

IPv6 – 6to4

José Maria Fonseca de Almeida,
ipv6@sapo.pt

Sobre o acesso a IPv6 com o Tunel 6to4

Janeiro de 2009

Resumo

Pretende este pequeno trabalho pretende dar indicações para um fácil acesso ao IPv6 com túnel 6to4 num router ADSL **Cisco C837, com o IOS (C837-K9O3SY6-M), versão 12.4(19)**, embora a configuração possa ser facilmente adaptada a outros router Cisco.

Índice

Resumo	1
1. Explicação do funcionamento do túnel 6to4	2
2. Segurança no túnel 6to4	4
3. Configuração	6
4. Bibliografia.....	8

1. Explicação do funcionamento do túnel 6to4

Este túnel descrito no RFC 3056 permite que redes IPv6 isoladas comuniquem com outras através da rede IPv4 no modo ponto – multiponto e é conhecido por túnel automático ou 6to4.

É usado um *relay router* com endereço IPv4 *anycast* (192.88.99.1). Este *anycast* foi definido para que, independentemente do ISP usado, se possa encontrar o *relay router* 6to4 mais próximo (menor número de saltos).

Usa o prefixo global 2002:wwxx:yyzz::/48, em que wwxx:yyzz é o IPv4 público em hexadecimal. O endereço IPv6 fica então: 2002:wwxx:yyzz:[Site ID]:[Interface ID].

Os *routers* não são configurados aos pares (como os túneis manuais) porque usam a estrutura IPv4 como um NBMA (*NonBroadcast MultiAccess link*), tal como o FR ou o X25. O endereço IPv4 é “embutido” no endereço IPv6 e é usado para encontrar o outro ponto do túnel automático.

Depois de estabelecido o túnel (interface virtual designado por “Tunnel64”) a partir do *router* ADSL, e anunciado o prefixo 2002::/16 a toda a rede local, foi então concretizada a ligação global ao mundo IPv6 de todos os PC ligados na rede local.”

A próxima figura representa o funcionamento deste tipo de túnel.

