IPV6 – PROCESSO DE TRANSIÇÃO: IMPLANTAÇÃO DE TUNNEL BROKER PELA APLICAÇÃO GOGO6

Carlos Alexandre Carvalho Tojeiro[1]; Eduardo Moraes Alves[2]; Thiago José Lucas[3]

Resumo
Este trabalho tem como objetivo trazer uma pesquisa relacionada ao processo de transição do protocolo IPv4 para o IPv6, com a técnica de tunelamento pela aplicação Gogo6, bem como os resultados obtidos na navegação em IPv6 por esta técnica.
Palavras-chave: IPv4; IPv6; transição; tunelamento; Gogo6.

Abstract
This work aims to bring a research related to the transition process from IPv6 to IPv6, with a tunneling technique by Gogo6 application, as well as the results obtained in IPv6 navigation by this technique.
Keywords: IPv4; IPv6; transition; Tunneling; Gogo6.

Introdução

A motivação para uma nova versão do protocolo IP é lidar com problemas de expansão e alocação de endereços ocasionados pelo aumento exponencial de dispositivos conectados à Internet. Algumas técnicas ajudaram a conter o problema de esgotamento de endereços e controlaram o aumento de informações da tabela de roteamento. Entretanto, o problema de expansão chegou a um ponto que estas técnicas já não se adequam mais ao cenário atual (WU, PENG, et al. 2013). Como conter o esgotamento eminente de IPv4? Computadores, aparelhos de TV, celulares, tablets, dentre outros dispositivos, estão conectados à Internet. Este grupo compõe um número superior a quatro milhões de hosts conectados, cujo espaço fornecido por um endereçamento de 32 bits não consegue atender.

Para entender as razões desse esgotamento, é importante considerar que a Internet não foi projetada para uso comercial.

[1] Especialista em Segurança de Redes de Computadores pela Faculdade de Tecnologia de Ourinhos - FATEC. E-mail: carlos.tojeiro@fatecourinhos.edu.br.
[2] Mestrando em Ciências da Computação pela Universidade Estadual de Londrina-UEL, professor da Faculdade de Tecnologia de Ourinhos - FATEC; E-mail: eduardo.moraes@fatecourinhos.edu.br.
[3] Especialista em Projeto e Implementação de Redes de Computadores pela Universidade Tecnológica Federal do Paraná - UTFPR; professor da Faculdade de Tecnologia de Ourinhos - FATEC; E-mail: thiago.lucas@fatecourinhos.edu.br.

No início da década de 80, ela poderia ser considerada uma rede predominantemente acadêmica, com poucas centenas de computadores interligados. A Internet foi introduzida primeiramente com a intenção de conectar poucos nós, entretanto, mais tarde, evoluiu para uma rede de ligação completa e global (KALWAR, SAADULLAH, BOHRA, MENON. 2015). O IPv6 surgiu para suprir esta necessidade por endereçamento, pois, em tese, ele oferecerá cerca de 160.000 endereços por metro quadrado da superfície terrestre (PETERSON, DAVIE. 2007).

Este trabalho traz em sua estrutura o conceito sobre o protocolo IPv4, seus objetivos relacionados à fragmentação de pacotes e o endereçamento. Trás, também, os problemas relacionados ao crescimento demasiado de redes de computadores e os motivos que levaram ao esgotamento de endereços IPv4. Em seguida, são mostradas técnicas paliativas adotadas para conter a escassez de IPv4. Logo após, é mostrado o surgimento do IPv6, tipos de endereçamentos IPv6 e a técnica de transição por tunelamento denominado tunnel broker; técnica que permite que dispositivos isolados, ou toda uma rede IPv4, obtenham conectividade IPv6 por meio do estabelecimento de um túnel com um provedor, tornando-se, na prática, dispositivos de pilha dupla ou uma rede pilha dupla. É apresentado um estudo de caso, utilizando a aplicação denominada Gogo6, os resultados obtidos deste estudo e as considerações finais.

1 O Fim do IPv4 e o Estabelecimento do IPv6

O endereço de IP é representado por um número de 32 bits dividido por quatro octetos representados na forma decimal, como por exemplo: 192.168.2.45. O protocolo IP foi criado e devidamente especificado na RFC 791 com o objetivo de realizar duas funções: fragmentação, que trata do envio de pacotes maiores que o limite estabelecido num enlace, dividindo-os em fragmentos menores dentro do tráfego; e o endereçamento, que identifica o destino e a origem dos pacotes por meio dos endereços armazenados no cabeçalho do protocolo. A versão utilizada pelo protocolo é a 4, comumente referenciada como IPv4. Apesar do IPv4 apresentar robustez, interoperabilidade e implantação fácil, seu projeto original não previu alguns aspectos como:

- Crescimento das redes e, consequentemente, a escassez dos endereços IP;
- Aumento da tabela de roteamento;
- Problemas relacionados com a segurança dos dados transmitidos;
- Para um melhor entendimento sobre estes aspectos, é importante salientar que os endereços IPv4 foram divididos em três classes conforme Tabela 1:

Tabela 1 - Classes de IP

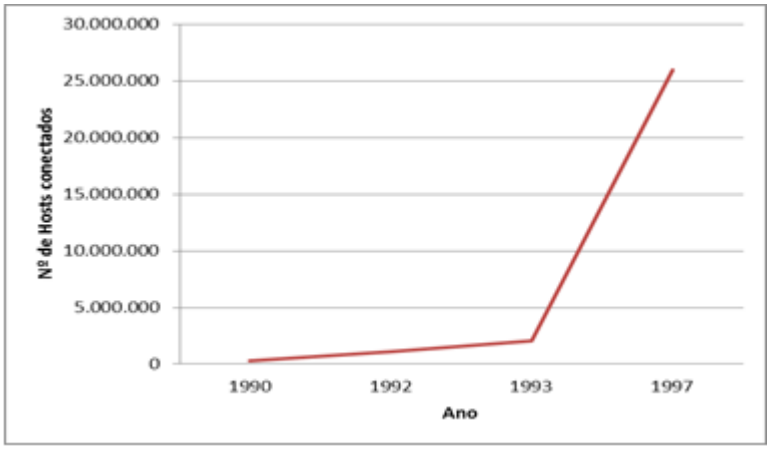
Classe	Formato	Redes	Hosts
A	7 bits Rede, 24 bits host	128	16.77.216
B	14 bits Rede, 16 bits host	16.384	66.536
C	21 bits Rede, 8 bits host	2.097.152	256

Fonte: Elaborada pelos autores.

O propósito desta divisão era tornar a atribuição de endereços mais flexível, envolvendo redes de diversos tamanhos, mas não se mostrou suficiente. A classe A atendia um número muito pequeno de redes e ocupava metade de todos os endereços de hosts disponíveis, enquanto com a classe C acontecia o contrário, pois permitia a criação de várias redes, mas com poucos endereços de hosts, acarretando desperdício para uma classe e, ao mesmo tempo, necessidade de endereçamento para outra classe.

Mais um fator agravante no desperdício foi a forma de distribuição de endereços IP da classe A para grandes empresas e instituições como Departamento de Defesa Americano, a MIT, AT&T, IBM, Apple, Xerox, Hewlett Packard, dentre outras. Faixas inteiras de endereços IP foram atribuídas a estas empresas, disponibilizando aproximadamente 17 milhões de endereços para cada empresa, que, dificilmente, seriam usadas efetivamente. Agravando ainda mais, 35 faixas de endereços classe A foram reservadas para usos específicos como multicast, loopback e uso futuro (EQUIPE IPv6.br. 2012). A figura 1 apresenta o crescimento da Internet.

Figura 1 - Hosts conectados à Internet



Fonte: Elaborada pelos autores.

Com o ritmo do crescimento da Internet, em 1990 já eram 313.000 hosts conectados; em 1992, 38% dos endereços da classe A, 43% dos endereços da classe B e 2% da classe C já estavam devidamente alocados, totalizando 1.136.00 hosts conectados; em 1993 com a criação do protocolo HTTP já eram 2.056.00 hosts conectados. A Internet

passou a ser utilizada comercialmente e pelas indústrias; de 1993 a 1997 houve um crescimento muito grande e já atingindo 26 milhões de hosts conectados.

2 Soluções Propostas e o Surgimento do IPv6

A *Internet Enginnering Task Force* – IETF discute estratégias para a falta de endereços IP e sobre o aumento da tabela de roteamento (CAPELA. 2003). As soluções apresentadas:

• Classless *Inter-domain Routing* – CIDR, permitindo a alocação de blocos conforme a necessidade da rede e a agregação de rotas, diminuindo o tamanho da tabela de roteamento, sendo que os blocos são referenciados como prefixo de redes. Outra forma de indicar o prefixo é por meio de máscaras, conforme Tabelas 2, 3 e 4:

Tabela 2 - Indicação de prefixo por meio de máscara Classe A

Subdivisões de uma identificação de rede classe A.			
Nº de sub-redes	Nº de bits para sub-rede	Máscara de sub-rede	Nº de hosts por sub-rede
1-2	1	255.128.0.0 ou /9	8.388.606
3-4	2	255.192.0.0 ou /10	4.194.302
5-8	3	255.224.0.0 ou /11	2.097.150
9-16	4	255.240.0.0 ou /12	1.048.574
17-32	5	255.248.0.0 ou /13	524.286
33-64	6	255.252.0.0 ou /14	262.142
65-128	7	255.254.0.0 ou /15	131.070
129-256	8	255.255.0.0 ou /16	65.534
257-512	9	255.255.128.0 ou /17	32.766
513-1.024	10	255.255.192.0 ou /18	16.382
1.025-2.048	11	255.255.224.0 ou /19	8.190
2.049-4.096	12	255.255.240.0 ou /20	4.094
4.097-8.192	13	255.255.248.0 ou /21	2.046
8.193-16.384	14	255.255.252.0 ou /22	1.022
16.385-32.768	15	255.255.254.0 ou /23	510
32.769-65.536	16	255.255.255.0 ou /24	254
65.537-131.072	17	255.255.255.128 ou /25	126
131.073-262.144	18	255.255.255.192 ou /26	62
262.145-524.288	19	255.255.255.224 ou /27	30
524.289-1.048.576	20	255.255.255.240 ou /28	14
1.048.577-2.097.152	21	255.255.255.248 ou /29	6
2.097.153-4.194.304	22	255.255.255.252 ou /30	2

Fonte: Elaborada pelos autores.

