Formação IPv6 - Maputo

Transição

Maputo 28 de Agosto de 2008

Carlos Friaças e Pedro Lorga

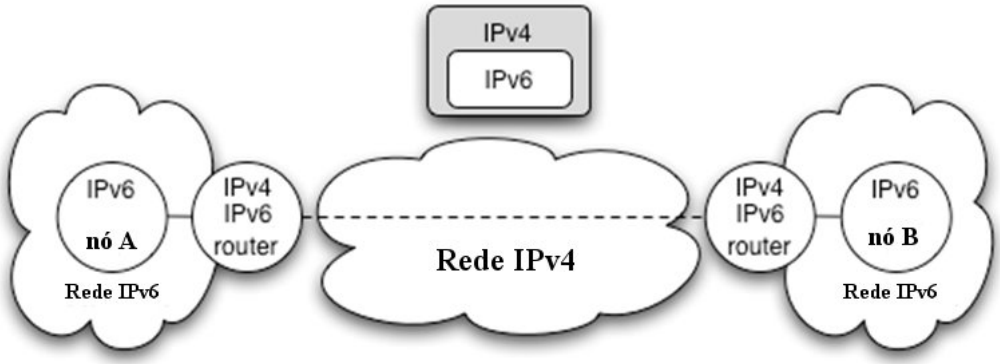
Transição

Agenda/Índice

- Túneis
- 6to4
- NAT-PT
- DUAL STACK
- Conclusões

Túneis

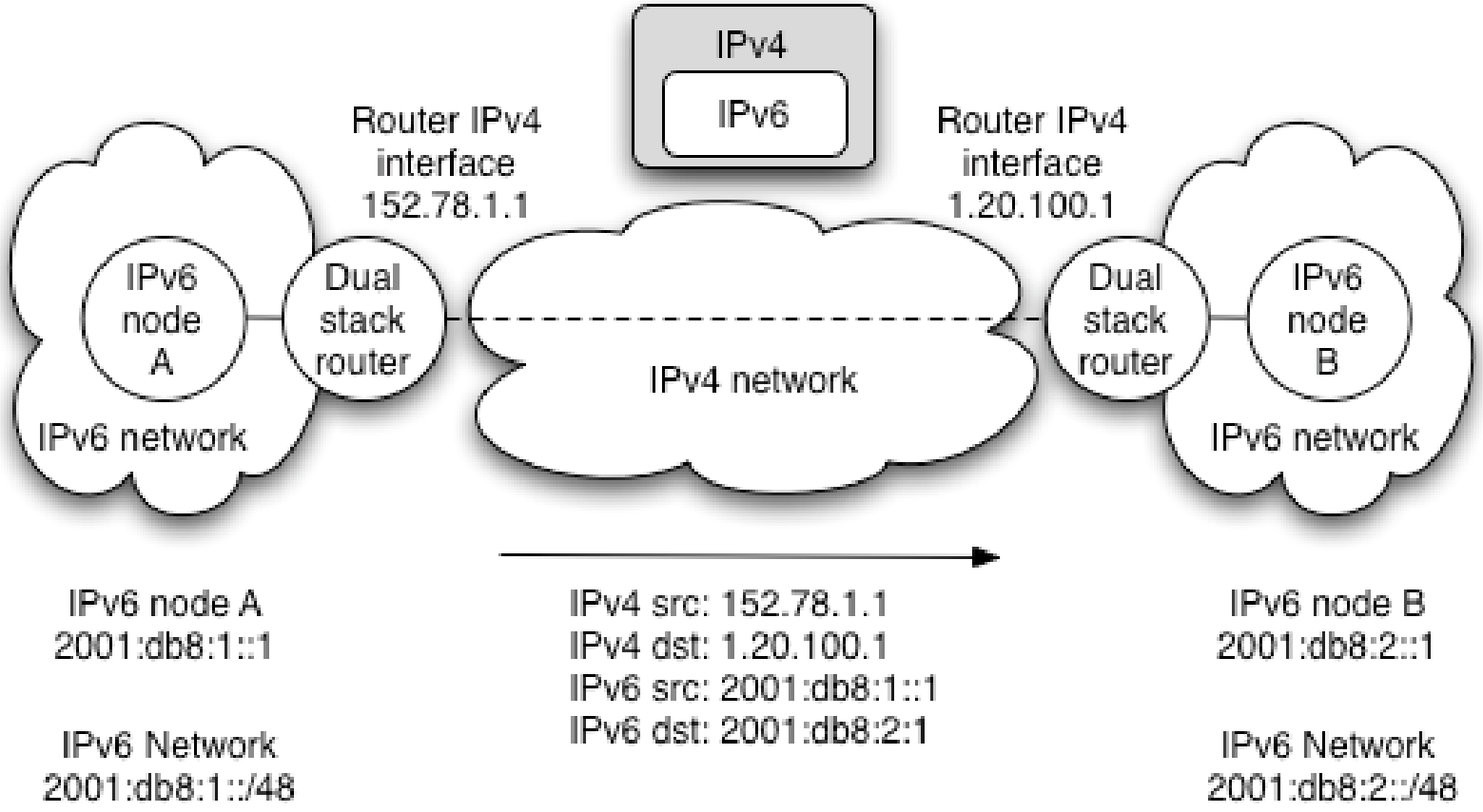
- Inicialmente IPv6 sobre IPv4 (no futuro, IPv4 sobre IPv6!)
- Pacotes IPv6 são encapsulados em pacotes IPv4
  - O pacote IPv6 é o «payload» do pacote IPv4
- Usualmente usado entre *routers* de forma a interligar «ilhas» de redes IPv6
  - O *router* de acesso fala IPv6 internamente com os sistemas na sua LAN
  - Encapsula pacotes IPv6 em pacotes IPv4 na direcção do outro extremo do túnel



