pacchetti[4].

Le principali differenze rispetto ad IPv4 sono:

- Semplificazione dell'header IP, per una più facile interpretazione da parte dei router;
- Estensione dello spazio indirizzo da 32 bit a 128 bit, permettendo quindi la creazione di una gerarchia di indirizzamento;
- supporto diretto del multicast;
- supporto del QoS, attraverso un flow-label inserito nell'header;
- supporto per la sicurezza a livello di trasporto;
- frammentazione dei pacchetti a carico solo del nodo sorgente.

Vediamo in dettaglio questi punti.

1.1 Il datagramma IPv6

La struttura del datagramma IPv6 è differente da quella di IPv4.

La lunghezza dell'header di base è fissa (40 bytes di cui 32 per gli indirizzi!), in contrapposizione alla lunghezza variabile in IPv4; è stato però introdotto il campo "*Next hdr*" per eventuali header aggiuntivi.

Non è più presente il campo checksum.

È stato aggiunto invece nell'header di base un nuovo importante campo, *flow label,* per discriminare i vari tipi di flussi (ad esempio flussi real-time con una specifica QoS); inoltre il campo *Priority* può essere usato per identificare e distinguere tra differenti classi o priorità di pacchetti IPv6.

Attualmente entrambi questi campi sono in fase di studio e non è stato possibile effettuare prove di funzionalità. È da ritenere tuttavia che questo meccanismo, unito ad un protocollo di prenotazione delle risorse, tipo RSVP, potrà rendere possibile la realizzazione di applicazioni che utilizzino QoS diverse, in modo piu` efficiente rispetto all'attuale RSVP su IPv4.

Altra caratteristica innovativa è che sia la frammentazione che la deframmentazione dei pacchetti possono essere effettuate solo dagli "end host" (con il vecchio protocollo la frammentazione poteva avvenire anche all'interno di router intermedi): quindi al momento della trasmissione viene determinato il minimo MTU sul percorso.

La maggiore differenza tra le due versioni è però l'indirizzamento di rete portato da 32 a 128 bit.

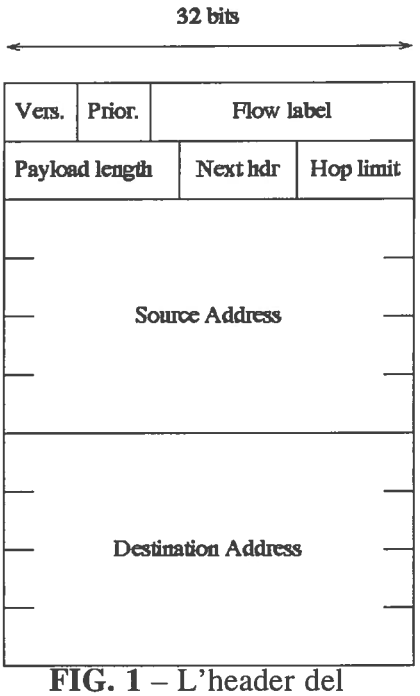


FIG. 1 – L'header del datagramma IPv6.

[4] IP significa Internet Protocol e la sua funzione principale è permettere l'interconnessione di reti, indipendentemente dalla tecnologia trasmissiva della singola rete.

1.2 L'indirizzamento IPv6[5]

Gli indirizzi IPv6 sono identificatori per interfacce (o insiemi di interfacce) a 128 bit. Esistono tre tipi di indirizzi:

- **Unicast**: un indirizzo per una singola interfaccia. Un pacchetto inviato ad un indirizzo unicast è consegnato all'interfaccia indicata dall'indirizzo. L'indirizzo è composto di due parti: il prefisso (che individua la rete) e l'identificativo dell'interfaccia di rete. Quest'ultimo può essere lungo 48 o 64 bit a seconda che sia usato il *MAC-address* o la nuova specifica EUI-64[6].

  IPv6 ha 3 tipi di indirizzi unicast[7]:

  - ***Aggregatable-global*** Indirizzi a validità globale, assegnati da un ISP (univoci su Internet).

	n bit	(125 – n) bit
001	Subnet Prefix	Interface ID

FIG. 2 – Indirizzo IPv6 unicast di tipo globale aggregabile

  - ***Site-local-use*** Indirizzi a validità locale. Analogo degli indirizzi "privati" in IPv4, sono stati pensati per le intranet. Con il meccanismo dell'autoconfigurazione (paragrafo 1.5), risulta semplice una successiva connessione ad Internet.

10 bit	38 bit	16 bit	64 bit
1111111011	0	Subnet ID	Interface ID

FIG. 3 – Indirizzo IPv6 unicast di tipo site-local

  - ***Link-local-use*** Indirizzi a validità su una linea di comunicazione punto-punto (es. connessione in *dial-up*).

10 bit	54 bit	64 bit
1111111010	0	Interface ID

FIG. 4 – Indirizzo IPv6 unicast di tipo link-local

- **Anycast**: un identificatore per un insieme di interfacce (tipicamente appartenenti a differenti nodi). Un pacchetto inviato ad un indirizzo anycast è consegnato a una delle interfacce indicate da quell'indirizzo (la "più vicina", secondo le misure di distanza dei protocolli di routing). Un indirizzo anycast è indistinguibile, strutturalmente, da un indirizzo unicast. Un possibile utilizzo di questi indirizzi è di identificare un insieme di router appartenenti ad una organizzazione che fornisce servizi su Internet, oppure di identificare l'insieme dei router connessi ad una particolare subnet o che forniscono accesso ad un particolare dominio di routing, o ancora di un cluster di macchine.

---

5 Per maggiori dettagli: draft-ietf-ipngwg-addr-arch-v2-06.txt

6 http://standards.ieee.org/db/oui/tutorials/EUI64.html

7 Sono stato riservati anche dei prefissi per indirizzi NSAP ed IPX.

FIG. 5 – Indirizzo IPv6 anycast

- **Multicast**: un identificatore per un insieme di interfacce (tipicamente appartenenti a differenti nodi). Un pacchetto inviato ad un indirizzo multicast viene consegnato a tutte le interfacce indicate da quell'indirizzo.
  Agli indirizzi multicast è riservato un sottoinsieme dello spazio globale.

FIG. 6 – Indirizzo IPv6 multicast

I protocolli IPv6, a differenza di quelli IPv4, non si basano sul ***broadcast****: per questo motivo non vi sono indirizzi di questo tipo in IPv6.*

1.3 Allocazione attuale degli indirizzi

Il tipo specifico di un indirizzo IPv6 è indicato dai primi bit in ogni indirizzo: il prefisso di lunghezza variabile che comprende questi bit è detto *Format Prefix* (FP). L'allocazione iniziale di questi prefissi è illustrata nella tabella 1.

