

IPv6@ESTG-Leiria – Mecanismos de transição IPv6

Luis Diogo, Óscar Brilha, Nuno Veiga
Escola Superior de Tecnologia e Gestão de Leiria
Instituto Politécnico de Leiria
Morro da Lena – Alto Vieiro – 2401-951 Leiria – Portugal
Telf: +351 244820300; Fax: +351 244 820310
e-mail: eic10429@student.estg.ipleiria.pt, eic09061@student.estg.ipleiria.pt,
nveiga@estg.ipleiria.pt

Resumo: Este artigo descreve os diversos mecanismos existentes na transição para o novo protocolo IPv6. Neste artigo vão se abordar os diversos mecanismos de transição de modo singular dando-se uma especial atenção aos túneis. Também se falará no DNS, o que está feito e o que se pretende fazer.

1. Introdução

O protocolo *Internet Protocol* (IP) é o protocolo responsável pelo transporte de dados na *Internet*. Actualmente, existem duas variantes deste protocolo: *IPv4* e *IPv6*.

Hoje em dia, o protocolo IPv4 ainda é o protocolo de rede mais usado no mundo.

Com o rápido crescimento da *Internet*, esta tecnologia (IPv4) tem-se esgotado e muitos esforços têm sido feitos para a sua evolução.

O protocolo IPv6 é uma nova versão do protocolo IP e encontra-se em plena fase de divulgação e cabe ao mundo académico divulgar e provar as inúmeras vantagens deste protocolo em relação ao seu antecessor, o protocolo IPv4.

O sucesso de uma nova tecnologia depende em grande parte da sua capacidade de adaptação à infra-estrutura já existente. Muitas tecnologias não obtiveram sucesso devido ao deficiente processo de transição.

A tecnologia IPv6 foi concebida de modo a que a sua transição seja efectuada suave e eficazmente. Este factor da transição foi tido como um factor muito importante na altura da sua concepção.

Durante os anos vindouros irão ocorrer duas etapas distintas, uma primeira em que existirão umas “ilhas” IPv6 num imenso “oceano” IPv4 e posteriormente o contrário, ou seja, quando todo o mundo tiver o protocolo ipv6 generalizado irão prevalecer umas ilhas IPv4 num imenso oceano IPv6.

Para assegurar a transição irão ser necessários mecanismos que permitam a coexistência dos dois protocolos, mecanismos esses que irão ser aprofundados neste projecto.

Para quem se questiona se o IPv6 será mesmo necessário, pensemos no rumo que as telecomunicações estão a tomar. Cada

terminal, móvel ou fixo, terá um ou mais endereços IP. É impensável continuar com os endereços actuais.

O protocolo ipv6 irá prevalecer com toda a certeza, o que não se sabe é durante quanto tempo irá coexistir com o seu antecessor.

2. Pilha dupla

Com a chegada do protocolo IPv6 os novos dispositivos passaram a utilizar uma Pilha protocolar TCP/IP dupla, em que a camada de rede suporta os dois tipos de endereços (IPv4 e IPv6).

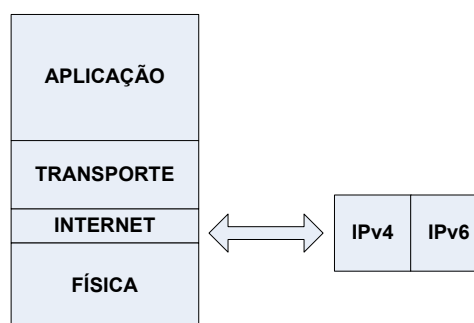


Figura 1 – Pilha protocolar TCP/IP dupla.

3. Funcionamento da pilha TCP/IP em Tunneling

Os pacotes que circulam numa rede provenientes de túneis têm o cabeçalho IPv6 encapsulado dentro do pacote IPv4. Observando a imagem apresentada é perceptível que a parte IPv4 antecede o cabeçalho IPv6. Isto acontece pois o encaminhamento entre um túnel que ligue dois routers é efectuada em IPv4. Após a chegada do pacote a um desses routers (proveniente do túnel) é que a parte IPv6 é analisada de modo a que o router saiba para onde encaminhar o pacote com base no seu endereço IPv6:

```

Internet Protocol, Src: 200.15.15.1 (200.15.15.1),
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: D
  Total Length: 120
  Identification: 0x0048 (72)
  Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: IPv6 (0x29)
  Header checksum: 0x07f4 [correct]
  Source: 200.15.15.1 (200.15.15.1)
  Destination: 200.15.20.1 (200.15.20.1)
Internet Protocol Version 6
  Version: 6
  Traffic class: 0x00
  Flowlabel: 0x00000
  Payload length: 60
  Next header: ICMPv6 (0x3a)
  Hop limit: 64
  Source address: 2002:c80f:f01::1
  Destination address: 2002:c80f:1401::c80f:1401

```

Figura 2 – Pacote IPv6 encapsulado em IPv4.

