IPV6 E COESISTENZA CON IPV4

Marco Sommani

1. UN PO' DI STORIA

Alla base del progetto che portò alla definizione dell'Internet Protocol (IP) c'era il presupposto di poter assegnare un indirizzo IP globalmente univoco (pubblico) alle interfacce di rete di tutti i sistemi connessi. Nella Internet che generalmente utilizziamo, basata sulla versione 4 del protocollo IP (IPv4) con indirizzi di 32 bit, da tempo questo presupposto progettuale viene violato. Già da più di un decennio la Internet IPv4 è costituita da un nucleo centrale in cui si usano indirizzi univoci (pubblici), contornato da numerose isole nelle quali vengono riutilizzati, in maniera non più univoca, gli indirizzi riservati per le "Private Internet" (RFC1918: blocchi 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16). Nei punti di contatto fra le isole e il nucleo centrale, i Network Address Translator (NAT) effettuano sul traffico in transito la conversione fra indirizzi pubblici e indirizzi RFC1918 e viceversa, generalmente mappando molti indirizzi RFC1918 dell'isola su un unico indirizzo pubblico. Questo accorgimento ha permesso ad Internet di continuare a crescere fino ad oggi, apparentemente sconfessando tutte le previsioni pessimistiche con cui, a partire dal 1991, è stato ripetutamente pronosticato l'imminente esaurimento degli indirizzi IPv4.

Coloro che, alla fine degli anni '70, progettarono l'IPv4, avevano in mente una rete che avrebbe collegato per lo più università e organismi di ricerca governativi e militari statunitensi. Avevano inoltre in mente un mondo in cui la densità dei computer era enormemente più bassa di quella odierna. Ai progettisti, un campo di 32 bit, che poteva assumere più di 4 miliardi di valori diversi, appariva addirittura sovradimensionato. In effetti per tutto il periodo iniziale (fino all'inizio degli anni '90) gli indirizzi IPv4 furono distribuiti come se si fosse trattato di una risorsa quasi inesauribile. Nell'arco di tempo fra il 1989 e il 1994 diventò evidente che Internet poteva essere utilizzata in un contesto enormemente più vasto di quello iniziale:

Nel 1991 le proiezioni mostravano che il tasso di assegnazione degli indirizzi IPv4 aveva raggiunto livelli tali da portare al loro esaurimento entro il 1994. A partire da quel momento furono introdotti controlli e regole, allo scopo di evitare l'assegnazione di blocchi di indirizzi di dimensioni superiori alle reali esigenze del richiedente. Nello stesso tempo si cominciò a pensare ad un possibile successore di IPv4. Nel dicembre 1995 l'Internet Engineering Task Force (IETF) pubblicò l'RFC1883 "Internet Protocol Version 6 (IPv6) Specification" (rimpiazzato nel dicembre 1998 dall'RFC2460), nel quale viene definita la versione 6 dell'Internet Protocol (IPv6), caratterizzata da indirizzi lunghi 128 bit. L'ampiezza dello spazio di indirizzamento di IPv6 è tale da rendere inimmaginabile un suo esaurimento.

Nel frattempo si scoprì che il passaggio ad una distribuzione regolamentata degli indirizzi IPv4 aveva provocato una riduzione del tasso di assegnazione assai superiore a quella ipotizzata da chi aveva definito le regole. Infatti, mentre per avere indirizzi pubblici (non RFC1918) era necessario sottostare alle verifiche ed ai controlli periodici dei Regional Internet Registries (RIR), gli indirizzi RFC1918 continuavano ad essere usabili in totale libertà. Questo fatto rese i NAT estremamente popolari. Il ricorso agli indirizzi RFC1918 fu ulteriormente favorito dalla convinzione, falsa ma assai diffusa, secondo la quale il NAT sarebbe uno strumento particolarmente adatto a rendere le reti più sicure.

Dunque, un effetto collaterale non previsto causato dalla decisione di regolamentare la distribuzione degli indirizzi IPv4 fu la scomparsa dell'univocità dell'indirizzamento globale. Da allora la distribuzione di nuovi indirizzi IPv4 è continuata, ma limitatamente al nucleo centrale di Internet ed a quegli ambienti (prevalentemente università e ricerca), dove non si è mai rinunciato al rispetto dei principi ispiratori dei progettisti dell'Internet Protocol. Più avanti si cercherà di evidenziare quali perdite di funzionalità e di potenzialità si sono avute su Internet in seguito all'abbandono dell'indirizzamento univoco.

Nel frattempo, la distribuzione degli indirizzi IPv4 è continuata, anche se a ritmo molto più moderato. All'inizio del 2009 si stima che la riserva possa esaurire in tempi assai brevi. La Internet Assigned Numbers Authority (IANA) dispone ancora di 34 blocchi /8 (blocchi di 224=16.777.216 indirizzi aventi i primi 8 bit uguali) da distribuire ai 5 Regional Internet Registries (AFRINIC, APNIC, ARIN, LACNIC e RIPE). I Regional Internet Registries (RIR) hanno il compito di distribuire gli indirizzi IP ai Local Internet Registries

(LIR), che il più delle volte coincidono con gli Internet Service Provider. I RIR controllano che i LIR facciano un uso oculato degli indirizzi loro assegnati. Un RIR, quando vede che il pool di indirizzi liberi a sua disposizione scende al di sotto di una determinata soglia, chiede a IANA che gli vengano allocati nuovi blocchi /8. La seguente tabella mostra l'andamento dell'allocazione dei blocchi /8 a partire da quando, nel 1993, la distribuzione fu regolamentata.

Pre-93	91	**2001**	7
1993	7	**2002**	4
1994	2	**2003**	6
1995	4	**2004**	9
1996	4	**2005**	11
1997	4	**2006**	10
1998	1	**2007**	13
1999	1	**2008**	9
2000	4	**2009**	8

In sintesi, dei 221 blocchi /8 usabili in tutto o in parte per distribuire indirizzi pubblici, 91 sono stati allocati in epoca non regolamentata, 104 nel periodo 1993-2009 e 26 saranno allocati negli anni successivi al 2009. In base ai dati disponibili, si può affermare che prima della fine del 2012 IANA avrà allocato tutti i blocchi; è anche possibile che questo evento avvenga già prima della fine del 2011.

Alcuni sostengono che sia possibile continuare a far crescere Internet con il solo IPv4 ancora per più di un decennio. Dal punto di vista strettamente tecnico, una tale tesi è pienamente lecita, ma non deve essere usata per giustificare l'inerzia e la diffidenza nei confronti di IPv6. Non si deve dimenticare che l'apertura a IPv6 rappresenta il cammino di minor costo per il futuro della rete. Piuttosto che spendere energie e denaro per assicurare alla Internet IPv4 una crescita stentata fra complessità e limitazioni, occorre prendere atto di quanto segue.