Entrega de pacotes através do túnel

- O nó A IPv6 envia pacotes para o nó B IPv6
  - Encaminhados localmente para o *router*
- O *router* (do lado A) conhece o melhor caminho para o destino (nó B) através do *interface* do túnel
  - Encapsula os pacotes IPv6 em pacotes IPv4
  - Envia os pacotes IPv6 para o *router* (do lado B)
  - A entrega é efectuada através da infraestrutura IPv4 que existe entre ambos (Internet)
- O *router* (do lado B) desencapsula os pacotes IPv6 a partir do *payload* dos pacotes IPv4 recebidos
  - Os pacotes IPv6 são encaminhados internamente até à rede onde está o nó B
  - O nó B recebe os pacotes IPv6

Túnel - Endereçamento



Manuais ou automáticos?

- Os túneis podem ser criados **manualmente** ou de forma **automática**
- Manualmente
  - Requer intervenção manual nos dois extremos
    - Não funciona quando os endereços IPv4 mudam (DSL, …)
  - Boa solução do ponto de vista da gestão: sabe-se o que está no outro extremo do túnel
- Automaticamente
  - Túneis criados a pedido, mas sem intervenção humana
  - Inclui o mecanismo 6TO4 (RFC3056)
  - Outros mecanismos: ISATAP (RFC4214) e Teredo (RFC4380)