Questo schema supporta l'allocazione diretta di indirizzi aggregati, indirizzi per uso locale e multicast; è stato assegnato anche un prefisso per gli indirizzi NSAP e uno per IPX. Attualmente soltanto il 15% dello spazio indirizzi è allocato, mentre il rimanente 85% è riservato ad usi futuri.

TABELLA 1 – Allocazione dei prefissi IPv6.

Allocazione	Prefisso (binario)	Frazione spazio 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
Aggregatable Global Unicast Address	001	1/8
Non Assegnato	010	1/8
Non Assegnato	011	1/8
Non Assegnato	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
Link-Local Address	1111 1110 10	1/1024
Site-Local Address	1111 1110 11	1/1024
Multicast Address	1111 1111	1/256

1.3.1 *Indirizzi "Provider based"*

Il primo tipo di indirizzo unicast usato per la sperimentazione nell'ambito di 6BONE è stato il "*provider based*"[8]. Esso permette un facile *mapping* tra gli indirizzi IPv4 e quelli IPv6: il prefisso (80 bit) viene infatti derivato dal numero di *Autonomous System*, dalla rete e dalla *subnet mask* IPv4 del sito, mentre l'identificatore dell'interfaccia di rete dell'host è il *MAC ADDRESS* (48 bit).

Questo tipo di indirizzo, replicando di fatto l'attuale situazione di IPv4, non permette una facile aggregazione delle reti e quindi non è adatto ad essere usato su larga scala.

Al suo posto, viene attualmente utilizzato un tipo di indirizzo detto "*aggregabile*".

1.3.2 *Indirizzi unicast globali aggregabili*

Gli indirizzi "unicast globali aggregabili"[9] permettono la realizzazione di una struttura completamente gerarchica degli indirizzi che rispecchi l'effettiva topologia della rete.

Poichè è stata scelta la specifica EUI-64 per identificare l'interfaccia di rete, la parte di prefisso è composta da 64 bit.

La struttura dell'indirizzo è la seguente:

FIG. 7 – Struttura di un indirizzo unicast IPv6 globale aggregabile

I primi 3 bit dell'indirizzo (001) costituiscono il *Format Prefix*, che, con il *Top Level Aggregation* (TLA) Identifier, forma il prefisso solitamente assegnato ad un provider di backbone (16 bit).

Il provider di backbone fornisce accesso a provider regionali, allocando loro sottoinsiemi del proprio spazio di indirizzi: i prefissi che assegna loro sono ottenuti usando tutta o parte dei 32 bit del *Next Level Aggregation* (NLA).

In generale, il prefisso di un provider regionale sarà formato dal TLA e da una parte dell'NLA (indicato come NLA_1). A propria volta un provider regionale può assegnare un sottoinsieme del proprio spazio di indirizzi ad un altro provider: il prefisso di quest'ultimo sarà formato dal TLA, dall'NLA_1 e da un altro "pezzo" di NLA (NLA_2).

Si formerà quindi una gerarchia NLA_1, NLA_2,... fino a completare i primi 48 bit: i 16 bit successivi formano il Site Level Aggregation (SLA), per la gestione delle sottoreti locali (ben 65536).

Questa struttura permette di aggregare gli annunci delle reti. Infatti ogni provider annuncia verso l'esterno solo il prefisso comune a tutte le sue reti: in particolare un provider di backbone annuncia tutto il suo spazio di indirizzi (ben 2^{32} reti) mediante un solo prefisso di 16 bit.

Si noti infine che il limite di 2^{13} TLA può essere superato allocando ulteriori FP per questo tipo di indirizzo.

1.4 Rappresentazione degli indirizzi IPv6

Un indirizzo IPv6 è comunemente rappresentato in forma esadecimale, separando in blocchi di 16 bit tramite ":". Ad esempio:

---

8 RFC 1897

9 draft-ietf-ipngwg-unicast-aggr-xx.txt

3ffe:2300:0000:0000:02a0:24ff:fe99:0da7

Tuttavia questa rappresentazione può essere compattata: per valori inferiori a 0x1000 gli zeri iniziali possono essere omessi.

Quindi il precedente indirizzo diventa:

3ffe:2300:0:0:2a0:24ff:fe99:da7

Inoltre una sequenza di bit uguali a 0, se in numero multiplo di 16, può essere sostituita con la stringa "::".

L'indirizzo precedente può essere quindi riscritto come:

3ffe:2300::2a0:24ff:fe99:da7

La stringa "::" può essere usata solo una volta quando si scrive un indirizzo.

Infine, la parte di indirizzo che si riferisce al prefisso è univocamente determinata indicando il numero di bit che lo compongono. Ad esempio *3ffe:2300::0/64* indica il prefisso *3ffe:2300:0000:0000.*

1.5 Autoconfigurazione

Una delle caratteristiche più innovative di IPv6 è l'autoconfigurazione degli indirizzi, sia locali che globali[10]. Con IPv4 questo è possibile solo tramite un protocollo esterno "statefull", DHCP, mentre in IPv6 questa funzionalità è integrata nel protocollo in modo "stateless".

Il vantaggio di questo approccio è che non è mai richiesta la configurazione manuale degli host, e solo una minima configurazione del router senza nessun server aggiuntivo (come accade invece per DHCP).

È comunque previsto anche per IPv6 l'approccio "statefull" tramite l'estensione a DHCP chiamata DHCPv6[11].

Questo meccanismo consente ad un host di generare il proprio indirizzo usando una combinazione di informazioni reperibili localmente e dal router.

Il router, opportunamente configurato, propaga periodicamente sulla LAN il prefisso che identifica la sottorete associata al link (notifica anche di essere il default gateway), mentre l'host genera un identificatore univoco per l'interfaccia di rete.

In assenza di annuncio un host può generare soltanto indirizzi link-local (comunque presenti).

Attualmente ogni host utilizza il "MAC address", convertito secondo lo standard EUI-64, come identificatore dell'interfaccia di rete.

Ad esempio, il prefisso annunciato dal router sulla LAN del CNAF è: *3ffe:2300::0/64*; l'interfaccia di rete di uno dei nostri nodi, con indirizzo locale: *fe80::2a0:24ff:fe99:da7*, assume di conseguenza l'indirizzo globale *3ffe:2300::2a0:24ff:fe99:da7*.

Questo meccanismo permette, in caso di cambiamento di ISP (e conseguente cambiamento di indirizzi), un'immediata rinumerazione con la sola riconfigurazione del router.

I nostri test non hanno evidenziato nessun problema di funzionamento; in realtà, finora, l'autoconfigurazione è una delle poche novità di IPv6 già completamente implementata!