- IPv6 oggi è una tecnologia più matura di quello che era IPv4 nei primi anni '90
- L'attivazione di IPv6 su un sistema o una sottorete non provoca nessun inconveniente sul traffico IPv4
- IPv6 è utilizzabile contemporaneamente a IPv4 su tutti i moderni sistemi operativi
- Qualunque computer con un sistema operativo recente, che non si trovi dietro firewall particolarmente restrittivi, può essere inserito nella Internet IPv6 tramite tunnel agendo esclusivamente sul computer stesso, senza che sia necessario aggiornare i router o contrattare con ISP o gestori di "tunnel brokers"
- Può capitare di essere collegati alla Internet IPv6 senza saperlo: Windows Vista e Windows 7 in configurazione "nativa" aprono automaticamente tunnel di tipo "Teredo" o "6to4"
- Molte applicazioni (per esempio i web browser), quando si trovano su un computer dotato di indirizzo IPv6 globale, scelgono il trasporto IPv6 quando dalla consultazione del DNS risulta che anche il destinatario possiede un indirizzo IPv6: può dunque capitare di essere utilizzatori inconsapevoli di IPv6
- Anche su quei sistemi in cui l'attivazione di IPv6 o dei tunnel non è automatica, i comandi di attivazione sono di tipo ON/OFF e non richiedono l'immissione di parametri particolari
- IPv6 merita di essere apprezzato per la sua semplicità e immediatezza di uso.

All'inizio del 2010 la Internet IPv6 è viva e vegeta e coesiste senza problemi con la Internet IPv4, ma rappresenta una porzione veramente esigua dell'intera rete. Di tutto il traffico che transita da AMS-IX (l'Internet Exchange di Amsterdam), quello IPv6 nativo (cioè non trasportato dentro tunnel IPv4) si aggira intorno allo 0,2 % del totale (in termini assoluti si tratta di flussi oscillanti fra minimi di 700 Mbps e massimi di 1800 Mbps). Naturalmente le statistiche di AMS-IX tengono conto solo del traffico IPv6 "nativo" e non di quello incapsulato in tunnel IPv4.

Stando così le cose, quale strategia consigliare ai pianificatori ed ai gestori di reti? Dare retta a chi consiglia di non fare niente, sostenendo che, ammesso che IPv6 sia destinato ad uscire dallo stato di tecnologia di nicchia, passeranno molti anni prima che ciò avvenga? In realtà, anche a voler dare credito a questa opinione, resta il fatto che IPv6 è già in mezzo a noi e che, quanto più continua ad essere trattato come un oggetto ignoto e misterioso, tanto più può essere sfruttato da malintenzionati per fare danni. Anche i più scettici sulle probabilità di successo di IPv6 non possono ignorare che parte delle energie dei gestori e dei pianificatori di reti ormai devono essere dedicate a IPv6.

2. PRINCIPALI CARATTERISTICHE DI IPV6

2.1 Il formato degli indirizzi (RFC4291)

Per rappresentare gli indirizzi IPv6 in formato testo si usa la notazione

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

In altre parole, i 128 bit vengono suddivisi in 8 gruppi di 16 bit. Gli 8 gruppi sono separati dal carattere ":". I 16 bit di ciascun gruppo sono rappresentati con 4 cifre esadecimali:

2001:0db8:0000:0000:00a9:0000:0000:0001

È consentito omettere gli "0" iniziali di ciascun gruppo:

2001:db8:0:0:a9:0:0:1

Se l'indirizzo contiene una o più sequenze di gruppi di valore 0, una di queste sequenze può essere sostituita dalla notazione "::":

2001:db8::a9:0:0:1 oppure 2001:db8:0:0:a9::1

Come in IPv4, per designare un blocco di indirizzi aventi lo stesso prefisso di n bit si usa la notazione "/n":

2001:db8::/32	indirizzi da 2001:db8:0:0:0:0:0:0 a 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff
2001:db8::/64	indirizzi da 2001:db8:0:0:0:0:0:0 a 2001:db8:0:0:ffff:ffff:ffff:ffff
::/0	tutti gli indirizzi IPv6

Non tutti i 2^{128} valori possibili degli indirizzi IPv6 sono usabili come indirizzi unicast globali. La tabella 1 mostra le principali categorie di indirizzi IPv6, generalmente distinguibili in base al valore dei primi bit.

Le assegnazioni degli indirizzi globali (Global Unicast) sono fatte attingendoli da quelli che hanno nei primi 16 bit valori da 2000 a 3fff, spazio che rappresenta 1/8 di tutti i valori possibili. In futuro potranno essere usati come indirizzi Global Unicast anche quelli che nei primi 16 bit hanno valori da 1000 a 1fff , da 4000 a fe7f e da fec0 a feff. Lo spazio totale disponibile per indirizzi Global Unicast corrisponde quindi a 955/1024 dei valori possibili (circa il 93%).

Come in IPv4, gli indirizzi globali di tutte le interface di rete che condividono lo stesso *link* (LAN, collegamento PPP, etc.) hanno lo stesso prefisso e al blocco di indirizzi usabile sul *link* si dà il nome di *subnet*. La scelta della lunghezza del prefisso della *subnet* è libera, ma è fortemente raccomandato l'uso di prefissi lunghi 64 bit. Tipicamente tutti i sistemi collegati ad una stessa LAN hanno un indirizzo IPv6 identico nei primi 64 bit. Su una tipica *subnet* IPv6 si possono dunque usare 2^{64} indirizzi IPv6 diversi: il quadrato del numero di valori possibili per gli indirizzi IPv4.

Il processo di distribuzione degli indirizzi globali avviene attenendosi ai seguenti criteri: IANA distribuisce ai Regional Internet Registries (RIR) prefissi di 12 bit, i RIR distribuiscono ai LIR prefissi di 32 bit e questi distribuiscono ai loro clienti prefissi di 48 bit, per cui il tipico cliente può distribuire i suoi sistemi fra 2^{16} diverse *subnet* con prefisso di 64 bit.

Prefissi	Uso
::1/128	Indirizzo loopback
1000::/4	usabili in futuro per indirizzi Global Unicast
2000::/3	Global Unicast - in distribuzione
da 4000::/16 a fe7f::/16	usabili in futuro per indirizzi Global Unicast
fe80::/10	Link-Local Unicast
fec0::/10	Site-Local Unicast - deprecati dall'rfc3879 Spazio riassegnabile ai Global Unicast
ff00::/8	Multicast
ff02::/16	Multicast con link-local scope

Tabella 1: Principali categorie di indirizzi IPv6

Un'interfaccia di rete di un sistema IPv6 può non avere un indirizzo globale IPv6 (per esempio, se si trova su una sottorete non collegata all'IPv6 globale), ma dispone sempre almeno di un indirizzo IPv6 della categoria *Link Local Unicast*, che viene usato per comunicare con i sistemi IPv6 adiacenti (vale a dire quelli raggiungibili attraverso un singolo *link*, senza attraversamenti di router). I primi 10 bit degli indirizzi di questa categoria hanno il valore 1111111010; di solito i bit dall'11esimo al 64esimo hanno valore 0; gli ultimi 64 sono calcolati a partire da qualche identificatore univoco interno al sistema stesso, per esempio l'indirizzo MAC dell'interfaccia di rete. Un sistema, subito dopo aver determinato l'indirizzo IPv6 *Link Local Unicast* usabile su un link a lui adiacente, può comunicare con gli altri sistemi presenti sullo stesso link in unicast o in multicast. Per le comunicazioni multicast si usano indirizzi di destinazione della categoria "multicast con link local scope" (prefisso ff02::/16). Le comunicazioni multicast con indirizzi link local scope sono indispensabili per il funzionamento di IPv6, perché vengono usate per molti compiti di servizio, come scoprire gli indirizzi MAC associati agli indirizzi IPv6 (compito che in IPv4 è affidato al protocollo ARP), scoprire i router presenti sul link, apprendere dai router i prefissi globali usabili sul link.