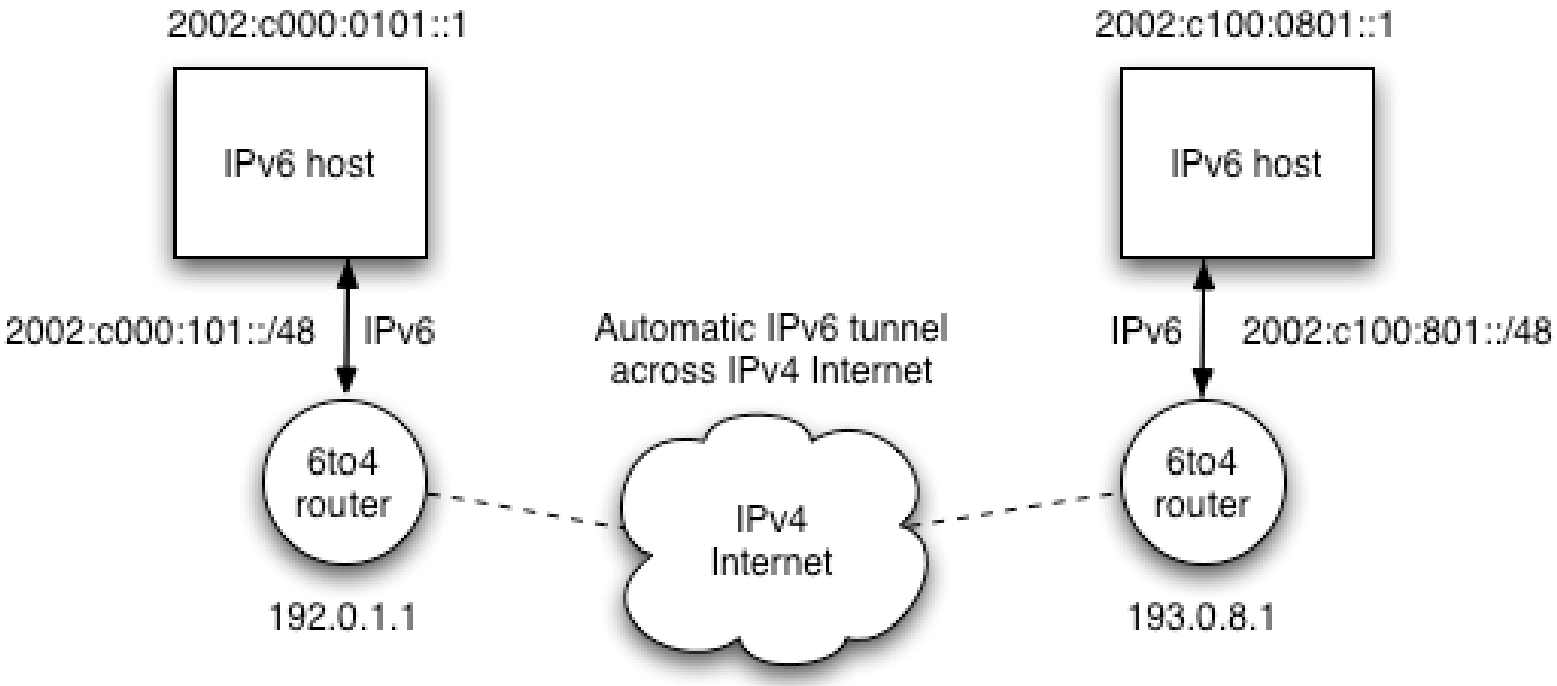
Tunnel Broker

- Modo de Operação:
  - processo de registo, para permitir posterior autenticação, quando o pedido de criação de um túnel é efectuado/recebido de um determinado endereço IPv4
  - o «broker» configura o seu lado do túnel e envia as configurações necessárias para que o outro extremo seja configurado pelo «cliente»
- Este mecanismo está descrito no RFC3053, de forma a possibilitar a conectividade de sistema a router, e também de *router* a *router*
- Exemplos:
  - www.freenet6.net (CA)
  - ipv6tb.he.net (US)
  - www.sixxs.net (EU)

6to4

- O mecanismo 6to4 é usado para ligar duas «ilhas» IPv6 através da rede IPv4
- O prefixo de rede IPv6 2002::/16 está reservado para este mecanismo
  - Os 32 bits seguintes do endereço são os bits do endereço IPv4 do *router* 6to4
  - Exemplo: um *router* 6to4 com o endereço 192.0.1.1 usará um prefixo IPv6 2002:c000:0101::/48 para a rede do seu *«site»* de transição
- Quando um *router* 6to4 recebe um pacote para um destino com um prefixo 2002::/16, ele sabe que tem de enviá-lo encapsulado através do mundo IPv4 para o endereço indicado nos 32 bits seguintes

6to4 - Mapa


2002:c000:0101::1
IPv6 host
2002:c000:101::/48
IPv6
6to4
router
192.0.1.1
Automatic IPv6 tunnel
across IPv4 Internet
IPv4
Internet
2002:c100:0801::1
IPv6 host
IPv6
2002:c100:801::/48
6to4
router
193.0.8.1