---

[10] draft-ietf-ipngwg-addrconf-v2-xx.txt

[11] draft-harrington-ngtrans-dhcp-option-00.txt

1.6 DNS

Il DNS è stato modificato per supportare gli indirizzi a 128 bit di IPv6[12].

A tale scopo, sono stati introdotti i record AAAA (*quad-A*), supportati a partire dalla versione 4.9.5 di bind.

Un esempio:

gandalf.ipv6.cnaf.infn.it AAAA 3ffe:2300::2a0:24ff:fe99:da7

Inoltre, in analogia al dominio *in-addr.arpa* per gli indirizzi IPv4, è stato definito il dominio *ip6.int* per permettere il reverse DNS.

In questo dominio un indirizzo IPv6 è rappresentato come un nome: le cifre esadecimali che lo compongono sono rappresentate in ordine inverso (senza omettere alcun "0") e separate da punti.

Ad esempio per l'indirizzo precedente, abbiamo:

7.a.d.0.9.9.e.f.f.f.4.2.0.a.2.0.0.0.0.0.0.0.0.0.0.0.3.2.e.f.f.3 IN PTR

gandalf.ipv6.cnaf.infn.it.

Il meccanismo non è però agevole: un cambiamento di ISP, con conseguente variazione del prefisso assegnato, comporterebbe la necessità di modificare manualmente tutti i record!

Sono allo studio modifiche per rendere più "automatico" il meccanismo.

1.7 Protocolli di routing

Gli algoritmi per i protocolli di routing in IPv6 sono sostanzialmente gli stessi di IPv4: le implementazioni sono di fatto il "*porting*" da IPv4 ad IPv6.

In particolare anche in IPv6, come in IPv4, vi e' distinzione tra protocolli di routing interni agli Autonomous System (es. RIPng) e protocolli di routing esterni (BGP4+).

Una differenza tra IPv4 ed IPv6, è pero' nella definizione degli AS: con gli indirizzi unicast globali aggregabili ad ogni AS corrisponde solitamente un prefisso di rete.

Nel corso della della sperimentazione effettuata al CNAF (si veda la seconda parte) abbiamo effettuato prove di funzionamento sia con RIPng che con BGP4+.

1.7.1 *RIPng*[13]

RIPng è la semplice estensione di RIP1/2 a IPv6: ne mantiene quindi la semplicità e le limitazioni. Come in IPv4, la metrica RIPng di una rete è un intero appartenente all'intervallo [1,15]: RIPng si presta quindi ad essere impiegato solo all'interno di AS di piccole dimensioni (la sua implementazione in IPv6 ha avuto essenzialmente scopo di test).

Ogni voce (RTE) nelle tabelle di routing contiene (almeno):

- il prefisso IPv6 della destinazione
- il numero di bit del prefisso
- l'indirizzo IPv6 del router successivo verso la destinazione (non necessario se direttamente connessa)

---

[12] RFC 1886

[13] RFC 2080, 2081

Esiste inoltre un RTE di formato speciale che indica un router adiacente ("*next hop*"); l'indirizzo in tal caso è di tipo link-local (con la lunghezza del prefisso posta uguale a 0 e la metrica pari a 0xFF).

Gli RTE, a differenza di RIP1/2, non contengono esplicitamente l'informazione del "*next hop*" (per non rendere le tabelle troppo grosse) e quindi vengono raggruppati in base al "next hop" in blocchi preceduti dall'RTE speciale di riferimento.

Non c'è autenticazione come in RIP2 perchè ciò è garantito (in teoria!) da IPv6.

1.7.2 *BGP4+*[14]

BGP4+ è l'estensione multiprotocollo di BGP4: permette cioè il trasporto delle informazioni di routing, oltre che per il protocollo IPv4, anche di IPX e IPv6.

Un vincolo forte è il fatto che il router BGP deve avere, per compatibilità con le versioni precedenti, un indirizzo IPv4: in questo modo i router BGP4 possono interoperare con i router BGP4+ limitandosi ad ignorare gli annunci non relativi ad IPv4.

Con gli indirizzi unicast globali aggregabili, viene realizzata una struttura gerarchica in cui ogni router annuncia solo l'aggregato delle reti che transitano attraverso di esso, con notevole miglioramento dell'efficienza.

Non vi sono comunque differenze concettuali rispetto alla versione precedente di BGP.

Operativamente abbiamo osservato, per quanto riguarda l'implementazione CISCO, una certa instabilità nelle sessioni BGP.

2. SPERIMENTAZIONE AL CNAF

La sperimentazione effettuata al CNAF si inserisce nel contesto di 6BONE.

6BONE è la rete di test IPv6, creata dal working group *ipng* di IETF, come banco di prova per comprendere le problematiche della transizione al protocollo IPv6, dell'implementazione e della realizzazione pratica delle molte idee ancora al vaglio dei working group.

6BONE è basata su *tunnel*: questa tecnica permette di stabilire un "collegamento virtuale" tra due nodi IPv6 per trasmettere pacchetti IPv6 attraverso una rete IPv4; dal punto di vista dei due nodi questo collegamento (tunnel IPv6) appare come un collegamento *point-to-point.*

6BONE ha una struttura gerarchica: ai nodi del *backbone*, il piu` possibile magliati tra loro, sono connessi nodi di transito e nodi foglia.

---

[14] RFC 2283

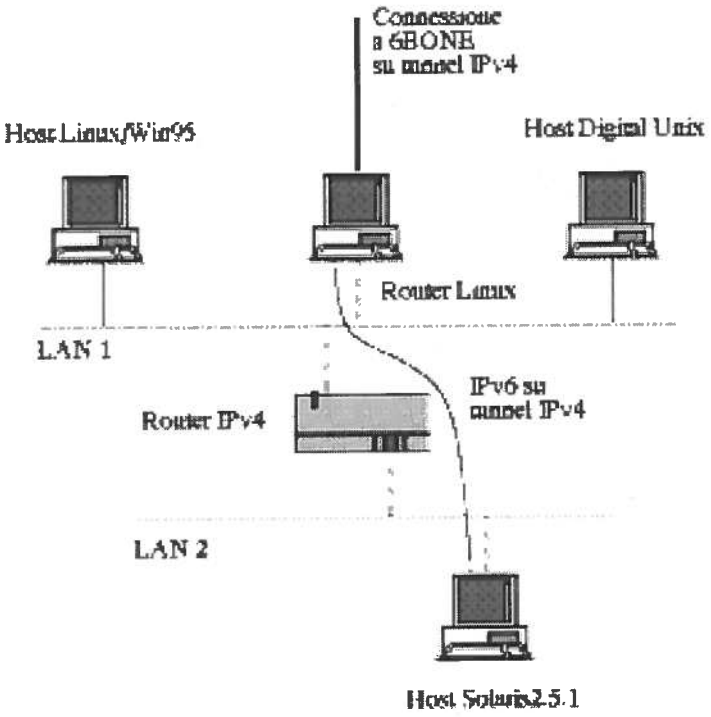


FIG.8 - Layout di test (prima fase)

2.1 Prima fase

Il CNAF, da Febbraio a Settembre '97, ha partecipato a 6BONE come foglia di ESNET (USA) e JOIN (Germania).