Per assegnare gli indirizzi globali alle interfacce dei sistemi, oltre ai metodi già presenti in IPv4 (assegnazione manuale, via DHCP, etc.), è stato ideato un nuovo metodo, detto StateLess Address AutoConfiguration (SLAAC), che prevede che il sistema apprenda il prefisso della *subnet* (non più lungo di 64 bit) dai *Router Advertisement* emessi dai router presenti sul *link* e che si autoassegni i rimanenti bit usando meccanismi analoghi a quelli con cui vengono determinati i 64 bit meno significativi dell'indirizzo *Link Local Unicast*.

Tutti questi meccanismi rendono possibile l'uso di IPv6 senza che siano necessarie configurazioni manuali; tutto ciò facilita notevolmente l'inserimento in rete delle

più svariate *appliances*.

2.2 Il pacchetto IPv6

I protocolli di livello più basso (Ethernet, PPP, etc.) trattano IPv6 come un nuovo protocollo: i pacchetti IPv6 sono preceduti da un "protocol identifier" diverso da quello di IPv4. Per esempio, Ethernet II usa l'identificatore 0x86dd e il PPP 0x0047 (gli identificatori IPv4 sono, rispettivamente, 0x0800 e 0x0021).

Il formato dell'*header* IPv6 è riportato nella tabella 2.

ver=6	traffic class	flow label	
payload length		next header	hop limit
source address			
destination address			

Tabella 2: IPv6 header

È stato fatto uno sforzo per limitare la lunghezza dell'IPv6 header. Infatti, benché, rispetto a IPv4, la lunghezza degli indirizzi quadruplichi (da 4 a 16 ottetti), la lunghezza dell'*header* si limita a raddoppiare (da 20 a 40 ottetti). Sono state eliminate varie informazioni, che erano presenti nell'header IPv4, ma che sono state giudicate di scarsa utilità e/o di ostacolo al *forwarding* veloce dei pacchetti.

Di particolare importanza è l'eliminazione dei campi necessari per la frammentazione dei pacchetti; per questo motivo possono arrivare a destinazione solo quei pacchetti che già in partenza hanno una lunghezza sufficientemente piccola da poter essere trasmessi su tutti i link del percorso. Dunque, una sorgente di pacchetti IPv6 deve essere in grado di reagire correttamente ai messaggi di errore "maximum transfer unit exceeded" ricevuti dai router sul percorso. Su tutti i link IPv6 deve essere possibile trasmettere pacchetti lunghi fino a 1280 ottetti (il limite era di 512 ottetti in IPv4).

Alcune informazioni dell'header IPv4 si ritrovano, spesso in forma modificata, in campi che hanno cambiato nome:

- TTL ==> hop limit,
- protocol number ==> next header,
- TOS ==> traffic class,
- total length ==> payload length.

Di particolare interesse è il cambio di nome da *protocol number* a *next header*: come in IPv4, il numero contenuto nel campo serve a specificare quale tipo di contenuto si trova immediatamente dopo l'header; il *next header* può essere usato, come in IPv4, per identificare un protocollo di livello superiore (ICMP, TCP, UDP, GRE, OSPF...), ma può anche identificare un secondo tipo di header, che a sua volta conterrà un campo "next header" per identificare il tipo di contenuto che lo segue (tabella 3).

Ipv6 Header	Routing Header	Fragment Header	
Next Header = Routing (43)	Next Header = Fragment (44)	Next Header = TCP (6)	Fragment of TCP header + data

Tabella 3: concatenazione degli header nel pacchetto IPv6

La concatenazione degli header permette, in particolare, di semplificare alcuni meccanismi, quali quelli necessari per la frammentazione, la mobilità e la sicurezza (IPSEC).

Da notare la differenza che c'è fra la frammentazione IPv4 e l'utilizzo del Fragment Header in IPv6: mentre in IPv4 la frammentazione di un pacchetto troppo lungo può avvenire su un qualunque router lungo il percorso, in IPv6 lo stesso host che produce i dati deve preoccuparsi di inviare in rete solo pacchetti che non eccedano la Maximun Transfer Unit dei link sul percorso; nel caso in cui la lunghezza del segmento da inviare in rete ecceda tale limite, il segmento deve essere suddiviso alla fonte in più pacchetti, ciascuno dei quali deve contenere un *Fragment Header*. Questa scelta è stata fatta allo scopo di minimizzare il numero di operazioni sui router di transito.

2.3 DNS

Per associare ad un nome a dominio un indirizzo IPv6, il DNS usa i record di tipo AAAA (al posto del tipo A usato per gli indirizzi IPv4).

Sui sistemi IPv6-only le applicazioni interrogano il DNS solo per ottenere i record AAAA.

Sui sistemi con entrambe le versioni (detti *dual stack*) le applicazioni *dual stack* interrogano il DNS per ottenere record di entrambi i tipi (A e AAAA); in presenza di entrambi, l'applicazione generalmente dà la preferenza al trasporto IPv6, ripiegando sull'IPv4 solo se il tentativo IPv6 va in time-out (tipicamente dopo più di 60 secondi). È dunque importante evitare

di inserire nel DNS i record AAAA se la qualità della connettività IPv6 del sistema in questione è sensibilmente inferiore a quella IPv4.

I record per la risoluzione inversa, che permettono di conoscere il nome a dominio partendo dall'indirizzo IPv6 si trovano sotto il nome a dominio ip6.arpa. Per esempio, il nome a dominio corrispondente all'indirizzo 2001:db8:0:0:a9::1 è il valore del record di tipo PTR con nome

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.a.0.0.0.0.0.0.0.0.0.0.8.b.d.
0.1.0.0.2.ip6.arpa.

Nel settembre 2007 è stato pubblicato l'RFC5006 "IPv6 Router Advertisement Option for DNS Configuration", con il quale viene data la possibilità di usare i *Router Advertisement* per comunicare, oltre alle informazioni di indirizzamento come il prefisso della subnet, anche una lista di server DNS usabili dai client come resolver. Questo era il tassello che mancava per rendere l'attivazione di un host IPv6 pienamente *plug-and-play;* prima la lista dei DNS consultabili poteva essere fornita al client solo usando metodi analoghi a quelli di IPv4.

Con la diffusione di IPv6 potrebbero cambiare alcune consuetudini sull'uso del DNS. Oggi si raccomanda di fare in modo che ogni host con indirizzo IPv4 pubblico (anche dinamico) abbia un nome a dominio e che tramite DNS sia possibile sia la risoluzione diretta (da nome a indirizzo) sia la inversa (da indirizzo a dominio). Questa consuetudine potrebbe cambiare con IPv6:

- gli indirizzi sono molto lunghi, scomodi da inserire nella risoluzione inversa
- se si usa l'autoconfigurazione (SLAAC), gli ultimi 64 bit sono derivati dal MAC address
- la percentuale di *appliances plug-and-play* dotate di indirizzo IPv6 è destinata a crescere

Probabilmente in futuro continueranno ad essere inseriti manualmente nel DNS i nomi a dominio di quei sistemi (generalmente i server) che devono necessariamente avere un nome, ma prenderanno sempre più piede altre soluzioni, come quella di aggiornare dinamicamente i record servendosi dei DNS Dynamic Updates (RFC2136 e RFC3007). Per i gestori dei server DNS è molto interessante la lettura dell'RFC 4472 "Operational Considerations and Issues with IPv6 DNS".

2.4 Routing

Per quanto riguarda i protocolli di routing, il passaggio da IPv4 a IPv6 non introduce sostanziali differenze.