6to4 - Características

- Positivo: Simples de instalar e usar
  - Completamente automático; não necessita de intervenção humana para que seja configurado um novo túnel
  - Os pacotes atravessam os túneis até ao destino usando o melhor caminho disponível na rede IPv4
- Negativo: Os *relays* 6to4 podem ser usados em ataques (DoS attacks)
  - O RFC3964 descreve alguns cuidados a ter em conta

6to4 *Relay*

- Um *router* que seja um 6to4 R*elay* possui um endereço 6to4 mas também um endereço no mundo IPv6
- Dois casos a considerar:
  - Pacotes IPv6 enviados de um *«site»* 6to4 para um destino no mundo IPv6 (fora de 2002::/16) atravessam um túnel até ao *relay* e aí são encaminhados para a Internet IPv6 até ao seu destino
    - Os *relays* 6to4 são anunciados no endereço IPv4 anycast **192.88.99.1**.
  - Pacotes IPv6 enviados da Internet IPv6 até um *«site»* 6to4 (portanto num prefixo 2002::/16) são encaminhados até um *relay* 6to4 e então atravessam um túnel até ao destino.
    - O *relay* anuncia a rede **2002::/16** aos seus vizinhos na Internet IPv6

6to4 *Relay* @ FCCN - Rotas

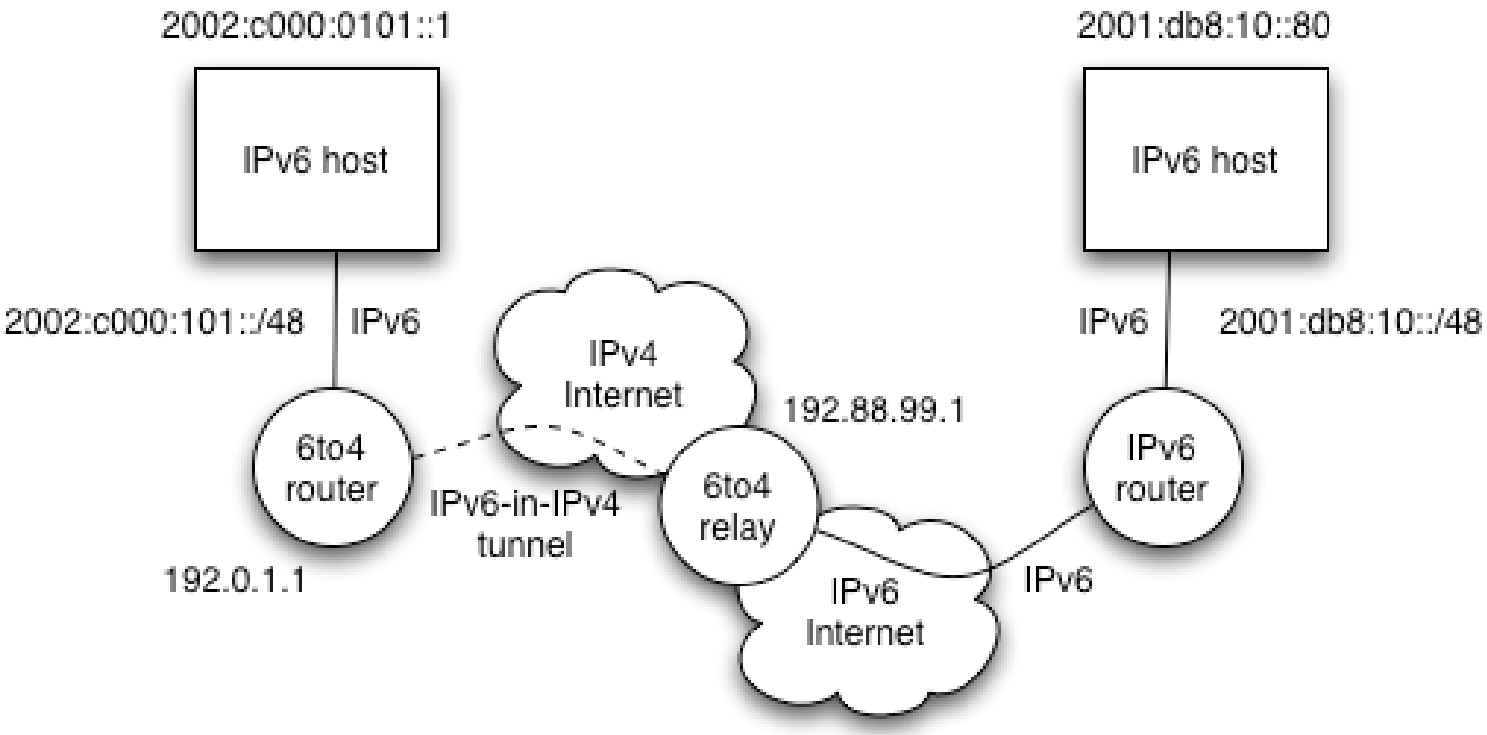
- (IPv4)
  * 139.83.0.0/16
  * **192.88.99.0/24**
  * 193.136.0.0/15
  * 194.210.0.0/16