Durante questo periodo gli indirizzi usati su 6BONE erano del tipo "*provider based*": il prefisso della LAN principale del CNAF era *5f15:4100:839A:300:0/80*.

Inoltre poichè non era ancora disponibile il supporto di IPv6 per CISCO, in questa fase il routing è stato effettuato da un host Linux.

Gli host impiegati nella sperimentazione (due PC con Linux e Windows95, una workstation Sun con Solaris ed una Alpha con Digital Unix) hanno permesso di verificare l'implementazione di IPv6 sulle varie piattaforme. In tutti i casi gli host hanno doppio *stack* (IPv4 ed IPv6 sono indipendenti).

- **IPv6 per Linux**: disponibile a partire dai kernel 2.1.x, si è dimostrato funzionale e affidabile. È sottoposto ad un continuo aggiornamento.

- **IPv6 per Solaris**: IPv6 su Solaris è direttamente supportato, seppure in via solo sperimentale, da SUN che periodicamente aggiorna le versioni del software disponibili e le distribuisce in un unico pacchetto, ottenibile gratuitamente dalla rete. L'implementazione appare stabile e perfettamente funzionante, offrendo anche un server DNS e WWW.

- **IPv6 per Digital UNIX**: anche in questo caso, IPv6 è supportato, sebbene solo il via sperimentale, da DIGITAL, che fornisce una serie di pacchetti gratuiti di semplice installazione. La documentazione è migliore di quella Solaris, con un buon manuale stampabile. Il comportamento del pacchetto è buono.

- **Windows '95**: la versione Windows 95 da noi provata è quella reperibile con licenza di 30 giorni da FTP Software, inclusa nel pacchetto "Secure Client". Scaduto il periodo di prova è

necessario acquistare il prodotto. Il comportamento è parso sufficiente. È ora disponibile la versione Microsoft del protocollo IPv6 per Windows NT 4.0, ma fino a questo momento non siamo stati in gradi di provare applicativi.

Su Linux e Digital Unix è stata installata la versione di *bind* compatibile con IPv6 (per il supporto dei record AAAA), e creato il dominio *ipv6.cnaf.infn.it* (primario gandalf.cnaf.infn.it) per registrare gli indirizzi IPv6 dei nodi del CNAF. È stata inoltre ottenuta la delega da *isi.edu* per la risoluzione inversa degli host della rete *5f15:4100*.

Sull'host Linux che fungeva da router abbiamo installato *mrtd*[15]*:* prima la versione 1.3.6A e successivamente la 7-8-97, quest'ultima stabile e ben funzionante. Sono supportati i seguenti protocolli di routing: BGP4, RIP1/2 e RIPNG.

Nel nostro caso era attiva una sessione *RIPng* verso JOIN. L'interfaccia di *mrtd* e' molto simile a quella di un router CISCO (è riportato un esempio in Appendice).

Sullo stesso host Linux è stato installato *radvd*, il daemon per l'autoconfigurazione.

La sua configurazione è semplice: è sufficiente indicare il prefisso da annunciare sulla LAN e la sua lunghezza in bit.

2.2 Seconda fase

La crescita disorganica di 6BONE ha reso necessaria una "riorganizzazione": al 39° IETF (Munich 11-15 Agosto '97) è stato quindi deciso di adottare gli indirizzi unicast globali aggregabili ed il BGP4+ come protocollo di routing fra i nodi del backbone.

Alla rete 6BONE è stato assegnato il prefisso TLA *3ffe/16* ; a propria volta è stato assegnato, ad ogni nodo del backbone, un pTLA ID (pseudo Top Level Aggregation Identifier) ovvero un prefisso di 24 bit.

Al CNAF, diventato in tale occasione sito di backbone, è stato assegnato il prefisso *3ffe:2300::0/24*.

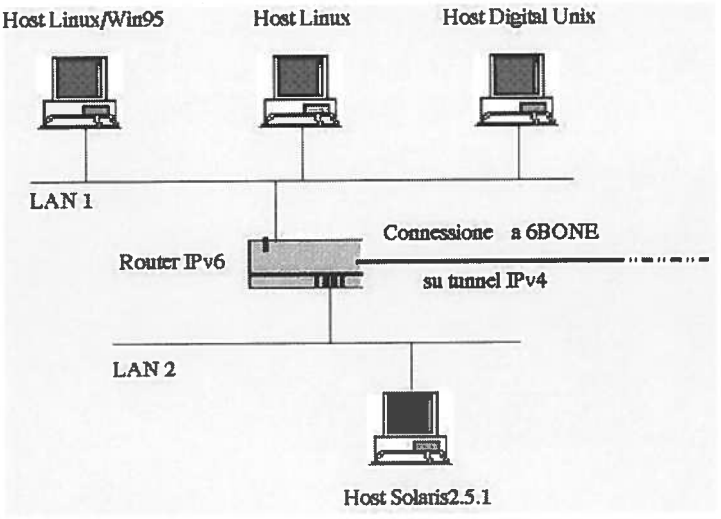


FIG.9 - Layout di test (seconda fase)

La riconfigurazione è avvenuta, come per tutti i siti di backbone, nel mese di Ottobre '97.

Contestualmente è stato attivato il processo il routing BGP4+ sui tunnel fra i nodi di

[15] Disponibile a ftp://ftp.merit.edu/net-research/mrt

backbone. In seguito a tutto questo è anche cambiata la topologia della nostra rete interna, con il passaggio del processo di routing dalla macchina Linux ad un router CISCO.

Attualmente abbiamo tunnel IPv6 (BGP4+) verso **ESNET**, **JOIN**, **G6** e **SWITCH** (siti di backbone); offriamo inoltre connessione a nodi italiani e greci ai quali abbiamo quindi assegnato dei prefissi.

Per tale motivo, abbiamo preparato un piano di assegnazione di indirizzi IPv6 per il GARR.

2.2.1 *Proposta di assegnazione delle reti IPv6 ai siti GARR*

Il prefisso (pTLA) assegnato al CNAF (**3ffe:2300/24**) sarà comune a tutte le reti 6BONE del GARR (GARR-PREFIX).

Lo schema di indirizzo proposto è illustrato nella seguente figura.

