EXPERIÊNCIA NO USO DO PROTOCOLO IPv6 COMO SUPORTE PARA A INTERNET DAS COISAS

AN EXPERIENCE OF USING IPV6 PROTOCOL AS SUPPORT FOR THE INTERNET OF THINGS

Henri Alves Godoy[1]

RESUMO
O objetivo dessa experiência realizada na Faculdade de Ciências Aplicadas (FCA) da Universidade Estadual de Campinas (UNICAMP) foi configurar na rede de dados a pilha dupla de protocolos *Internet Protocol version 4* (IPv4) e *Internet Protocol version 6* (IPv6) nos servidores e estações de trabalho. A experiência foi realizada montando-se um tunelamento para encapsular os endereços IPv6 dentro de tuneis IPv4 visto que não possuímos uma conexão nativa de endereços versão 6. Tanto o trânsito de saída como o de entrada foi controlado através de um *firewall* no túnel para melhorar a segurança dos serviços. Foram configurados os principais serviços como resolução de nomes, envio e recebimento de e-mail e páginas web de forma a entender os impactos na inserção desses tráfegos na rede. Como resultado, foi obtida uma velocidade maior nos tráfegos IPv6 em comparação com IPv4 e o convívio amigável entre as duas versões e protocolos. Mesmo não podendo ainda deixar configurado no ambiente somente o protocolo IPv6, a experiência serviu para entendermos melhor o funcionamento deste novo protocolo e as necessidades em termos de software e hardware.

PALAVRAS-CHAVE: IPv6. Tunelamento. 6to4.

ABSTRACT
The purpose of this experiment held at the Faculty of Applied Sciences (FCA) of the State University of Campinas (UNICAMP) was to set up on the data network the dual-stack Internet Protocol version 4 (IPv4) and the Internet Protocol version 6 (IPv6) on servers and workstations. The experiment was carried out by setting up a tunneling server to encapsulate the IPv6 addresses within IPv4 tunnels, since we do not have native connection of version 6 addresses. Both the outgoing and the incoming traffic were controlled through a firewall in the tunnel for providing better safety services. The main ones (such as name resolution, sending and receiving e-mail, and web pages) were configured in order to understand the impact caused by the integration of these kinds of traffic on the network. The result was a higher speed in IPv6 traffic compared to IPv4, and friendly coexistence between these two versions and protocols. Although it is not possible to set up only the IPv6 on the data network, this experiment was valuable to better understand the operation of this new protocol and the needs concerning software and hardware.

KEYWORDS: IPv6. Tunneling. 6to4.

[1] Analista de Redes da Diretoria de Tecnologia da Informação e Comunicação da Faculdade de Ciências Aplicadas da Universidade Estadual de Campinas, campus de Limeira. Graduação em Ciência da Computação pela Escola de Engenharia de Piracicaba. Mestre e Especialista em Redes de Computadores pela Universidade Estadual de Campinas. Limeira, SP. E-mail: henri.godoy@fca.unicamp.br
Submetido em: 12/11/2015 – **Aceito em**: 18/01/2016.

INTRODUÇÃO

O esgotamento de endereços de IPv4 é evidente (LACNIC, 2014) e cada vez mais a nova versão do IPv6 tem sido uma das alternativas viáveis para que a Internet continue crescendo, além de ser a única tecnologia possível para construir a Internet da Coisas. Em um futuro próximo, bilhões de dispositivos (coisas ao nosso redor) serão conectados à Internet. A cada dia novos serviços surgem na Internet e com o IPv4 será impossível atribuir endereços IP a todos esses serviços e dispositivos.

Para que essa transição aconteça, é necessário uma alteração no tamanho do endereço identificador de rede, o IP. Esse tamanho, que no IPv4 é de 32 bits, passa agora na nova versão para 128 bits além da introdução da notação em hexadecimal com 8 palavras e de 16 bits cada, por exemplo: 2801:8a:c040:fca0:2954:5001:6437:7fc8.

A experiência foi motivada primeiramente para adquirir conhecimento sobre o comportamento desse novo protocolo em conjunto com a infraestrutura de rede atual para analisar quais problemas poderíamos encontrar e como nos preparar para a Internet das Coisas. Além disso, seria possível a um docente ou visitante dispor de um endereço IPv6 ativo nas estações de trabalho, caso precisasse acessar alguma pesquisa ou documento fora ou dentro do Brasil que estivesse somente acessível através do protocolo IPv6.

Como a Faculdade de Ciências Aplicadas da UNICAMP (FCA) em 2012 participou do *WorldLaunch* IPv6 (INTERNET SOCIETY, 2012), foi possível colocar o seu *site* principal acessível em IPv6. Com isso, foram gerados questionamentos como: o que aconteceria se ativássemos outros serviços como e-mail e resolução de nomes? Como ficaria a navegação *web* utilizando IPv6? Quais os impactos em relação ao desempenho, problemas de configuração nas estações de trabalho e suporte a esse novo protocolo?

Para responder a todos esses questionamentos, foram realizadas experiências com o protocolo IPv6 em conjunto com a infraestrutura de rede existente. O objetivo principal foi ativar o protocolo IPv6 em diversos serviços básicos como por exemplo: *HyperText Transfer Protocol* (HTTP), *Domain Name System* (DNS), *Post Office Protocol* (POP), *Simple Mail Transport Protocol* (SMTP), *Internet Message Access Protocol* (IMAP). Adicionalmente, havia a intenção de entregar um endereço IPv6 além do endereço IPv4 atual, trabalhando assim em pilha dupla.

