Implementação prática de tunelamento para transporte de pacotes IPv4 sobre redes IPv6

Leonardo Koller[1]
leonardo.koller@hotmail.com

Matheus Herbstrith de Mattos[2]
matheus.h.mattos@gmail.com

Ricardo Becker[3]
ricardo.becker@senairs.org.br

RESUMO

O protocolo IP é um protocolo roteado que faz parte da camada de rede do modelo OSI, e é responsável por fornecer um serviço de transferência de dados independente da implementação da camada de ligação lógica (enlace de dados). Devido a diversas aplicações necessitando um endereço IP único, a versão 4 do protocolo IP está no sei limite operacional. Como solução, foi desenvolvido o protocolo IP na sua versão 6, onde foi calculada a expansão da Internet para os próximos anos, tornando-o uma solução cabível para o término de endereços IPv4. A principal diferença entre ambas as versões do protocolo, nota-se o número de bits, passando de 32 na versão 4 para 128 na versão 6. Porém, a transição de uma versão para a outra não se tem mostrado de maneira rápida. Neste documento é mostrado uma das diversas maneiras para transição entre as versões do protocolo – o tunelamento, onde, é utilizado juntamente outro modelo de transição, o de pilha dupla, tendo ambas as versões do protocolo nos roteadores da rede, tendo uma ligação em túnel entre as redes IPv6 através da rede IPv4, utilizando um protocolo de roteamento já conhecido na versão 4 do IP, o RIPv2.

Palavras Chave: IPv4, IPv6, Tunelamento.

ABSTRACT

The IP is a routed protocol which is part of the network layer of the OSI model. It is responsible for providing a data transfer service independent of the implementation over logical link layer. Due to many applications requiring a single IP address, the IP protocol version 4 is close to exhaust. As a solution, the IP protocol in its version 6. The main difference between the two protocol versions, it is the number of bits, from 32 to 128. However, the transition from version four to six has not proved quickly. This document shown one of several ways to transition between versions four to six of IP protocol - tunneling. It is used along the other transition model, the dual-stack, with both protocol versions working together over the network routers.

Keywords: IPv4, IPv6, tunneling.

1,2 Faculdade de Tecnologia SENAI Porto Alegre, RS.
3 Faculdade de Tecnologia SENAI Porto Alegre, RS – Universidade de Caxias do Sul, Bento Gonçalves, RS.

1. INTRODUÇÃO

Em 3 de fevereiro de 2011 foi anunciado pela NRO (*Number Resource Organization*) a transferência dos últimos blocos disponíveis de endereços padrão IPv4. Segundo o site Nic.br "Dois blocos foram designados para o APNIC, o Registro Regional da Internet (RIR) para a Região da Ásia e Pacífico, para atender a suas necessidades imediatas. Os cinco blocos restantes serão distribuídos igualitariamente entre os 5 RIRs existentes".

Patara (2011), gerente de recursos de numeração do NIC.br, relata que é inevitável a implantação do IPv6, e necessária para garantir a continuidade do crescimento da Internet, dizendo que: "trata-se de uma questão estrutural: as empresas, provedores, governos, universidades e outras instituições com redes ligadas à Internet precisam se preparar, já que novas aplicações e dispositivos serão utilizados num futuro próximo, como veículos, câmeras de vigilância, eletrodomésticos, sensores diversos, entre outros.". A qual já tem nome "*IPv6 Day*", porém, não há data – o IPv6, o qual é descrito na RFC 2460 (DEERING, 1998).

Por outro lado, esta transição entre os dois protocolos, IPv4 e IPv6, vem se mostrando lenta, de maneira que as estatísticas retiradas do site do Google (GOOGLE, 2012), mostram que não chega a 0,5% o número de usuários utilizando o protocolo IPv6. Este número deve-se principalmente a compatibilidade do IPv6, que ao invés de 32 bits opera com 128 bits. Essa diferença na formatação do endereçamento, mais extensa e complexa, gera a necessidade de novos equipamentos com suporte específico ao IPv6.

Segundo Moreiras (2011), coordenador do projeto IPv6.br, a respeito da implantação do IPv6: "tudo depende da tecnologia utilizada pela operadora de Internet e pelo usuário. Algumas empresas podem atualizar o software do modem do usuário remotamente. Mas o equipamento pode ser muito antigo e não suportar o protocolo mais novo".

Com o passar dos anos, mais redes serão baseadas somente no protocolo IPv6, por motivos de maior abrangência de endereçamento e também por segurança. Desta maneira, espera-se que com o esgotamento dos blocos IPv4, a demanda por IPv6 comece a aumentar, o que consequentemente, torna a migração para o novo protocolo inevitável.

Tendo em vista esta necessidade pela mudança de protocolo da camanda de rede, o objetivo deste trabalho é, via um cenário esperimental, implementar a aplicação do protocolo IP versão 6 realizando o tunelamento *6to4* (IPv6 sobre IPv4), de modo a exemplificar uma

das alternativas para a transição entre os protocolos IP versão 4 e 6, onde ambas as versões consigam trabalhar ao mesmo tempo, na mesma topologia.

2. REVISÃO BIBLIOGRÁFICA

Silva Adailton (1997) destaca que, em junho de 1992, ocorria um encontro do IAB (*Internet Activities Board*) em paralelo com o congresso da *Internet Society*. Desde já, se evidenciava a necessidade de um substituto, ou uma nova versão para o IP.

Neste encontro, surgiram três propostas como solução: A do CLNP que foi chamada de TUBA (*TCP and UDP over Bigger Address*); uma de Robert Ullman, denominada inicialmente como IP versão 7, vindo em 1993 a propor uma versão chamada TP/IX, impactando mudanças tanto no IP quando no TCP; em 1994, propôs uma nova versão chamada CATNIP, como compatibilidade entre endereços IP, CLNP e IPX.

A terceira e última proposta fora chamada de "*IP in IP*". No ano de 1993, esta proposta, após modificada, tornou-se a IPAE (*IP Address Encapsulation*). O IPAE foi adotado como estratégia de transição para o SIP (*Simple IP*), proposto em 1992.

O SIP ganhou prestigio de diversos fabricantes e cientistas devido a possibilidade de aumentar o endereço IP para 64 bits, fazendo com que sua fragmentação de pacotes fosse opcional e abolia diversos aspectos obsoletos do IP.

Paul Francis propôs uma nova especificação, o Pip (*Paul's Internet Protocol*) em setembro de 1993[1]. Baseado neste, o mesmo propôs uma implementação eficiente de políticas de roteamento, facilitando a implementação e mobilidade, através de um roteamento em listas diretivas. Da união do SIP com o Pip, surgiu o SIPP (*Simple Internet Protocol Plus*)[2].

A comissão do IPng (*Internet Protocol new generation*) em junho de 1994 revisando as propostas, publicou sua recomendação em julho de 1994, indicando o SIPP como base para o novo protocolo IP. Com algumas mudanças na especificação original, o novo protocolo teria 128 bits, e se chamaria IPv6. De acordo com FORGIE (1979), o novo protocolo só não se denominou IPv5, pois o mesmo já havia sido utilizado como uma pequena modificação experimental da versão 4 do protocolo IP para trafegar voz e vídeo sobre *multicast*, comumente chamado de *Internet Stream Protocol*, ou somente ST e em

[1] O Pip é uma *Internet Draft* (IETF), descrito no sítio http://tools.ietf.org/pdf/draft-ietf-pip-architecture-01.pdf
[2] FRANCIS Paul, GOVINDAN Ramesh(1994) "Flexible Routing and Addressing for a Next Generation IP," *ACM Computer Communication Review*, vol. 24, no. 4, pp. 116-125.

seguida ST-II. O qual nunca foi introduzido para uso público, porém, muitos de seus conceitos são utilizados ainda hoje no MPLS - *Multiprotocol Label Switching*.

Cabeçalho IPv6

Segundo a Cisco (2009), a figura 1 faz uma comparação das estruturas dos cabeçalhos IP versão 4 e versão 6 simplificada. O cabeçalho IPv4 possui 20 octetos e 12 campos de cabeçalho básicos. Enquanto o cabeçalho IPv6 possui 40 octetos, três campos de cabeçalho básicos de IPv4 e cinco campos de cabeçalho adicionais.