001	1111111111110	00100011	xxxxxxxx	rr	yyyyyyyyyyyyyy	ssssssssssssssss
FP (3 bit)	6bone TLA (13 bit)	GARR NLA1 (8 bit)	PdA ID (8 bit)	Riservati (2 bit)	User ID (14 bit)	SLA ID (16 bit)

FIG.10 - Schema di indirizzamento IPv6 proposto per il GARR

Gli 8 bit successivi al pTLA identificano il Punto di Accesso alla rete GARR (PdA ID); la numerazione avviene in maniera progressiva, a partire da 0 e assegnando i soli numeri pari. Ad esempio supponendo di assegnare a Bologna il PdA ID 0 ed a Roma il PdA ID 2, avremo:

- Bologna: 3ffe:2300/32
- Roma: 3ffe:2302/32

I 2 successivi bit sono riservati; il loro valore, per il momento deve essere uguale a 0. I rimanenti 14 bit vengono utilizzati per individuare gli utenti attaccati al PdA (User ID). Così il CNAF, con uno User ID assegnato uguale a 0, avrà allora come prefisso:

- CNAF: 3ffe:2300::0/48

All'interno dello spazio reti del CNAF, gli indirizzi con SLA ID uguale a ffff, sono riservati per individuare i tunnel tra il CNAF e gli altri siti IPv6: tali sottoreti hanno prefisso di lunghezza pari a 126. Quindi in ordine di uso le reti usate per i tunnel sono:

- 3ffe:2300:0:ffff::0/126 (riservata)
- 3ffe:2300:0:ffff::4/126
- 3ffe:2300:0:ffff::8/126
- 3ffe:2300:0:ffff::c/126

etc…

3. TEST DI CONNETTIVITÀ

Abbiamo realizzato alcune prove, mediante ping, per verificare la connettività IPv6 e la

differenza di prestazioni tra le due versioni del protocollo sia in ambito locale (IPv6 nativo) sia geografico (tunnel IPv6 su IPv4).

Le misure sono state ripetute piu' volte, a differenti orari (con diversi carichi della rete).

3.1 Ping locali

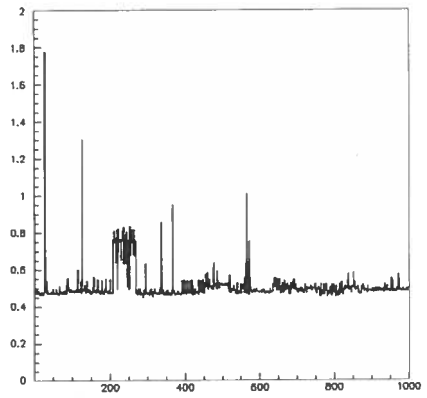
Durante la prima fase (Febbraio – Settembre '97) sono state effettuate misure in IPv6 nativo fra nodi appartenenti alla stessa LAN; nella seconda fase, con l'arrivo del router CISCO, collegandovi la seconda LAN, è stato possibile misurare anche le performance IPv6 del router.

3.1.1 *Connessioni IPv6 nativo su Ethernet*

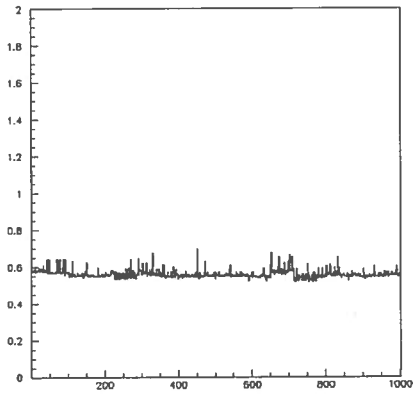
Abbiamo effettuato misure fra i vari nodi IPv6 della LAN, cercando di rilevare differenze di comportamento tra IPv4 ed IPv6.

I ritardi di trasmissione sono risultati però minimi: le prestazioni dei due protocolli risultano sostanzialmente identiche.

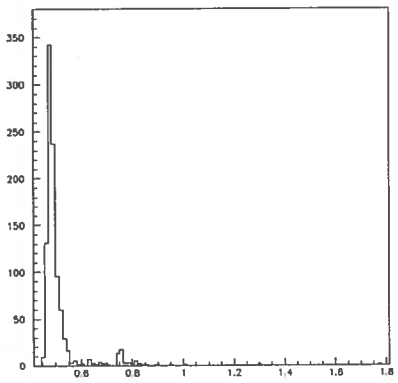
In particolare si può notare che il RTT medio è quasi uguale: IPv4 ha però un valore minimo minore ma uno sparpagliamento maggiore rispetto a IPv6.



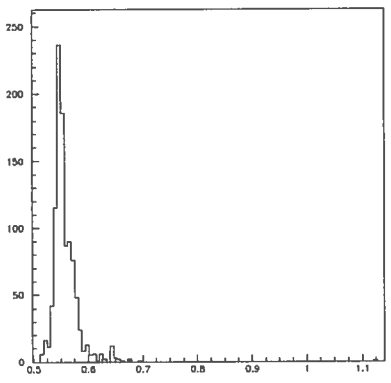
Andamento temporale ping (Ipv4)
In ascissa: numero progressivo. In ordinata: ms



Andamento temporale ping (Ipv6)
In ascissa: numero progressivo. In ordinata: ms



Distribuzione temporale ping (IPv4)
Istrogramma (unità in ascissa: ms)



Distribuzione temporale ping (IPv6)
Istrogramma (unità in ascissa: ms)

FIG.11 - Prove ping su Ethernet

Questo risultato conferma che, nonostante le ampie modifiche apportate nella nuova versione del protocollo, le prestazioni non sono peggiorate.

D'altra parte ciò indica anche che le implementazioni esaminate, tutte versioni preliminari, hanno già raggiunto un buon grado di affidabilità.

3.1.2 *Connessioni IPv6 nativo attraverso un router CISCO*

Le prove di connessione fra due nostre LAN in IPv6 nativo, attraverso un router CISCO, hanno confermato il buon comportamento del nuovo protocollo.

Anche in questo caso si nota un maggiore sparpagliamento del RTT in IPv4 rispetto a IPv6.

Questo effetto potrebbe essere imputabile all'implementazione di IPv4 nell'host con il quale sono state effettuate le misure.

