

Recursos de transição para IPv6

Andrey Vedana Andreoli, Leandro Márcio Bertholdo,
Liane M. R. Tarouco
POP-RS / UFRGS
Rua Ramiro Barcelos, 2574 - Porto Alegre – RS

{andrey, berthold, liane}@penta.ufrgs.br,

Sumário

- Motivação
- Visão geral dos recursos de uso de IPv6
- Apresentação de alguns recursos com exemplos de uso:
 - IPv6-over-IPv4, Tunnel Broker, 6to4
 - NAT-PT e ALG
- Planejamento de atividades na Rede Tche
- Dúvidas e perguntas

Motivação

- Surgimento da tecnologia
- Visão dos benefícios acadêmicos e comerciais
 - Capacidade de endereçamento
 - Segurança fim a fim
 - Facilidades com autoconfiguração
 - QoS
 - ...
- Projeto
 - Como integrar a tecnologia com o que já existe?
 - Quais recursos serão necessários?
 - Como lidar com limitações de equipamentos de rede?
 - Quais segmentos de rede serão envolvidos em cada etapa?
 - Quais recursos de transição poderão ser utilizados?

Visão geral dos recursos de transição de IPv6

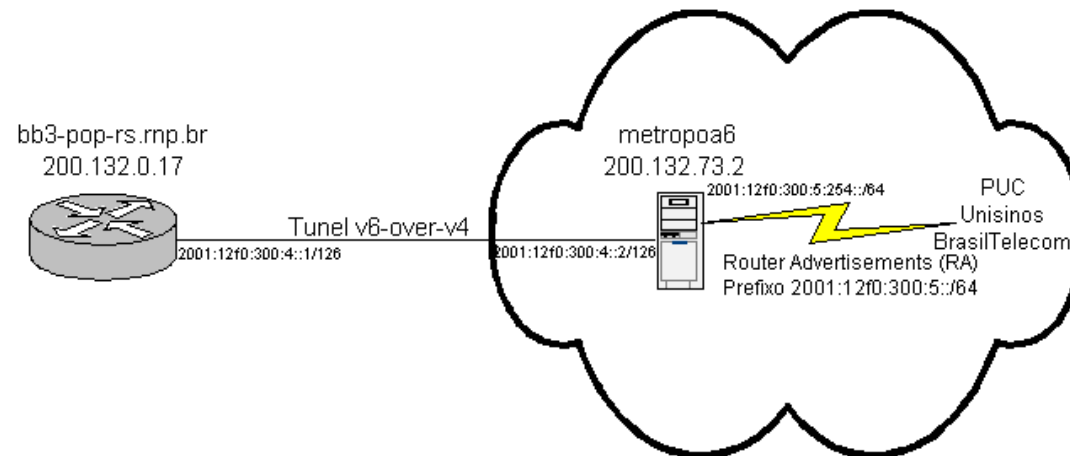
- 3 formas de uso de IPv6:
 - Nativa: Protocolos de roteamento com suporte a nativo a IPv6: RIPng, OSPFv3, MP-BGP; Equipamentos de rede com dual-stack.
 - Tunelamento: Diferentes recursos para transporte de IPv6 em redes com suporte apenas a IPv4: **IPv6-over-IPv4**, **Tunnel Broker**, **6to4**, ISATAP e Teredo; Hosts dual-stack.
 - Tradução: Grupo de recursos destinados a comunicação entre hosts IPv6-only e IPv4-only: **NAT-PT** e **ALG**

Tunelamento IPv6-over-IPv4 - Características

- Definido pela RFC 2893
- Envolve o encapsulamento de IPv6 sobre IPv4
 - Protocolo 41 (IPv6)
 - Protocolo 58 (ICMPv6)
- Deve ser feita ponto a ponto, definindo o início e final do túnel (IPv4) de forma explícita e manual.
- Podem ser utilizados com roteamento OSPFv3, exceto o IS-IS que é baseado em L2
- Necessidade de possuir bloco IPv6

Tunelamento IPv6-over-IPv4 – Estudo de caso

- Implementação de IPv6 no Rede Metropolitana (Metropoa);
 - Roteador de borda apenas com suporte a IPv4



Tunelamento IPv6-over-IPv4 – Estudo de caso

- Estrutura de um pacote IPv6-over-IPv4

```
p1: dial1.pop-rs.rnp.br -> 131.107.33.60
IP: 200.132.0.98 -> 131.107.33.60
  Status: Version = 4, IP Header Length = 20 Bytes
  Type of Service: Routine Precedence, Normal Delay, Normal Throughput, Normal Reliability, Normal Cost
  Total IP length: 80
  ID: 0xD2E9
  Fragment: Fragmentation Allowed, No Fragments Follow, Offset = 0
  Time to live: 40
  PROTOCOL: 41 = IPv6
  Header checksum: 0x520E (Good)
  IP Addresses: Source = 200.132.0.98, Destination = 131.107.33.60
    Source: 200.132.0.98
    Destination: 131.107.33.60
  IPv6: Version 6
    Flags: (01100000) Version = 6, Priority = 0
      0110....: Version = 6
      ....0000: Priority = 0
    Flow Label: 0x000000
    Payload Length: 20
    Next Header: 17 (User Datagram Protocol)
    Hop limit: 1
    Source address: 2002:C884:62:1::1
    Destination address: 2002:836B:213C:1:E0:8F08:F020:8
  UDP, [35914] -> [33435]
  UDP Data
    0000 01 01 00 00 23 58 60 41 38 76 09 00    ....#X`A8v..
```

Tunelamento IPv6-over-IPv4 - Conclusões

- Considerada uma das formas mais convencionais e seguras para roteamento de tráfego IPv6
- Não oferece escala; Outros métodos Tunnel-Broker oferecem recursos para escala devido a sua natureza
- Muito utilizado em cenários com limitações em equipamentos de rede
- Necessidade de um nível de segurança APÓS o desencapsulamento dos pacotes do túnel, visando o nível de segurança a nível de IPv6 e não como protocolos IPv4 41 e 58
- 1 hop IPv6 = n hops IPv4
- Diversas implementações tanto em equipamentos de rede, bem como sistemas operacionais UNIX.