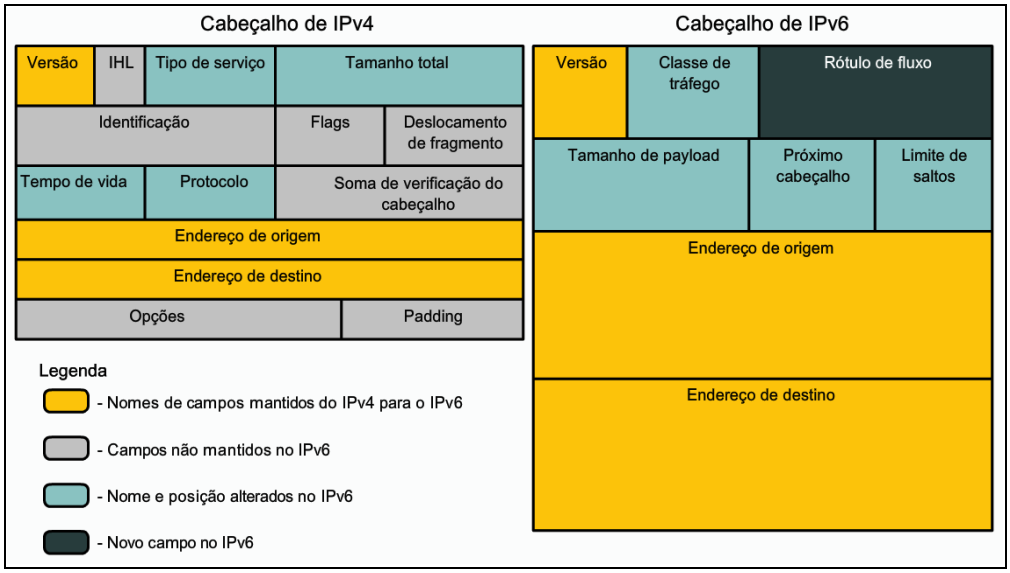

Figura 1 – Cabeçalho IPv4 e IPv6.
Fonte: CISCO, 2009.

O cabeçalho simplificado de IPv6 oferece várias vantagens com relação ao IPv4:

- Melhor eficiência de roteamento para desempenho e escalabilidade;

- Ausência de *broadcasts* e, desse modo, ausência de ameaças de *broadcast storms*;

- Sem necessidade de processar *checksums*;

- Mecanismos de cabeçalho de extensão simplificados e mais eficientes;

- Rótulos de fluxo para processamento sem a necessidade de abrir o pacote.

Endereçamento IPv6

Conforme Hinden (1998), há três tipos de endereços definidos e suas especificações: *Unicast*, *Anycast* e *Multicast*.

Unicast: Este tipo de endereço identifica uma única interface, de modo que um pacote enviado a um endereço é entregue a uma única interface, tendo suas definições;

- *Unspecified Address*: definido como 0:0:0:0:0:0:0:0 ou "::", indica a ausência de um endereço e nunca deverá ser utilizado em nenhum nó da rede. Um exemplo seria sua utilização como endereço de origem (*source address*) de estações ainda não inicializadas, ou seja, que ainda não tenham aprendido seus próprios endereços. Além disso, esse tipo de endereço não deve ser utilizado como destino ou em cabeçalho de pacotes IPv6;

- *Loopback Address*: representado por 0:0:0:0:0:0:0:1 ou "::1". Pode ser utilizado apenas quando um nó envia um datagrama para si mesmo da mesma forma que ocorre no IPv4. Não pode ser associado a nenhuma interface física, nem como endereço fonte, nem como endereço destino, mas pode ser imaginado como sendo de uma interface virtual (*loopback*). Não deve ser utilizado em endereço fonte de pacotes enviados. Um pacote IPv6 com endereço destino de *loopback* também não deve deixar o nó;

- *Embedded IPv4 Addresses*: trata-se de um endereço IPv6 com um IPv4 embutido, também denominado *IPv4-compatible IPv6 Address*. É formado anexando-se um prefixo nulo (96 bits zeros) a um endereço IPv4 como, por exemplo, ::172.16.25.32. Este tipo de endereço foi incluído como mecanismo de transição para hosts e roteadores "tunelarem" pacotes IPv6 sobre roteamento IPv4. Para *hosts* sem suporte a IPv6, foi definido um outro tipo de endereço (*IPv4-mapped IPv6 Address*) da seguinte forma: ::FFFF:172.16.25.32.

- *NSAP Addresses*: endereço de 121 bits identificado pelo prefixo 0000001, definido pela RFC 1888 - OSI NSAPs and IPv6 como mecanismo de suporte para endereçamento OSI NSAP (*Network Service Access Point*) em redes IPv6;

- *IPX Address*: endereço de 121 bits identificado pelo prefixo 0000010, incluído para prover mecanismo de mapeamento de endereços IPX em endereços IPv6. Os endereços IPX (*Internal Packet eXchange*) são utilizados em redes Netware;

- *Local-Use IPv6 Address*: há dois endereços para uso local: link-local e site-local:

- *Link-local*: endereço identificado por um prefixo de 10 bits (1111111010 em binário ou pelo prefixo FEC0::/10) , definido para uso interno num único enlace para funções como auto-configuração de endereços, descoberta do vizinho (*neighbor discovery*) ou quando não há roteador. Estações ainda não configuradas, ou com um endereço global unicast ou

com um site-local, poderão utilizar um endereço link-local. Os roteadores não devem repassar pacotes com endereço fonte ou destino deste tipo;

- *Site-local*: endereço identificado pelo prefixo de 10 bits (1111111011 em binário ou pelo prefixo FE80::/10), definido para uso interno numa organização que não se conectará à Internet, e não há necessidade de uso de um prefixo global. Os roteadores não devem repassar pacotes cujos endereços origem ou destino sejam endereços site-local.

Anycast: Identifica um conjunto de interfaces. Um pacote encaminhado a um endereço *anycast* é entregue a interface pertencente a este conjunto mais próxima da origem. Um endereço *anycast* é utilizado em comunicações de um para um de muitos.

- *Multicast*: Identifica um conjunto de interfaces, enviando um pacote a todas as interfaces associadas a esse endereço. Um endereço *multicast* é utilizado em comunicações de um para muitos, e utiliza o endereço FF00::/8 ou 11111111 em binário.

Diferente do IPv4, no IPv6 não existe endereço *broadcast*, responsável por direcionar um pacote para todos os nós de um mesmo domínio. No IPv6, essa função foi atribuída à tipos específicos de endereços *multicast*.

Dentro dos endereços *Multicast* já reservados, pode-se identificar alguns endereços especiais utilizados para funções específicas (URTADO E ALVES JR, 2008):

- FF01::1 – Indica todas as interfaces de escopo local;

- FF02::1 – Indica todas as interfaces de um escopo de enlace local;

- FF01::2 – Indica todos os roteadores dentro de um escopo local;

- FF02::2 – Indica todos os roteadores dentro de um escopo de enlace local;

- FF05::2 – Indica todos os roteadores dentro de um escopo site local, mesmo ID;

- FF02::1:FFxx:xxxx – Endereço especial chamado de *Solicited-Node Multicast Address*, onde xx:xxxx representam os últimos 24 bits do endereço IPv6 *Unicast* do *host*.

- *Solicited-Node Multicast Address*: Esse tipo de endereço *Multicast* especial é usado para mensagens de solicitação de vizinho que auxilia *Neighbor Discovery Protocol*. Esse é um grupo *Multicast* que corresponde a um endereço IPv6 *Unicast* em seus últimos 24 bits.

Definido por NARTEN (2007) na RFC 4861 (*Neighbor Discovery for IP version 6*), o protocolo de descoberta de vizinhança torna mais dinâmico alguns processos de configuração de rede em relação ao IPv4, combinando as funções de protocolos como ARP,

ICMP Router Discovery e ICMP Redirect, além de adicionar novos métodos não existentes na versão anterior do protocolo IP.

O protocolo de descoberta de vizinhança do IPv6 é utilizado por *hosts* e roteadores para determinar o endereço MAC dos nós da rede, encontrar roteadores visinhos, determinar prefixos da rede, detectar endereços duplicados, determinar a acessibilidades dos roteadores, redirecionamento de pacotes e autoconfiguração de endereços.