Tabela 3 - Indicação de prefixo por meio de máscara Classe B

Subdivisões de uma identificação de rede classe B.			
Nº de sub-redes	Nº de bits para sub-rede	Máscara de sub-rede	Nº de hosts por sub-rede
1-2	1	255.255.128.0 ou /17	132.766
3-4	2	255.255.192.0 ou /18	16.382
5-8	3	255.255.224.0 ou /19	8.190
9-16	4	255.255.240.0 ou /20	4.094
17-32	5	255.255.248.0 ou /21	2.046
33-64	6	255.255.252.0 ou /22	1.022
65-128	7	255.255.254.0 ou /23	510
129-256	8	255.255.255.0 ou /24	254
257-512	9	255.255.255.128 ou /25	126
513-1.024	10	255.255.255.192 ou /26	62
1.025-2.048	11	255.255.255.224 ou /27	30
2.049-4.096	12	255.255.255.240 ou /28	14
4.097-8.192	13	255.255.255.248 ou /29	6
8.193-16.384	14	255.255.255.252 ou /30	2

Fonte: Elaborada pelos autores.

Tabela 4: Indicação de prefixo por meio de máscara Classe C

Subdivisões de uma identificação de rede classe C.			
Nº de sub-redes	Nº de bits para sub-rede	Máscara de sub-rede	Nº de hosts por sub-rede
1-2	1	255.255.255.128 ou /25	126
3-4	2	255.255.255.192 ou /26	62
5-8	3	255.255.255.224 ou /27	30
9-16	4	255.255.255.240 ou /28	14
17-32	5	255.255.255.248 ou /29	6
33-64	6	255.255.255.252 ou /30	2

Fonte: Elaborada pelos autores.

• *Dynamic Host Configuration Protocol* – DHCP, onde o host tem a capacidade de adquiri automaticamente um endereço de IP, a mascará de sub-rede, gateway padrão e o endereço do servidor DNS local.

• *Network Address Translation* – NAT, técnica paliativa desenvolvida para resolver o problema de escassez dos endereços IPv4, que permite que vários hosts de uma rede interna com IPs privados trafeguem pela Internet por meio de um único endereço de IP público. É feita uma tradução de IP privado para público. O NAT é definido pela RFC 3022 e três faixas de IPs são reservados, conforme Tabela 5.

Tabela 5 - IPs Privados

Faixa de IP Privada	Máscara de sub-rede	Nº Hosts
10.0.0.0 a 10.255.255.255A	/8	16.777.216
172.16.0.0 a 172.31.255.255	/12	1.048.576
192.168.0.0 a 192.168.255.255	/16	65.536

Fonte: Elaborada pelos autores.

Na RFC 1752, apresentou recomendação final para o novo protocolo IP que passou a incorporar endereços de 128 bits e um endereçamento baseado no CIDR, com cabeçalhos de extensão. Passou a ser chamado oficialmente de IPv6.

No IPv4, o campo do cabeçalho reservado para o endereço possui 32 bits; isto possibilita um máximo de 4.294.967.296, ou seja, 232 endereços. Até então, esta quantia de endereços era suficiente para identificar todos os computadores na rede e suportar o surgimento de novas sub-redes. Porém, com o crescimento dinâmico da Internet, surgiu o problema do esgotamento dos endereços IPv4.

Com o IPv6, e seus 128 bits de espaço de endereçamento, é possível obter um número impressionante de endereços, cerca de 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços distintos, ou seja, 2128. São, aproximadamente, 79 octilhões, ou seja, 7,9×1028 de vezes a quantidade de endereços da sua versão anterior e representa, também, mais de 56 octilhões, ou seja, 5,6×1028 de endereços por ser humano no planeta, estimando-se uma população de seis bilhões de habitantes (EQUIPE IPv6.br. 2012).

O endereço IPv6 é dividido em 8 grupos de 16 bits, escrito em hexadecimal. Estes grupos são divididos por ":". Outra característica é a permissão de abreviamento de "zeros" à esquerda dentro do grupo de 16 bits ou a substituição de sequências de zeros por "::", apenas uma única vez, dentro do endereço, para que não haja mais uma interpretação dos endereços. Veja o exemplo de representações de um mesmo endereço IPv6:

- ..2001:0DB8:0000:0000:130F:0000:0000:140B
- ..2001:DB8:0:0:130F::140B
- ..2001:DB8::130F:0:0:140B

3 Processo de Transição

A transição entre as duas versões do protocolo deve ser feita, de modo que haja coexistência e interoperabilidade entre IPv4 e IPv6 (EQUIPE IPv6.br. 2012). Os mecanismos utilizados nessa transição consistem em alterações ao protocolo e nos mecanismos que afetam os hosts e roteadores de modo a serem projetados para evitar contratempos e facilitar uma transição suave (AHMED, SID, HASSAN, OTHMAN. 2014).

Estes cenários de transição representam uma generalização e extensão da enumeração feita na RFC 6144. Embora a RFC só trate de cenários com soluções de tradução, outras tecnologias auxiliares, conhecidas como técnicas de transição podem ser apresentadas, conforme Figura 2:

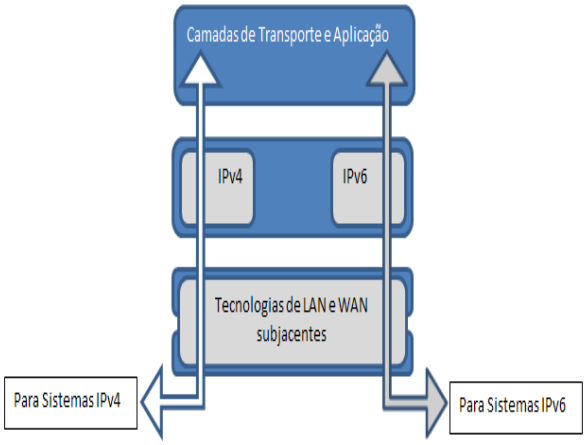
Figura 2 - Três estratégias de Transição

Fonte: Elaborada pelos autores.