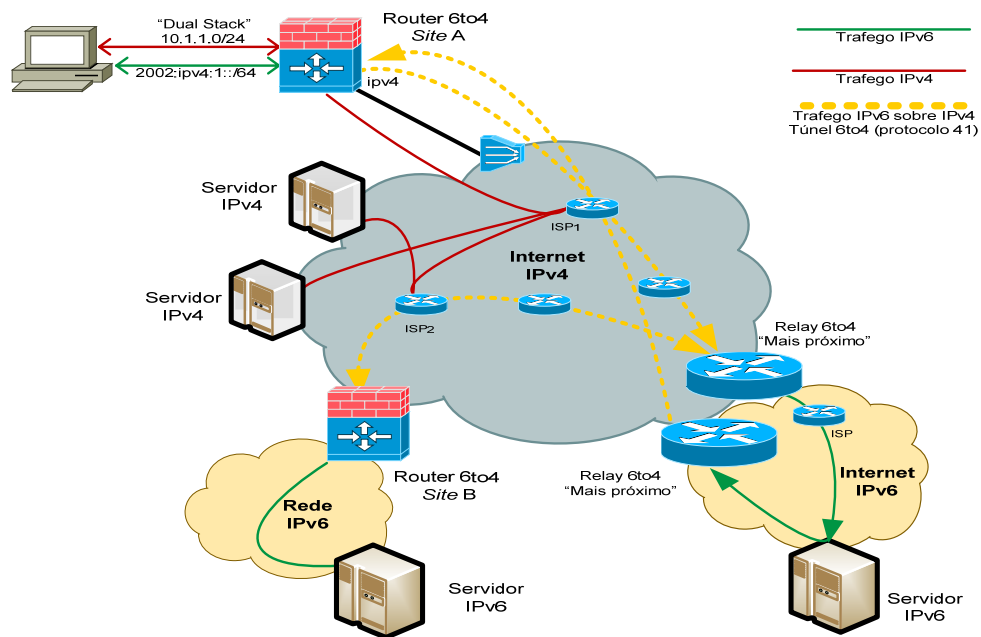


Fig. 1 – Funcionamento do túnel 6to4

O túnel automático ou *6to4* é a solução de transição mais eficaz (excluindo a *dual stack*). Existe um claro aumento da latência, mas com a manutenção da largura de banda. Infelizmente esta solução de recurso tem uma implementação relativamente complexa, e não é suportada de forma uniformemente eficaz devido a diferenças de *routing* dos ISPs para o IP anycast referido, nem é facilmente implementável em todos os equipamentos (*routers*).

2. Segurança no túnel 6to4

Seria aparentemente possível, pelo menos, restringir este tipo de tráfego (o protocolo 41: IPv6 sobre IPv4) ao túnel usado pelo nosso ISP, bloqueando todos os outros. O problema é que a resposta aos nossos pacotes pode não ter origem no IP *anycast* usado mas no IP do “*relay 6to4*” mais próximo do nosso destino. Obrigando no mínimo ao uso uma ACL do tipo: “access-list 111 permit 41 any any” (ou ao uso de uma lista permanentemente actualizada de legítimos servidores “*relay 6to4*”...

E a protecção assim oferecia é quase nula. Até porque o IP está sujeito a *spoofing* dada a ausência de qualquer tipo de autenticação.

Mas neste túnel temos a grande vantagem (ao contrário dos “tunnel brokers”) de poder controlar o tráfego IPv6 que circula na rede local (entre as máquinas e o *router* onde foi estabelecido o túnel).

- Controlo do tráfego IPv6 que passa dentro do túnel

Neste túnel o endereço 2000:xxxx:xxxx:0\64 varia em função do IPv4 (convertido em formato hexadecimal) atribuído pelo ISP à interface ADSL do *router*. Desta forma, para quem não tenha um acesso com IPv4 fixo, passa a ser impossível de uma forma estável filtrar correctamente os endereços com base do IPv6 global de origem, pois este não é constante, já que (como já foi referido) é construído a partir endereço IPv4 público.

Seria teoricamente filtrar pelo interface ID, mas a construção da ACL não o permite (baseia-se no prefixo, à semelhança do que acontece no IPv4). Mas tal também não seria muito seguro pois o Windows por omissão atribui endereços temporários (para garantir o anonimato do utilizador).

É assim pouco eficaz tentar filtrar o tráfego com base no IP de origem em IPv6, sem o recurso a um servidor de DHCPv6!

Outra possibilidade seria usar um “general prefix name”, mas ACLs da Cisco não comportam esta possibilidade.

Mas continua a ser possível estabelecer políticas de segurança com base no porto de origem, no porto destino, ou ainda com base no valor da “flow label” e outros parâmetros específicos do IPv6.

Como se demonstra:

```
# sh ipv6 access-list RedeInterna-Net
IPv6 access list RedeInterna->Net
deny ipv6 host 2002:529A:4036:1:21D:60FF:FEBA:266 any (24 matches) sequence 10
permit ipv6 host FD00:A:B:3:21D:60FF:FEBA:266 any log (36 matches) sequence 20
permit ipv6 host FD00:A:B:3:2E0:FF:FE9B:B0CF any log (635 matches) sequence 30
permit tcp host 2002:529A:4036:1:2E0:FF:FE9B:B0CF gt 1024 any eq www flow-label 43946
log sequence 40
permit tcp host 2002:529A:4036:1:2E0:FF:FE9B:B0CF gt 1024 any eq www flow-label 0 log
(66 matches) sequence 50
deny tcp host 2002:529A:4036:1:2E0:FF:FE9B:B0CF gt 1024 any eq telnet (3matches)
sequence 60
permit icmp any any nd-na (44 matches) sequence 70
permit icmp any any nd-ns (22 matches) sequence 80
deny ipv6 any any log-input (59 matches) sequence 90
```

NOTA:

Não é possível neste router implementar IPSec em IPv6 devido a limitações do IOS, o que me parece constituir uma importante incoerência perante as promessas de segurança do novo protocolo IP.