Tabela de Roteamento IPv6

No IPv6, de acordo com NIC.br, as entradas da tabela de roteamento são:

- Um prefixo de endereço;

- A interface em que os pacotes correspondem ao prefixo de endereço são enviados;

- Um endereço de encaminhamento ou de próximo salto;

- Um valor usado para fazer a seleção entre várias rotas com o mesmo prefixo;

- A vida útil da rota;

- A especificação que informa se a rota é publicada ou não;

- A especificação que informa como a rota expirará;

- O tipo de rota.

O processo de escolha das rotas é idêntico em IPv4 e IPv6, porém, as tabelas RIB (*Routing Information Base*) são independentes, tendo uma para o IPv4 e outra IPv6.

Através de mecanismos de otimização as melhores rotas são adicionadas à tabela de encaminhamento. A FIB (*Forwarding Information Base*) é criada a partir da RIB, e, assim como a RIB, a FIB também é duplicada.

RIPng

O protocolo de roteamento RIPv2 do IPv4 foi adaptado ao IPv6, e é chamado de RIPng (*Routing Information Protocol next generation*), como descrito por MALKIN (1997) na RFC 2080. Protocolo de roteamento baseada no número de saltos, tendo preferência a rota com menor número de saltos. Utiliza o endereço *multcast* FF02::9 (*All RIP Routers*) como

destino nas mensagens de atualização de tabela de roteamento. Em um ambiente onde há IPv4 e IPv6 necessita-se utilizar RIPv2 (IPv4) e RIPng (IPv6).

As principais limitações do RIPng são o diâmetro máximo da rede que chega a 15 saltos, a utilização apenas dos saltos como fator determinante ao melhor caminho, havendo ainda a chance de *loops* de roteamento e contagem até o infinito.

As atualizações nas tabelas de rotas são feitas das seguintes maneiras:

- Envio automático a cada 30 segundos – independente de mudanças ou não;

- Quando detecta mudanças na topologia de rede;

- Quando recebe uma mensagem do tipo *Request*.

OSPFv3

Outro protocolo de roteamento que recebeu uma nova versão para ser compatível com o IPv6 foi o OSPF. Descrito por COLTUN (2008) na RFC 5340, nomeado OSPFv3 (*Open Shortest Path First version 3*). Também, assim como o RIPng, é um protocolo IGP (*Interior Gateway Protocol*) do tipo *link-state*. Baseando-se no OSPFv2, o OSPFv3 também agrupa roteadores em áreas.

Seus roteadores descrevem seu estado atual enviando diversos LSA´s (*Link-State Advertisement*). Utiliza o algoritmo de caminho mínimo de Dijkstra, onde o custo de uma interface costuma ser inversamente proporcional à largura de banda da mesma. Em um ambiente onde há IPv4 e IPv6, necessita-se utilizar OSPFv2 (IPv4) e OSPFv3 (IPv6).

As principais semelhanças entre OSPFv2 e OSPFv3 são:

- Tipos básicos de pacotes: *Hello*, DBD, LSR, LSU, LSA;

- Mecanismos para descoberta de vizinhos e formação adjacências;

- Tipos de interfaces;

- A lista de estados e eventos das interfaces;

- O algoritmo de escolha do *Designated Router* e do *Backup Designated Router*;

As principais diferenças entre OSPFv2 e OSPFv3 são:

- OSPFv3 roda por enlace e não mais por sub-rede;

- Foram removidas as informações de endereçamento;

- Adição de escopo para *flooding*;

- Suporte explícito a múltiplas instâncias por enlace;

- Uso de endereços link-local;

- Identificação de vizinhos pelo *Router ID*;.

- Utiliza endereços *multicast*: ALLSPFRouters FF02::5 e AllDRouters FF02::6.

DHCPv6

O DHCPv6 (*Dynamic Host Configuration Protocol for IPv6*) foi padronizado pela IETF através da RFC 3315. Segundo BOUND (2003), o DHCPv6 permite que os servidores DHCP passem parâmetros de configuração, como endereços de rede IPv6 para nós IPv6. Ele oferece a capacidade de alocação automática de endereços de rede reutilizáveis e flexibilidade de configuração adicional. O conceito básico do DHCPv6 cliente-servidor é similar ao DHCPv4. Se um cliente quer receber parâmetros de configuração, ele irá enviar uma requisição para detectar servidores DHCPv6 disponíveis. Isto é feito através das mensagens de "*Solicit*" e "*Advertise*". Endereços *multicast* DHCPv6 são utilizados para este processo. Em seguida, o cliente DHCPv6 utilizará o "*Request*" para solicitar parâmetros de configuração de um servidor disponível, o qual, irá responder com mensagem de "*Reply*".

O cliente DHCPv6 saberá quando quer usar DHCPv6, sendo baseado ou nas instruções do roteador anexo, ou quando nenhum *gateway* padrão estiver presente.

Novas mensagens no DHCPv6:

- *CONFIRM (4)* - Um cliente manda uma mensagem de confirmação para qualquer servidor disponível para determinar se o endereço atribuído ainda é adequado para o cliente.

- *RELAY-FORW (12)* - Um agente de retransmissão envia uma mensagem "*Relay-forward*" para retransmitir mensagens aos *servers*.

- *RELAY-REPLY (13)* - Um servidor DHCPv6 envia uma mensagem "*Relay-reply*" para um agente retransmissor contendo uma mensagem que a mesma foi entregue ao cliente.

Endereços *multicast* comumente utilizados com DHCPv6 são:

• "ff02:::1:2" (todos agentes de retransmissão e servidores DHCPv6)

• “ff05::1:3” (todos servidores DHCPv6)

Portas utilizadas pelo DHCPv6:

• Clientes utilizam a porta UDP 546 para receber mensagens;

• Servidores e agentes utilizam a porta UDP 54 para receber mensagens DHCP.

NAT-PT

O NAT-PT (*Network Address Translation – Protocol Translation*), RFC 2766, segundo Lapukhov Petr (2008), é utilizado em cenários de migração e seu propósito é oferecer a conectividade bi-direcional entre domínios IPv4 e IPv6. A Cisco (2008) apontou que muitas outras técnicas de transição são possíveis, e que o NAT-PT não deve ser utilizado quando outras, opções “nativas” existirem, como ter *hosts* pilha dupla comunicando-se diretamente através de roteadores pilha dupla. Outro exemplo de quando o NAT-PT não se faz necessário, é quando duas “ilhas” IPv6 querem se comunicar através de um *backbone* IPv4, pois sabe-se, que há diferentes tipos de túneis existentes para esse propósito.

Para trabalhar com o NAT-PT, um roteador pilha dupla com interfaces em ambas as redes, IPv4 e IPv6, é capaz de realizar esta tarefa. A diferença para o clássico IPv4 NAT é que a tradução deve ser realizada nos dois caminhos: pacotes IPv6 roteados para hosts IPv4 devem ter suas origem/destino alterados para um endereço IPv4 equivalente e vice versa, enquanto pacotes IPv4 enviados para hosts IPv6 devem ter ambos endereços de origem e destino substituídos para endereços IPv6.

Pode-se programar de forma manual o roteador para reescrever endereços de destino em pacotes IPv6 enviados para endereços IPv6, por exemplo 2000::960B:0202, que de maneira decimal é descrito como 150.11.2.2. Para traduzir o endereço de origem, por exemplo o endereço 3001:11:0:1::1, pode-se definir outro mapeamento que diz ao roteador para reescrever pacotes IPv4 (direção oposta) enviados para 150.11.1.1 para o endereço 3001:11:0:1::1. Já que o mapeamento é bi-direcional, pacotes IPv6 com o par de endereços origem/destino [3001:11:0:1::1,2000::960B:0202] obteriam pacotes IPv4 reescritos com o par de endereços [150.11.1.1, 150.11.2.2] e vice-versa – um pacote IPv4 origem/destino [150.11.2.2, 150.11.1.1] seria reescrito para [2000::960B:0202, 3001:11:0:1::1].

A figura 2 exemplifica o cenário de NAT-PT ligando diferentes redes (IPv4 e IPv6), de maneira que o roteador R3 seria responsável por esta tradução, onde endereços IPv4 poderiam se conectar aos endereços IPv6 (R2 para R1) e ao contrário, de R1 para R2.