(...)

- (IPv6)
  * 2001:690::/32 (RCTS)
  * 2001:7f8:a::/48 (GIGAPIX)
  * **2002::/16 (6TO4)**

- «Anúncios» do AS1930
  - *Border Gateway Protocol* (BGP)

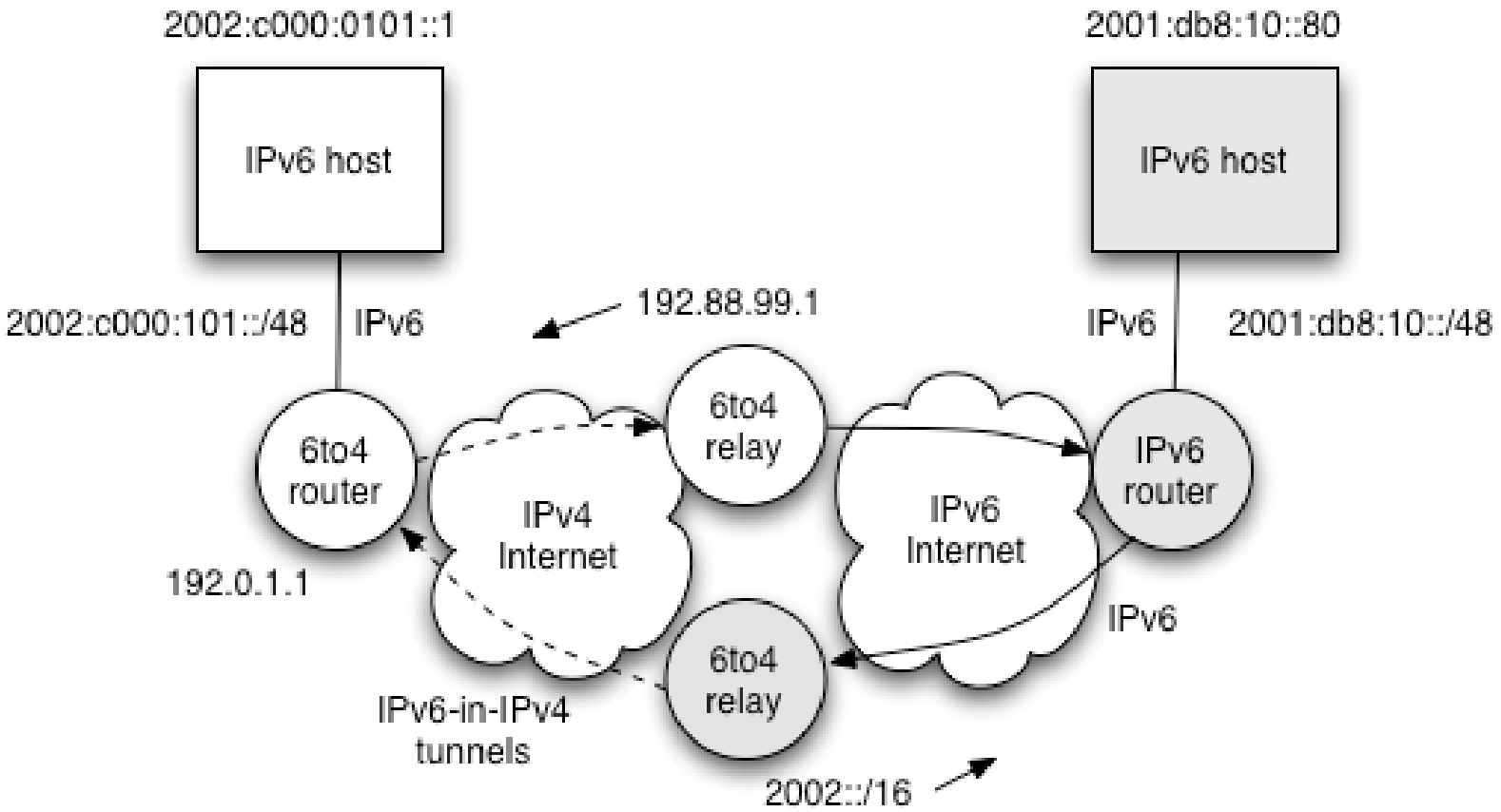
6to4 *Relay* - Exemplo



6to4 - Aspectos

- 6to4 é um mecanismo de transição interessante
  - Embora possua alguns detalhes operacionais menos positivos
- Problema 1: Possibilidade de abuso do *relay*
  - Pode ser usado num ataque DoS
  - Os endereços IPv6 que atravessam os túneis automáticos podem ser falsificados (*spoofed*)
- Problema 2: Modelo assimétrico/robustez
  - Um *«site»* 6to4 pode usar um *relay* 6to4 diferente de cada vez que comunica com um destino na Internet IPv6 (isso depende apenas do estado das rotas IPv6 e IPv4).
  - Alguns *relays* 6to4 podem ficar inatingíveis caso os ISPs filtrem a informação de *routing* como forma de apenas os seus clientes poderem alcançar o *relay* 6to4 que disponibilizam