4. Túneis manuais

Os túneis manualmente configurados são simples de usar e eficazes.

Nestes túneis os endereços IPv6 e IPv4 são manualmente configurados (atribuídos) nas interfaces dos routers destino e origem.

Este tipo de configuração é usada quando se pretende uma conectividade permanente ou dedicada e requer configuração específica em cada extremidade do túnel. Como é necessária configuração nos routers em cada ponta do túnel requer um bom conhecimento acerca da topologia da rede. Este tipo de configuração ponto a ponto fornece uma segurança bastante robusta a tráfego injectado no troço.

Túneis manuais são usados em ligações Router-to-Router e Host-to-Router.

No entanto, é claro que este mecanismo pode ter problemas de escalabilidade quando se considera um vasto número de locais que precisam de comunicar uns com os outros. Supondo que, por exemplo, 1000 locais pretendem comunicar uns com os outros. Cada local tem de ter configurado um túnel com 999 pontos de saída para cada prefixo IPv6. Se um ponto de saída do túnel falhar, é necessário altera-lo nos outros 999 locais. Desta forma, os túneis automáticos são mais robustos a falhas na rede.

5. Túneis automáticos

Nos túneis automáticos os endereços IPv6 das extremidades do túnel são configurados (atribuídos) com base nos endereços IPv4. Os endereços IPv6 derivam dos endereços IPv4 e são atribuídos aos routers automaticamente sem necessidade de configurações manuais. A maioria dos túneis automáticos foi planeada para coexistir durante muito tempo com o IPv4

e IPv6 de modo a garantir uma migração simples e eficaz para o protocolo IPv6.

5.1. Túneis 6to4

O objectivo dos túneis 6to4 é o de permitir a comunicação de vários domínios IPv6 (ilhas IPv6) sobre um Backbone IPv4 sem ser necessário configurar o túnel nos routers de fronteira situados nesses domínios IPv6. Desta forma, este tipo de túneis foram desenvolvidos para permitir que os routers de fronteira descubram automaticamente o endereço IPv4 da outra extremidade do túnel.

Os túneis 6to4 estabelecem o endereço das extremidades do túnel com base no endereço IPv4. O principal objectivo e propósito dos túneis 6to4 é o de permitir a comunicação entre máquinas IPv6 sem a configuração explícita de túneis, usando para isso *relay routers*.

Estes endereços são usados em locais onde exista pelo menos um endereço IPv4 público. Para endereços privados são usados endereços ISATAP.

São usados alguns routers denominados *relay routers* (estes routers são disponibilizados publicamente na Internet) que têm a função de assegurar a um utilizador comum o acesso à rede IPv6.

Estes túneis são usados em ligações entre dois routers em extremidades opostas do túnel, ou entre um router de uma das extremidades e um terminal.

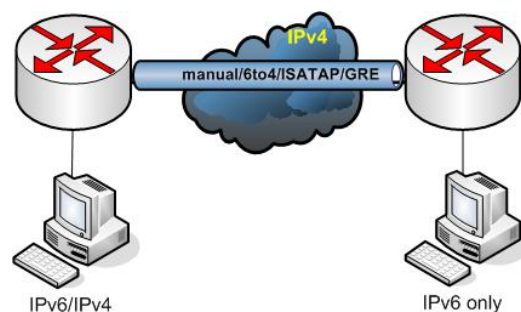


Figura 3 – Exemplo de implementação de vários tipos de túneis.

5.2. Túneis ISATAP

É um mecanismo em tudo semelhante ao 6over4 com a excepção de não usar o *Multicast* do protocolo IPv4. Esta particularidade torna-o ligeiramente mais complexo que o mecanismo 6over4 ou 6to4. Apesar de ser um mecanismo de túnel muito semelhante aos outros, foi concebido para transporte de tráfego IPv6 numa intranet permitindo a comunicação entre máquinas IPv6 através de infra-estruturas IPv4.