Por ser considerada uma unidade remota da UNICAMP, situada na cidade de Limeira – São Paulo, todo nosso tráfego de rede depende de uma conexão até o Centro de Computação em Barão Geraldo – Campinas, através de um enlace de dados fornecido pelo Governo Estadual de São Paulo chamado IntraGov (SÃO PAULO, 2014) o qual fornece hoje apenas trânsito IPv4. Precisávamos então encontrar uma solução para escoar todo tráfego IPv6, além de utilizar o bloco de endereços IPv6 atribuído à FCA para que fosse possível a identificação de qualquer dispositivo de rede como sendo da UNICAMP, no caso de uma auditoria.

Para a realização desse estudo, foi necessário um treinamento da equipe envolvida por meio de um programa oferecido gratuitamente pelo NIC.BR (NIC.BR, 2012), que atualmente dispõe de um programa de treinamento técnico teórico e prático com o objetivo de fomentar a implantação do protocolo IPv6 no Brasil. Os tópicos abordados durante o treinamento foram replicados em um ambiente de teste na FCA antes de serem colocados em produção, de forma a não interferir ou interromper em momento algum o acesso à Internet.

O esforço e o envolvimento da equipe para pode entender o funcionamento do protocolo IPv6 foi necessário para que pudéssemos alcançar os objetivos deste experimento e incluir esse suporte aos usuários no nosso catálogo de serviços.

CONFIGURANDO OS ENDEREÇOS IPv6

A maioria dos sistemas operacionais para *desktops* hoje suportam o protocolo IPv6 nativo em suas configurações de rede. Além disso, outros dispositivos como câmeras, smartphones, roteadores e consoles de jogos já suportam o protocolo IPv6. Para a Internet das Coisas, a tendência é a configuração do endereço IPv6 em roupas, eletrodomésticos e veículos.

As configurações foram realizadas em sistemas operacionais *Windows* e no *Linux* mais especificamente utilizando a distribuição CentOS (THE CENTOS PROJECT, 2015).

Distribuição dos endereços IPv6

Ter um bom plano de endereçamento IP é essencial para a organização e provisionamento de novos dispositivos de rede. De modo diferente do IPv4, não nos preocupamos muito no IPv6 com a falta de endereços, pois é comum a atribuição de bloco de redes inteiras para uma porção pequena de dispositivos.

Ao receber o bloco 2801:8a:c040::/48, foi pensada uma forma de identificar a unidade FCA nos endereços de rede para facilitar a localização dos computadores em caso de uma auditoria. Como agora tratamos com endereços em notação hexadecimal, foi possível embutir no endereço IPv6 a sigla fca no bloco de rede, por exemplo: 2801:8a:c040:**fca**0:8dfc:c9c7:4cff:229. A inclusão dessa localização da unidade no endereço de rede foi elogiada pela equipe de *Computer Security Incident Response Team* (CSIRT) da UNICAMP pois facilita o trabalho na busca e investigação nos diversos endereços que transitam pelos *backbone*.

Uma das primeiras dificuldades encontradas foi como entregar os números IPv6 de forma prática e automática, sem ter que ir à estação de trabalho do usuário e fixá-los manualmente. A entrega dos endereços foi realizada então por meio de processo de Autoconfiguração *stateless* (EQUIPE IPV6.BR, 2015), baseado em informações locais das interfaces de rede

que o identifica e atribuiu um endereço único por meio de mensagens do tipo *Router Advertisement* (RA).

Para o envio das mensagens RA foi empregado o software radvd em um Linux CentOS que atuará como roteador. As configurações foram realizadas no arquivo /etc/radvd.conf conforme ilustra a figura 1.

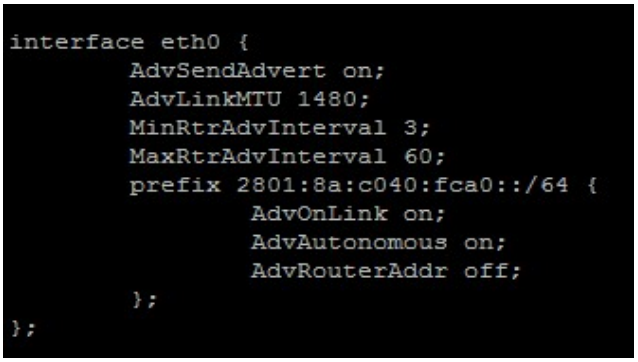


FIGURA 1 – Configuração do serviço radvd.
Fonte: Autoria própria. Imagem capturada no terminal *Linux.*

Ao iniciar o serviço, os *desktops* que estavam com o protocolo IPv6 ativo em sua configuração de rede passaram a receber um endereço IPv6 em conjunto com o endereço IPv4 já atribuído. A resolução de nomes neste momento ficou ainda por conta do protocolo IPv4, pois o serviço radvd não informa no seu processo o endereço do servidor de nomes DNS.

Configurando o Windows Server

Antes de configurar os serviços oferecidos pelos servidores *Windows Server 2008* a responderem os pedidos via protocolo IPv6, é necessário configurar suas interfaces de rede. Por se tratar de servidores, o uso do endereço fixo e não automático é recomendado. A configuração é feita escolhendo a interface de rede e selecionando as propriedades do Protocolo IPv6, conforme figura 2.