Tunnel Broker - Características

- Definido pela RFC 3053
- Representa a automatização do processo de estabelecimento de túneis
- Uso do protocolo TSP (Tunnel Setup Protocol)
- Client acessa sistema, se autentica e recebe um script que estabelece o tunel até um determinado servidor
- Pode ser usado em apenas um host, em subredes e também em roteadores
- Pode incluir o fornecimento de bloco IPv6

Tunnel Broker– Estudo de caso

- Freenet6
 - Forma gratuita de conectividade automática através de tunel
 - Registro pelo site www.freenet6.net (Hexago)
 - Download de software para TSP client, em diversas plataformas
 - Necessita apenas de registro ao site
 - O programa faz acesso a base, autentica, obtém as informações para estabelecimento do tunel
 - Por fim, define rota default e fornece ao usuário acesso ao backbone de produção IPv6

6to4 - Características

- Definido pela RFC 3056
- Permite que hosts IPv6 (IPv6-only ou dual stack) acessem demais redes IPv6 a partir de uma mínima configuração
- Método de tunelamento implícito. Não há tunel estabelecido.
- Pode ser usado por um host apenas ou por uma rede inteira, através de seu gateway
- Faz uso do prefixo 2002::/16 para distribuição automática de endereços
- Necessita que o gateway possua endereçamento IPv4 para comunicação e definição de bloco de endereço na forma de 2002:IPV4ADDR::/48

6to4 - Características

- Exemplo de conversão automática de endereço:

IPv4 gateway: 200.132.0.99

Conversão para hexadecimal:

200: C8

132: 84

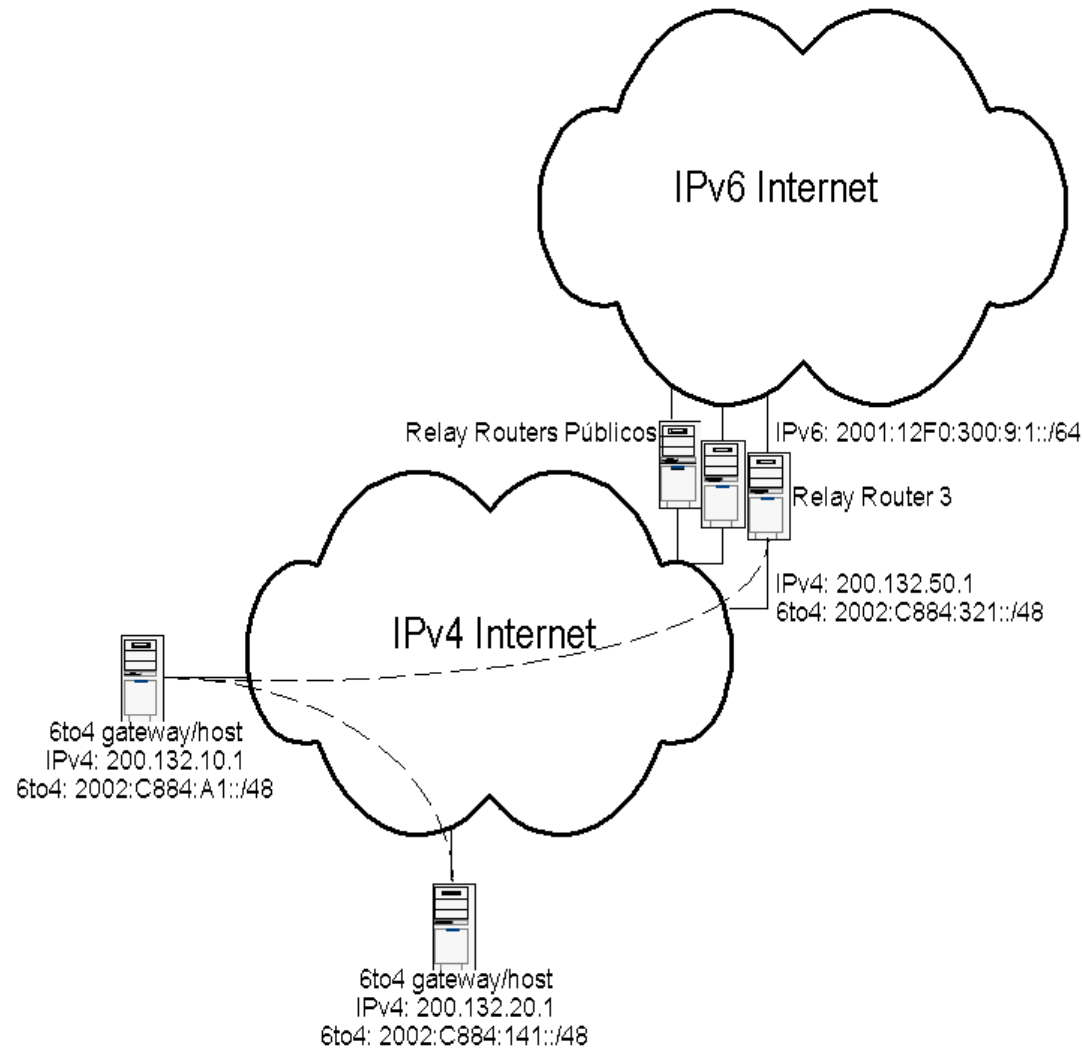
0: 0

99: 63

Bloco 6to4 para uso: 2002:C884:63::/48

6to4 - Características

- Comunica-se com demais redes 6to4 encapsulando o os pacotes IPv6 em IPv6-over-IPv4, roteando-os naturalmente sobre IPv4
- Comunica-se com o backbone mundial IPv6 de produção (2001::/16 por exemplo), através dos **relay routers**



6to4 - Características

- Relay Routers:
 - A proximidade do relay router em uso é fundamental para melhor performance do acesso.
 - Aproximadamente 12 relay routers disponíveis pelo Mundo.
 - Existência de endereço anycast: 2002:c058:6301:: (RFC 3068)
 - Cada relay router deve fazer anúncio do bloco 2002::/16
 - Não é mantido o estado de conexões; Há apenas o repasse de pacotes entre 2002::/16 e redes de produção IPv6 (2001::/16, ...)

