Guida all'attivazione di una

CONNESSIONE IPv6
tramite tunnelling Freenet6

Emanuele Goldoni

Università degli studi di Pavia
Sede di Mantova

Laboratorio di Reti di Calcolatori
2006

1 Introduzione

A distanza di parecchi anni dall'introduzione di IPv6, ancora pochi sono i provider che forniscono ai clienti un servizio di connettività nativa per questo protocollo. Fortunatamente, grazie a meccanismi di tunneling, è possibile comunque connettere in pochi minuti la propria macchina o rete alla dorsale mondiale IPv6.
In questa guida, in particolare, illustreremo le operazioni necessarie per effettuare una connessione utilizzando il servizio gratuito Freenet6. Questi, infatti, non solo è diffuso ed efficiente ma è anche estremamente semplice da utilizzare, nonché tra i pochi in grado di fornire connettività v6 anche all'interno di reti connesse ad Internet tramite dispositivi NAT.

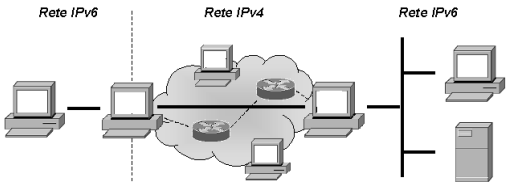

Figura 1: Esempio di tunneling per interconnettere due 'isole' IPv6

2 Installazione di IPv6

2.1 Microsoft Windows

Il supporto ad IPv6 è stato introdotto nativamente nei sistemi operativi Microsoft a partire da Windows XP e oggi è disponibile anche in Windows 2003 e Vista.
L'installazione del protocollo è estremamente semplice: dal menù Start occorre selezionare Esegui e digitare quindi nella casella di testo:

```
netsh interface ipv6 install
```

In Windows 2000 la procedura è analoga ma è necessario scaricare ed installare esplicitamente l'estensione dal sito Microsoft; la versione per questo sistema operativo è comunque di sperimentale e non più aggiornata da tempo. Per versioni precedenti di Windows esistono solo estensioni proprietarie, comunque non più aggiornate. Al termine della procedura occorre, infine, riavviare il sistema. Se l'installazione è avvenuta correttamente tra le proprietà della scheda di rete dovrebbe essere presente il nuovo protocollo.

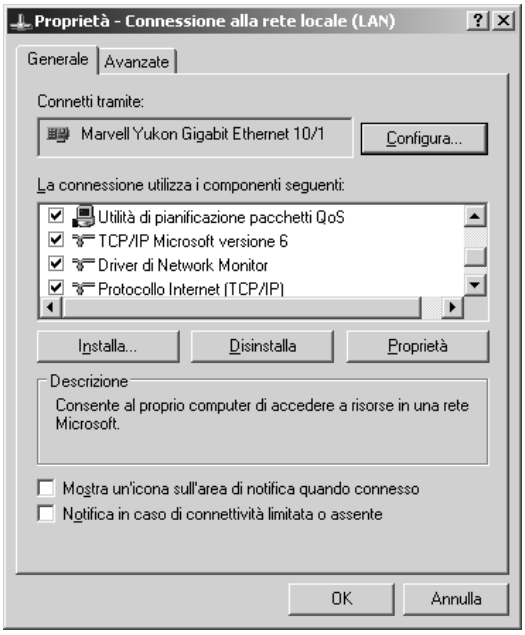

Figura 2: IPv6 è stato correttamente installato in Windows XP.

2.2 Linux - BSD - Unix

Lo stack IPv6 all'interno di Linux viene normalmente fornito, insieme a moltissimi altri componenti del kernel, come modulo da caricare all'occorrenza e, in alcune distribuzioni più recenti, il supporto ad IPv6 è persino già abilitato di default. Per visualizzare i moduli caricati è possibile utilizzare il comando:

```
# lsmod
```

É bene verificare che, all'interno della lista presentata, compaia anche il modulo `ipv6`. Nel caso in cui un modulo necessario non sia ancora stato attivato, è possibile caricarlo in maniera esplicita utilizzando il comando modprobe seguito dal nome del modulo desiderato; per attivare ad esempio IPv6 è necessario digitare:

```
# modprobe ipv6
```

oppure, per i vecchi kernel 2.4

```
# insmod ipv6
```

Conviene poi verificare l'avvenuto caricamento sempre utilizzando `lsmod`. Se si volesse infine rendere automatico il caricamento di questo modulo all'avvio del sistema, sarà sufficiente inserire nel file `/etc/modules.conf` (o `/etc/modprobe.conf`) la riga di configurazione:

```
alias net-pf-10 ipv6
```

Gli utenti che invece utilizzano un kernel compilato in casa devono abilitare, in fase di compilazione, il supporto per il protocollo IPv6. Dopo l'installazione dell'IP di nuova generazione, digitando il comando `ifconfig` verranno visualizzati anche gli indirizzi IPv6 associati alle interfacce di rete.

```
eth0  encap:Ethernet HWaddr 00:50:FC:CD:20:2A
      inet6 addr:  3ffe:1001:1c0:2::/64 Scope:Global
      inet6 addr:  fe80::250:fcff:fecd:202a/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      ...
```