Una novità è che sui router devono essere inseriti comandi per provocare l'invio dei *Router Advertisement* su tutte le interfacce su sui si trovano client che usano l'autoconfigurazione SLAAC.

Sui collegamenti fra router non è obbligatorio assegnare indirizzi IPv6 globali alle interfacce, perché queste hanno comunque un indirizzo link-local ottenuto in maniera automatica. Le comunicazioni IPv6 fra router adiacenti sono dunque possibili utilizzando gli indirizzi link-local.

La "IPv6 Prefix Option" del DHCPv6 (RFC3633) introduce importanti novità. La nuova opzione permette ad un router a valle di ricevere un prefisso IPv6 da un router a monte. Il tipico caso in cui la nuova opzione risulta utile è quello dei piccoli router da "accesso broadband" destinati alle case o ai piccoli uffici. Oggi il tipico router di un utente ADSL riceve dinamicamente via PPP o DHCP un unico indirizzo IPv4 (pubblico o privato) dal router a monte; sulle subnet interne si usano solo indirizzi RFC1918 e il router provvede a fare da NAT. In IPv6, dove si vuole che ogni sistema abbia un indirizzo pubblico, è stata prevista la possibilità per il piccolo router di ottenere un prefisso IPv6 (tipicamente di lunghezza compresa fra 48 e 64 bit) da utilizzare per l'indirizzamento dei sistemi che si trovano sulle subnet interne.

2.5 Trasporto di IPv6 su IPv4

Un host *dual stack* o una rete periferica su cui sia attivo IPv6 possono agganciarsi all'IPv6 globale anche se sono separati da questo da porzioni di rete in cui sia presente solo l'IPv4. In questi casi è necessario che l'host *dual stack* o un router IPv6 della rete periferica siano in grado di scambiare pacchetti IPv6 con destinazioni non raggiungibili in maniera nativa incapsulandoli all'interno di pacchetti IPv4. In questi casi si parla di soluzioni di "tunneling".

A seconda della tecnica adottata per realizzare il tunnel, cambia il tipo di indirizzi globali IPv6 usabili sulla rete periferica o sull'host dual stack. Ciò porta a classificare le tecniche più comuni in tre categorie: *Tunnel Broker*, *6to4* e *Teredo*.

2.5.1 Tunnel Broker

Questa tecnica permette di utilizzare sulla rete periferica (o sull'host *dual stack*) normali indirizzi IPv6 globali. Generalmente all'end-point periferico del tunnel vengono forniti in configurazione l'indirizzo IPv4 dell'end-point centrale (*Tunnel Broker*) e le credenziali per essere riconosciuto da questo; dalle credenziali il Tunnel Broker può dedurre quali prefissi IPv6 devono essere usati sulla rete periferica (o sull'host dual stack). I prefissi della rete periferica possono essere annunciati dal Tunnel broker sulle sue interfacce IPv6 native usando i normali protocolli di routing.

Se l'end-point periferico possiede un indirizzo IPv4 pubblico, i pacchetti IPv6 sono incapsulati in pacchetti

IPv4 con protocol number 41; se invece il tunnel deve attraversare un NAT, l'IPv6 viene incapsulato in pacchetti UDP. Sono già in uso protocolli (come il Tunnel Setup Protocol, descritto sull'internet-draft "draft-blanchet-v6ops-tunnelbroker-tsp") con cui i due end-point possono negoziare le modalità di incapsulamento. Talvolta, per l'attivazione del tunnel, l'end-point periferico si serve di un software fornito dal gestore del Tunnel Broker.

Il Tunnel Broker è la soluzione più idonea se sulla rete periferica si vogliono usare indirizzi IPv6 permanenti. Offre anche maggiori garanzie di sicurezza, visto che l'end-point periferico accetta i pacchetti IPv6 solo se incapsulati in pacchetti IPv4 provenienti dall'altro end-point. Rispetto alle altre due soluzioni ha lo svantaggio di non essere totalmente automatico e di avere un collo di bottiglia costituito dall'end-point centrale.

2.5.2 6to4 (RFC3056)

I primi 48 bit di tutti gli indirizzi IPv6 usati sulla rete periferica (o sull'host dual stack) devono avere il valore 2002:wwxx:yyzz::/48, dove ww,xx,yy,zz sono i valori dei quattro ottetti dell'indirizzo IPv4 dell'end-point periferico del tunnel.

L'end-point periferico del tunnel funge da default router IPv6 per l'intera isola periferica e invia i pacchetti con destinazioni non 6to4 incapsulandoli in pacchetti IPv4 con protocol number 41 e destinati all'indirizzo IPv4 192.88.99.1. Questo indirizzo appartiene al prefisso 192.88.99.0/24, che viene annunciato da tutti i "6to4 Relay Router", vale a dire tutti i router che fanno forwarding fra zone con indirizzi 6to4 e zone con indirizzi IPv6 nativi (RFC3068).

Tutti i sistemi configurati con un'interfaccia 6to4 trasmettono i pacchetti destinati ad indirizzi 6to4 non locali incapsulandoli in pacchetti IPv4 con protocol number 41 destinati all'indirizzo IPv4 deducibile dai 32 bit che seguono i primi 16.

Tutti i "6to4 Relay Router" annunciano sulle interfacce IPv6 native il prefisso 2002::/16.

Un pacchetto originato su un host con indirizzo 6to4 viene inoltrato come segue:

- se i primi 48 bit dell'indirizzo destinatario sono uguali a quelli del mittente, il percorso è tutto interno alla rete periferica;
- altrimenti, il pacchetto arriva al router della rete periferica dotato di interfaccia 6to4;
- se l'indirizzo del destinatario ha il prefisso 2002::/16, il pacchetto viene incapsulato in pacchetti IPv4 destinati all'indirizzo IPv4 deducibile dai 32 bit che seguono i primi 16;
- altrimenti, il pacchetto viene incapsulato in pacchetti IPv4 destinati all'indirizzo IPv4 192.88.99.1.

Viceversa, un pacchetto originato su un host IPv6 nativo e destinato ad un indirizzo 6to4, percorre la rete IPv6 nativa fino ad arrivare ad un "6to4 Relay Router" che annuncia il prefisso "2002::/16, dopo di che viene incapsulato in pacchetti IPv4 destinati all'indirizzo IPv4 deducibile dai 32 bit che seguono i primi 16.

Nella maggior parte dei casi, le sessioni fra host 6to4 e host nativi hanno percorsi asimmetrici, perché il passaggio fra i due mondi avviene generalmente su due "6to4 Relay Router" diversi. Viceversa, il traffico fra coppie di host con indirizzo 6to4 segue generalmente percorsi simmetrici, anche quando i due host si trovano su due isole diverse.

La soluzione 6to4 è attivabile su tutti i router e i sistemi operativi dual stack recenti, purché dispongano di un indirizzo IPv4 pubblico. Non è attivabile su un sistema che si trovi sul lato interno di un NAT. L'indirizzamento IPv6 generato dal 6to4 può essere permanente solo se l'indirizzo IPv4 dell'end-point locale del tunnel è permanente.