6to4 - Características

- Alguns relay routers públicos:
 - 6to4.ipv6.microsoft.com
 - kddilab.6to4.jp
 - 6to4.ipv6.ascc.net
 - 6to4.ipv6.bt.com
 - 6to4.ipv6.fh-regensburg.de
 - asterix.ipv6.bt.com
 - 6to4.kfu.com
 - ipv6-router.cisco.com (sob registro)
- Relay router em testes no POP-RS. Aguardando liberação da RNP para divulgação internacional em caráter experimental.

6to4 - Características

- Caso Windows XP

Comando: ipv6 install

Caso não haja Router Advertisement (RA) na rede, será utilizado o endereçamento 6to4 automaticamente:

Exemplo de endereçamento da interface:

Adaptador de túnel 6to4 Tunneling Pseudo-Interface:

Sufixo DNS específico de conexão . :

Endereço IP : 2002:c884:4974::c884:4974

Gateway padrão. : 2002:836b:213c:1:e0:8f08:f020:8 / 2002:c058:6301::c058:6301

Exemplo de traceroute:

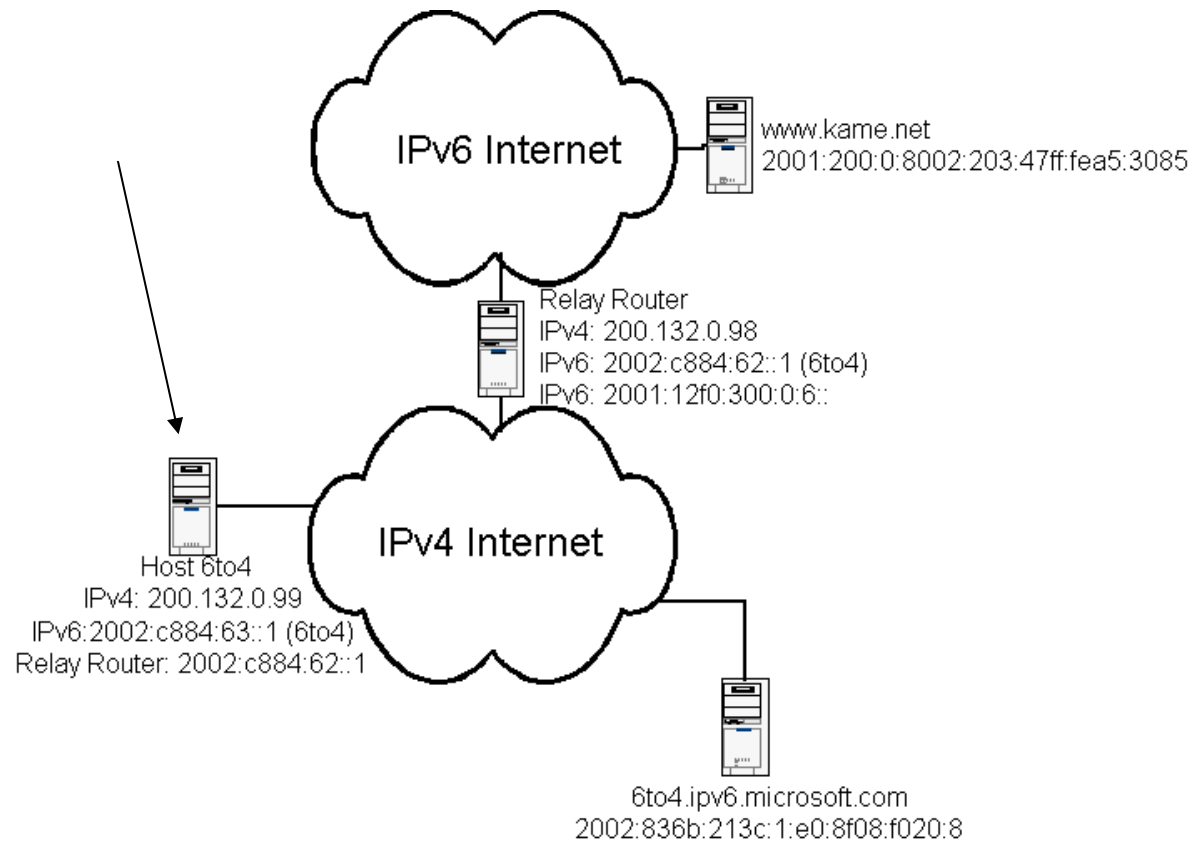
Rota de rastreamento para 6bone.net [3ffe:b00:c18:1::10]

de 2002:c884:4974::c884:4974 acima de um máximo de 30 saltos:

```
 1  226 ms  226 ms  225 ms  2002:836b:213c:1:e0:8f08:f020:8
 2  300 ms  301 ms  301 ms  sl-bb1v6-sea-t-1.sprintv6.net [3ffe:2900:1010:1::1]
 3  300 ms  300 ms  300 ms  sl-bb1v6-rly-t-1004.sprintv6.net [2001:440:1239:1009::2]
 4  334 ms  332 ms  332 ms  rap.ipv6.viagenie.qc.ca [3ffe:b00:c18:1:290:27ff:fe17:fc0f]
 5  335 ms  334 ms  333 ms  www.6bone.net [3ffe:b00:c18:1::10]
```

Rastreamento concluído.