Para entender as tecnologias de transição é necessário entender os cenários existentes, as necessidades apresentadas e as dificuldades envolvidas em cada ambiente (FOROUZAN. 2010). A transição não se dará repentinamente, levando-se um tempo considerável para que todos os sistemas mudem de IPv4 para IPv6 (RIVATTO, LIZANDRO, MANFRON, SOLDAN. 2015). As três técnicas são:

- Pilha Dupla: antes da migração por completa para IPv6, os hosts trabalharão com IPv4 e IPv6 simultaneamente, implementando um sistema de pilha dupla, até a mudança final. A vantagem é que o IPv4 e o IPv6 rodam em pilhas separadas. Sendo assim, as falhas de uma pilha não devem interferir diretamente na outra (JUNIOR, FORTUNATO. 2015). O host consulta o DNS; se o mesmo retornar um endereço IPv4, o host de origem transmite pacotes em IPv4, caso contrário, ele transmite pacotes em IPv6, conforme mostrado na Figura 3:

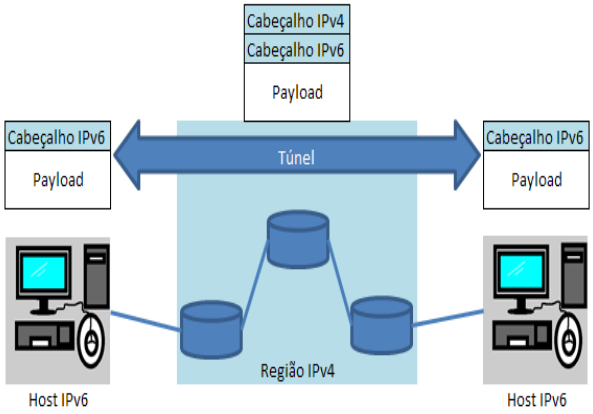
Figura 3 - Pilha Dupla



Fonte: Elaborada pelos autores.

- Tunelamento: Dois hosts em IPv6 desejam estabelecer uma comunicação, onde os pacotes passarão por uma região que utiliza IPv4. Para que isto ocorra, os pacotes deverão ter um endereço IPv4, ou seja, o pacote IPv6 é encapsulado em um pacote IPv4 no momento que entra nesta região e, desencapsulado no momento que sai da região. É o pacote IPv4 que carrega o pacote IPv6, formando um túnel entre as extremidades, como mostra a Figura 4:

Figura 4 - Tunelamento



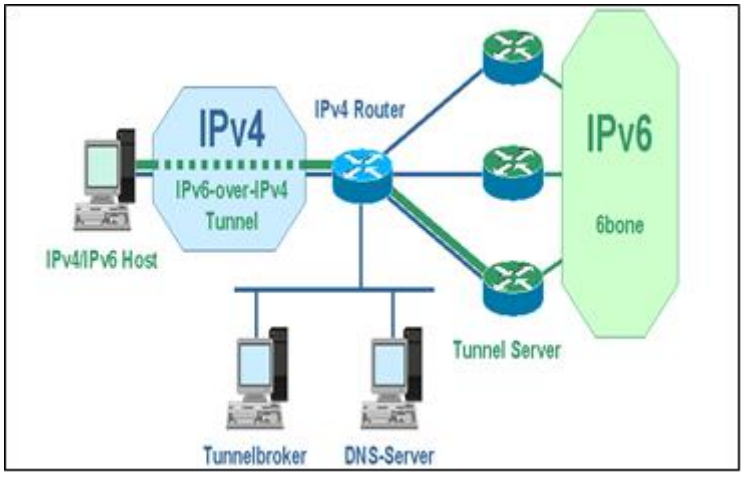
Fonte: Elaborada pelos autores.

- Tradução: técnica utilizada quando maior parte da Internet tiver migrado para IPv6, mas alguns sistemas ainda estiverem usando IPv4, ou seja, de um lado tem-se um host IPv4 e, do outro, um host IPv6. Nesta situação o cabeçalho é totalmente modificado e convertido de IPv6 para IPv4, no ponto de tradução do cabeçalho, como mostra a figura 5.

4 Métodos e Materiais Utilizados

O método de transição utilizado no estudo de caso foi o tunelamento; o mecanismo de transição designado de "Tunnel Broker" está definido no RFC 3053 e permite configurar túneis entre o servidor e o cliente, de forma transparente. É uma alternativa de conexão a Internet via IPv6, onde permite que hosts IPv6/IPv4 isolados em uma rede IPv4 acessem redes IPv6, colocando pacotes IPv6 dentro de pacotes IPv4 (PAMPLONA, GUSTAVO, TOKUNAGA. 2015). Essa abordagem é útil para estimular o crescimento de redes IPv6, aumentando os hosts que possuam suporte ao novo protocolo de IP. O mecanismo de Tunnel Broker é uma abordagem alternativa baseada na oferta de servidores dedicados, a gerenciar automaticamente os pedidos vindos dos túneis dos usuários (BERGAMIN, EVERTON E FERREIRA, JOSÉ O. 2013). O túnel pode ser visto como um provedor virtual, que proporciona conectividade para os usuários já conectados na rede, conforme Figura 6.

Figura 6 - Topologia Tunnel Broker



Fonte: Elaborada pelos autores.

O cliente do túnel envia um pacote pela Internet IPv4 para autenticar-se e requisitar o serviço do Tunnel Broker, onde o usuário se conecta para registrar e ativar o túnel. Na continuidade, o próprio Tunnel Broker gerencia a criação, alteração e exclusão do túnel pelo usuário e cria registros para utilização de nomes de IPv6 no DNS.