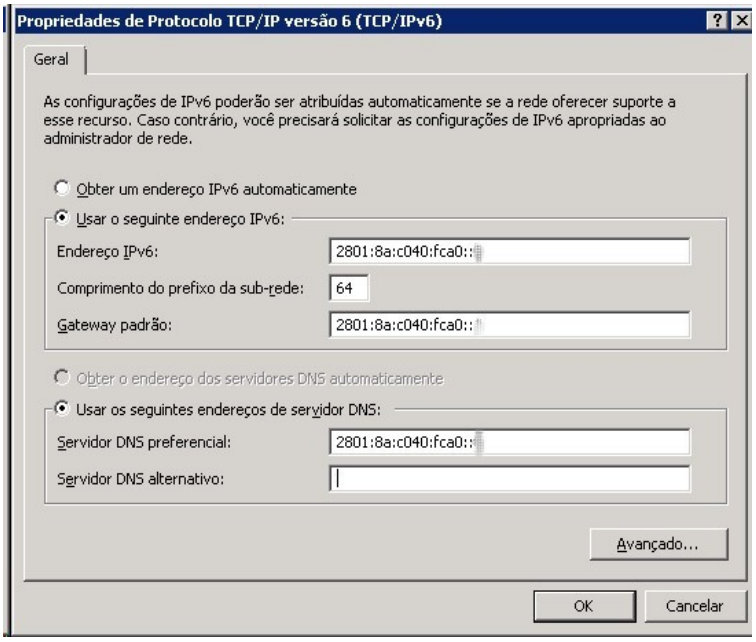


FIGURA 2 – Configuração das propriedades do protocolo IPv6.
Fonte: Autoria própria. Imagem capturada do *Windows Server* 2008.

Os sistemas operacionais *Windows* habilitam por padrão técnicas de tunelamento Teredo e 6to4 (NIC.BR, 2012), que são estabelecidas de forma automática sem que os usuários tenham conhecimento. Tudo isso para que se obtenha conectividade IPv6 através dos relays públicos como por exemplo o IP 192.88.99.1. A figura 3 mostra o dispositivo de rede de um Adaptador 6to4 que podemos encontrar de forma oculta ao listar os dispositivos de rede.

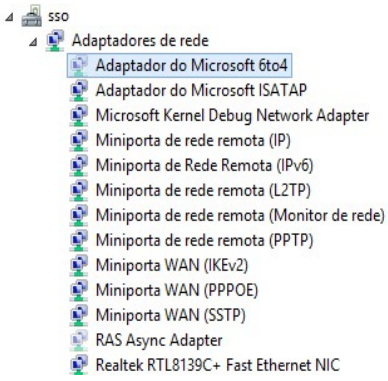


FIGURA 3 – Adaptador oculto de Rede 6to4.
Fonte: Autoria própria. Imagem capturada do *Windows Server* 2008

Em redes acadêmicas ou corporativas esses túneis devem ser desabilitados, pois o tráfego pode seguir caminhos que não passam pelo sistema de *firewall* ou percorrer caminhos diferentes e longos, o que pode degradar a performance de navegação *web*, por exemplo. Todo tráfego tunelado 6to4 é identificado pelo protocolo 41, o qual pode ser aplicado em uma regra no *firewall* de saída, evitando a tentativa de estabelecer tal túnel.

Outra forma bem prática de desativar os túneis automáticos ocorre através da Política de Grupos quando utilizamos uma rede *Windows* com *Active Directory* (AD), conforme ilustra a figura 4.

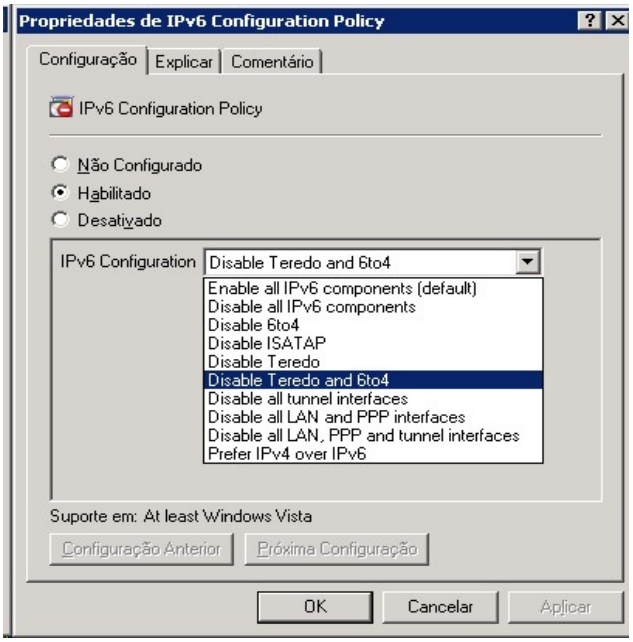


FIGURA 4 – Configuração da política do IPv6 pelo AD.
Fonte: Autoria própria. Imagem capturada do *Windows Server* 2008.

Esse modelo de configuração do IPv6 precisa ser adicionado nas diretivas de grupo e pode ser encontrado para instalação na página da Microsoft Technet (MICROSOFT TECHNET, 2011).