3 Attivazione di un tunnel IPv6-over-IPv4

3.1 Il meccanismo di tunneling

Come già accennato in precedenza, IPv4 si è ormai radicato a tal punto da rendere impossibile un passaggio rapido ad IPv6; quello che invece sta avendo luogo (e accadrà ancora per diversi anni) è una graduale transizione di Internet, dove però ancora per lungo tempo i due protocolli convivranno.
A questo proposito il gruppo di lavoro *ngtrans* della Internet Engineering Task Force ha proposto un gran numero di strategie di migrazione, essenzialmente riconducibili a tre principali tipologie: Dual stack, Translation e Tunneling.
Il tunneling come meccanismo di transizione è utilizzato per interconnettere tra loro host che altrimenti non potrebbero comunicare poiché 'separati' da reti incompatibili. I datagram IP sono quindi trasportati all'interno di altri datagram IP, in modo che il protocollo incapsulato veda quello incapsulante come un DLC, un 'link virtuale'. In base alle esigenze si possono utilizzare differenti combinazioni di tunneling IP: IPv4 in IPv6 o viceversa ma anche, per la realizzazione ad esempio di VPN, IPv4 in IPv4. Un'ulteriore possibilità è data dall'incapsulamento di pacchetti IPv6 all'interno di datagram UDP IPv4: questa soluzione semplifica, ad esempio, l'instaurazione di tunnel attraverso NAT.

3.2 Il Tunnel Server Protocol

Un tunnel IPv6-over-IPv4 è attivato quando entrambi gli endpoint configurano opportunamente gli indirizzi IP della controparte comunicante. Questo implica che, quando una delle due entità cambia il proprio indirizzo IPv4 con cui è connessa ad Internet, entrambi i nodi devono riconfigurare di conseguenza il tunnel. Una situazione come questa può risultare di difficile gestione nel caso in cui una delle entità cambi frequentemente il proprio indirizzo, come accade ad esempio nel caso di connessioni dialup. Il servizio fornito da Freenet6 fornisce invece una implementazione di tunneling IPv6-over-IPv4 che supera questi limiti sfruttando il protocollo TSP (Tunnel Server Protocol). Basato su un approccio client/server, questo protocollo prevede che la negoziazione dei parametri del tunnel e la sua attivazione avvenga in maniera del tutto automatizzata utilizzando messaggi XML.
In sostanza, l'attivazione di un tunnel di sessione utilizzando il protocollo Freenet6 TSP avviene nel seguente modo:

1. Il client TSP, attivo sul host IPv6 connesso ad Internet, si autentica presso il server TSP ed invia quindi la richiesta di attivazione di un tunnel, indicando il proprio indirizzo IPv4.

2. Il server autentica il client e, in base al tipo richiesta, assegna un indirizzo IPv6 (/128) e un pool di indirizzi al client

3. Il server attiva il tunnel IPv6-over-IPv4, in base alle informazioni ricevute nella richesta

4. Il client riceve i parametri di configurazione del tunnel, ricevuti dal server, e configura di conseguenza la propria interfaccia

3.3 Le caratteristiche del servizio Freenet6

3.3.1 Autenticazione

L'accesso al servizio di Freenet6 può essere effettuato secondo due diverse modalità: anonimo o autenticato.
Un accesso anonimo non richiede alcuna registrazione e l'indirizzo IPv6 cambia al variare dell'indirizzo IPv4. Discorso diverso invece per gli utenti registrati: in questo caso l'indirizzo IPv6 e il prefisso sono assegnati permanentemente all'utente e non cambiano quando questo si connette da un indirizzo v4 diverso. L'autenticazione tra client e server può, a sua volta, avvenire in due diverse modalità: semplice o cifrata. Mentre nel primo caso userID e password sono inviate in chiaro, l'algoritmo SASL-DIGEST-MD5 è invece utilizzato per cifrare le informazioni dell'account nel secondo caso.

3.3.2 Indirizzi IPv6 assegnati

Nel caso di singoli indirizzi, la lunghezza del prefisso assegnato ai tunnel configurati è di 128 bit (/128). I tunnel anonimi sono assegnati in sequenza dal pool di indirizzi 2001:5c0:8fff:ffff::/64 mentre quelli autenticati a partire dal 2001:5c0:8fff:fffe::/64. In particolari i tunnel anonimi di Freenet6 utilizzano un formato speciale per gli indirizzi IPv6 degli endpoint. Al fine di identificare eventuali utenti malintenzionti, l'indirizzo IPv4 sorgente è inserito negli ultimi 32 bit dei 128 che compongono l'indirizzo IPv6.

```
|<-----network---->|<------host------>|
XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:AABB:CCDD
```

Per esempio, se l'indirizzo di un utente anonimo fosse 24.200.194.27, traducendo opportunamente in esadecimale l'indirizzo IPv4, il corrispondente indirizzo IPv6 potrebbe essere 2001:05C0:8FFFF:FFFF::18C8:C21B

```
|<-----network----->|<------host------>|
                                  |<-IPv4->|
2001:05C0:8FFFF:FFFF:0000:0000:18C8:C21B
```

Per quel che riguarda invece l'assegnazione di prefissi IPv6 /48, questi vengono assegnati in sequenza dal pool 2001:5c0:8000::/34 ma solo gli utenti registrati possono farne richiesta (e in questo caso è necessario che l'host disponga di una connessione permanente ad Internet). Con ciascuno dei prefissi /48 possono essere utilizzati per gestire 65536 differenti link: i meccanismi di autoconfigurazione, utilizzabili per la generazione di indirizzi IPv6 globali unicast, necessitano di un prefisso /64 assegnato al link.