2.5.3 Teredo (RFC4380)

Permette solo di collegare un host *dual stack* (non una rete periferica) ed è stato studiato tenendo conto della necessità di permettere anche agli host situati sul lato interno di un NAT di utilizzare tunnel automatici; per questo motivo Teredo, diversamente da 6to4, incapsula i pacchetti IPv6 in pacchetti UDP. L'host all'end-point periferico del tunnel (detto "Teredo Client") assume un indirizzo con prefisso 2001::/32 (il secondo gruppo di 16 bit ha valore 0). I rimanenti bit dell'indirizzo IPv6 permettono di conoscere l'indirizzo del "Teredo Server" da cui dipende il "Teredo Client", il tipo dell'eventuale NAT dietro il quale si trova il client e l'indirizzo IPv4 e il port number "pubblici" a cui devono essere indirizzati i pacchetti UDP a lui destinati.

Per funzionare, un "Teredo Client" ha bisogno di un server. Il "Teredo Server" è coinvolto solo in operazioni di controllo, per cui un singolo server può controllare un numero molto elevato di client. Molti "Teredo Client" sono preconfigurati con l'indirizzo di un server, per cui possono essere attivati senza fornire parametri. Il server assiste il client, facendogli conoscere l'indirizzo IPv4 e il port number con cui l'end-point locale è conosciuto sulla rete pubblica, mantenendo attivi i mapping sul NAT relativi ai tunnel e permettendo al client di scoprire, per ogni destinazione IPv6 nativa, un indirizzo IPv4 ed un port number di un "Teredo Relay" a cui indirizzare i pacchetti IPv6.

Un "Teredo Relay" è un router che fa forwarding fra zone con indirizzi Teredo e zone con indirizzi IPv6 nativi. I "Teredo Relay" annunciano sulle interfacce IPv6 native il prefisso 2001::/32.

Un pacchetto originato su un host con indirizzo Teredo viene inoltrato come segue:

- se l'indirizzo del destinatario ha il prefisso 2001::/32, il pacchetto viene incapsulato in pacchetti UDP destinati all'indirizzo IPv4 ed al port number deducibili dall'indirizzo IPv6 del destinatario;
- se l'indirizzo IPv6 del destinatario ha un prefisso diverso da 2001::/32 e non è presente nella cache locale del "Teredo Client", viene inviato al "Teredo Server" un pacchetto UDP contenente un *ping* IPv6 indirizzato al destinatario; la risposta al *ping*, essendo indirizzata ad un indirizzo 2001::/32, raggiunge un "Teredo Relay", che la incapsula in un pacchetto UDP destinato all'indirizzo IPv4 ed al port number deducibili dall'indirizzo Teredo a cui è destinata la risposta; il "Teredo Cient" memorizza in una cache locale l'indirizzo IPv4 ed il port number da cui ha ricevuto la risposta al *ping*, associandoli all'indirizzo IPv6 del destinatario; da questo momento i pacchetti destinati a quell'indirizzo IPv6 nativo vengono incapsulati in pacchetti UDP destinati all'indirizzo IPv4 ed al port number presenti in cache.

Viceversa, un pacchetto originato su un host IPv6 nativo e destinato ad un indirizzo Teredo, percorre la rete IPv6 nativa fino ad arrivare ad un "Teredo Relay" che annuncia il prefisso "2001::/32, dopo di che viene incapsulato in pacchetti UDP destinati all'indirizzo IPv4 ed al port number deducibili dall'indirizzo del destinatario.

Diversamente da quanto avviene nella soluzione 6to4, generalmente le sessioni fra host Teredo e host nativi hanno percorsi simmetrici, perché il passaggio fra i due mondi avviene in entrambe le direzioni sul "Teredo Relay" più vicino all'host con indirizzo IPv6 nativo.

La soluzione Teredo è presente sui sistemi Windows e sui router *dual stack* recenti. Negli altri sistemi operativi Teredo è attivabile installando software di pubblico dominio.

3. PRINCIPALI NOVITÀ INTRODOTTE DA IPV6

Si sente spesso la domanda: "quali altri vantaggi si ottengono con IPv6, in aggiunta a quello di disporre di più indirizzi?". Una risposta onesta, anche se un po' radicale, è "nessuno". A dire il vero il progetto IPv6 partì proponendosi anche altri obiettivi, in aggiunta all'esigenza di uno spazio di indirizzamento più vasto. Gran parte degli obiettivi iniziali sono stati raggiunti, solo che nel frattempo è cambiata la tecnologia ed è evoluto anche IPv4, per cui molti degli obiettivi iniziali o hanno perso valore o sono diventati realizzabili anche con IPv4.

In realtà, il vero punto di forza di IPv6 è quello di permettere ad Internet di crescere facendo a meno dei NAT. Più avanti ci si soffermerà maggiormente su questo punto.

3.1 Forwarding veloce e quality of service

Una buona parte delle innovazioni avevano lo scopo di rendere il forwarding dei pacchetti più veloce: l'eliminazione dall'header dei campi *options* e *header checksum* e la scomparsa delle informazioni per la frammentazione dei pacchetti dovevano servire a semplificare le operazioni richieste ai router di transito, in modo che divenisse possibile effettuare il forwarding dei pacchetti in hardware, senza impegnare la CPU del router. In realtà, già prima della fine degli anni '90 la tecnologia era progredita al punto di rendere possibile il forwarding in hardware dei pacchetti IPv4, cosa fino a poco tempo prima del tutto impensabile.

In maniera analoga, il campo *flow label* (tuttora inutilizzato) avrebbe dovuto facilitare l'identificazione dei flussi in transito su un router allo scopo di semplificare il forwarding dei pacchetti e la loro classificazione ai fini della quality of service. La classificazione ai fini della quality of service viene oggi realizzata, in IPv6 così come in IPv4, servendosi dei bit 0-5 del campo *traffic class* (*ToS* in IPv4), che vengono utilizzati per trasportare il *Differentiated Services Codepoint*. Anche in questo caso, ciò che nei primi anni '90 era una carenza di IPv4, è stato poi colmato con la definizione delle tecniche *DiffServ* (primi RFC usciti nel 1998).

3.2 Sicurezza

In varie occasioni si sente affermare "IPv6 offers better security, as IPsec is mandatory". Questa affermazione ha assai poco senso, perché il fatto che le funzionalità IPsec siano presenti in uno stack IPv6 non costringe nessuno a servirsene. L'affermazione aveva una sua validità all'epoca in cui IPv6 fu progettato, visto che IPsec è nato più o meno nello stesso periodo (primi RFC usciti nel 1995). Oggi IPsec è disponibile su tutti i sistemi IPv4 sui quali il suo utilizzo abbia un senso, per cui sul piano pratico differenze di rilievo rispetto a IPv6 non ci sono. Resta pur sempre una maggiore eleganza della soluzione IPsec di IPv6, che sfrutta efficacemente il meccanismo della concatenazione degli header.

Meno sbandierata ma più vera è la sicurezza data dal fatto che l'elevato numero di indirizzi è un serio ostacolo alla propagazione di quei virus e worm, che cercano di indovinare a caso gli indirizzi IP delle vittime da infettare.

Un ulteriore contributo alla sicurezza è fornito dalla stessa scomparsa dei NAT. Questo punto, che contraddice una delle convinzioni più diffuse (NAT=sicurezza), è approfondito nel capitolo 4.

3.3 Mobilità

Con il termine *IP mobility* si intende la possibilità per un host mobile di comunicare con nodi corrispondenti utilizzando il suo "indirizzo IP di casa" (*home address*), anche quando l'host mobile è collegato a link su cui sono usate subnet IP diverse da quella della "rete di casa". Grazie alla IP mobility, un host mobile (per esempio un apparato wireless), anche se nel corso dei suoi spostamenti passa da una sottorete ad un'altra, può mantenere attive le sessioni (trasferimenti di file, telefonate,...) con i suoi corrispondenti.