Podemos também desabilitar o túnel diretamente manipulando o registro do *Windows* através de comandos do *powershell* de forma prática quando se precisa de um resultado imediato. A figura 5 mostra o caminho no registro e os valores de cada configuração possível.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
\DisabledComponents (32-bit DWORD value)


Configuration combination                          DisabledComponents value
Disable all tunnel interfaces                                0x01
Disable 6to4                                                 0x02
Disable ISATAP                                               0x04
Disable Teredo                                               0x08
Disable all LAN and PPP interfaces                           0x10
Disable all LAN, PPP, and tunnel interfaces                  0x11
Prefer IPv4 over IPv6                                        0x20
Disable Teredo and 6to4                                      0xA
Disable IPv6 over all interfaces and prefer IPv4 to IPv6     0xFF
```

FIGURA 5 – Configuração através do registro do *Windows*.
Fonte: (MICROSOFT TECHNET, 2011)

A técnica de tunelamento Teredo da *Microsoft* utiliza o protocolo *User Datagram Protocol* (UDP) mais especificamente na porta 3544 para estabelecer a conexão. Em 2014 a *Microsoft* desativou os servidores de relay Teredo em uma tentativa de incentivar os usuários a procurarem um endereço IPv6 nativo.

O estudo e o tratamento prévio desses túneis automaticamente estabelecidos antes da continuação da experiência foram também problemas encontrados, com os quais tivemos que lidar, para que não houvesse interferência nos testes de desempenho e conectividade.

Configurando CentOs *Linux*

A configuração da interface de rede para endereços IPv6 dos servidores de *e-mail* e *web* foi feita de forma manual editando o arquivo /etc/sysconfig/network-scripts/ifcfg-eth0 de cada servidor e depois reinicializando a interface de rede novamente, conforme figura 6.

```
[root@webservice network-scripts]# cat ifcfg-eth0
DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
TYPE=Ethernet
IPADDR=143.106.230.5
NETMASK=255.255.255.0
GATEWAY=143.106.230.1
DNS1=143.106.230.8
IPV6INIT=yes
IPV6_AUTOCONF=no
IPV6ADDR=2801:8a:c040:fca0::5/64
IPV6_DEFAULTGW=2801:8a:c040:fca0::1
NM_CONTROLLED=no
```

FIGURA 6 – Configuração da interface eth0.
Fonte: Autoria própria. Imagem capturada no terminal *Linux*.

Para o servidor *Linux* CentOS que servirá como *gateway* e o túnel 6to4 até o Centro de Computação foi necessário configurar manualmente também o seguinte arquivo /etc/sysconfig/network-scripts/ifcfg-sit1 conforme figura 7.