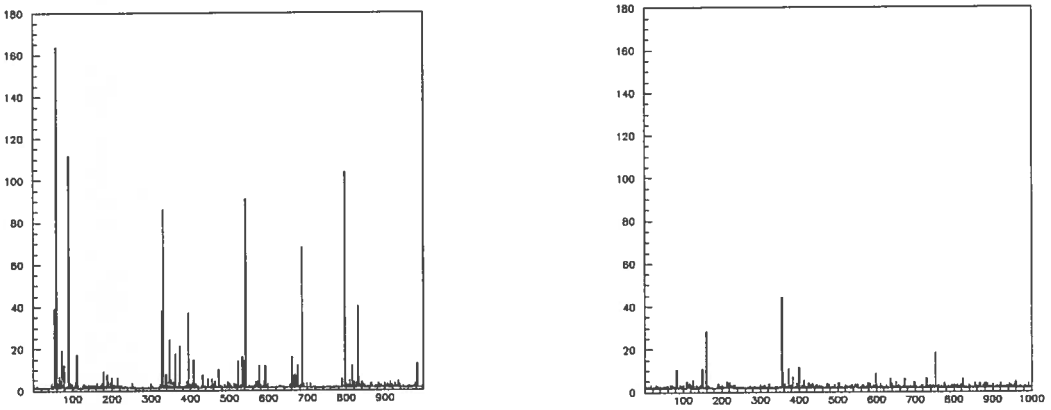


FIG.12 - Prove ping attraverso un router IPv4/IPv6

3.2. Connessioni IPv6 su WAN

Per ottenere un confronto tra le prestazioni di IPv6 e quelle di IPv4, dobbiamo essere certi di seguire lo stesso percorso con ambedue i protocolli.

Dato che le connessioni IPv6 in geografico avvengono tramite tunnel su IPv4, e poichè il routing IPv6 è completamente indipendente dal routing IPv4, solo i nodi a noi direttamente connessi tramite tunnel offrono questa garanzia.

Inoltre, è intuitivo aspettarsi prestazioni inferiori per IPv6 a causa dell'*overhead* dovuto all'incapsulamento.

Abbiamo misurato la connettività verso tre dei siti di backbone con i quali abbiamo un tunnel diretto (verificando preliminarmente che fosse operativo!): JOIN, ESNET ed INRIA.

3.2.1 *JOIN*

JOIN (Germania), è connesso, come il CNAF, alla rete europea TEN-34 e questo permette prestazioni eccellenti a livello IPv4. Dal grafico della figura si vede infatti che il "Round Trip Time" medio è normalmente circa 40 msec.

Anche IPv6 offre ottime prestazioni, confrontabili con IPv4.

Nel grafico si possono osservare due intervalli durante i quali è mancata la connessione per

entrambi i protocolli.

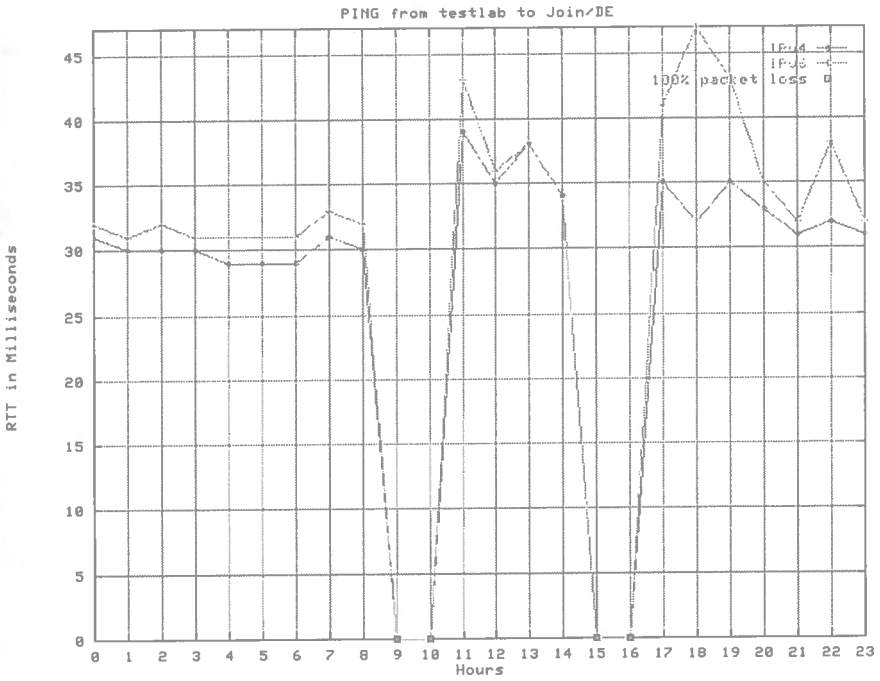


FIG.13 - Prove ping verso JOIN

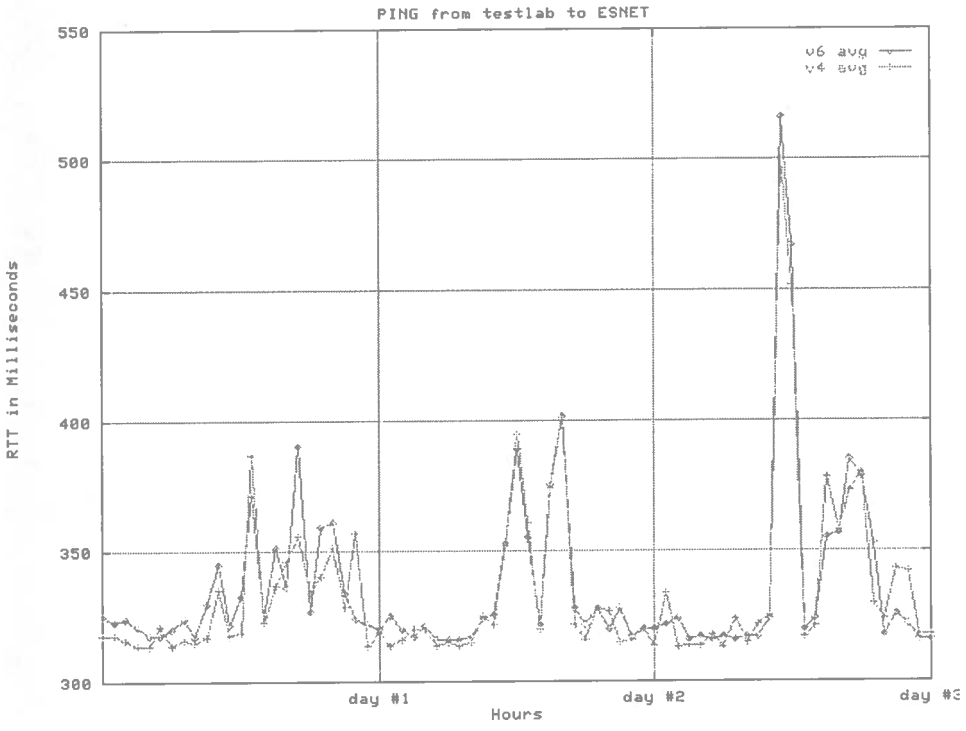


FIG.14 - Prove ping verso ESNET

3.2.2 *ESNet*

Il CNAF è connesso alla rete ESNet in USA tramite un link dedicato (T1), dalle prestazioni relativamente buone. Come si vede dal grafico nella figura, il comportamento di IPv4 ed IPv6 sono

pressoché identici nell'arco di una giornata.