O servidor (Tunnel Server) funciona como pilha dupla (IPv4 e IPv6) conectada a Internet global. Após a recepção de uma ordem do Tunnel Broker, o servidor cria, modifica ou excluí o servidor de cada túnel, podendo também manter as estatísticas dos mesmos. O servidor fecha o túnel com o cliente do túnel (Figura 6), trabalhando para fazer o intercâmbio entre o IPv6 e o IPv4.

O Tunnel Server gerencia o cliente da seguinte forma:

- Escolhe o prefixo IPv6 que deverá ser alocado para o cliente;
- Determina uma vida útil para o Tunnel Broker;
- Registra no DNS os endereços de IPv6 globais de forma automática;
- Exerce as configurações necessárias para o túnel;
- Notifica informações importantes e relevantes para a configuração do cliente, incluindo parâmetros do túnel e registros de DNS.

O usuário do Tunnel Broker utiliza um sistema de IPv6 de Pilha-Dupla (*dual-stack*) conectado a Internet IPv4, trabalhando com os dois protocolos. Antes do usuário se conectar, deverá se identificar e inserir as credenciais de autenticação, de modo que o túnel seja adequado conforme a configuração. O Tunnel Broker é o responsável por receber as requisições, autenticação do cliente e também por fazer as trocas de pacotes IPv6 e IPv4 entre o Tunnel Server e o cliente para o fechamento do túnel. Os tipos de endereçamento IPv6 recebido pelo Tunnel Broker são unicast global, o mesmo que receberia diretamente do provedor de Internet. Após as etapas de configuração ser concluídas, o túnel IPv6, sobre IPv4, estará ativado e operando, permitindo que o usuário possa ter acesso ao 6Bone ou qualquer outra rede IPv6.

O 6Bone é uma rede internacional de IPv6; projeto de colaboração entre instituição de pesquisa em IPv6 situadas pelo mundo, conforme RFC 3701, que serve de suporte a testes e implementações em diversas plataformas que utilizam o protocolo. A infraestrutura deste *backbone* IPv6 é composta de muitos provedores de serviços de Internet (ISPs) e redes de utilizadores ligados em conjunto para fornecer este tipo de serviço. O 6Bone é composta de redes que podem manipulam diretamente os pacotes IPv6, ligadas por laços virtuais ponto-a-ponto chamados "túneis". Os pontos finais de túnel são tipicamente máquinas de classe de estação de trabalho com suporte do sistema operacional para o IPv6. Ao longo do tempo, conforme a confiança no IPv6 for aumentando, a tendência do 6Bone é desaparecer (FINK, HINDEN. 2004).

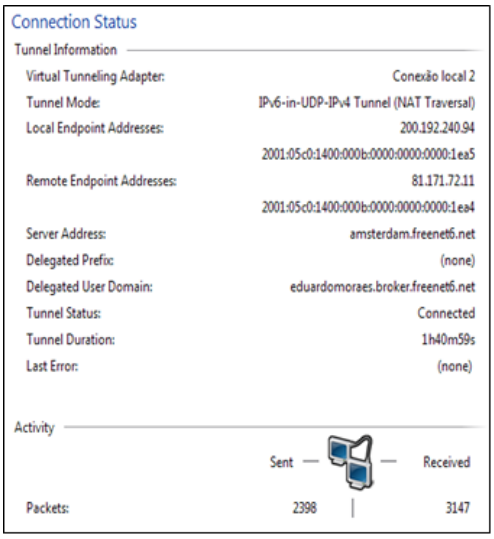
A Figura 7 mostra a aplicação Gogo6-freenet em funcionamento:

Figura 7 - Aplicação GOGO6-FREENET

Fonte: Elaborada pelos autores.

A Figura 8 mostra a configuração da interface virtual criada pela aplicação:

Figura 8 - Configuração da interface virtual



Fonte: Elaborada pelos autores.

A instalação da aplicação Gogo6 é simples e intuitiva. Dentre as várias opções avançadas que a aplicação oferece, está a escolha do tipo de túnel a ser configurado:

- IPv6-in-IPv4 Tunnel: valor padrão, escolhe automaticamente, se é uma rede nativa ou se esta utilizando NAT
- IPv6-in-IPv4 Tunnel (native)
- IPv6-in-IPv4 Tunnel (NAT Traversal)
- IPv4-in-IPv6 (DSTM)
- IPv4-in-IPv6 (DS-Lite)

Antes da realização do estudo de caso, foi necessária a criação de uma conta, para a autenticação no serviço de conexão. Gogo6 utiliza este serviço de criação para estabelecer um controle de pesquisas realizadas em seus servidores IPv6, bem como para enviar notícias e avanços das pesquisas sobre o processo de transição.