```
[root@gw-tunnel ~]# cat /etc/sysconfig/network-scripts/ifcfg-sit1
ONBOOT=yes
DEVICE=sit1
BOOTPROTO=none
IPV6INIT=yes
IPV6TUNNELIPV4=143.106.2.
IPV6TUNNELIPV4LOCAL=143.106.230.
IPV6ADDR=2801:8a:2000::2
IPV6_MTU=1280
NM_CONTROLLED=no
```

FIGURA 7 – Configuração da interface do túnel sit1.
Fonte: Autoria própria. Imagem capturada no terminal *Linux*.

O ajuste do parâmetro do *Maximum Transmission Unit* (MTU) em 1280 foi extremamente importante, pois, como se trata de um tráfego tunelado, temos que considerar o cabeçalho encapsulado de cada pacote.

CONFIGURANDO OS SERVIÇOS EM IPv6

Para que fosse possível, após as configurações dos endereços IPv6, a realização de testes no tráfego e navegação *web*, foram escolhidos alguns serviços básicos a serem configurados como servidores de nomes (DNS recursivo e autoritativo), os servidores *web* (protocolos HTTP) e o serviço de *e-mail* (protocolos POP/IMAP/SMTP).

Configurando Serviço Web Apache

O suporte ao IPv6 é aceito pelo Apache desde a versão 2.0.x. A configuração é realizada alterando-se o arquivo de configuração principal httpd.conf, precisamente nas linhas 1 e 2.

Listen 143.106.230.x:80 (1)

Listen [2801:8a:c040:fca0::x]:80 (2)

Em seguida devemos reinicializar o serviço do Apache. Para certificarmos que a configuração foi realizada com sucesso, podemos comprová-la executando o comando *netstat*, o qual deverá retornar à linha 3, caso haja conexão à linha 4.

tcp 0 0 :::80 :::* OUÇA (3)

tcp 0 0 2801:8a:c040:fca0::x:80 2801:8a:c040:fca0:53b:59830 ESTABELECIDA (4)

Configurando o Serviço *Microsoft* DNS

A configuração principal a ser realizada no *Microsoft DNS Server* é ativar a interface de rede IPv6 para que seja feita a ligação do serviço e passar a escutar na porta 53, conforme figura 8.

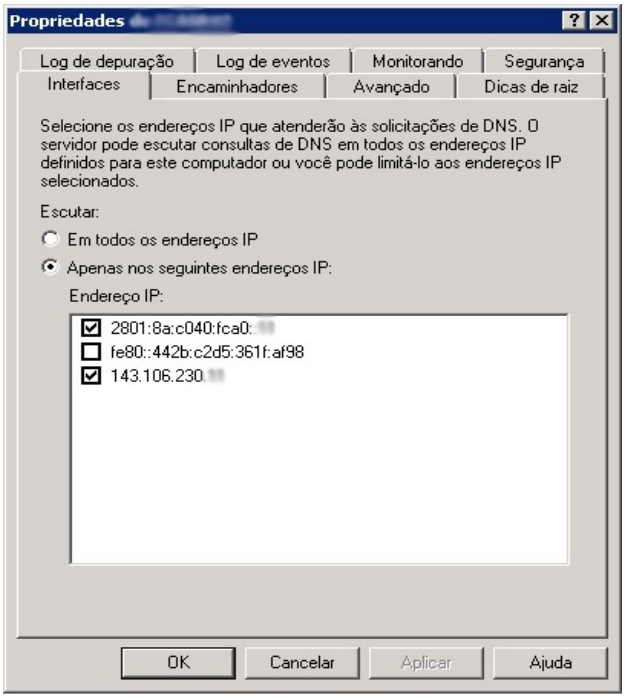


FIGURA 8 – Propriedades IPv6 no *Microsoft DNS*.
Fonte: Autoria própria. Imagem capturada do *Windows Server* 2008.

Após feita essa configuração, a criação das zonas de pesquisa reversa deve ser criada de acordo com o endereçamento IPv6 recebido, conforme figura 9.

FIGURA 9 – Configuração da zona de pesquisa reversa.
Fonte: Autoria própria. Imagem capturada do *Windows Server* 2008.

Foi necessário adicionar o endereço do *Mail Exchanger* (MX) IPv6 do servidor de *e-mail* nas configurações de *Sender Policy Framework* (SPF) no registro TXT do DNS para que problemas de *Sending and Posting Advertisement in Mass* (SPAM) fossem evitados conforme linha 5.

v=spf1 mx ip4:143.106.230.3 ip4:143.106.230.14 ip6:2801:8a:c040:fca0::3 ~all (5)

Configurando Serviço Postfix e Dovecot

O serviço de entrega e recebimento de *e-mails*, utilizando-se o programa *Dovecot* e *Postfix*, pode ser configurado acrescentando no arquivo /etc/postfix/main.cf as linhas 6 e 7.

smtp_bind_address6 = 2801:8a:c040:fca0::3 (6)

mynetworks = 143.106.230.0/24 127.0.0.0/8 [2801:8a:c040::]/48 (7)