3.2.3 *INRIA*

Anche INRIA è collegato a TEN-34. Come si vede dalla figura, le prestazioni dei protocolli sono ottime, e tendono a coincidere. In alcuni punti, addirittura IPv6 è più veloce di IPv4! Questo risultato, a meno che non ci siano difetti nell'implementazione dell'utility ping, indica che l'*overhead* dovuto al *tunneling* può pesare meno di altri fattori come l'occupazione maggiore dello *stack* IPv4 negli end-node.

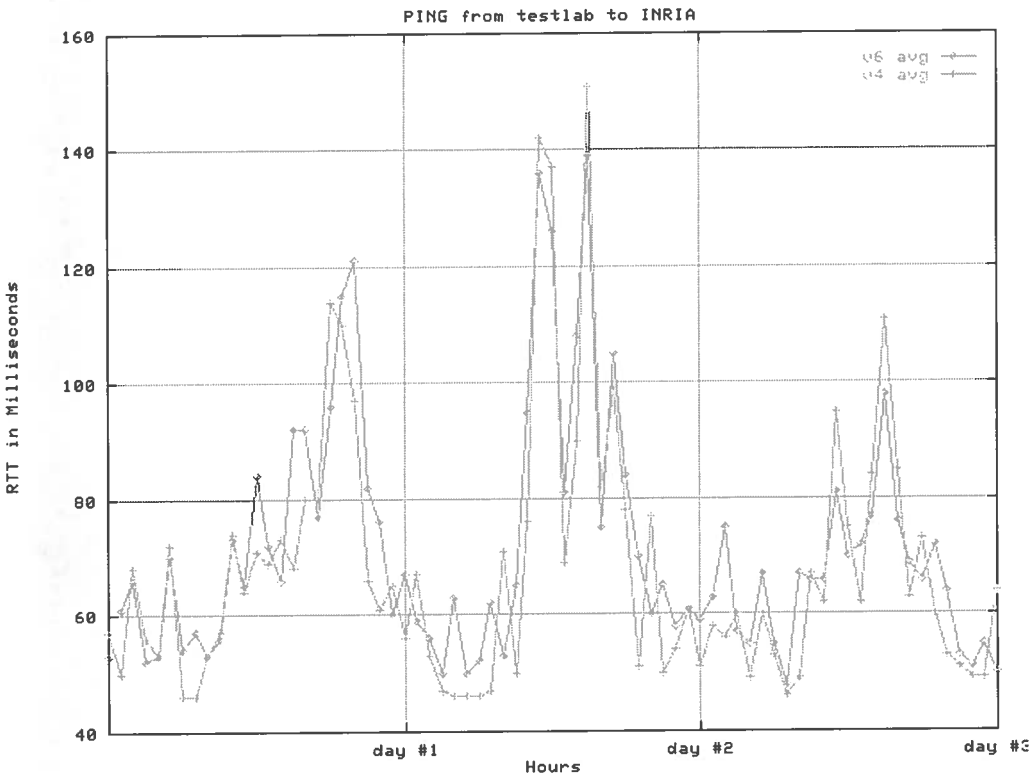


FIG.15 - Prove ping verso INRIA

4 RICERCHE FUTURE

Data la vastità e l'importanza dell'argomento, ci sono ancora molti punti da chiarire e su cui investigare: supporto della qualità di servizio, l'evoluzione del DNS per ottimizzare l'autoregistrazione ed il renumbering, l'evoluzione del routing finalizzato al renumbering trasparente ed il supporto per la mobilità degli host.

Riteniamo importante, in particolar modo, per il futuro di IPv6 lo sviluppo di nuove applicazioni che beneficino di servizi a qualità garantita, essendo questo un aspetto sempre piu' importante nelle funzionalità di una rete.

Da un punto di vista operativo, dovrà essere seguita con attenzione la migrazione da IPv4 a IPv6: nella prima fase, i nodi IPv6 dovranno implementare entrambi i protocolli; questa architettura *dual stack* permetterà agli host ed ai router di comprendere entrambi i protocolli.

Una delle strategie di migrazione più probabili potrebbe consistere nel movimento di interi domini verso IPv6 per semplificare l'amministrazione del dominio stesso.

Un altro punto ancora non chiarito è tutta la parte relativa alla sicurezza del protocollo, attualmente non implementata, ma di grande interesse non appena soluzioni operative saranno disponibili.

BIBLIOGRAFIA

Oltre alla documentazione citata nelle varie sezioni, indichiamo:

- S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification,* Internet Draft, july 1997
- R. Hinden and M. O'Dell, *TLA and NLA Assignment Rules*, Internet Draft, july 1997
- S. Thomson and T. Narten, *IPv6 Stateless Address Autoconfiguration*, Internet Draft, july 1997
- R. Hinden and S. Deering, *IP Version 6 Addressing Architecture*, Internet Draft, july 1997
- A. Conta and S. Deering, *Generic Packet Tunneling in IPv6 Specification*, Internet Draft, december 1996
- C. Huitema and S. Thomson, *DNS Extensions to Support IPv6*, Internet Draft, february 1998
- Dan Harrington, *DHCP Option for IPv6 Transition*, Internet Draft, July 1997
- R. Hinden, M. O'Dell and S. Deering, *An IPv6 Aggregatable Global Unicast Address Format*, Internet Draft, march 1998

APPENDICE A: SOFTWARE E DOCUMENTAZIONE IN RETE

Ci sono numerosi siti dedicati all'argomento. Il più completo è sicuramente quello della SUN[16], dove è presente la maggior parte del materiale informativo aggiornato (draft e RFC) oltre a una completa lista di implementazioni per varie piattaforme.
A questo proposito, i siti per le varie piattaforme, da noi provate, sono:

- SUN Solaris: http://playground.sun.com/ipv6
- DIGITAL UNIX: ftp://sipper.zk3-x.dec.com/pub/
- Linux: in un qualunque mirror del *sunsite*
- Windows 95: http://www.ftp.com all'interno del pacchetto secure-client

Si noti che il supporto CISCO deve essere richiesto alla CISCO.

Deve essere poi menzionato il sito 6BONE, curato da Bob Fink (chairman del working group ngtrans dedicato proprio alla transizione verso IPv6): http://www.6bone.net

Per ottenere informazioni aggiornate, è consigliabile iscriversi alle mailing list:

- IPNG: ipng@sunroof.sun.eng.com
- 6BONE: 6bone@isi.edu

Per quanto riguarda invece la documentazione più recente sull'argomento ci si può collegare a: http://www.nis.garr.it/netdoc cercando i file del tipo: *draft-ietf-ipng-xxxx*.