Para este estudo de caso, foi utilizada a primeira opção por oferecer as configurações automáticas na escolha do melhor tipo de túnel e melhor servidor IPv6. No host cliente, com sistema operacional Microsoft Windows de 64 bits, foi instalada a aplicação e conectado à Internet por um roteador IPv4 (Figura 7). É importante salientar

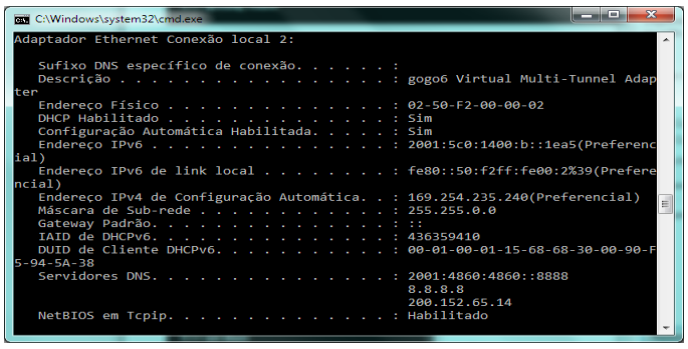
que a Gogo6 oferece suporte também para sistemas operacionais com Kernel Linux. O Gogo6 é um serviço roteamento especializado, concebido para oferecer todas as vantagens do IPv6 para redes IPv4 existentes (GOGO6. 2014).

Além de sua simplicidade, tanto na instalação como no manuseio, Gogo6 oferece uma aba com informações pertinente sobre o estado da conexão:

- Nome da interface virtual;
- Modo de conexão do túnel;
- Endereço local em IPv4 e IPv6;
- Endereço do ponto final em IPv4 e IPv6. No caso estes endereços são do provedor Eweka Internet Services B.V., da cidade de Alkamar, na Holanda;
- Endereço do servidor;
- Prefixo;
- Domínio do usuário;
- Estado do túnel;
- Duração do túnel;
- Último erro encontrado;
- Informações de pacotes enviado e recebido.

A Figura 9 mostra as informações sobre o estado de conexão na própria aplicação,

Figura 9 - Estado da conexão



Fonte: Elaborada pelos autores.

Além do acompanhamento em tempo real do estado de conexão, é possível armazenar os logs de monitoramento, para conferência posterior, exibido na Figura 10:

Figura 10 - Visualização de Log

Fonte: Elaborada pelos autores.

Por meio dos logs, é possível verificar qual porta o Gogo6 utiliza para realiza a comunicação dos serviços em IPv6; é importante realizar configurações extras no firewall do sistema operacional, para que o serviço funcione corretamente. A porta utilizada é 3653 TCP.

5 Resultados Obtidos

Para a obtenção dos resultados na navegação em Ipv6, foi utilizado o próprio site da Equipe IPv6 Brasil (http://ipv6.br). O IPv6.br engloba uma série de iniciativas do NIC.br para disseminar o IPv6 no Brasil; também oferece cursos presenciais gratuitos, com teorias e práticas, para provedores de Internet e outros Sistemas Autônomos (EQUIPE IPv6.br. 2012). Todos os testes foram realizados no navegador Internet Explorer, versão 11; no próprio site da IPv6.br pode ser verificado se a navegação está em IPv6, como mostra a Figura 11.

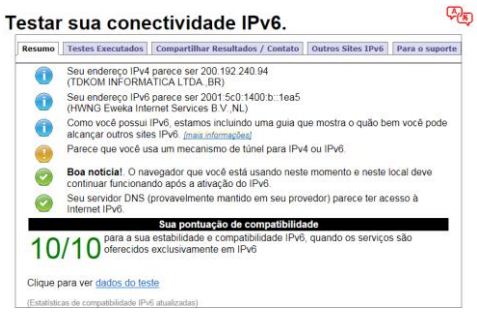
Figura 11 - Teste de conectitividade

Fonte: Elaborada pelos autores.

Outra opção de teste mais detalhada sugerida pela Equipe IPv6 Brasil é o Test IPv6 (http://www.test-ipv6.com), um web site de código aberto dedicado a ajudar os usuários finais a identificar se sua rede IPv6 está trabalhando e se os erros específicos são encontrados. É baseado em javascript, incluindo scripts auxiliares em PHP e módulo do Apache (mod_ip), retornando informações importantes como endereço de IP, informações sobre o provedor de serviço de Internet e informações adicionais (FESLER, JASON. 2015).

A Figura 12 exibe um resumo das informações coletadas no teste e uma pontuação, dizendo a estabilidade e compatibilidade de serviços oferecidos em IPv6.

Figura 12 - Teste de conectividade IPv6



Fonte: Elaborada pelos autores.

De acordo com o resumo das informações coletadas, é possível constatar a utilização de um mecanismo de túnel para a navegação em IPv6. Outras informações importantes coletadas estão na aba “Testes Executados” que explica como os testes foram realizados:

• Teste com um registro DNS em IPv4 – busca apenas um registro A do DNS.

• Teste com um registro DNA em IPv6 – busca um registro AAAA do DNS, esperado no uso de IPv6.

• Teste com um registro DNS duplo – verifica se seu navegador consegue acessar sites que possuem tanto um registro IPv4 quanto um IPv6.

• Teste de DNS duplo e pacote grande – verifica o funcionamento de conexões a um servidor de pilha dupla e se pode enviar e receber pacotes grandes nessa conexão.

• Teste de IPv4 sem DNS –tentativa de uma conexão usando um endereço IPv4, o que deve funcionar para a maioria dos usuários.

• Teste de IPv6 sem DNS – tentativa de uma conexão usando um endereço IPv6 hexadecimal. A ideia é fazer a separação da conectividade IPv6 de capacidade de utilizar DNS para isso.

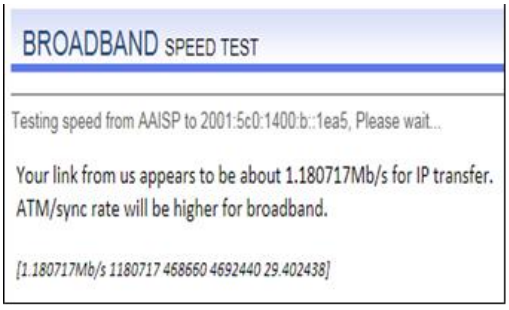
• Teste do servidor DNS do provedor – teste executado no provedor; diz se o servidor DNS (frequentemente mantido em seu provedor) é capaz de acessar servidores DNS autoritativos baseados exclusivamente em IPv6.