6to4- Estudo de caso



Caso A

Acesso a www.kame.net
(IPv6 de produção)

Caso B

Acesso a site 6to4
6to4.ipv6.microsoft.com
(IPv6 6to4)

6to4– Estudo de caso

Caso A - Acesso a www.kame.net via Relay Router

```
# traceroute6 www.kame.net
```

```
traceroute6 to orange.kame.net (2001:200:0:8002:203:47ff:fea5:3085) from 2002:c884:63::1, 30 hops  
max, 12 byte packets
```

```
1 2002:c884:62::1 0.793 ms 0.561 ms 0.534 ms  
2 2001:12f0:300:0:202:4aff:fe64:8820 313.258 ms 285.885 ms 285.541 ms  
3 2001:12f0:1:2200::2 285.452 ms * 285.267 ms  
4 2001:12f0:1:2200::1 286.359 ms 285.891 ms 285.890 ms  
5 2001:12f0:1:2011::1 310.061 ms 310.376 ms 310.333 ms  
6 2001:450:1:1::15 363.368 ms 364.029 ms 364.029 ms  
7 2001:cc8:102:5::1 469.256 ms 471.971 ms 468.556 ms  
8 hitachi1.otemachi.wide.ad.jp 450.310 ms 449.442 ms 450.704 ms  
9 pc3.yagami.wide.ad.jp 450.009 ms 449.994 ms 450.422 ms  
10 gr2000.k2c.wide.ad.jp 451.611 ms 451.771 ms 451.829 ms  
11 orange.kame.net 479.913 ms 450.853 ms 451.830 ms
```

```
#
```

6to4– Estudo de caso

Caso B - Acesso a 6to4.ipv6.microsoft.com

```
# traceroute6 6to4.ipv6.microsoft.com
traceroute6 to 6to4.ipv6.microsoft.com (2002:836b:213c:1:e0:8f08:f020:8) from 2002:c884:63::1, 30
hops max, 12 byte packets
 1 2002:836b:213c:1:e0:8f08:f020:8 223.792 ms 223.114 ms 223.249 ms
#
```

6to4 - Conclusões

- Trata-se da forma observada mais trivial e abrangente, sem depender de suporte em equipamentos de rede
- Fornece bloco de endereçamento /48 exclusivo, permitindo que grandes redes também sejam contempladas
- Não requer nada mais do que a própria conexão via IPv4
- Não exige o uso de protocolos de roteamento adicionais
- Solução contemplada por grandes fabricantes (Microsoft)
- Fornece a nível de usuário “conectividade nativa”
- A rede por “trás” do gateway 6to4 pode ser dual stack ou IPv6-only.

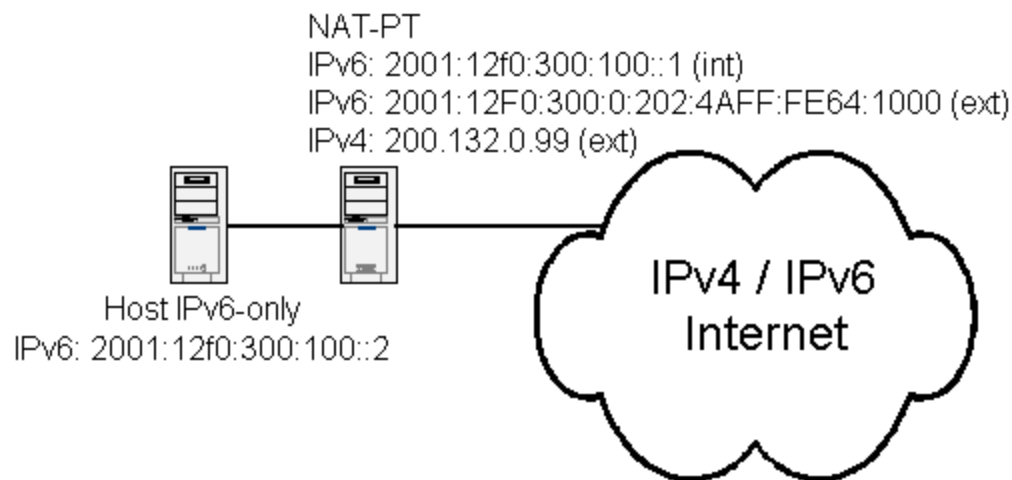
NAT-PT Características

- Definido pela RFC 2766
- Diferentemente dos anteriores, trata-se de um método de tradução (“Header Translator”)
- Atua na tradução semântica de pacotes IPv4 para IPv6 ou vice-versa
- Por consequência, pode ser usado em redes IPv4-only ou IPv6-only
- Oferece features semelhantes aos NATs IPv4, como uso de um pool de endereços de acordo com a demanda