Soluzioni per la IP mobility esistono per IPv4 (RFC3344) e per IPv6 (RFC3775). La soluzione IPv6, nella quale viene fatto un uso sapiente degli "extension header", è superiore a quella IPv4 per vari motivi. I motivi più importanti sono i seguenti:

- in IPv6 è ragionevole supporre che sulla rete visitata il nodo mobile possa servirsi della SLAAC per acquisire un nuovo indirizzo IPv6 globale; in IPv4, ammesso che sulla rete visitata esista un metodo di distribuzione dinamico degli indirizzi (es.: DHCP), è improbabile che gli indirizzi ottenuti in tal modo siano pubblici; nel caso in cui sulla rete visitata non sia prevista la distribuzione dinamica di indirizzi pubblici, la mobilità IPv4 funziona solo se sulla rete visitata è presente un router con funzioni particolari, detto "Foreign Agent"
- con IPv6, se il nodo corrispondente possiede le necessarie funzionalità, il pacchetto può percorrere il precorso più breve sia nella direzione da nodo mobile a nodo corrispondente sia in quella opposta; la soluzione IPv4, invece, prevede che il percorso da nodo corrispondente a nodo mobile transiti sempre attraverso un router che si trova sulla "home network" del nodo mobile;

La IP mobility è dunque una funzionalità in cui IPv6 è superiore a IPv4. Anzi, si può affermare che in IPv4 la mobilità può essere utilizzata solo in casi molto particolari. D'altra parte, pensare ad un uso in larga scala della mobility IPv6 è prematuro, perché fruitori e fornitori di servizi non sono ancora organizzati per trarne benefici.

3.4 Multicast

Grazie alla maggiore lunghezza degli indirizzi, in IPv6 diventa assai più facile il dispiegamento dei servizi basati su Any Source Multicast (ASM). L'ASM è quella modalità di uso del multicast in cui l'ascoltatore dichiara di essere interessato a ricevere tutti i pacchetti destinati ad un dato indirizzo IP multicast, qualunque sia il nodo che li ha originati. L'ASM si differenzia dal Source Specific Multicast (SSM), in cui l'ascoltatore si dichiara interessato a ricevere i pacchetti destinati ad un dato indirizzo IP multicast solo se provengono da un mittente ben preciso. Mentre la fruibilità dell'SSM con il passaggio da IPv4 a IPv6 rimane grossomodo invariata, per l'ASM si ottengono vantaggi notevoli.

Un problema di difficile soluzione nell'ASM IPv4 è quello di come evitare che lo stesso indirizzo IP multicast sia utilizzato contemporaneamente da attività completamente scorrelate; quando ciò avviene, gli ascoltatori ricevono tutti i pacchetti destinati all'indirizzo IP multicast, non solo quelli relativi all'attività a cui vogliono partecipare. In IPv4, una parziale soluzione al problema è data dall'indirizzamento GLOP (RFC3180), che riserva agli assegnatari di un Autonomous System a 16 bit un blocco di 256 indirizzi multicast. La soluzione disponibile in IPv6 (detta degli "Unicast-Prefix-based IPv6 Multicast Addresses", RFC3306), invece, riserva agli assegnatari di un prefisso Global Unicast di lunghezza non superiore a 64 bit un blocco di 2^{32} indirizzi multicast: in pratica, ogni gestore di LAN può disporre liberamente di ben 2^{32} indirizzi multicast a lui riservati. Appartengono a questa categoria gli indirizzi con prefisso ff30::/12 e con un valore non nullo nei bit dal 25esimo al 32esimo.

Un'altra difficoltà nella gestione di infrastrutture ASM in ambiente multi-domain nasce dal problema di individuare il *Rendez-vous Point* (RP) competente per ciascun gruppo multicast. L'RP di un gruppo multicast è l'indirizzo IP di un server (generalmente un router) su cui si registrano tutte le sorgenti del gruppo, in modo da permettere agli ascoltatori di scoprire dove si trovano le sorgenti. Una attività ASM, basata su un dato indirizzo multicast, può funzionare solo se tutti i router che si trovano sul cammino fra i partecipanti all'attività e l'RP sanno quale è l'RP competente per quell'indirizzo multicast. Approfittando della maggiore lunghezza degli indirizzi, l'IPv6 introduce un nuovo tipo di indirizzo multicast, detto "Embedded-RP Multicast Address" (RFC3956). Negli indirizzi di questo tipo, caratterizzati dal prefisso ff70::/12, 68 bit permettono di ricostruire l'indirizzo dell'RP relativo al gruppo. L'unico vincolo che deve essere rispettato da chi vuole usare indirizzi Embedded-RP è che l'RP del gruppo deve avere un indirizzo del tipo:

xxxx:xxxx:xxxx:xxxx::x

In altre parole, i bit dal 65esimo al 124esimo dell'indirizzo dell'RP devono avere valore 0. Da notare che, pur con questa restrizione, viene data la possibilità di attivare fino a 15 RP su ogni subnet /64. Gli indirizzi Embedded-RP rendono possibile l'uso del multicast ASM senza richiedere la presenza di tabelle di mapping coerenti su tutti i router.

Riassumendo, IPv6 semplifica notevolmente la gestione del multicast di tipo ASM. Anche in questo caso, però, ci si trova di fronte ad una funzionalità la cui utilità è ancora assai poco compresa. Quindi, se è vero che con l'IPv6 il multicast potrà avere una grande

diffusione, sarebbe sbagliato pensare che la conoscenza dei vantaggi del multicast possa servire da stimolo per accelerare l'adozione del nuovo protocollo.

3.5 Autoconfigurazione

Rispetto ad altri protocolli per LAN comunemente usati alla fine degli anni '80 (NETBEUI, IPX, AppleTalk), l'IP delle origini appariva assai poco "user friendly". Infatti, mentre per gli altri protocolli era sufficiente l'allacciamento fisico alla rete (o, nei casi più complessi, l'attivazione di un server di rete), nel caso di IP era necessario un piano di indirizzamento per la rete ed un intervento manuale su tutti i sistemi da collegare.

Solo nell'ottobre 1993, più o meno nello stesso periodo in cui iniziava la progettazione di IPv6, veniva pubblicato l'RFC1541, il primo relativo al DHCP. Con il DHCP l'IPv4 faceva un notevole passo avanti nel cammino verso l'autoconfigurazione, anche se rimaneva ancora necessario configurare il DHCP server.

IPv6 fu invece progettato fin dall'inizio con l'intento di rendere possibile l'inserimento di nuovi apparati in rete riducendo al minimo o eliminando del tutto la necessità di configurarli. Vengono incontro a questa esigenza gli indirizzi Link Local e la SLAAC.

Se oggi si prova a fare un confronto fra le possibilità di autoconfigurazione di IPv4 e quelle di IPv6, si vede che le differenze si sono assai ridotte. IPv4 ha fatto un grande passo in avanti da quando il blocco di indirizzi 169.254.0.0/16 è stato riservato per l'indirizzamento IPv4 Link-Local (RFC3927, maggio 2005).

Riassumendo, per quanto riguarda gli indirizzi non Link-Local, in IPv4 manca la SLAAC, ma, se si considera che la maggior parte dei router foglia dispongono anche di un DHCP server interno, il vantaggio di IPv6 è piuttosto marginale. Per i Link-Local, la soluzione IPv6 è più solida ed affidabile ed ha in particolare il vantaggio di essere presente su qualunque prodotto IPv6 e non solo su quelli recenti. In IPv6, inoltre, la coesistenza sulla stessa interfaccia di un indirizzo Link-Local e di uno *routable* è la norma, mentre in IPv4 viene impedita perché può dar luogo ad effetti indesiderabili.