Como neste tipo de túnel não é usado *Multicast* é necessário uma RPL (*routers potencial list*). Cada router desta lista é sondado pelo ICMPv6 para se determinar quais estão em funcionamento assim como para efectuar a auto configuração dos endereços *Unicast* (obtendo a lista de prefixos que podem ser usados).

5.3. Túneis GRE

O tráfego IPv6 pode ser transportado através de túneis GRE. Estes túneis são usados para fornecer ligação ponto a ponto (*point-to-point*). Tal como acontece nos túneis manuais, os túneis GRE fornecem ligação entre dois pontos usando um túnel por cada *link* (ligação). Os pacotes designados para serem enviados pelo túnel (já encapsulados com um cabeçalho de um protocolo, por exemplo o IP) são encapsulados com um novo cabeçalho (cabeçalho GRE) e colocados no túnel com o endereço de destino do final do túnel.

Os túneis não são associados a um protocolo de transporte, no entanto neste tipo de túnel o IPv6 ou IPv4 é usado como protocolo de transporte.

O principal motivo para o uso destes túneis é a necessidade de ligação segura entre dois routers fronteira ou entre um router fronteira e um terminal. Também neste caso os routers e terminais têm de ter suporte para pilha dupla.

5.4. Túneis Teredo

O principal propósito dos túneis Teredo é o de proporcionar conectividade IPv6 a máquinas que se encontrem por trás de um mecanismo NAT. Com a escassez de endereços IPv4 muitas instituições e pequenas redes informáticas usam o mecanismo NAT para que apenas seja necessário um ou dois endereços públicos por instituição.

Os túneis 6to4 não funcionam em máquinas que estejam por trás de NAT, pois o NAT apenas traduz TCP e UDP ficando o campo protocolo do cabeçalho IP (essencial para indicar a existência de um endereço proveniente de um túnel) descartado. Os túneis 6to4 apenas funcionam se a máquina que faz as funções de 6to4 router for a mesma que assegura o NAT.

Os túneis Teredo permitem que uma máquina que se encontre numa rede IPv4 por trás de um mecanismo NAT se possa ligar ao *Backbone* do IPv6 sem qualquer envolvimento da infraestrutura existente.

6. Routers a usar nas extremidades de um Túnel

Dos routers existentes na rede ou nos possíveis routers a adquirir é preciso ter em conta os seguinte factores:

- O router deve ser actualizado com software com funcionalidades IPv6
- O router tem de ter pilha dupla
- Para os mecanismos de túnel, o router deve possuir uma ligação IPv4 fiável com outro router remoto.

7. Suporte nos diversos Sistemas operativos



Windows XP:

Suporta todos os túneis falados, tem um bom suporte dual stack IPv6.



Fedora Core:

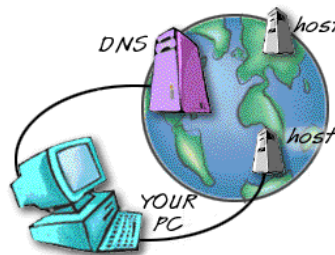
As versões kernel posteriores á 2.4 não suportam os túneis ISATAP (problema de patentes). Por este motivo as máquinas linux apresentam algumas limitações na conectividade IPv6 dentro de uma intranet.



IOS Cisco:

Suportam todo o tipo de túneis excepto os túneis Teredo.

8. DNS



Um *Domain Name System* (DNS) é necessário para uma coexistência fiável dos protocolo IPv4 e IPv6. O DNS é das ferramentas mais importantes da *Internet* actual e ganha uma importância ainda maior com a progressiva adopção do protocolo IPv6. O utilizador comum acede a uma página através de um nome e não através de um IP, mesmo que pensemos em pessoas especializadas em informática que saibam usar os endereços IP para aceder a

recursos isso torna-se um pouco mais difícil com os novos endereços IPv6. A actualização da infra-estrutura DNS passa pela implementação nos servidores DNS de suporte para resolução de endereços IPv6 para nomes e vice-versa.

No entanto o “upgrade” para o suporte de endereços IPv6 não é simples uma vez que as aplicações assumem que as consultas apenas devolvem endereços de 32 bits IPv4.

Extensões à estrutura DNS para suporte para IPv6:

- Criado um novo tipo de registo para os endereços IPv6 (registo AAAA).
- Criado um novo domínio IP6.ARPA para substituir o obsoleto domínio IP6.INT.
- Os mecanismos de consultas existentes foram actualizados para que efectuem consultas em endereços IPv4 e IPv6.