[16] http://playground.sun.com/ipv6

APPENDICE B: PACCHETTI SOFTWARE

Riportiamo alcune note sull'installazione di IPv6 su alcune piattaforme.

- **Linux**: il supporto IPV6 nei kernel Linux è presente nelle versioni sperimentali 2.1.x e verrà incluso nella versione stabile 2.2.0 e successive. Partendo dalla distribuzione Slackware standard di Linux (kernel 2.0.x), per installare correttamente le release 2.1.x del kernel è necessario compiere alcuni upgrade preliminari di librerie di sistema, utility di rete che supportino IPv6 etc... La lista completa delle operazioni preliminari da effettuare è contenuta nella documentazione dei sorgenti del kernel (Doc/Changes). Il passo successivo è la compilazione del nuovo kernel: nella sezione relativa al network, è necessario ovviamente attivare la voce IPv6 (anche come modulo). La configurazione per un host secondario è automatica: al boot contatta il router IPv6 e acquisisce le informazioni relative al routing (stabilisce la default verso il router) ed al prefisso. Il router deve essere invece configurato: va assegnato il prefisso, configurate le interfacce (sia quella di rete che i tunnel) e attivato il processo di routing.

- **Solaris**: il pacchetto è disponibile al seguente URL: http://playground.sun.com/pub/solaris2-ipv6/html/solaris2-ipv6.html
  È ben documentato e di facile installazione attraverso il programma standard pkgadd.
  Attualmente può essere installato unicamente su macchine con sistemi solaris 2.5 e 2.5.1 senza patch.

- **DIGITAL Unix**: il pacchetto è disponibile tramite ftp al seguente indirizzo: ftp://sipper.zk3-x.dec.com/pub/ipv6_binary_X6.1.tar.gz .È disponibile separatamente anche un web server versione 6: ftp://sipper.zk3-x.dec.com/pub/ipv6_www_X6.1.tar.gz ed un programma per testare l'implementazione: ftp://sipper.zk3-x.dec.com/pub/bricks-v6kit.tar.Z. Il comportamento è buono e non sono stati riscontrati particolari problemi. Può essere installato unicamente su sistemi operativi con versione 4.0 o superiore.

- **Windows 95**: l'implementazione si ottiene presso il sito di FTP Software (http://www.ftp.com) all'interno del pacchetto "Secure Client". Il programma si installa facilmente e crea un nuovo Stack IP con la possibilità di attivare il protocollo IPv6. Il tutto avviene in maniera "nascosta" per l'utente, come sempre in Windows, e l'utente deve solo verificare che tutto funzioni tramite i programmi di prova, ping ed un packet sniffer, presenti nella stessa distribuzione software. Non è necessario nessun altro pacchetto oltre a quello indicato.

APPENDICE C: ESEMPI DI CONFIGURAZIONE

1. Esempio di configurazione di processo di routing RIPng con mrtd su sistema Linux[17]

```
!
! definizione delle interfacce
!

! interfaccia ethernet
ifconfig eth0 add 5F15:4100:839A:0300:0000:00A0:2499:0DA7/80 ! prefisso di 80 bit
route -A inet6 add 5F15:4100:839A:0300::0/80 eth0                ! rete locale

! tunnel verso ESNET
ifconfig sit0 tunnel ::${TUNNEL1}
ifconfig sit1 up
route -A inet6 add 5f01:2500::0/32 gw fe80::${TUNNEL1} sit1

! tunnel verso JOIN
ifconfig sit0 tunnel ::${TUNNEL2}
ifconfig sit2 up

! tunnel verso fenice (su altra LAN del CNAF)
ifconfig sit0 tunnel ::${TUNNEL3}
ifconfig sit3 up
route -A inet6 add 5f15:4100:c087:1700::0/80 gw fe80::${TUNNEL3} sit3

!
! processo di routing
!
router ripng
network sit2                                          ! tunnel verso JOIN
redistribute static
!
ip route 5f01:2500::/32 ::131.154.3.24                ! statica verso ESNET
ip route 5f15:4100:c087:1700::0/80 ::131.154.3.24     ! statica verso fenice
```

[17] TUNNEL1, TUNNEL2 e TUNNEL3 sono gli indirizzi IPv4 dell'*end-node* dall'altro lato del tunnel.

2. Esempio di configurazione di processo di routing BGP su router CISCO

```
!
ipv6 unicast-routing
ipv6 bgp neighbor 3FFE:700:20:2::9 remote-as 293
ipv6 bgp neighbor 3FFE:302:11:2:0:2:0:51 remote-as 1717
ipv6 bgp neighbor 3FFE:2000:0:1::61 remote-as 559
ipv6 bgp neighbor 3FFE:401::2C0:33FF:FE02:14 remote-as 1275
ipv6 bgp network 3FFE:2300::0/24 summary                    ! aggregazione
ipv6 bgp redistribute connected
!
! definizione tunnel
!
interface Tunnel100
 description tunnel BGP4+ -----> ESNET
 no ip address
 ipv6 address 3FFE:700:20:2::A/126
 tunnel source Ethernet3/0
 tunnel destination 198.128.2.27
 tunnel mode ipv6ip
!
interface Tunnel101
 description tunnel BGP4+ -----> IMAG
 no ip address
 ipv6 address 3FFE:302:11:2:0:2:0:52/124
 tunnel source Ethernet3/0
 tunnel destination 129.88.26.7
 tunnel mode ipv6ip
!
interface Tunnel102
 description tunnel BGP4+ -----> SWITCH
 no ip address
 ipv6 address 3FFE:2000:0:1::62/124
 tunnel source Ethernet3/0
 tunnel destination 130.59.15.6
 tunnel mode ipv6ip
!
interface Tunnel103
 description tunnel BGP4+ -----> JOIN
 no ip address
 ipv6 enable
 ipv6 address 3FFE:2300:0:FFFF::9/126
 tunnel source Ethernet3/0
 tunnel destination 128.176.191.66
 tunnel mode ipv6ip
!
! definizione interfacce sulla LAN
!
interface Ethernet3/0
 ip address 131.154.3.58 255.255.255.0
 ip route-cache flow
 ipv6 address 3FFE:2300::0/64 eui-64          ! prefisso annunciato sulla LAN
!
interface Ethernet3/1
 ip address 131.154.100.1 255.255.255.0 secondary
 ip address 192.135.23.1 255.255.255.0
 ip pim dense-mode
 ip dvmrp default-information only
 no ip mroute-cache
 no ip route-cache optimum
```

```
 ip route-cache flow
 ipv6 address 3FFE:2300:0:1::0/64 eui-64                ! prefisso annunciato sulla LAN
!
router bgp 137
!
! l'AS di JOIN non è direttamente collegato
!
ipv6 route 3FFE:401::2C0:33FF:FE02:14/128 Tunnel103
```