Anche riguardo a questo punto si può quindi affermare che con IPv6 si ha qualche vantaggio, ma non di entità tale da servire da stimolo per l'adozione del nuovo protocollo.

4. PERCHÉ I NAT SONO DANNOSI?

Nelle sezioni precedenti si è affermato più volte che i NAT limitano eccessivamente le potenzialità di Internet. In termini tecnici, le limitazioni introdotte dai NAT sono facilmente elencabili:

1. Sono utilizzabili solo i protocolli ICMP (protocol number 1), TCP (6) e UDP (17); sono per esempio inutilizzabili molti protocolli di tunneling come IPv4 in IPv4 (4), IPv6 in IPv4 (41), General Routing Encapsulation (47);
2. Le connessioni TCP sono possibili solo se iniziate da un host sul lato interno del NAT; dopo un periodo di assenza di traffico (la durata dipende dal NAT, ma generalmente è superiore all'ora), la connessione TCP diventa inutilizzabile;
3. Un pacchetto UDP proveniente dall'esterno e destinato all'indirizzo pubblico del NAT viene consegnato al destinatario corretto solo se sul NAT è presente una regola che associa il *destination port* presente nel pacchetto con una porta di un host interno; queste associazioni vengono create sul NAT solo quando l'host interno invia un pacchetto UDP verso l'esterno e vengono cancellate dopo un tempo molto breve (tipicamente 30 secondi);
4. Comunicazioni fra due host che si trovino sulle zone interne di due diversi NAT sono possibili solo se c'è un gateway di livello applicativo ("complice") su un host dotato di indirizzo pubblico;
5. Non funzionano le applicazioni che trasmettono indirizzi IP e numeri di porte nella parte dati dei pacchetti (FTP in modalità "active", SIP, H.323,...);
6. Non è possibile firmare digitalmente gli indirizzi IP e i port number dei pacchetti, perché questi vengono alterati dai NAT presenti sul percorso;
7. L'identificazione a posteriori del mittente di un pacchetto originato su un host sul lato interno di un NAT è possibile solo se il gestore del NAT dispone di log dettagliati;
8. Il NAT è un collo di bottiglia che riduce le prestazioni e in caso di guasto causa l'interruzione delle comunicazioni.

Si noti come i limiti 4, 6 e 7 diminuiscono la sicurezza delle reti, in contrasto con quanto viene comunemente affermato circa la funzione "protettiva" dei NAT. A questo proposito è molto istruttiva la lettura dell'RFC 4864 "Local Network Protection for IPv6". Vi si dimostra come in IPv6, pur senza ricorrere all'uso dei NAT, esistono gli strumenti per riprodurre sulle reti locali gli stessi effetti "protettivi" comunemente attribuiti ai NAT.

Gli inconvenienti tecnici introdotti dai NAT sono dunque tanti, ma ciò contrasta con la percezione di tutti quegli utilizzatori della rete (la maggior parte), che, pur trovandosi a valle di uno o più NAT, assai

raramente si rendono conto di essere soggetti a limitazioni. In parte ciò è dovuto al fatto che un gran numero di utilizzatori della rete continua a servirsene come ai tempi delle connessioni *dial-up*: accedere dal proprio computer a server dotati di indirizzi pubblici. Tutti sanno però che molti utenti, pur trovandosi dietro ai NAT, riescono anche a usare applicazioni come P2P, Skype, VoIP, apparentemente contraddicendo quanto si è detto sopra. In realtà, in tutti questi casi, ci si trova di fronte ad applicazioni "NAT-aware", che operano potendo contare su "complici" dotati di indirizzo pubblico (fanno parte della categoria "complici" anche i Teredo Server).

Si noti che tutte le comunicazioni che funzionano solo grazie all'intervento di una terza parte sono potenzialmente meno sicure di quelle interamente end-to-end; nel caso poi di applicazioni il cui codice sorgente è segreto (come Skype), affidare le nostre comunicazioni a computer esterni di cui non sappiamo nulla equivale ad avere una notevole dose di fiducia nella correttezza della società che ha prodotto il software.

Qualcuno potrebbe suggerire che, nonostante tutte le limitazioni alla funzionalità ed alla sicurezza della rete causate dalla presenza dei NAT, sia tuttavia più comodo continuare a seguire il modello di crescita di Internet seguito finora: incoraggiare l'uso degli indirizzi RFC1918 e restringere sempre di più l'uso degli indirizzi pubblici. Anche questo modello, però, potrebbe andare in crisi assai presto. Basta ricordare che il NAT, per sapere a quale sistema interno deve essere consegnato un pacchetto TCP o UDP ricevuto dall'esterno sul suo indirizzo IP pubblico, si basa sul *port number* di destinazione del pacchetto stesso. Il *port number* può assumere valori da 1 a 65535. Dunque, l'insieme dei computer dell'isola privata che vengono mappati sullo stesso indirizzo pubblico non può avere più di 65535 sessioni contemporanee con l'esterno dell'isola. Poiché non è raro avere un centinaio di sessioni contemporaneamente attive sullo stesso computer e questo numero è in costante crescita, è opportuno evitare di mappare più di 500 indirizzi IP privati sullo stesso indirizzo pubblico. Si potrebbe anche pensare a modificare il funzionamento dei NAT in modo che il sistema interno destinatario del pacchetto non sia più identificato dal solo *port number* di destinazione, ma dalla terna <*dest-port, source-ip, source-port*>. Una modifica così radicale, però, renderebbe inutilizzabili tutte le applicazioni (in particolare quelle VoIP) che utilizzano un "complice esterno" per scoprire quale mapping viene effettuato dal NAT .

Riassumendo:

- Il NAT non protegge più di quanto possa proteggere un normale firewall che lasci invariati gli indirizzi e i port number
- Il NAT favorisce l'anonimato, il furto di identità e l'intercettazione di comunicazioni riservate
- Anche volendo rinunciare per sempre alla univocità degli indirizzi IP, l'attuale modello della Internet IPv4 ha un margine di crescita piuttosto ridotto
- Occorre convincersi che la scelta di IPv6 porta alla semplificazione e permette di ridirigere verso scopi assai più produttivi tante risorse umane che oggi sono dedicate al superamento delle difficoltà create dai NAT.

5. CONSIGLI E SUGGERIMENTI PER UTILIZZARE IPV6

Pochi si rendono conto del fatto che chi possiede un computer con sistema operativo recente può agganciarsi all'IPv6 globale indipendentemente da ciò che fa il suo ISP. Addirittura molti usano IPv6 senza saperlo. È il caso di chi ha Windows Vista o Windows 7, che attivano automaticamente lo stack IPv6 e che, in assenza di un indirizzo IPv6 globale nativo, attivano automaticamente un tunnel 6to4 se l'indirizzo IPv4 è pubblico e Teredo se è privato. Anche con Windows Vista e Windows 7, ci sono casi in cui l'attivazione automatica dell'IPv6 globale fallisce:

- Se il software di protezione del PC blocca IPv6 (in questo caso occorre modificare opportunamente la configurazione del software di protezione)
- Se la rete è protetta da un Firewall che blocca i tunnel

Su Windows XP bisogna dare il comando "netsh interface ipv6 install" per attivare IPv6 e "netsh interface ipv6 set teredo client" per attivare il tunnel Teredo. Le funzioni restano attive anche dopo un reboot, fino a quando vengono disattivate con i comandi "netsh interface ipv6 set teredo disable" e "netsh interface ipv6 uninstall".