Parte deste texto foi transcrito de um meu trabalho sobre IPv6 disponível em:
<http://www.sendspace.com/file/3g2e45>

3. Configuração

A configuração que se segue não está completa, e pretende apenas focar-se fundamentalmente nas linhas a acrescentar a uma configuração IPv4 num acesso ADSL para estabelecer um túnel 6to4 (a verde negrito). Foram acrescentados alguns comentários (a azul itálico).

```
ip cef
ipv6 unicast-routing
```

ipv6 general-prefix net-IPv6 6to4 Dialer1

```
#Associa o prefixo "net-IPv6" do tunel 6to4 ao IPv4 obtido no interface Dialer1 (IP obtido do ISP #da ligação ADSL por DHCP
ipv6 cef)
```

interface Tunnel64

```
description IPv6 6to4 Tunnel
no ip address
no ip redirects
ipv6 enable
#activa endereçamento IPv6 na interface.
ipv6 mtu 1472
#Se aos 1500 bytes do MTU do Ethernet subtrairmos 8 bytes para o PPPOE e 20 bytes para o
#IPv4, que transportará o IPv6 obtemos 1472
tunnel source Dialer1
# A interface externa IPv4, onde chegaram os pacotes "protocolo 41": IPv6 sobre IPv4
tunnel mode ipv6ip 6to4
# Definição do tipo de túnel
tunnel path-mtu-discovery
!
```

interface Ethernet0

```
description Interface local
ip address 10.99.99.1 255.255.255.0
no ip redirects
no ip unreachable
ip nat inside
ip virtual-reassembly
ip tcp adjust-mss 1452
ipv6 address net-IPv6 ::1:213:C3FF:FE37:6F96/64
#EndereçoIPv6 a ser assumido pela interface local do router, constituída pelo prefixo "net-
#IPv6" (ver ponto 1), o site ID (valor 1), e o interface ID, que neste caso é um exemplo
#conversão de um MAC de 48bits num IID IPv6 (EUI-64), o que recomendo, mas pode
#assumir outro valor. Consultar a pagina 45 do meu trabalho sobre IPv6 em:
#http://www.sendspace.com/file/qlxe9o
na pagina 45
ipv6 nd ra-interval 50
ipv6 nd prefix default 180 120
#Valores a usar pelo Neighbor Discovery Protocol neste router, mas podem ser usados
#outros.
no keepalive
no cdp enable
hold-queue 100 out
!
```

interface ATM0

```
no ip address
```

```

no ip redirects
no ip unreachable
no ip proxy-arp
load-interval 30
no atm ilmi-keepalive
dsl operating-mode auto
!
interface ATM0.1 point-to-point
pvc 0/35
pppoe-client dial-pool-number 1
!
interface Dialer1
mtu 1492
ip address negotiated
ip access-group 111 in
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat outside
ip virtual-reassembly
encapsulation ppp
ip tcp adjust-mss 1452
load-interval 30
dialer pool 1
ppp pap sent-username asxxxxx@zzzz password 7 xxxxxxxxxxxxxxxx
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer1
!
ip nat inside source list 22 interface Dialer1 overload
!
access-list 22 permit 10.0.0.0 0.255.255.255
access-list 111 remark acesso tunel 6to4
access-list 111 permit 41 any any log
#Consultar o ponto 2
access-list 111 permit icmp any any echo-reply

ipv6 route 2002::/16 Tunnel64
ipv6 route ::/0 2002:C058:6301::
# Consultar o "post": "Rotas IPv6 para o túnel 6to4"

```

4. Bibliografia

- [1] <http://www.sendspace.com/file/3g2e45>
- [2] <http://www.sendspace.com/file/qlxe9o>
- <http://ipv6.blogs.sapo.pt/>
- www.anyweb.co.nz
- Deploying IPv6 Networks
Por Ciprian Popoviciu, Eric Levy-Abegnoli, Patrick Grossetete
Da Cisco Press