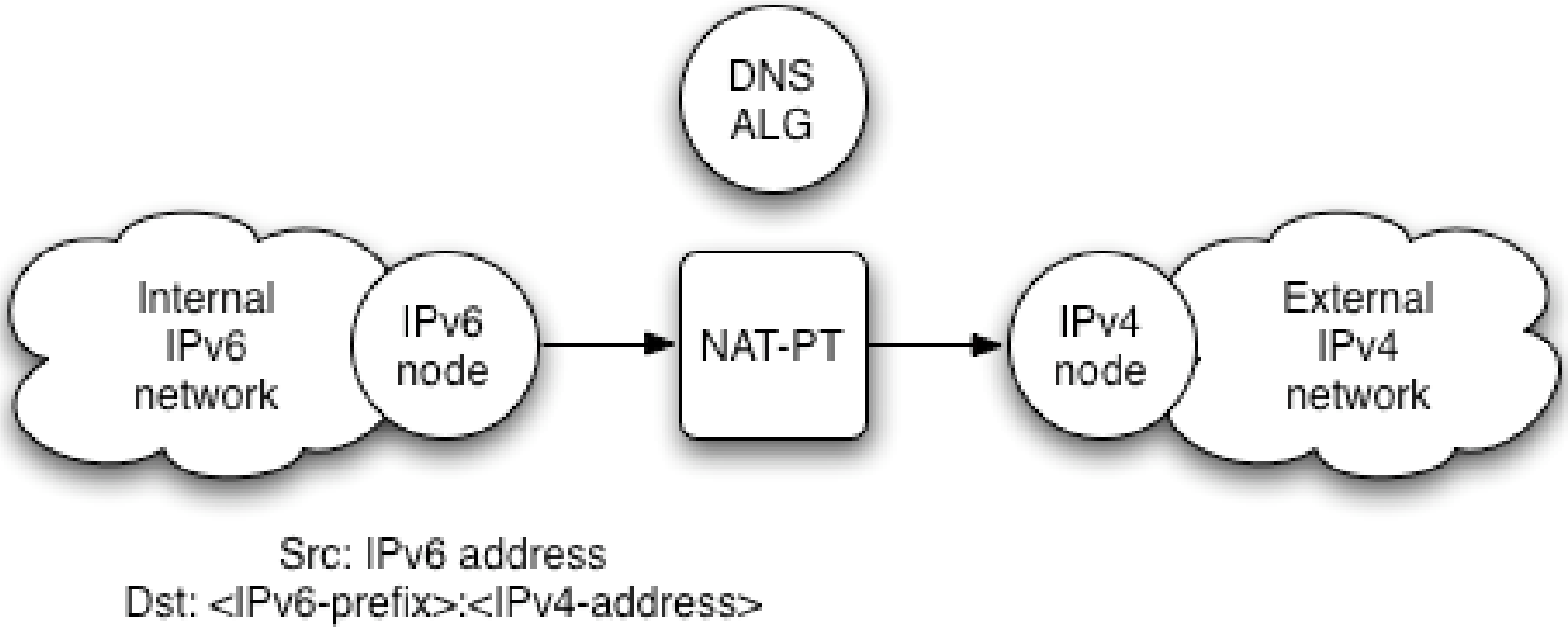
6to4 – Encaminhamento Assimétrico



Network layer: NAT-PT

- *Network Address Translation - Protocol Translation*
  - Definido no RFC2766, Descontinuado no RFC4966
  - Similar ao NAT do IPv4, mas com tradução de protocolo
- Usa o protocolo SIIT (RFC2765)
  - O SIIT define algoritmos para traduzir os cabeçalhos de pacotes IPv4 e IPv6, quando possível
- O NAT-PT adiciona ao SIIT gamas de endereços IPv4
  - Traduções IPv4-para-IPv6 e IPv6-para-IPv4 são suportadas

NAT-PT: Topologia



NAT-PT e DNS

- O protocolo *DNS ALG* traduz *queries* DNS de registos IPv6 (AAAA), para *queries* DNS de registos IPv4 (A).
- Quando a resposta com o registo (A) é recebida, o DNS ALG traduz o resultado para um endereço IPv6
  - Guardando o tuplo <IPv6-prefix>:<IPv4 address>
- O sistema cliente vai usar o endereço IPv6 para contactar o destino, que será traduzido pelo mecanismo de NAT-PT para o destino «real» em IPv4

NAT-PT: Aspectos Negativos

- Todas as desvantagens do NAT em IPv4, e um pouco mais:
  - Necessita de manter os estados nos equipamentos que suportam o NAT-PT
  - Necessita de lidar com os endereços IP embebidos no *payload* do pacote (ex: FTP)
  - Os aspectos relacionados com o DNS são complexos
- A principal dificuldade é não ser escalável para ambientes de média/grande dimensão