Quando Windows è collegato all'IPv6 globale solo attraverso un tunnel Teredo o 6to4, il DNS resolver, se scopre che per un dominio IP c'è sia il record A (IPv4) sia l'AAAA (IPv6), passa all'applicazione solo il record A, per cui la destinazione viene raggiunta in IPv4, anche se la via IPv6 sarebbe disponibile. La scelta è stata fatta allo scopo di ottimizzare i tempi di risposta, ipotizzando che le prestazioni di un tunnel siano sempre inferiori a quelle di un collegamento nativo. Su Internet si trovano siti in cui si suggeriscono trucchi per neutralizzare questo comportamento (si veda, ad esempio, http://yorickdowne.wordpress.com/tag/teredo/).

Per Linux e BSD Teredo è disponibile su http://www.remlab.net/miredo/. Il sito per l'OSX è http://www.deepdarc.com/miredo-osx/ .

Per avere IPv6 su tutta la LAN invece che su un singolo computer, bisogna disporre di un oggetto che si comporti da router IPv6. Questa funzione può anche essere svolta da un PC con 6to4, purché sia dotato di indirizzo pubblico. Molto meglio è utilizzare per questo scopo un apparato la cui funzione primaria sia proprio quella di fare da router. Sui router di media ed alta fascia il problema non si pone, mentre fino a tempi molto recenti sui router di fascia bassa IPv6 è stato completamente assente. Negli ultimissimi tempi le cose cominciano a cambiare e stanno facendo la loro comparsa sul mercato i primi router ADSL con IPv6. Questi router, se l'ISP lo consente, possono usare IPv6 nativamente sul collegamento ADSL, altrimenti attivano un tunnel 6to4 o uno con un *tunnel broker*.

Lo svantaggio principale della soluzione 6to4 è che il prefisso IPv6 delle subnet locali cambia ogni volta che cambia l'indirizzo pubblico IPv4 sul collegamento WAN. Per chi vuole mettere la sua LAN su IPv6 senza cambiare il router, esistono piccoli server a basso consumo energetico da collegare alla LAN (quindi con indirizzo IPv4 privato), che possono attivare un tunnel con un *tunnel broker* e annunciare un prefisso IPv6 sulla LAN, assumendo la funzione di router IPv6 della LAN.

Un vantaggio immediato che si ottiene attivando IPv6 su una LAN residenziale è quello di poter attivare, senza ricorrere a trucchi complicati, dall'esterno collegamenti verso gli *host* della LAN. Diventano inoltre immediatamente utilizzabili tutte le *appliances* dotate di stack IPv6, fra cui alcuni apparati per giochi elettronici. Via via che escono sul mercato apparati VoIP IPv6 (alcuni già esistono), anche l'uso del VoIP diventa molto più semplice.

Per i gestori delle reti aziendali, i vantaggi derivanti dall'adozione di IPv6 sono meno evidenti nei tempi brevi. È tuttavia necessario rendersi conto del fatto che l'introduzione di IPv6 nelle reti aziendali presuppone un minimo di pianificazione e di sperimentazione preliminari.

Anche se si prevede che il grosso del traffico continui ad essere IPv4 per un lungo periodo, occorre iniziare a studiare per tempo gli aspetti legati alla sicurezza (es.: devo cambiare il firewall?, come lo devo configurare?, come mi proteggo dai "rogue router advertisement"?, le mie procedure di Network Access Control funzionano anche in IPv6?) ed alla gestione degli indirizzi (DHCP?, SLAAC?, DNS dinamico o statico?, risoluzione inversa per tutti gli indirizzi o solo per alcuni?).

Si tratta di problemi che, se affrontati in anticipo, possono essere risolti senza troppe difficoltà, ma che, se rinviati al giorno in cui IPv6 sarà indispensabile, potrebbero rendere l'introduzione del nuovo protocollo un vero incubo.

6. LA SITUAZIONE ATTUALE

Si è detto che la tecnologia è matura per iniziare ad usare IPv6 anche per attività produttive e non soltanto per la sperimentazione. Ciò è vero, ma non si deve dimenticare che c'è ancora della strada da fare. I principali punti su cui c'è ancora da lavorare sono:

- la sicurezza: la stragrande maggioranza degli apparati continuano ad essere solo IPv4
- il VoIP: stranamente proprio le applicazioni che sono maggiormente danneggiate dai NAT (e il VoIP è fra queste), sono quelle più indietro nell'evoluzione verso IPv6
- implementazioni parziali sui sistemi operativi: per esempio, non tutti i sistemi prevedono la configurazione via DHCPv6, la IPv6 mobility in genere è assente o presente solo in parte
- la scarsa presenza di IPv6 sulle reti degli ISP.

Ora, mentre per i primi tre aspetti le cose stanno rapidamente cambiando, molti ISP continuano a comportarsi come se il problema dell'esaurimento degli indirizzi IPv4 non esistesse. Le eccezioni non mancano, ma questi ISP "virtuosi" hanno dovuto verificare che le loro nuove offerte di connettività IPv6 riuscivano al massimo a destare l'interesse di un numero molto limitato di "smanettoni". Non ci si deve stupire se, in un mercato altamente competitivo come quello della connettività ad Internet, gli sforzi degli ISP sono diretti verso innovazioni più redditizie.

Più in generale, il fenomeno cui si assiste è che i produttori di tecnologia, che impostano i loro piani di sviluppo con logiche pluriennali, stanno arrivando preparati all'appuntamento con IPv6. Viceversa, gli utilizzatori della tecnologia (e gli ISP sono fra questi) stentano a rendersi conto della necessità di iniziare per tempo a prendere confidenza con il nuovo protocollo.

Se si pensa quanto poco vengano prese in considerazione questioni assai più gravi, come l'inquinamento o l'esaurimento delle fonti energetiche, non ci si deve stupire se sul problema dell'esaurimento degli indirizzi IPv4 la lungimiranza scarseggia. Fortunatamente in questo caso le conseguenze della mancata lungimiranza sono assai meno catastrofiche: anche se in ritardo, il nuovo protocollo prenderà piede in tutti casi; l'unico rammarico sarà quello di aver prolungato l'agonia di IPv4 molto più a lungo di quello che si sarebbe potuto fare.

Per il futuro della rete e della società dell'informazione occorrerebbe adoperarsi per una rapida diffusione del nuovo protocollo. Il problema è che, in assenza di

motivazioni valide, ben pochi sono disposti ad impegnarsi. Invocare interventi governativi per incentivare l'adozione di IPv6 può essere giustificato, anche se ciò suona un po' come una sconfitta per il modello di sviluppo che Internet ha seguito finora.

Sicuramente rientra nella sfera di competenza dei governi occuparsi di ciò che viene fatto nelle amministrazioni pubbliche. Molti governi (USA incluso) hanno fornito già da alcuni anni direttive tese a favorire l'adozione di IPv6 da parte delle amministrazioni. Un intervento del governo italiano in questa direzione potrebbe produrre risultati assai positivi. La speranza è che, qualora una comunità importante come l'amministrazione pubblica facesse il primo passo, IPv6 diventerebbe commercialmente interessante per ISP, società informatiche, produttori di contenuti e altri.