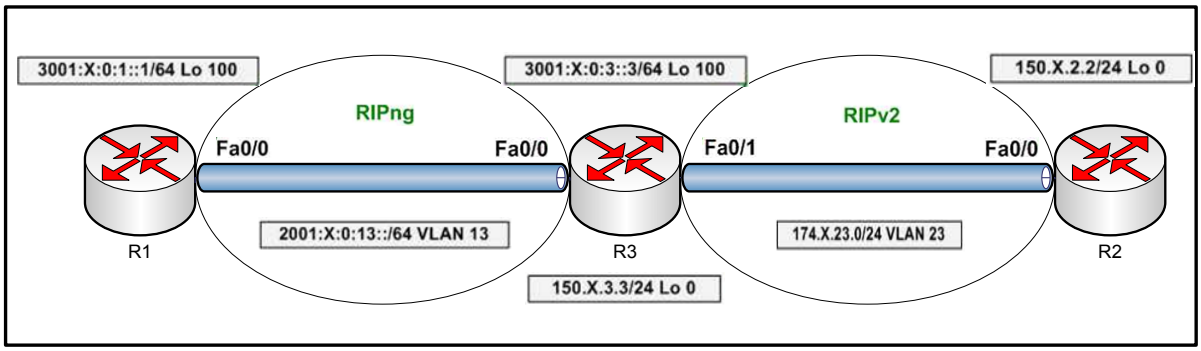

Figura 2 - NAT-PT.
Fonte – adaptado de LAPUKHOV, 2011.

DNS – *Domain Name System*

De acordo com THOMSON, HUITEMA, KSINANT e SOUISSI (2003) na RFC 3596, a resolução de nomes DNS para usuários IPv6 é dada de maneira similar a IPv4. Existem algumas mudanças, dentre as mesmas:

- Tanto endereços IPv4 como IPv6 estão presentes no mesmo sistema DNS e podem até mesmo estarem em um mesmo domínio;

- Diferente dos endereços IPv4, que são armazenados em registros "A", os endereços IPv6 são armazenados em registros "AAAA", conforme THOMSON (1995), desta maneira, uma consulta deve-se ser específica entre um ou outro registro – "A" IPv4 e "AAAA" IPv6;

- Um mesmo nome de máquina pode ser sobrecarregado com registros "A" e "AAAA", portanto uma máquina pode ter o mesmo nome DNS tanto em IPv4 como em IPv6.

- Endereços reversos são ambos armazenados em registros PTR. A distinção é feita pela raiz das árvores de endereçamento reverso: "in-addr.arpa.net" para IPv4 e "ip6.int" para IPv6. Com raízes diferentes, não há confusão entre as versões do IP. Naturalmente cada consulta PTR deve especificar ou uma ou outra versão.

- Juntamente com o registro "AAAA", existe também o registro A6, proposto por CRAWFORD e HUITEMA (2000). No registro A6, consta o sufixo do endereço IPv6, o tamanho do prefixo em bits, e um "nome" correspondente ao prefixo. Esse "nome" é outro registro DNS "AAAA" ou "A6", que deve ser recursivamente consultado, até que seja

possível montar o endereço IPv6 completo, encontrando um registro “AAAA”. O prefixo de rede sendo representado por um “nome” torna mais fácil a criação e atualização dos registros DNS, tornando-os até mesmo mais claros. De forma atender clientes de legado que não suportem ainda registros “A6”, BUSH (2002) sugere que o servidor DNS possa responder consultas “AAAA” interpretando os registros “A6” de forma transparente.

- O DNS dinâmico, diferente do IPv4, deve ser adotado em IPv6, já que os endereços de 128 bits são difíceis de memorizar e eventualmente baseados na placa de rede;

- Tendo em vista que cada usuário da Internet poderá ter uma faixa de endereços IPv6 gigantesca para si, será muito mais para pequenos domínios manterem seu próprio servidor DNS. Juntamente, o velho problema da delegação do DNS reverso fica automaticamente sanado.

Algo importante de ser levado em conta é que o BIND, servidor DNS para UNIX, suporta tanto IPv4 quanto IPv6 na sua versão 9. Assim uma instalação com este servidor DNS tem suporte a IPv6 sem qualquer modificação em *hardware* e/ou *software*.

Em sua página o Google retrata como é feito o Google sob IPv6, dizendo que utiliza-se de seu DNS IPv4 para determinar quando uma rede é capaz de interpretar IPv6. Sendo apto, o usuário recebe um registro “AAAA” para habilitar os serviços do Google em IPv6. A figura 3 ilustra esse provesso descrito.

Mecanismos de transição

Nesta fase inicial de implementação do IPv6, ainda não é aconselhável ter nós com suporte apenas a esta versão do protocolo IP, visto que muitos serviços e dispositivos de rede ainda trabalham somente sobre IPv4. Visto isso, uma possibilidade de transição é a pilha dupla. O empilhamento duplo é um método de integração no qual um nó possui implementação e conectividade a uma rede IPv4 e a uma rede IPv6, e envolve a execução de IPv4 e IPv6 ao mesmo tempo. Cada nó IPv6/IPv4 é configurado com ambos os endereços, utilizando mecanismos IPv4, por exemplo o DHCP, para adquirir seu endereço IPv4, e mecanismos do protocolo IPv6, por exemplo o DHCPv6, para adquirir seu endereço IPv6.

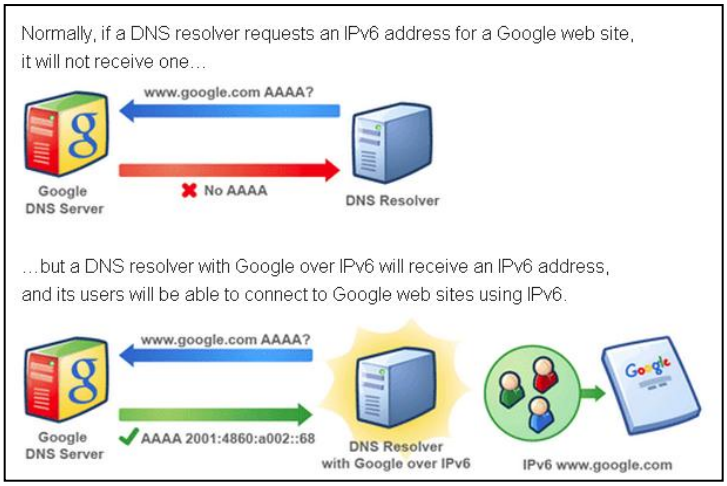

Figura 3 - *How it works DNS Google.*
Fonte – GOOGLE, 2011

Este método de transição pode facilitar o gerenciamento da implantação do IPv6, por permitir que este seja feito de forma gradual, configurando pequenas seções do ambiente de rede de cada vez. Além disso, caso no futuro o IPv4 não seja mais usado, basta simplesmente desabilitar a pilha IPv4 de cada nó.

Em relação ao DNS, é preciso que este esteja habilitado para resolver nomes e endereços de ambos os protocolos. No caso do IPv6, é preciso responder a consultas de registros do tipo AAAA (quad-A), que armazenam endereços no formato do IPv6, e para o domínio criado para a resolução de reverso, o ip6.arpa.

Em uma rede IPv6/IPv4, a configuração do roteamento IPv6 normalmente é independente da configuração do roteamento IPv4. Isto implica no fato de que, se a rede antes de ser implementada a pilha dupla utilizava apenas o protocolo de roteamento interno OSPFv2, com suporte apenas ao IPv4, será necessário migrar para um protocolo de roteamento que suporte tanto IPv6 quanto IPv4, como IS-IS por exemplo, ou forçar a execução de um IS-IS ou OSPFv3 paralelamente com o OSPFv2.

A segunda técnica de transição mais importante é o tunelamento. A técnica de criação de túneis, ou tunelamento, permite transmitir pacotes IPv6 através da infra-estrutura IPv4 já existente, sem a necessidade de realizar qualquer mudança nos mecanismos de roteamento, encapsulando o conteúdo do pacote IPv6 em um pacote IPv4.

Existem várias técnicas de tunelamento disponíveis, incluindo:

- Tunelamento manual de IPv6 sobre IPv4 - Um pacote de IPv6 é encapsulado dentro do protocolo IPv4. Esse método exige roteadores de pilha dupla.

- Tunelamento dinâmico *6to4*, de acordo com CARPENTER e MOORE (2001) na RFC 3056, estabelece a conexão das ilhas de IPv6 automaticamente através de uma rede IPv4, normalmente a Internet. Ele aplica automaticamente um prefixo de IPv6 válido e exclusivo a cada ilha de IPv6, permitindo a rápida implantação do IPv6 em uma rede corporativa sem que ocorra a recuperação de endereço dos ISPs ou dos registros.