• Encontrar provedor de serviços de IPv4 – verifica qual é o ISP de IPv4.

• Encontrar provedor de serviços de IPv6 – verifica qual é o ISP de IPv6.

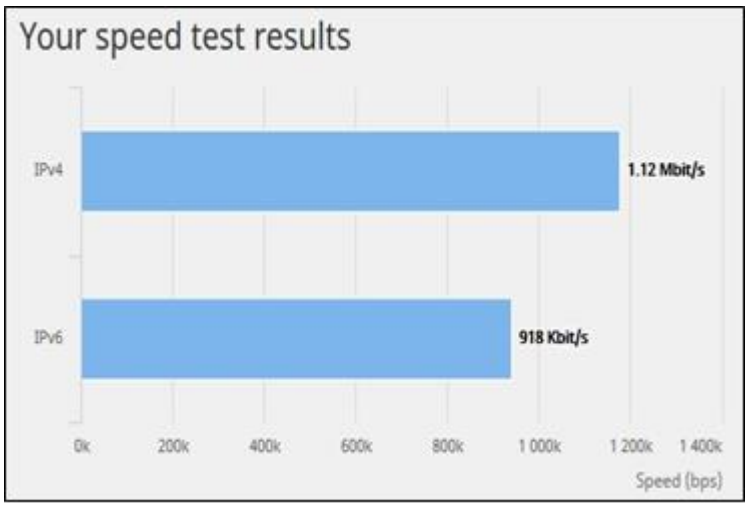
Além dos testes recomendados pela Equipe IPv6 Brasil, outros testes foram realizados para verificar a conectividade deste estudo. Gogo6 recomenda dois: Andrews & Arnold Internet Service e IPv6-Test.com.

Figura 12 - Teste da Andrews & Arnold Internet Service



Fonte: Elaborada pelos autores.

Figura 13 - Teste da IPv6-Test.com



Fonte: Elaborada pelos autores.

Foi realizado um comparativo de velocidade entre as duas ferramentas. Os testes foram realizados em dois dias seguidos, no horário entre 15h00 às 15h20. Em cada minuto foi realizado o teste de velocidade; os primeiros dez minutos com a ferramenta da IPv6-Test.com e os últimos dez minutos com a ferramenta da Andrews & Arnold Internet Service. Ao final do teste, foram registradas as médias de cada dia, conforme Tabela 6 e Tabela 7.

Tabela 6 - Teste de Velocidade: Dia 1

Dia 1			
HORÁRIO	IPv6-Test	HORÁRIO	Andrews & Arnold
	IPv6 - Mbit/s		IPv6 - Mbit/s
15:00	0,918	15:10	1,180717
15:01	2,000	15:11	1,031508
15:02	1,860	15:12	1,070517
15:03	1,390	15:13	0,965544
15:04	1,040	15:14	0,973369
15:05	1,310	15:15	1,807231
15:06	1,800	15:16	1,562378
15:07	2,530	15:17	1,288019
15:08	1,320	15:18	1,567892
15:09	1,420	15:19	1,551537
MEDIA	**1,56**	**MEDIA**	**1,299871**

Fonte: Elaborada pelos autores.

Tabela 7 - Teste de Velocidade: Dia 2

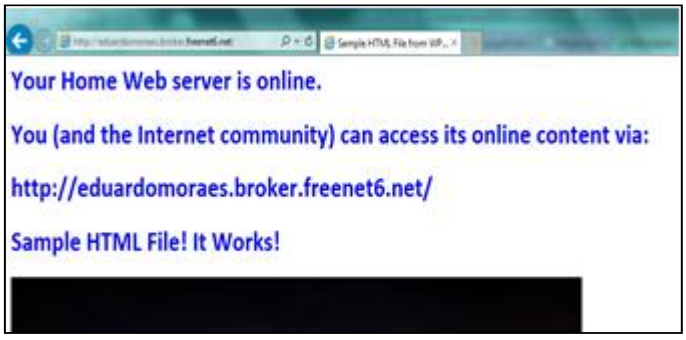
Dia 2			
HORÁRIO	IPv6-Test	HORÁRIO	Andrews & Arnold
	IPv6 - Mbit/s		IPv6 - Mbit/s
15:00	1,150	15:10	1,510506
15:01	0,975	15:11	1,023430
15:02	1,310	15:12	1,666700
15:03	1,020	15:13	1,425670
15:04	1,930	15:14	0,985221
15:05	1,760	15:15	0,900655
15:06	1,400	15:16	1,985725
15:07	0,980	15:17	1,554233
15:08	1,810	15:18	1,388950
15:09	1,270	15:19	1,377975
MEDIA	**1,361**	**MEDIA**	**1,381907**

Fonte: Elaborada pelos autores.

Na ferramenta IPv6-Test.com, no primeiro dia mostrou a velocidade máxima de 2,53 Mbit/s e a mínima de 918 Kbit/s. No segundo dia mostrou máxima de 1,93 Mbit/s e a mínima de 975 Kbit/s. Na ferramenta Andrews & Arnold Internet Service, no primeiro dia mostrou a velocidade máxima de 1,81 Mbit/s e a mínima de 970 Kbit/s. No segundo dia mostrou máxima de 1,99 Mbit/s e a mínima de 900 Kbit/s. Em relação à média, as duas ferramentas mostrou certo equilíbrio no segundo dia de teste, mostrando velocidades próximas uma da outra. Outro resultado importante é que as medições não apresentaram valores constantes ou, pelo menos, próximos uns dos outros, para as duas ferramentas, concluindo-se que a velocidade não é constante.