Após a adição nas linhas e a reinicialização do serviço, podemos confirmar as configurações realizadas utilizando o comando *netstat*, por meio do qual deveremos obter os resultados da linha 8, relacionados ao protocolo SMTP.

tcp 0 0 :::25 :::* OUÇA (8)

A configuração dos serviços de POP e IMAP é realizada através da edição do arquivo de configuração /etc/dovecot/dovecot.conf, como mostra a linha 9.

listen = *, :: (9)

Novamente com o comando *netstat* podemos ver nas linhas 10 e 11 o resultando das portas habilitadas e prontas para responder uma requisição.

tcp 0 0 :::110 :::* OUÇA (10)

tcp 0 0 :::143 :::* OUÇA (11)

RESULTADOS

Inicialmente foram realizados testes de conectividade entre os endereços IPv6 internos da rede e a interface local. Em todos os testes realizados procurou-se manter um critério de utilização de forma que todos os serviços testados em IPv4 fossem os mesmos testados em IPv6, sem diferença alguma. Os testes de conectividade para fora de rede, através do túnel montado, foram realizados utilizando os comandos *ping* e *traceroute* nos quais foi percebida uma diferença no caminho dos pacotes. A figura 10 mostra o resultado do comando *traceroute* a partir de um *desktop Windows 7* até o endereço do *site* do provedor UOL, utilizando a conexão via IPv6, totalizando 6 saltos.

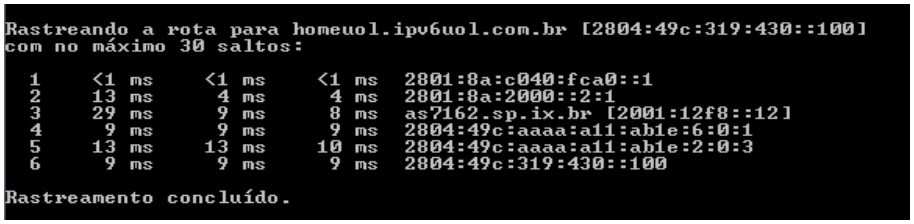


FIGURA 10 – Resultado do comando *netstat* via IPv6.
Fonte: Autoria própria. Imagem capturada no terminal *Linux.*

A figura 11 mostra a execução do mesmo comando até o *site* do provedor UOL, agora utilizando conexão via IPv4. Podemos notar uma grande diferença no trajeto e uma quantidade maior de saltos (13) quando utilizamos o IPv4.

FIGURA 11 – Resultado do comando *netstat* via IPv4.
Fonte: Autoria própria. Imagem capturada no terminal *Linux.*

Ao ativar os serviços de DNS, SMTP, POP e IMAP, percebemos de imediato a troca de tráfego de preferência em IPv6 nas estações de trabalho da rede local. Não demorou muito para recebermos *e-mails* do mundo externo, principalmente de contas do *Gmail* já no formato IPv6, como ilustra o *log* obtido pelo servidor de *e-mail* na figura 12.

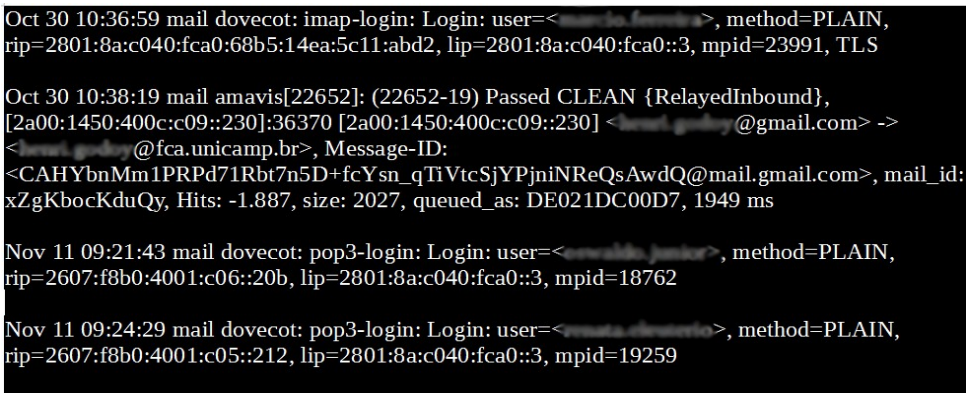


FIGURA 12 – Arquivo de *log* do servidor de *e-mail*
Fonte: Autoria própria. Imagem capturada no terminal *Linux.*

Com a ativação e configuração do servidor DNS, a transferência de zona do bloco IPv6 reverso foi realizada com sucesso para o servidor primário da UNICAMP, conforme figura 13. O serviço de DNS da unidade passou a responder em IPv6 e também propagar os endereços para o mundo.

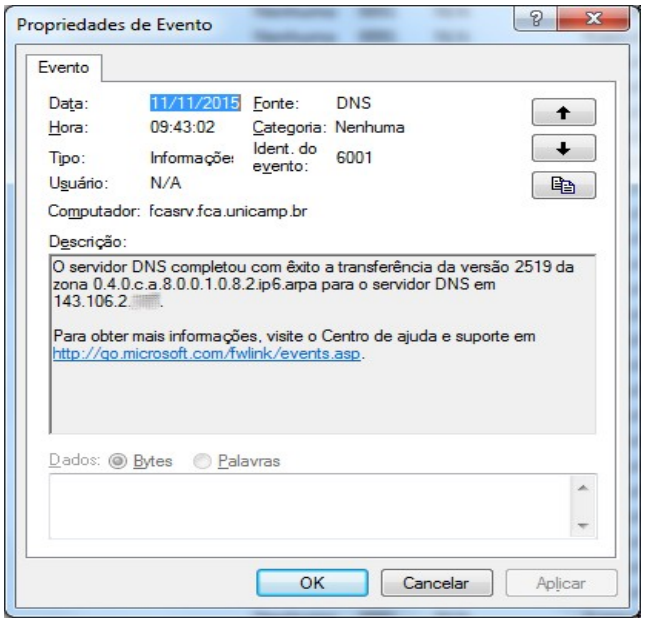


FIGURA 13 – Log do evento de transferência de zona.
Fonte: Autoria própria. Imagem capturada do *Windows Server* 2008.

Verificando os *logs* do serviço *web* no Apache, constatamos o acesso a documentos disponíveis já na página principal da FCA, vindo como endereços de origem em IPv6 conforme figura 14.