NAT-PT Estudo de Caso

Host IPv6-only conectado ao NAT-PT

Objetivo: Fornecer conectividade IPv4



Regras do NAT-PT

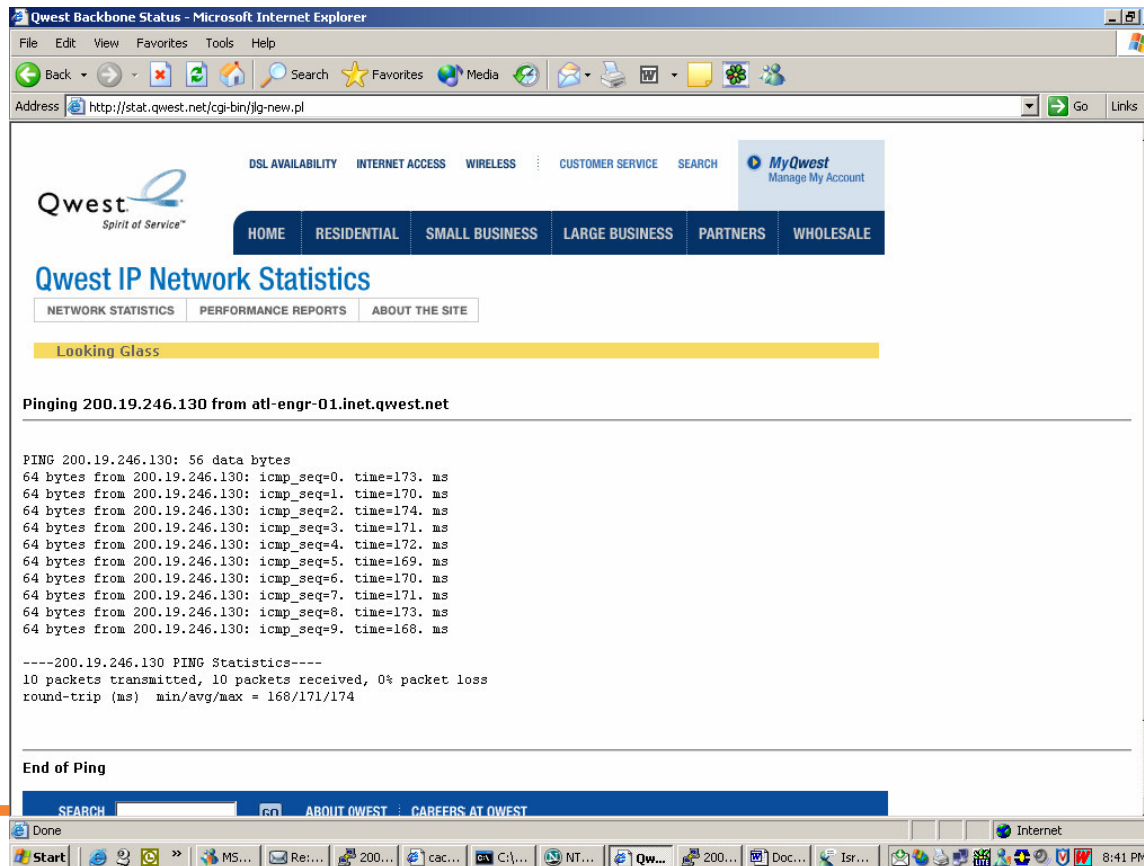
prefix 2001:12f0:300:101::
map from daddr 200.19.246.130
to daddr 2001:12f0:300:100::2

map from 2001:12f0:300:100::2
to 200.19.246.130

map enable

NAT-PT Estudo de Caso

Acesso da Internet IPv4 ao host IPv6 via NAT-PT (200.19.246.130)



Qwest Backbone Status - Microsoft Internet Explorer

Address <http://stat.qwest.net/cgi-bin/jlg-new.pl>

Qwest Spirit of Service™

DSL AVAILABILITY INTERNET ACCESS WIRELESS CUSTOMER SERVICE SEARCH MyQwest Manage My Account

HOME RESIDENTIAL SMALL BUSINESS LARGE BUSINESS PARTNERS WHOLESALE

Qwest IP Network Statistics

NETWORK STATISTICS PERFORMANCE REPORTS ABOUT THE SITE

Looking Glass

Pinging 200.19.246.130 from atl-engr-01.inet.qwest.net

```
PING 200.19.246.130: 56 data bytes
64 bytes from 200.19.246.130: icmp_seq=0. time=173. ms
64 bytes from 200.19.246.130: icmp_seq=1. time=170. ms
64 bytes from 200.19.246.130: icmp_seq=2. time=174. ms
64 bytes from 200.19.246.130: icmp_seq=3. time=171. ms
64 bytes from 200.19.246.130: icmp_seq=4. time=172. ms
64 bytes from 200.19.246.130: icmp_seq=5. time=169. ms
64 bytes from 200.19.246.130: icmp_seq=6. time=170. ms
64 bytes from 200.19.246.130: icmp_seq=7. time=171. ms
64 bytes from 200.19.246.130: icmp_seq=8. time=173. ms
64 bytes from 200.19.246.130: icmp_seq=9. time=168. ms

----200.19.246.130 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 168/171/174
```