- Protocolo de endereçamento automático de túnel intra-site (ISATAP, *Intra-Site Automatic Tunnel Addressing Protocol*) – Mecanismo de tunelamento de sobreposição automática que usa a rede de IPv4 subjacente como uma camada de enlace para o IPv6, é tratado por TEMPLIN, GLEESON e THALER (2008) na RFC 5214. Os túneis do ISATAP permitem que os *hosts* de pilha dupla individuais de IPv4 ou IPv6 dentro de um local se comuniquem com outros *hosts* em um link virtual, criando uma rede de IPv6 que utiliza a infraestrutura de IPv4.

- Tunelamento Teredo - Uma tecnologia de transição de IPv6 que fornece o tunelamento automático de *host* para *host* em vez de um tunelamento de *gateway*, é descrito na RFC 4380(2006). Essa abordagem transmite o tráfego *unicast* de IPv6 quando os *hosts* de pilha dupla (*hosts* que executam tanto o IPv6 quanto o IPv4) estão localizados atrás de um ou de vários NATs de IPv4.

Pilha dupla do IOS Cisco:

Para a CISCO (2009), “o empilhamento duplo é um método de integração que permite que um nó tenha conectividade a uma rede IPv4 e a uma rede IPv6 simultaneamente. Cada nó possui duas pilhas de protocolo com a configuração na mesma interface”.

A abordagem da pilha dupla para a integração de IPv6, na qual os nós possuem tanto as pilhas de IPv4 quanto as de IPv6, tende a ser um dos métodos de integração mais comuns já que o IPv4 não sofre alteração, adicionando-se apenas o IPv6 nas interfaces. Um nó de pilha dupla escolhe qual pilha usar com base no endereço de destino do pacote como visto na figura 4, lembrando-se que o mesmo deve preferir o IPv6 quando ele estiver disponível. Os aplicativos antigos exclusivos de IPv4 continuam funcionando como antes. Os aplicativos novos e modificados tiram proveito de ambas as camadas de IP.

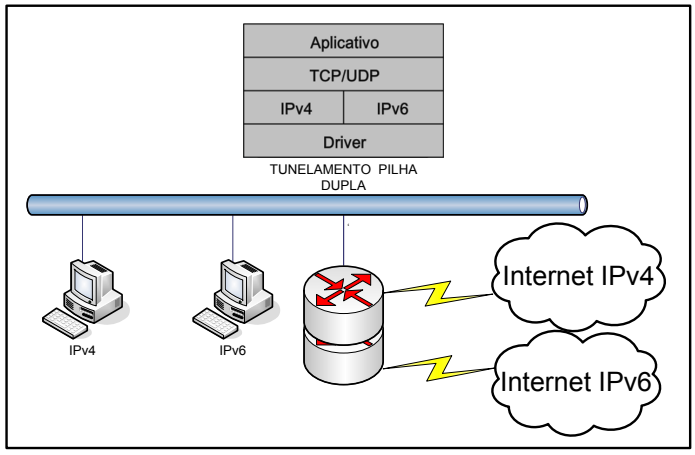

Figura 4 - Pilha dupla do IOS Cisco
Fonte – adaptado de CISCO, 2009

Uma nova interface de programação de aplicativos (API, *Application Programming Interface*) foi definida para suportar os endereços de IPv4 e de IPv6 e solicitações de DNS. Uma API facilita a troca de mensagens ou de dados entre dois ou mais aplicativos de *softwares* diferentes. A API é integrada aos aplicativos de *software* para traduzir o IPv4 em IPv6 e vice-versa, usando o mecanismo de conversão de IP.

A experiência de portar os aplicativos de IPv4 para IPv6 sugere que, para a maioria dos aplicativos, há uma alteração mínima em alguns pontos localizados dentro do código-fonte. Essa técnica é bastante conhecida e tem sido aplicada nas últimas transições de protocolo. Ela permite a adaptação gradual dos aplicativos para o IPv6.

Segundo Cisco (2009), o IOS Cisco Release 12.2(2)T e versões mais recentes são habilitados para o IPv6. Logo após a configuração do IPv4 e IPv6 na interface, a interface sofre o empilhamento duplo e encaminha o tráfego de IPv4 e de IPv6 na interface.

O uso do IPv6 em um roteador com IOS Cisco exige que se use o comando de configuração global IPv6 *unicast-routing* como visto na figura 5. Esse comando habilita o encaminhamento de datagramas de IPv6.

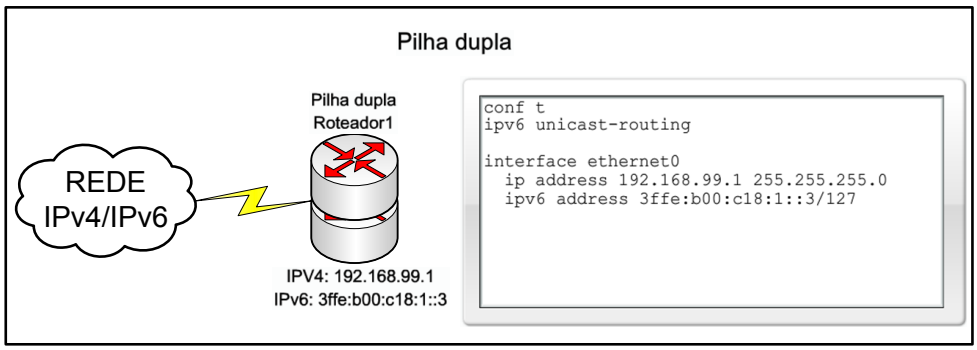

Figura 5 - Pilha dupla do IOS Cisco
Fonte – Adaptado de Cisco, 2009.

Deve-se ainda configurar todas as interfaces que encaminham o tráfego de IPv6 com um endereço de IPv6 usando o comando de interface *IPv6 addressIPv6-address [/prefix length]*.

Tunelamento de IPv6

O tunelamento é um método de integração onde um pacote de IPv6 é encapsulado dentro de outro protocolo, como o IPv4. Esse método permite a conexão das ilhas de IPv6 sem que haja a necessidade de converter as redes intermediárias para o IPv6. Quando o IPv4 for usado para encapsular o pacote de IPv6, o pacote incluirá um cabeçalho de IPv4 de 20 bytes sem opções, um cabeçalho de IPv6 e a *payload*. Ele também exige roteadores de pilha dupla como exibido na figura 6.

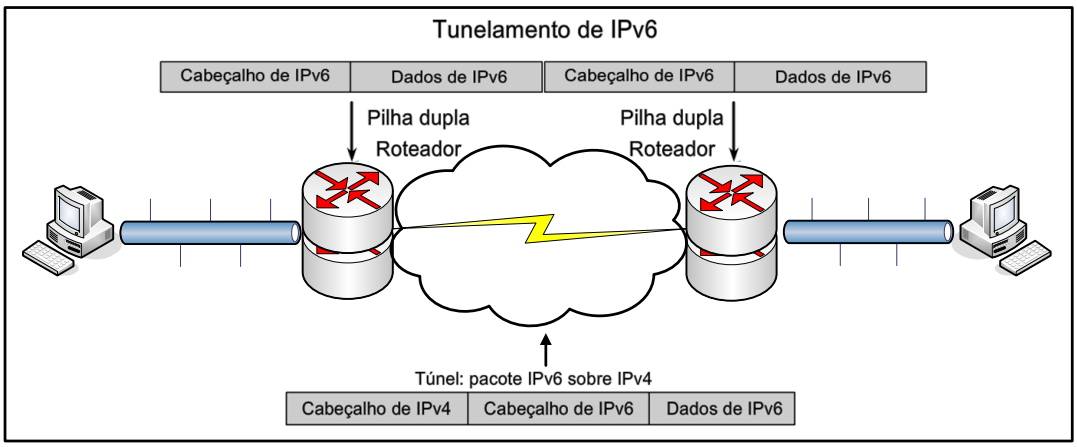

Figura 6 - Tunelamento de IPv6
Fonte – Adaptado de Cisco, 2009

O tunelamento apresenta dois problemas. Primeiramente a unidade máxima de transmissão - MTU (*Maximum Transmission Unit*) será diminuída efetivamente em 20 octetos se o cabeçalho de IPv4 não contiver nenhum campo opcional. Além disso, segundo a CISCO (2009), é mais complexo identificar e solucionar problemas de uma rede "tunelada". Sabe-se também que o tunelamento é uma técnica de integração e transição intermediária e não deve ser considerada como uma solução final.