A aplicação Gogo6 oferece a possibilidade de conectividade ao IPv6, por meio da técnica de tunelamento. Além disto, oferece a possibilidade de transformar o cliente local em um servidor Web para testes em IPv6, através da aba "HomeWeb".

Figura 14 - Teste com a aba "HomeWeb



Fonte: Elaborada pelos autores.

6 Conclusões

Mesmo com todos esses benefícios da nova versão do protocolo IP, a transição do IPv4 para o IPv6 apresenta algumas dificuldades, tais como a mudança do tamanho do endereçamento, instabilidade na velocidade de conexão, atualização dos firmwares dos equipamentos de interconexão de redes que já estão em funcionamento, conhecimento dos técnicos da área de redes de computadores, para prestação de suporte adequado, produção de novo equipamentos que atenda a funcionalidade do novo protocolo; é importante que empresas e instituições de pesquisas acadêmicas comecem os estudos para a utilização do IPv6. Em relação ao processo de transição, estima-se um período em longo prazo para mudança definitiva; até lá, a participação das empresas e das academias interessadas no progresso do IPv6 será fundamental para que este processo aconteça de forma adequada e gradual.

Referências

AHMED, A. S.; HASSAN, R.; OTHMAN, N. E. Security threats for IPv6 transition strategies: A review. **Engineering Technology and Technopreneuship** (ICE2T), 2014 4th International Conference on. IEEE, 2014. p. 83-88.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores**. AMGH Editora, 2009.

BERGAMIN, E.; FERREIRA, J. **Técnica de utilização do mecanismo de transição "Tunnel Broker" para a comunicação do protocolo IPv6 em redes IPv4.** Programa Pós Graduação em Redes e Segurança de Sistemas: Curitiba: Pontifícia Universidade Católica do Paraná, 2003. Disponível: <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS11/Everton%20Bergamin%20_%20TCC%20PUCPR%20_%20Redes%20e%20Seg.%20de%20Sistemas%20_%20Everton%20_%20Jose.pdf >. Acesso em: 21 fev. 2015.

IPV6.BR. **Introdução ao IPv6.** 2012**.** Disponível em: <http://ipv6.br/entenda/introducao>. Acesso em: 21 fev. 2015.

IPV6.BR. **Quem Somos.** 2012. Disponível em: <http://ipv6.br/quem>. Acesso em: 21 fev. 2015.

PV6.BR **Transição IPv6**. 2012. Disponível em: <http://ipv6.br/entenda/transicao>. >. Acesso em: 21 fev. 2015.

FESLER, J. **Testar sua conectividade IPv6.** Test-IPV6.COM, 2015. Disponível em: http://www.test-ipv6.com>. Acesso em: 21 fev. 2015

FINK, R.; HINDEN, R. **6bone (IPv6 testing address allocation) phaseout**. No. RFC 3701. 2004.

GOGO6. **Freenet6 Tunnel Broker**. GOGO6, 2014. Disponível em: <http://www.gogo6.com/freenet6/tunnelbroker>. Acesso em: 21 fev. 2015.

JUNIOR, E. F. **Estratégia de migração para IPV6: análise de implantação do dual stack**. 2014. 53f. Trabalho de Conclusão de Curso (Especialização) – Pós-Graduação em Teleinformática e Redes de Computadores. Universidade Tecnológica Federal do Paraná - UFTPR, 2014. Disponível em: < http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3863/1/CT_TELEINFO_2013_1_03.pdf>. Acesso em: 21 fev. 2015.

KALWAR, S.; BOHRA, N.; MEMON; A. A survey of transition mechanisms from IPv4 to IPv6 - Simulated test bed and analysis. Digital Information, Networking, and Wireless Communications (DINWC), 2015 **Third International Conference on. IEEE**, 2015.

PAMPLONA, E. G.; TOKUNAGA, R. K.: **Transição IPv4/IPv6: técnica de tunelamento**. 2014. 41f. Trabalho de Conclusão de Curso (Graduação) – Curso de Tecnologia em Sistemas de Telecomunicações do Departamento Acadêmico de Eletrônica. Universidade Tecnológica Federal do Paraná - UFTPR, 2014. Disponível em:<http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3417/1/CT_COTEL_2014_1_10.pdf >. Acesso em: 21 fev. 2015.

PETERSON, L. L.; DAVIE, B. S. **Redes de Computadores: Uma Abordagem de Sistemas.** Rio de Janeiro: Elsevier, 2015.

RIVATTO, L.; MANFRON, M. A.; SOLDAN, T. A. **Tunnel IPV6**. 2014. 44f. Trabalho de Conclusão de Curso (Graduação) – Curso de Tecnologia em Sistemas de Telecomunicações do Departamento Acadêmico de Eletrônica. Universidade Tecnológica Federal do Paraná - UFTPR, 2014. Disponível em:<http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3970/1/CT_COTEL_2014_2_04.pdf>. Acesso em: 21 fev. 2015.

WU, P. et al. Transition from IPv4 to IPv6: A state-of-the-art survey. **IEEE Communications Surveys & Tutorials**, v. 15, n. 3, p. 1407-1424, 2013.