End of Ping

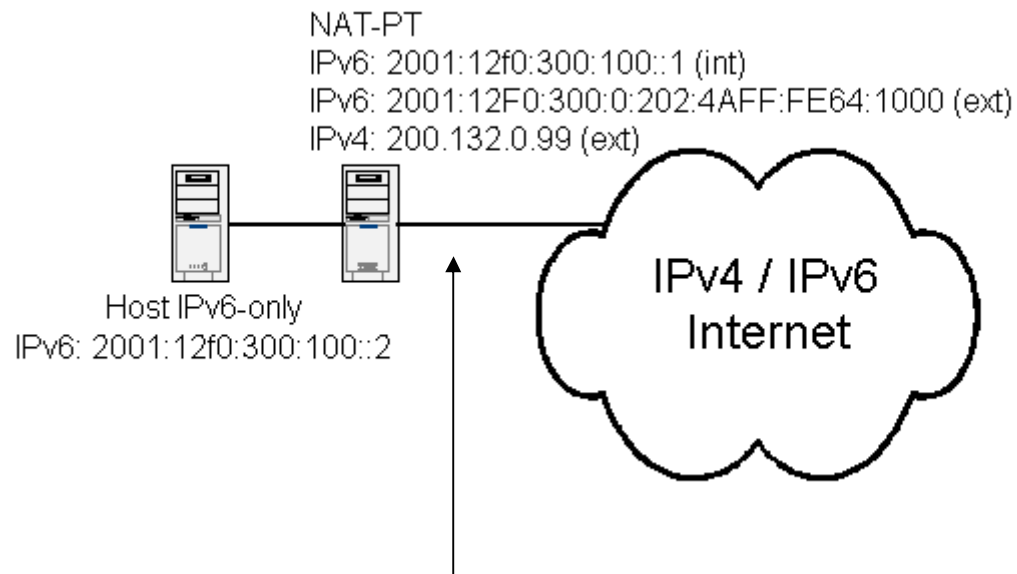
SEARCH GO ABOUT QWEST CAREERS AT QWEST

Done

Start MS... Re... 200... cac... C:\... NT... Qw... 200... Doc... Isr... 8:41 PM

NAT-PT Estudo de Caso

Ponto de Observação: antes da conversão pelo NAT-PT



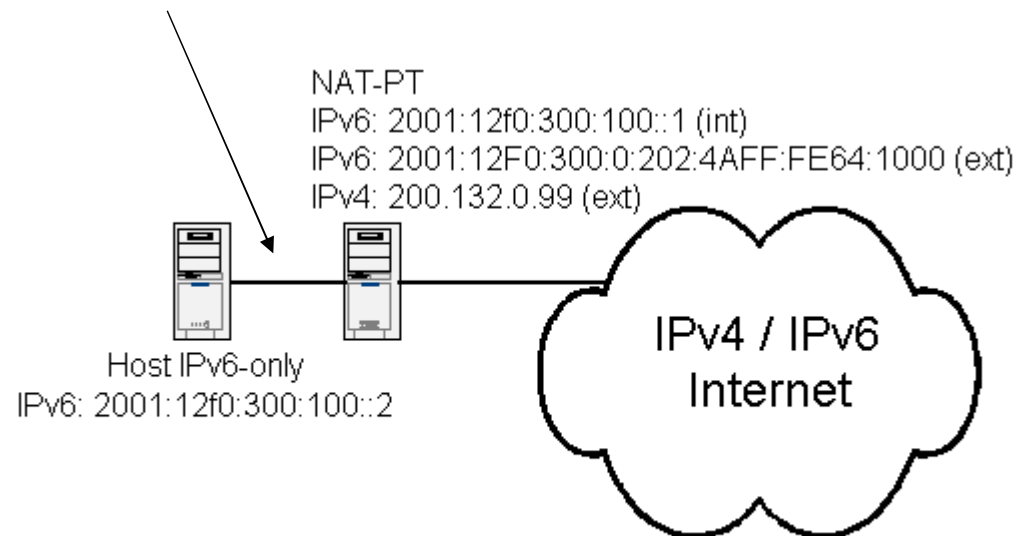
NAT-PT Estudo de Caso

Tudo tratado como IPv4...

20:39:27.524678 **205.171.21.253** > **200.19.246.130**: icmp: echo request (DF)
20:39:27.525282 200.19.246.130 > 205.171.21.253: icmp: echo reply (DF)
20:39:28.512939 205.171.21.253 > 200.19.246.130: icmp: echo request (DF)
20:39:28.513437 200.19.246.130 > 205.171.21.253: icmp: echo reply (DF)
20:39:29.517025 205.171.21.253 > 200.19.246.130: icmp: echo request (DF)
20:39:29.517539 200.19.246.130 > 205.171.21.253: icmp: echo reply (DF)
20:39:30.514663 205.171.21.253 > 200.19.246.130: icmp: echo request (DF)
20:39:30.515162 200.19.246.130 > 205.171.21.253: icmp: echo reply (DF)
20:39:31.515160 205.171.21.253 > 200.19.246.130: icmp: echo request (DF)
20:39:31.515659 200.19.246.130 > 205.171.21.253: icmp: echo reply (DF)
20:39:32.512531 205.171.21.253 > 200.19.246.130: icmp: echo request (DF)
20:39:32.513039 200.19.246.130 > 205.171.21.253: icmp: echo reply (DF)

NAT-PT Estudo de Caso

Ponto de Observação: depois do NAT-PT (rede interna V6-only)



NAT-PT Estudo de Caso

Tudo é visto como IPv6..

20:39:26.983808 **2001:12f0:300:101::cdab:15fd** > **2001:12f0:300:100::2**: icmp6: echo request
20:39:26.983974 2001:12f0:300:100::2 > 2001:12f0:300:101::cdab:15fd: icmp6: echo reply
20:39:27.971832 2001:12f0:300:101::cdab:15fd > 2001:12f0:300:100::2: icmp6: echo request
20:39:27.971969 2001:12f0:300:100::2 > 2001:12f0:300:101::cdab:15fd: icmp6: echo reply
20:39:28.975739 2001:12f0:300:101::cdab:15fd > 2001:12f0:300:100::2: icmp6: echo request
20:39:28.975882 2001:12f0:300:100::2 > 2001:12f0:300:101::cdab:15fd: icmp6: echo reply
20:39:29.973187 2001:12f0:300:101::cdab:15fd > 2001:12f0:300:100::2: icmp6: echo request
20:39:29.973327 2001:12f0:300:100::2 > 2001:12f0:300:101::cdab:15fd: icmp6: echo reply
20:39:30.973503 2001:12f0:300:101::cdab:15fd > 2001:12f0:300:100::2: icmp6: echo request
20:39:30.973645 2001:12f0:300:100::2 > 2001:12f0:300:101::cdab:15fd: icmp6: echo reply
20:39:31.970696 2001:12f0:300:101::cdab:15fd > 2001:12f0:300:100::2: icmp6: echo request
20:39:31.970836 2001:12f0:300:100::2 > 2001:12f0:300:101::cdab:15fd: icmp6: echo reply
20:39:32.971724 2001:12f0:300:101::cdab:15fd > 2001:12f0:300:100::2: icmp6: echo