3.3.3 DNS e Uptime dei tunnel

Per ogni tunnel attivato, un record AAAA viene creato all'interno del server DNS di Freenet6, eccezion fatta per gli utenti anonimi dietro un dispositivo NAT. A meno che non vengano riattivato, i tunnel standard v6v4 scadono dopo sette giorni dall'ultima connessione del client TSP e le entry DNS eliminate. I tunnel attivati da un client posto in una rete dietro NAT, invece, cadono invece dopo pochi minuti dalla disconessione del client TSP.

4 Installazione del client TSP

Il client TSP sviluppato da Hexago, rilasciato sotto licenza GNU GPL, è disponibile sia per Windows che per piattaforma *nix (Linux/BSD/Darwin). La versione attuale, rilasciata a giugno 2001, è la 4.1 ed è stata testata con successo in laboratorio sia su Windows XP che su Linux 2.6.15. I file necessari possono essere scaricati dal sito http://www.hexago.com; sempre sullo stesso sito è possibile anche effettuare la registrazione gratutita, per poter così usufruire delle funzionalità avanzate del servizio Freenet6.

4.1 Windows client

L'installazione del client per Windows è assolutamente automatizzata e non richiede particolari compentenze. Il client dispone inoltre di un'intuitiva interfaccia grafica ed il sistema è già impostato per effettuare una connessione anonima, riconoscendo automaticamente se l'host è connesso direttamente ad Internet o se si trova dietro ad un dispositivo di tipo NAT (è comunque possibile modificare le impostazioni premendo il pulsante Advanced). Per attivare il tunnel è sufficiente premere il pulsante Start ed attendere che si accenda la luce verde in basso.

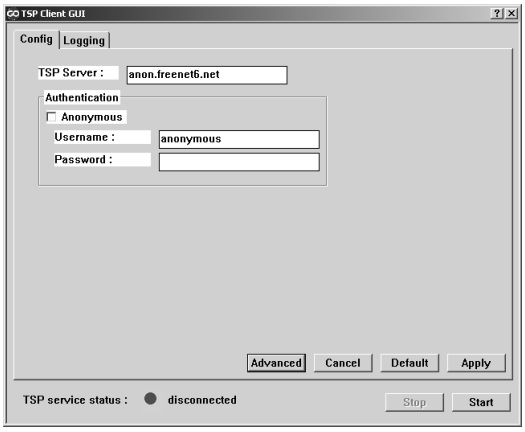

Figura 3: L'interfaccia grafica del TSP Client per Windows

Il client viene installato anche come servizio di Windows ed il tunnel IPv6 attivato quindi automaticamente ogni qualvolta viene rilevata una connessione ad Internet. Se si desidera invece che il tunnel venga attivato solo su richiesta, occorre modificare le proprietà del servizio Hexago TSP Client dal Pannello di Controllo → Strumenti di amministrazione → Servizi impostando l'avvio manuale

4.2 Unix client

L'installazione del client in un sistema Unix-like deve essere invece effettuata compilando i sorgenti, disponibili sempre sul sito sito http://www.hexago.com. Insieme al compilatore ed al linker, è necessario anche che sulla macchina siano presenti i sorgenti di OpenSSL nonché le librerie condivise di OpenSSL stesso.
Per compilare è sufficiente eseguire il comando

```
# make all target=linux
```

specificando eventualmente un'altra tra le piattaforme disponibili (freebsd, netbsd, darwin, openbsd), e lanciare quindi

```
# make install target=linux install-dir=/usr/local
```

o una directory alternativa in cui installare il TSP client.
Per l'impostazione dei parametri di connessione è necessario modificare manualmente il file di configurazione, utilizzando come base il file di esempio `tspc.conf.sample` presente nella directory /usr/local/bin (o analoga).
Infine, per avviare l'instaurazione del tunnel, occorre impartire il comando

```
# tspc -f /etc/tspc.conf
```

avendo cura di indicare con l'opzione -f il percorso corretto del file di configurazione desiderato.

5 Test della connessione

Per verificare il corretto funzionamento della connessione IPv6 è possibile impartire, dal prompt dei comandi o dalla shell, il comando

```
ping6 www.kame.net
```

e controllare quindi che il sito risulti raggiungibile.
In alternativa, aprendo dal browser il sito web http://netlab-mn.unipv.it, lo sfondo dovrebbe apparire di colore verde anziché rosso.

Indice