A infra-estrutura DNS deve conter os seguintes registos:

- Registo dos nós IPv4 nativos (*IPv4 only nodes*) e registo dos nós IPv4/IPv6.
- Registo de nós AAAA para nós IPv6 nativos (*IPv6 only nodes*) e IPv4/IPv6.
- Registos PTR no domínio IN-ADDR.ARPA para nós IPv4 nativo e IPv4/IPv6
- Registos PTR no domínio IP6.ARPA para IPV6 nativo e IPv4/IPv6 (Opcional)
- Novo tipo de registo *DNAME* análogo ao *CNAME* para registos A6 (Opcional).

Registos AAAA:

Os quatro As (AAAA) é um nome relativo aos endereços de rede indicando que os endereços IPv6 são quatro vezes maiores que os endereços IPv4. Os registos estão estruturados praticamente do mesmo modo que os registos IPv4 de 32 bits, mas com um tamanho maior.

Registos A6:

Na estrutura DNS foram recentemente criados para além do *Resource records* (RR) “AAAA” os RR “A6”. Actualmente e durante alguns anos ainda usar-se-ão os “AAAA”, no entanto prevê-

se que os RR transitem gradualmente para os “A6” (o valor do campo “Type” é 38 em decimal).

Para facilitar a transição, os registos A6 poderão guardar registos “AAAA”.

O formato A6 tem diferenças significativas em relação aos “AAAA”. Pretende tornar toda a estrutura DNS ainda mais hierarquizada e torná-la mais flexível.

Os RR A6 são mais flexíveis. É possível criar vários tipos de registos: registos completos ou registos concatenados.

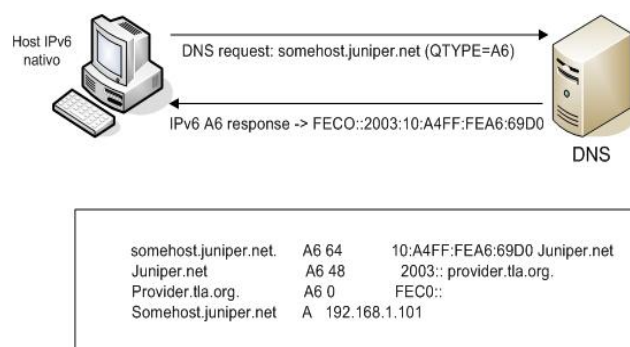


Figura 4 – Exemplo da resolução de nomes para endereços IPv4/IPv6 através de um servidor DNS.

9. Conclusões

Actualmente existe um grande esforço em permitir uma migração do protocolo IPv4 para o protocolo IPv6 sem grandes complicações, no entanto, ainda existem falhas e soluções que nem sempre são simples de implementar. Alguns mecanismos de transição como os túneis 6over4 estão já obsoletos pois assentam em pressupostos (*Multicast*) que nem sempre são os mais apropriados para o sucesso da solução.

Uma grande parte do cenário real é coberto pelos mecanismos existentes, no entanto existem ainda algumas limitações quando falamos de ligar intranets a IPv4 e IPv6 apesar de ser possível.

No campo do DNS actualmente usam-se os registos AAAA prevendo-se que estes sejam progressivamente substituídos pelos registos A6. Os registos A6 são no entanto recentes e ainda têm algumas limitações que entretanto serão eliminadas.

Nota-se uma clara aposta em transitar para IPv6 mas neste momento parece-nos que o protocolo IPv4 irá predominar (apesar de não haverem endereços suficientes) durante alguns anos.

Referencias

Wikipedia–IPv6,
<http://pt.wikipedia.org/wiki/IPv6>

Wikipedia-6to4,
<http://en.wikipedia.org/wiki/6to4>.

Wikipedia-ISATAP,
<http://en.wikipedia.org/wiki/ISATAP>

Wikipedia-TEREDO,
http://en.wikipedia.org/wiki/Teredo_tunneling

Cisco – Implementing Tunnelling for IPv6,
http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00801d6604.html

HAGEN, S. - *Ipv6 Essencials*, O'Reilly,
ISBN 0596001258, 2002

DAVID SERAFIM; VITOR SANTOS -
*IPv6@ESTG-
Leiria_Relatorio_Final_Projecto*