```
2804:7f7:a582:1974::2 - - [30/Oct/2015:10:30:45 -0200] "GET
/portal/images/Documentos/FISPQs/FISPQ-%20BicarbonatodeSodio.pdf HTTP/1.1" 200 123008

2a01:4f8:121:34ec::2 - - [30/Oct/2015:10:38:52 -0200] "GET
/portal/images/Documentos/congragacao-1extra-anexo-a.pdf HTTP/1.1" 200 3580824
```

FIGURA 14 – *Log* do acesso do servidor *web*.
Fonte: Autoria própria. Imagem capturada no terminal *Linux*.

Para medição do tráfego IPv6 de entrada e saída, utilizamos a ferramenta *Multi Router Traffic Grapher* (MRTG) (OETIKER, 2011), que começou a coletar as informações a partir de maio de 2015, na interface do túnel criado no servidor CentOS. A figura 15 mostra o tráfego medido até o Centro de Computação.

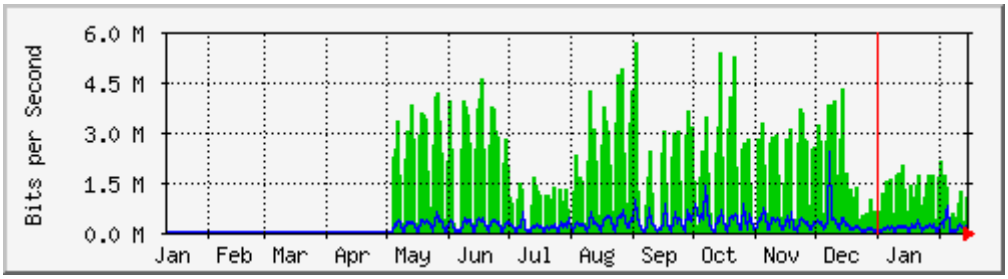
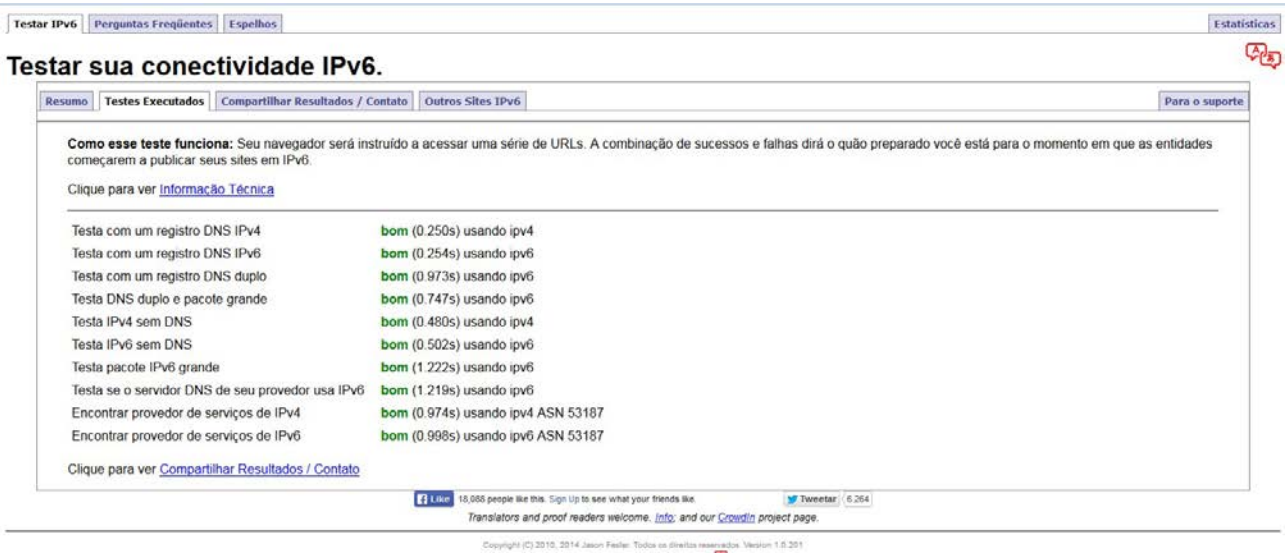


FIGURA 15 – Monitoramento na interface do túnel.
Fonte: Autoria própria. Imagem extraída da ferramenta MRTG

Foram utilizadas, para a execução de testes de conectividade e desempenho, duas ferramentas online durante o período de realização dos testes. A primeira ferramenta, ilustrada pela figura



16, mostra a conectividade do *desktop* e o resultado dos testes para navegação em IPv6.

FIGURA 16 – Teste de conectividade IPv6.
Fonte: Autoria própria. Imagem extraída da ferramenta (TEST-IPV6.COM, 2014)

A segunda ferramenta online mostra uma comparação de velocidade, seguindo o mesmo critério de testes, entre os protocolos IPv4 e IPv6 realizados a partir de uma estação de trabalho *Windows* 7. Percebe-se uma velocidade maior no tráfego IPv6 (2,70 Mbit/s) em comparação com o IPv4 (550 Kbit/s), conforme resultado ilustrado pela figura 17.

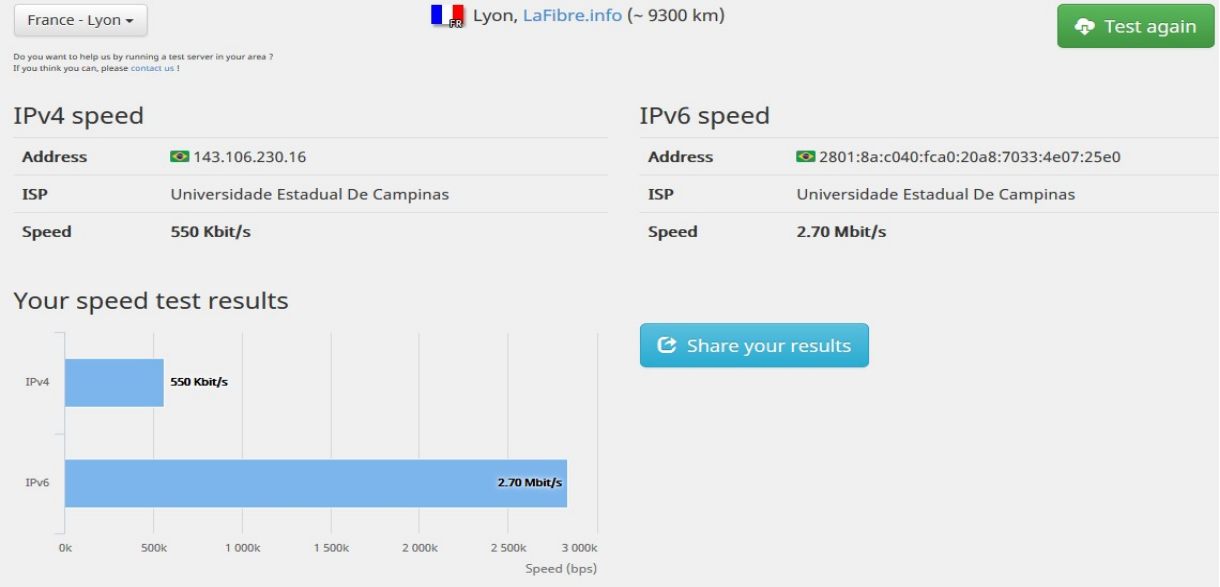
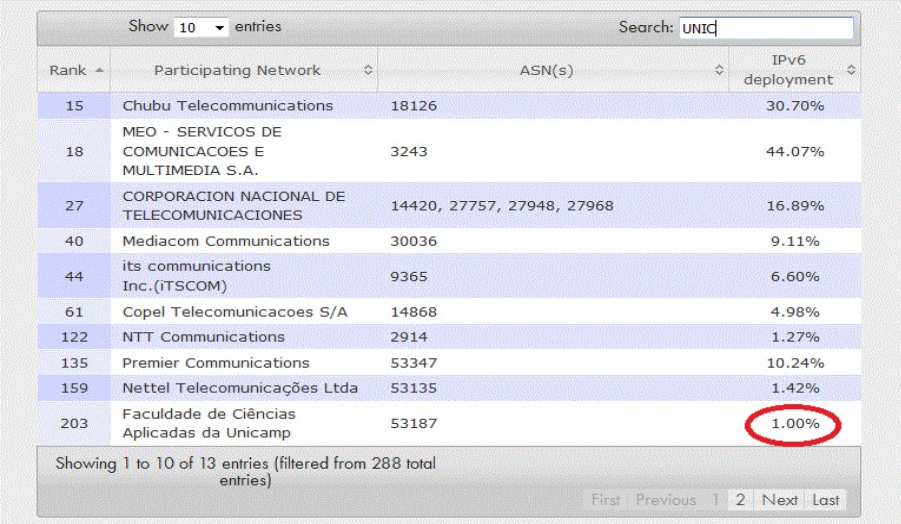


FIGURA 17 – Teste comparativo de velocidade IPv4/IPv6.
Fonte: Autoria própria. Imagem extraída da ferramenta (IPV6-TEST.COM, 2014)

Por segurança, foi necessário aplicar um *firewall* no servidor onde o túnel foi configurado para tratar o tráfego IPv6, pois o *firewall* atual só trata tráfego IPv4. Um *script* padrão sugerido pela equipe do NIC.BR foi utilizado, liberando apenas os tráfegos para os serviços de resolução de nomes, *e-mail* e *web*.

Na estatística gerada pelo projeto *WorldLaunch IPv6* (INTERNET SOCIETY, 2012) em 16 de outubro de 2015, a UNICAMP apareceu no *Ranking* pela primeira vez, confirmando assim o tráfego de dados utilizando o bloco de endereçamento recebido em escala mundial, conforme figura 18.



Show 10 entries Search: UNIC

Rank	Participating Network	ASN(s)	IPv6 deployment
15	Chubu Telecommunications	18126	30.70%
18	MEO - SERVICOS DE COMUNICACOES E MULTIMEDIA S.A.	3243	44.07%
27	CORPORACION NACIONAL DE TELECOMUNICACIONES	14420, 27757, 27948, 27968	16.89%
40	Mediacom Communications	30036	9.11%
44	its communications Inc.(iTSCOM)	9365	6.60%
61	Copel Telecomunicacoes S/A	14868	4.98%
122	NTT Communications	2914	1.27%
135	Premier Communications	53347	10.24%
159	Nettel Telecomunicações Ltda	53135	1.42%
203	Faculdade de Ciências Aplicadas da Unicamp	53187	1.00%

Showing 1 to 10 of 13 entries (filtered from 288 total entries)

First Previous 1 2 Next Last

FIGURA 18 – *Ranking* de acesso *WorldLaunch* IPv6