Um túnel manualmente configurado equivale a um link permanente entre dois domínios de IPv6 sobre um *backbone* de IPv4. A utilização principal é para conexões estáveis que exigem uma comunicação regular segura entre dois roteadores de extremidade ou entre um sistema final e um roteador de extremidade, ou para a conexão com redes IPv6 remotas. Os roteadores finais devem ter passado por empilhamento duplo, e a configuração

não pode mudar dinamicamente conforme as necessidades da rede e do roteamento quando os mesmos precisarem passar por mudanças, o que limita este tipo de configuração.

Os administradores configuram um endereço IPv6 estático manualmente em uma interface de túnel, e atribuem endereços IPv4 estáticos configurados manualmente à origem do túnel e ao destino do túnel. O *host* ou o roteador em cada extremidade de um túnel configurado deve suportar as pilhas do protocolo IPv4 e IPv6.

3. MATERIAIS E MÉTODOS

Retrataremos o cenário em que será realizado o procedimento esperimental, como por exemplo, quais serão os equipamentos utilizados, como será a disponibilidade dos mesmos dentro da topologia, qual o protocolo utilizado em cada parte da topologia, tanto nos roteadores como entre os roteadores, e o mais importante que é configurar um tunelamento IPv6 para IPv4.

Dentro da perspectiva de ser necessária uma abrangência maior em números de IP para os dispositivos atuais e os que virão, se evidencia a oportunidade de desenvolvimento deste trabalho, de forma que possa se apresentar uma técnica prática de transição para o IPv6, a qual, nomeia-se tunelamento 6to4 (IP versão 6 para IP versão 4). Aqui consiste em duas "ilhas" IPv6 conectando-se através de uma rede inteiramente IPv4. Para tanto, utilizando o protocolo de roteamento RIPng o qual já existe na versão 4 do protocolo IP e agora tem sua alteração para a nova versão do protocolo.

A topologia implementada é apresentada na figura 7.

Os endereços IPv6 nos roteadores foram configurados de maneira a serem "práticos" para a configuração (com boa parte do endereço sendo 0). Sendo eles:

- R1(túnel): 3000::1/64, R1(lan): 2001::1/64
- R3(túnel): 3000::3/64, R3(lan): 2003::1/64

Os endereços IPv6 configurados nos hosts foram baseados no número MAC da NIC de cada *host*, sendo configurados automaticamente de acordo com o prefixo de rede configurado na porta LAN dos roteadores. Neste caso, o prefixo utilizado foi o 64.

Aqui são mostrados alguns dos comandos de configuração que merecem maior destaque e se aplicam a outros contextos, tendo como referência o roteador R1:

R1(config)#ipv6 unicast-routing:

Responsável por habilitar o roteamento IPv6 no roteador.

R1(config)#ipv6 router rip paper:

Cria uma configuração de roteamento RIPng com o nome indicado, neste caso o nome utilizado foi a palavra "paper".

R1(config-if)#ipv6 rip paper enable:

Utilizado dentro de uma configuração de interface, seja ela FastEthernet, Serial ou Tunnel, habilitando a configuração de roteamento RIPng previamente configurada.

R1(config-if)#ipv6 enable:

Assim como o "*rip WORD enable*", deve ser realizado dentro das configurações de uma interface. Assim que o "*ipv6 unicast-routing*" estiver habilitado, este comando faz com que seja possível a configuração de um IP versão 6 na interface.

R1(config-if)#ipv6 address 3000::1/64:

Para a configuração de um endereço IPv6 ser feita em uma interface, segue-se o mesmo padrão do IPv4, porém, ao invés de se colocar uma máscara após o endereço, colocasse o prefixo da rede.

R1(config-if)#tunnel source fastethernet 0/1:

Designa a interface que será utilizada para saída do pacote enviado pelo túnel. Neste caso, a interface FastEthernet 0/1.

R1(config-if)#tunnel destination 200:20:10:2:

Adiciona um endereço IPv6 de destino para o túnel *6to4*. O mesmo endereço deve ser configurado na outra ponta como endereço do túnel.

R1(config-if)#tunnel mode ipv6ip:

Define o tipo de túnel utilizado na interface tunnel, neste caso foi configurado o tunelamento IPv6 (IPv6 através de IPv4, ou apenas *6to4*).

Esta técnica de transição do IPv4 para o IPv6 é interessante pois, se mantém os endereços IPv4 já configurados na rede, só habilitando o IPv6 nos roteadores das pontas da topologia para dois hosts em pontas distintas poderem se comunicar sem a rede inteira ter que ser baseada no IPv6. Os roteadores R1 e R3 são o que é chamado de pilha-dupla, quando um roteador tem configurado tanto a versão quatro quanto a versão seis do protocolo IP.

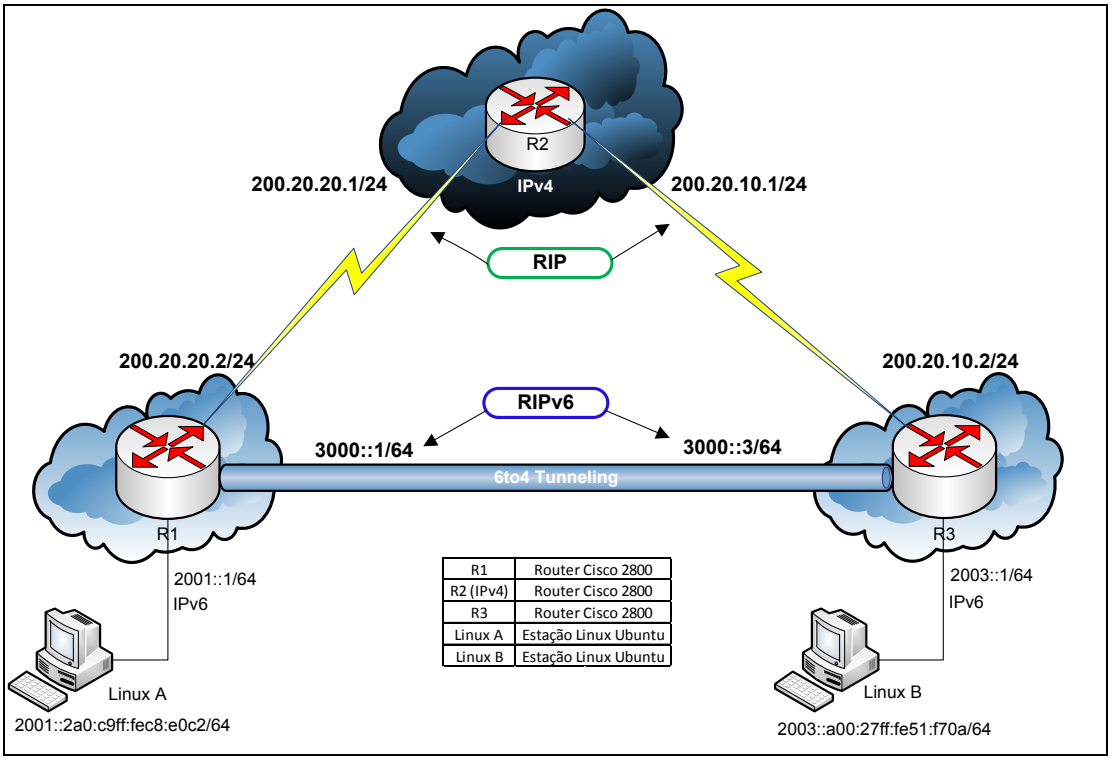

Figura 7– Topologia túnel 6to4.
Fonte – O próprio autor, 2012.

4. RESULTADOS

Aqui é demonstrada a forma como se analisou o funcionamento da topologia e de que maneira se verificou a disponibilidade do túnel em IPv6. É demonstrando também como é feita uma análise de tráfego no programa Wireshark.