Dual Stack

- Suporte para IPv4 e IPv6 em todos os nós
- Necessita suporte em:
  - Hosts
  - Routers
  - Aplicações e serviços
- Ter em consideração que:
  - Devem securizar-se ambos os protocolos

Dual Stack

- As aplicações podem escolher o protocolo a usar
  - A resposta do pedido DNS retorna endereço IPv4 e IPv6
  - Não registar o AAAA no DNS para uma máquina a menos que haja boa conectividade IPv6 (e com todos os serviços a funcionar em IPv4 e IPv6)
- Activar o IPv6 não deve ter impacto adverso na performance do funcionamento das aplicações sobre IPv4
- Os níveis de segurança devem ser os mesmos para IPv4 e IPv6
  - Se uma máquina corre ambos os protocolos, ambos possuir a mesma política de segurança

Conclusões

- Há um vasto conjunto de ferramentas de transição disponíveis
  - Não há uma única melhor solução
  - O plano de transição é específico para cada caso
- A melhor prática actual é ter toda a rede em dual stack
  - IPv4 + IPv6

Conclusões

- Podem ser criadas redes apenas IPv6
  - Mas há muito poucas ainda.
  - Não são acessíveis ainda por uma vasta comunidade.
  - Para testar conectividade IPv6:
    - servidor.apenasipv6.fccn.pt
- No final, tudo depende do espaço de endereçamento IPv4 disponível
  - Continua a ser necessário endereçamento IPv4 para uma transição suave

Questões ?

Obrigado !