NAT-PT Estudo de Caso

E no caso de acesso a um host IPv6? Acesso normal, sem conversão

```
# traceroute6 -n www.kame.net
traceroute6 to orange.kame.net (2001:200:0:8002:203:47ff:fea5:3085) from
2001:12f0:300:100::2, 30 hops max, 12 byte packets
 1 2001:12f0:300:100::1 0.634 ms 0.528 ms 0.510 ms
 2 2001:12f0:300:0:202:4aff:fe64:8820 1.578 ms 1.071 ms 0.899 ms
 3 2001:12f0:0:fd::6e 103.033 ms * 25.468 ms
 4 2001:12f0:1:2200::1 27.382 ms 25.930 ms 29.165 ms
 5 2001:468:700:1803::1 137.174 ms * 139.097 ms
 6 2001:468:ff:e47::1 155.451 ms 156.071 ms 157.774 ms
 7 2001:468:ff:e11::2 176.451 ms 187.388 ms 175.751 ms
 8 2001:468:ff:1114::2 206.782 ms 210.629 ms 211.560 ms
 9 3ffe:8140:101:1::2 310.656 ms 311.923 ms 311.322 ms
10 2001:200:0:1800::9c4:2 311.232 ms 311.326 ms 311.244 ms
11 2001:200:0:1c04::1000:2000 357.510 ms 312.551 ms 312.646 ms
12 2001:200:0:4819::2000:1 313.467 ms 312.820 ms 312.401 ms
13 2001:200:0:8002:203:47ff:fea5:3085 312.600 ms 312.542 ms 312.327 ms
```

NAT-PT Estudo de Caso

E no caso de acesso a um host IPv4? Os endereços são “mascarados” para a classe interna 2001:12f0:300:101::/64

```
# traceroute6 -n www.google.com.br
traceroute6 to www.google.akadns.net (2001:12f0:300:101::4266:968) from
2001:12f0:300:100::2, 30 hops max, 12 byte packets
 1 2001:12f0:300:100::1 0.732 ms 0.501 ms 0.451 ms
 2 2001:12f0:300:101::c884:11 1.516 ms 1.150 ms 0.997 ms
 3 2001:12f0:300:101::c88f:fd6e 25.639 ms 25.188 ms 25.043 ms
 4 2001:12f0:300:101::c88f:fd66 31.097 ms 32.059 ms 31.174 ms
 5 2001:12f0:300:101::40d7:bb1d 148.018 ms 191.924 ms 139.387 ms
 6 2001:12f0:300:101::4311:4421 181.962 ms 181.546 ms 180.553 ms
 7 2001:12f0:300:101::d033:4a0e 180.258 ms 184.150 ms 183.100 ms
 8 2001:12f0:300:101::4056:53d5 263.138 ms 261.457 ms 321.348 ms
 9 2001:12f0:300:101::426e:88e 253.782 ms 251.611 ms 257.177 ms
```

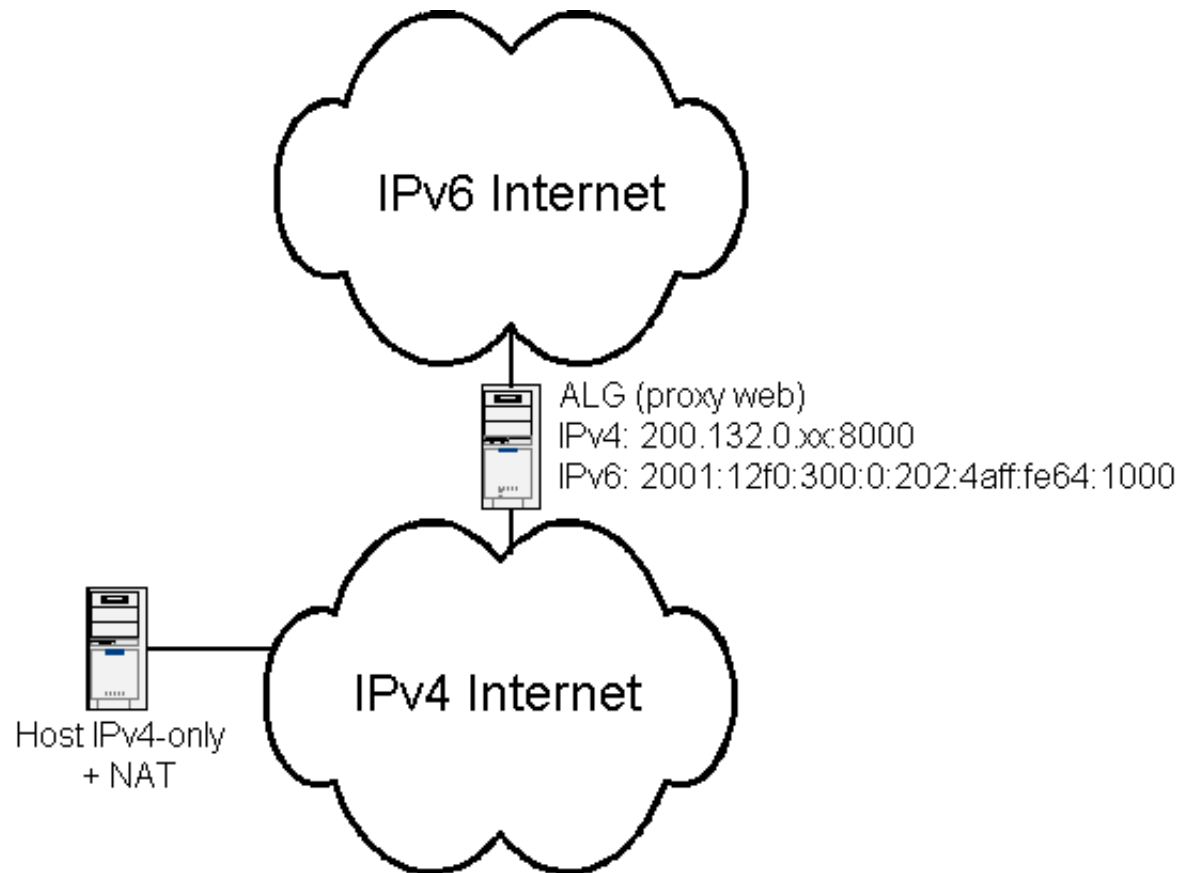
NAT-PT Conclusões

- Pode fornecer a devida transparência a hosts IPv6-only e/ou IPv4-only
- Sujeito aos mesmos problemas e limitações do NAT convencional IPv4
- “Quebra” o paradigma de segurança fim a fim do IPv6
- Introduz um ponto único de falha
- Pode ser uma forma de acessibilidade global a hosts IPv6-only
- Poderá ser usado no futuro para manter sistemas legados em IPv4