Fonte: Autoria própria. Imagem extraída do site (INTERNET SOCIETY, 2012) no dia 28/10/2015.

CONCLUSÃO

Durante toda a realização da ativação e configuração dos serviços e endereços, não foram percebidas quedas no desempenho da rede durante o convívio entre os dois protocolos ou indisponibilidade no acesso à Internet. Para o usuário final, não foi percebida a mudança, pois os endereços IPv6 foram entregues de forma automática.

Ainda não foi possível deixar configurado nas estações de trabalho somente o protocolo IPv6, pois o acesso ficaria restrito aos poucos serviços e sites que já estão em IPv6 como *Netflix*, *Youtube*, *Google*, *Facebook*, *Yahoo*, Terra, UOL, *Linkedin* e outros. Porém, é importante que tenhamos já um contato com esse novo protocolo de alguma forma para nos habituar e conhecer seu funcionamento e sua interação com os diversos dispositivos ou “coisas” que poderão surgir.

De forma a dar continuidade à experiência, o próximo passo é a troca de como os endereços IPv6 são entregues para trabalharem junto com o serviço de DHCP*v6 e* desse modo teremos um registro da conexão dos clientes e seus endereços atribuídos. Também será possível a entrega de outras configurações em conjunto com o DHCP*v6*, como por exemplo o endereço do servidor de nomes DNS.

A configuração dos *hardwares* de rede *switches* e roteadores só fará sentido quando tivermos o acesso nativo ao IPv6 e não mais por meio de túnel. Para isso, é necessário que todo o *backbone* da rede IntraGov esteja preparada para a versão 6. Além disso, é de extrema necessidade que os novos equipamentos e dispositivos a serem adquiridos no futuro tenham

já o suporte ao protocolo IPv6 em suas especificações técnicas para que todo o investimento não seja perdido, visto que em algum momento a ativação do IPv6 será necessária.

REFERÊNCIAS

THE CENTOS PROJECT. 2015. Disponível em: <https://www.centos.org/>. Acesso em: 12 nov. 2015.

EQUIPE IPV6.BR **Laboratório de IPv6**: aprenda na prática usando um emulador de redes. São Paulo: Novatec Editora, 2015. p. 35.

INTERNET SOCIETY. **World IPv6 launch**. 2012. Disponível em: <http://www.worldipv6launch.org>. Acesso em: 12 nov. 2015.

IPV6-TEST.COM. IPv6 Test. 2014. Disponível em: <http://ipv6-test.com/>. Acesso em: 12 nov. 2015.

LACNIC. **Esgotamento IPv4**. 2014. Disponível em: <http://www.lacnic.net/web/lacnic/agotamiento-ipv4>. Acesso em: 12 nov. 2015.

MICROSOFT TECHNET. **How to disable IPv6 through group policy.** 2011. Disponível em: <http://social.technet.microsoft.com/wiki/contents/articles/5927.how-to-disable-ipv6-through-group-policy.aspx>. Acesso em: 12 nov. 2015.

NIC.BR . Núcleo de Informação e Coordenação do Ponto BR. **Endereçamento e transição**. 2012. Disponível em: <http://www.ipv6.br/>. Acesso em: 12 nov. 2015.

OETIKER, Tobi. **The multi router traffic grapher**. 2011. Disponível em: <https://oss.oetiker.ch/mrtg/>. Acesso em: 12 nov. 2015.

SÃO PAULO (Estado). Governo do Estado. **IntraGov**. 2014. Disponível em: <http://www.intragov.sp.gov.br>. Acesso em: 12 nov. 2015.

TEST-IPV6.COM. **Testar IPv6**. 2014. Disponível em: <http://test-ipv6.com/>. Acesso em: 12 nov. 2015.