Para analisar o tráfego de dados no túnel *6to4* da topologia, foi colocado um switch entre dois roteadores da topologia, e ligou-se, juntamente com os dois roteadores no switch, um terceiro computador, com o intuito de analisar o tráfego passando pelos dois roteadores também ligados ao *switch*. Para tanto, utilizou-se o espelhamento de portas do *switch*. Enviando todos os dados passados por ele para todos os computadores ligados ao mesmo. Assim, pode-se ver o pacote IPv6 encapsulado em um pacote IPv4.

O espelhamento de portas, segundo a própria Cisco (2007), fabricante do *switch*, é assim configurado, sendo o elemento "x" referente à porta FastEthernet no switch:

switch(config)#monitor session 1 destination interface fastEthernet 0/x

switch(config)#monitor session 1 source interface fastEthernet 0/x

switch(config)#monitor session 1 source interface fastEthernet 0/x

switch(config)#monitor session 1 source interface fastEthernet 0/x

O *destination* é a porta FastEthernet que receberá os dados passados na rede por qualquer porta adicionada como *source*, como na figura 8.

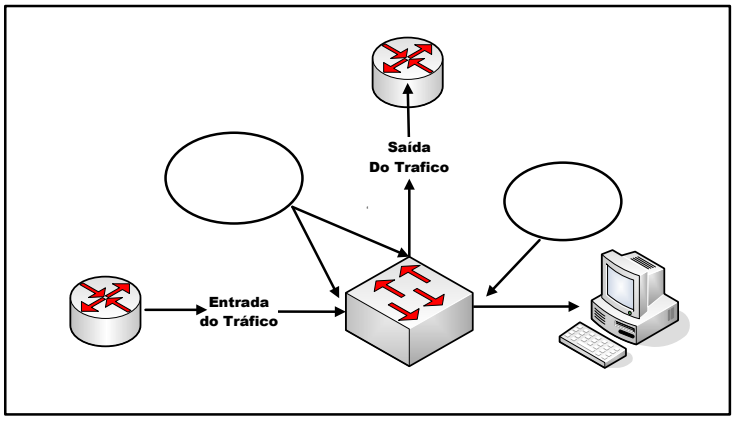

Figura 8 – Espelhamento de portas.
Fonte – O próprio autor, 2012

A figura 9 mostra as configurações da NIC e o endereço de IPv6, vistos nas ferramentas de rede do Linux no dispositivo. Este endereço de IPv6 foi recebido automaticamente através do roteador R3 por ter o prefixo da rede como 64, o IP do Linux 2 recebeu seu endereço iniciado por "2003:":. Nota-se também que o endereço dado ao Linux 2 foi baseado no endereço MAC da sua NIC, a qual está com estado definido como ativo, como se pode observar na figura 20 sendo o "08:00:27:51:f7:0a", este endereço é um endereço link-local como visto anteriormente. Percebe-se também que não há endereço IPv4 configurado já que o foco é observar o tráfego pelo túnel IPv6.

Figura 9 – Dispositivo de rede Linux 2
Fonte – O próprio autor, 2012.

Para fazer a análise através do programa Wireshark, foi executado um *ping*, de um *host* Linux para um roteador da outra ponta da topologia, através de um endereço IPv6 para ver a funcionalidade do túnel *6to4* como mostrado na figura 10. Para se visualizar os

pacotes IPv6 no Wireshark se executou 15 solicitações de *ping* do Linux 2 ao roteador R1, lembrando que o analisador está recebendo os pacotes trafegados entre R1 e R2.

Figura 10 – Ping Linux 2 ao R1
Fonte – O próprio autor, 2011

O *ping* foi realizado através da interface gráfica do Linux Ubuntu, executando-se o comando *ping*, no endereço "3000::1" correspondente ao endereço IPv6 configurado na interface túnel no roteador R1, e teve o sucesso de 100% nas 15 solicitações.

Na figura 11 observa-se o ICMPv6 no *ping*. O ICMPv6 é uma norma obrigatória do IPv6, definida no RFC 2463, e através dele pode-se enviar mensagens *echo* e detectar falhas de comunicação da rede.

A figura 12 destaca o elemento analisado de número 8, que se refere a uma mensagem ICMPv6 *request* de *ping*. Identificando a passagem do pacote IPv6 de origem "2003::a00:27ff:fe51:f70a" referente ao Linux 2 ao destino "3000::1" referente a interface túnel do roteador R1. O pacote foi encapsulado dentro do protocolo IPv4 recebendo a referência no seu campo do cabeçalho protocolo como 41, o que indica que há um protocolo IPv6 no pacote. A origem do pacote IPv4 é o endereço 200.20.10.2 que é o endereço da interface FastEthernet 0/1 do roteador R3 que é a interface conectada ao roteador R2 via RIP, e tendo como destino o endereço IPv4 200.20.20.2 referente ao endereço IPv4 da interface FastEthernet 0/1 do roteador R1 que está conectada ao roteador R2 via RIP.

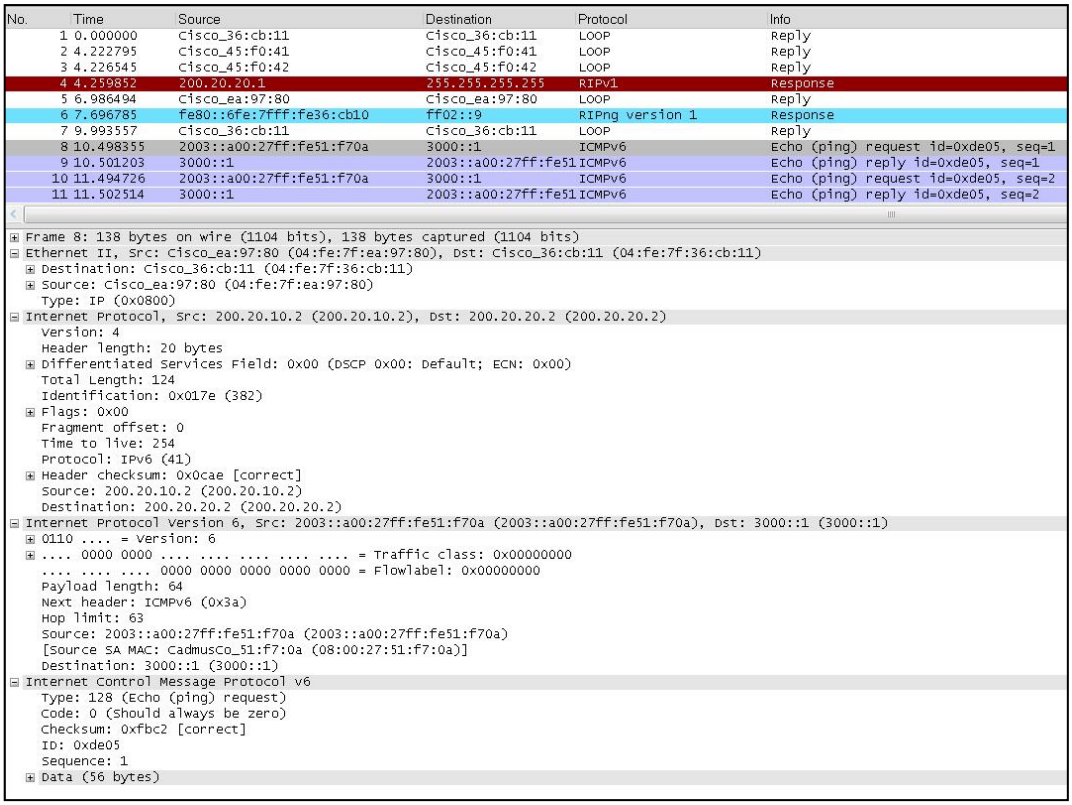

Figura 11 – Interface Wireshar apresentando um *Ping request*
Fonte – O próprio autor, 2012

Pode-se observar na figura 12 que a origem é o endereço “fe80::226:99ff:fe88:78e8” para o destino “ff02::9”, sendo que este corresponde ao número de endereço *multicast* no IPv6. Esta é uma mensagem de resposta do protocolo de roteamento RIPng. A mensagem está encapsulada dentro de um pacote IPv4, enviado do endereço 200.20.10.2 para o endereço 200.20.20.2, recebendo em seu cabeçalho a especificação de protocolo como 41 (IPv6). A porta utilizada no encaminhamento do pacote é a 521, designada para as mensagens RIPng. Também, é exibido a versão do protocolo RIPng como 1, e a métrica do caminho do pacote, como tem-se apenas um roteador até o destino é mostrada como 1.