ALG Características

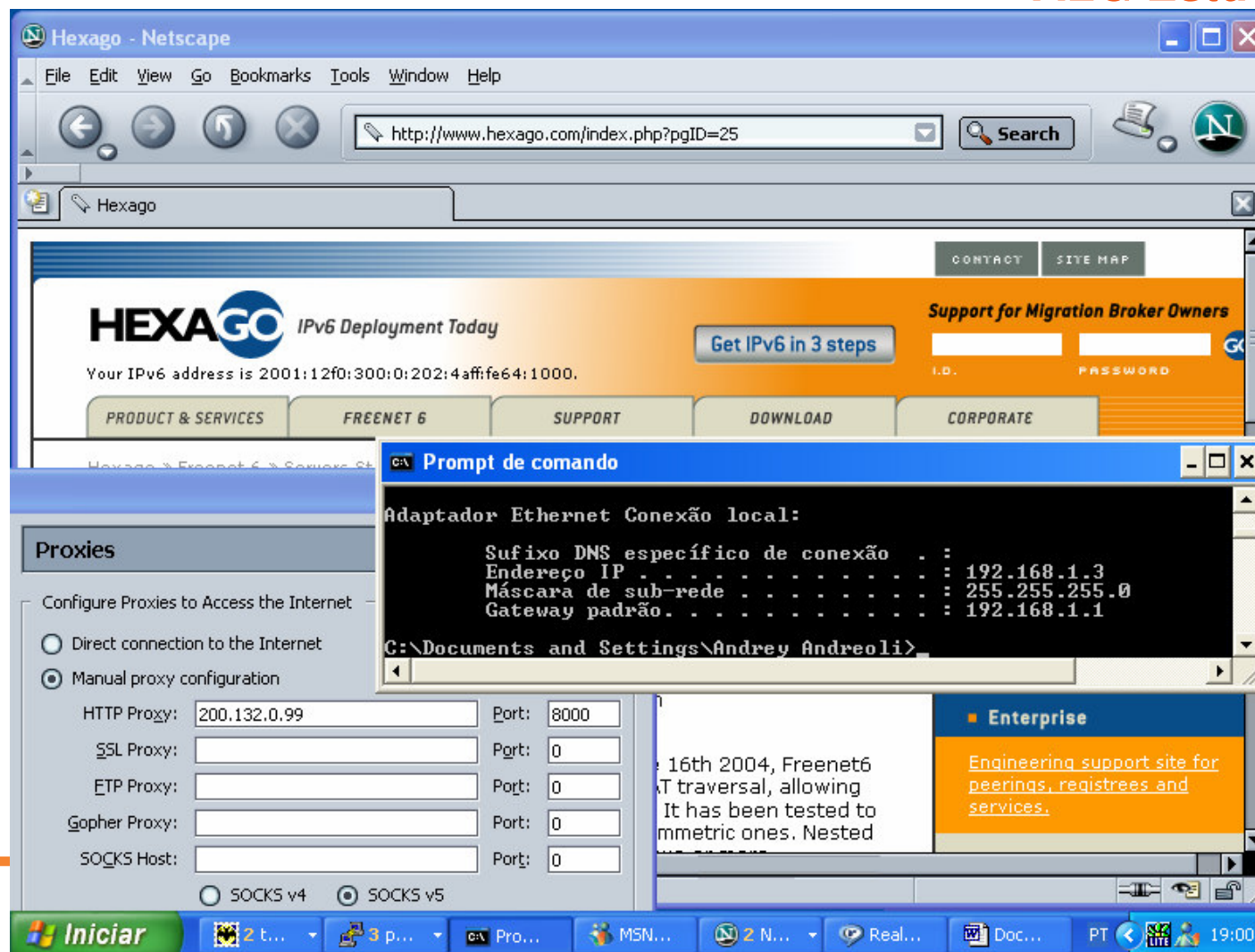
- O recurso de Application Level Gateway destina-se ao uso por usuários sem permissões de acesso através de firewalls ou NAT
- Exemplo clássico deste recurso é o HTTP Proxy
- Cenários exemplos são:
 - Rede IPv4-only sem acesso a redes IPv6
 - Redes IPv6-only sem acesso a redes IPv4
- Os clientes acessam diretamente o ALG e este, por sua vez, faz o acesso externo até o host/protocolo desejado

ALG Estudo de Caso



- Configuração de ALG para proxy web
- Acesso de um host IPv4-only a uma rede IPv6

ALG Estudo de Caso



ALG Conclusões

- Atua como um “squid dual stack”
- Sujeito a limitações pela falta de comunicação fim a fim
- Pode ser uma boa solução se a necessidade for apenas o acesso a algum serviço específico, no caso, HTTP
- Garante que sites IPv4-only acessem sites IPv4 e IPv6, e vice-versa, de forma transparente

Projetos e testes no POP-RS

- Em formação de um grupo de aproximadamente 12 instituições interessadas nos testes para transição ao IPv6 na Rede Tche
- Finalização das homologações dos métodos mais eficientes e documentação de cada método
- Métodos a serem empregados, por ordem de preferência
 - Conectividade nativa
 - Tunelamento IPv6-over-IPv4
 - 6to4

Dúvidas, questionamentos, sugestões...



Obrigado!