Outro modo de observação da convergência da rede, é através do próprio prompt no roteador, dando-se comandos “*show*”. São eles: *Show ipv6 rip* e *Show ipv6 route.*

5. CONCLUSÃO

O IPv6 já não se trata de uma alternativa nova como é pensado por muitos. Porém, é muito provável que ocorra um esgotamento de endereços IPv4 antes que se consiga uma transição completa. Tendo isso em vista, surgiram como meios de adaptação na transição entre as versões quatro e seis do protocolo IP, alternativas que utilizassem ambos os protocolos, afim de não impactar tanto no dia-a-dia do usuário final, já que muitas das

aplicações utilizadas atualmente se mantém baseadas em endereçamento IPv4. Desta forma, necessita-se de um aprendizado sobre as novas formas de roteamento, que não são tão diferentes das habituais, mas merecem uma atenção especial.

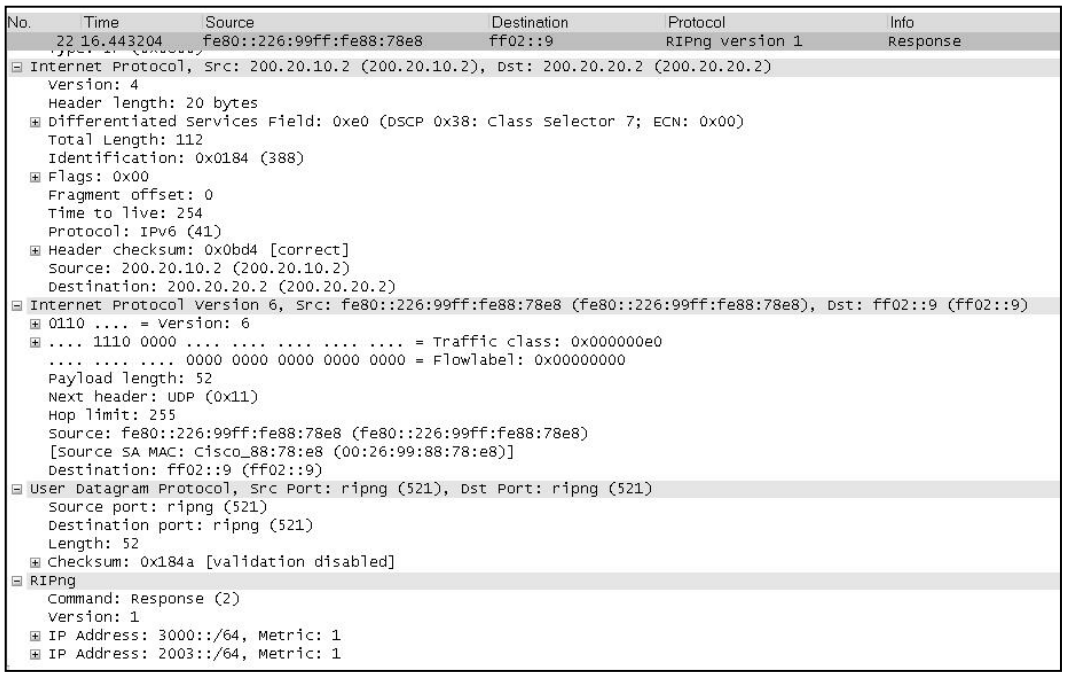

Figura 12 – *RIPng Response*.
Fonte – O próprio autor, 2012

Conhecer também o protocolo IPv6 é de grande ajuda para a migração de *hosts* IPv4, já que houve mudanças significativas no endereçamento, tendo um número consideravelmente maior de endereços em relação a versão anterior. Se torna visível este aumento ao usuário que, tendo ao invés de quatro octetos formando seu endereço IP como são os endereços IPv4, tem-se agora dezesseis octetos formando seu endereço IPv6.

Já que os últimos blocos de endereços IPv4 foram distribuídos aos RIR no começo de 2011, torna-se mais provável e necessário que se tomem atitudes para a implementação do IPv6. Algumas tais como o *World IPv6 Day*, realizado em 8 de junho de 2011, que disponibilizou a diversos sites como Google e Facebook, para terem seu conteúdo disponível em IPv6 durante 24 horas. Após o acontecido, foi relatado que não foi encontrado nenhum problema ou indicação de lentidão, e notou-se que o aumento de usuários IPv6 no dia do evento foi consideravelmente maior do que de outros dias, mostrando que a adoção ao IPv6 é uma questão de tempo.

As alternativas de transição, em sua grande maioria, já são do conhecimento de profissionais da área das redes e telecomunicações. Como o tunelamento, que já era uma ferramenta do IPv4 e que agora no IPv6 tem ainda mais cenários capaz de suprir. Os

protocolos de roteamento sofreram alterações que implicaram em mudanças de versões para suportar o novo protocolo, mas sua arquitetura de configuração permanece quase a mesma.

Tem-se dúvida quanto a real necessidade desta mudança para o IPv6, já que muitos acreditam que não há um real porque já que têm em suas casas e empresas uma Internet funcionando perfeitamente sem necessidade de alterações. Porém, as novas aplicações de Internet e televisão, tais como VoIP e IPTV, e também novos dispositivos, os quais necessitam de um único endereço IP, tornam indiscutíveis uma alternativa para a limitação do IPv4. O IPv6 mostra-se necessário, já que mesmo com muitas ferramentas para contornar o esgotamento do IPv4, tais como o NAT, não se foi capaz de administrar o crescimento da rede e de endereços IP necessários para a mesma.

6. REFERÊNCIAS

BOUND, J.; VOLZ, B.; LEMON, T.; PERKINS, C. E; CARNEY, M.: RFC 3315 - Dynamic host configuration protocol for IPv6 (DHCPv6), 2003. Disponível em: < http://www.ietf.org/rfc/rfc3315.txt>. Acesso em: 15 abril 2011.

CISCO. CCNA Exploration: accessing the WAN, 2009. Disponível em: <cisco.netacad.net>. Acesso em: 7 abril 2011.

COLTUN, Rob; FERGUSON, Dennis; MOY, John. RFC 5340 - OSPF for IPv6, 2008. Disponível em: < http://tools.ietf.org/html/rfc5340>. Acesso em: 12 de abril 2011.

DEERING, S; HINDEN, R.: Internet Protocol, Version 6 Specification. IETF, 1998. Disponível em http://tools.ietf.org/html/rfc2460. Acessado em 04/04/2012;

FORGIE, James. IEN 119, ST : a proposed internet stream protocol, 1979. Disponível em: <http://www.rfc-editor.org/ien/ien119.txt>. Acesso em: 2 jun 2011.

GOOGLE: IPv6 Statistics. Disponível em http://www.google.com/intl/en/ipv6/statistics/. Acessado em 04/04/2012.

HINDEN, R. M; DEERING, S.: RFC 2373 - IP version 6 addressing architecture, 1998. Disponível em: <http://www.ietf.org/rfc/rfc2373.txt>. Acesso em: 22 de mar 2011.

MALKIN, Gary Scott; MINNEAR, Robert E. RFC 2080 - RIPng for IPv6, 1997. Disponível em: <http://www.ietf.org/rfc/rfc2080.txt>. Acesso em: 12 abr 2011.

MOREIRAS, Antonio. Entenda o esgotamento do IPv4, 2009. Disponível em: <http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4>. Acesso em: 22 maio 2011.

NARTEN, T.; NORDMARK, E.; SIMPSON, W. A.; SOLIMAN, H.: RFC 4861 - Neighbor discovery for IP version 6 (IPv6), 2007. Disponível em: <http://www.ietf.org/rfc/rfc4861.txt>. Acesso em: 3 maio 2011

PATARA, .; MOREIRAS,.: Últimos blocos IPv4 são alocados pela IANA, 2011. Disponível em: <http://www.nic.br/imprensa/releases/2011>. Acesso em: 20 mar 2011.

SILVA, A.: O que vai mudar na sua vida com o IPv6 – RPN, 1997. Disponível em: <http://www.rnp.br/newsgen/9706/n2-1.html>. Acesso em: 22 mar 2011.

URTADO, A.; ALVES, N.: Implementação do protocolo IPv6 na RedeRio, 2008. Disponível em: http://www.ipv6.br/IPV6/ArtigoImplementacaoRedeRio. Acesso: maio 2011.