Protocolo IPv6 com pilha dupla em um *campus* universitário

Fernando Barreto[1]

Resumo: Com o esgotamento do endereçamento IPv4 sendo uma realidade, a adoção do IPv6 se torna cada vez mais necessária. Os protocolos IPv4 e IPv6 são incompatíveis e têm questões de operação diferentes, o que torna a implementação do IPv6 relativamente difícil para administradores de rede IPv4. Com o objetivo de reduzir essa dificuldade, este artigo apresenta uma comparação entre IPv4 e IPv6 com foco no dia a dia de administração de rede de *campus*. Esse artigo também apresenta as soluções, experiências e lições adquiridas de uma implementação de sucesso do IPv6, utilizando a técnica de Pilha Dupla em um pequeno *campus* universitário.

Palavras-chave: Administração de rede. Implementação do IPv6.

Abstract: *Due the shortage of IPv4 addresses becoming eminent, the adoption of IPv6 becomes even more necessary. IPv4 and IPv6 protocols are incompatible and have different operational issues, which makes the IPv6 implementation relatively difficult for many IPv4 network administrators. In order to help reducing this gap, this article presents a comparison between IPv4 and IPv6 related to a day-by-day campus network administration. It also presents the acquired experiences and solutions from a successful IPv6 implementation using the Dual-Stack technique in a small university campus.*

Keywords: *Network Administration, IPv6 Implementation.*

1 Introdução

O objetivo da infraestrutura da internet é permitir a troca de informação entre qualquer dispositivo conectado, desde que opere segundo um conjunto de regras padronizadas para a comunicação. Tais regras são definidas por vários protocolos organizados pela pilha TCP/IP. O protocolo dessa pilha responsável pelo endereçamento de cada dispositivo na internet é o Internet Protocol (IP). A versão 4 do protocolo IP (IPv4) [1] surgiu no início da década de 1980 e ainda é o protocolo predominante na internet por ser bem robusto e de fácil implementação pelos administradores de rede [2]. O IPv4 define que qualquer dispositivo com acesso à internet (host) seja identificado por um endereço IP único de 32 bits, que é hierárquico e utilizado nas decisões de roteamento das mensagens entre um host origem e destino. Mesmo com a possibilidade de ter em torno de 4,5 bilhões de endereços IP, desde o início da década de 1990 já existiram preocupações sobre a escassez futura de endereços IPv4. Esse problema teve como origem a política de distribuição desses endereços com base em classes (A, B e C) [1], que foi adotada desde o início da internet, utilizando IPv4 [2].

No início da década de 1990, várias abordagens temporárias surgiram na tentativa de estender o uso do IPv4. Várias delas permitiram a redução da demanda por novos endereços, e a racionalização na forma como eles eram alocados, adiando assim seu esgotamento. Dentre essas soluções, estão o Classless Inter Domain Routing (CIDR) e Network Address Translation (NAT). O CIDR [3] eliminou a distribuição e o roteamento IPv4 que estava fixo por classes, possibilitando a distribuição racional de blocos de endereços IP com tamanho flexível (prefixos de rede e comprimento do prefixo) de acordo com a necessidade. Já o NAT tornou possível o uso de faixas de endereços IP privados [4] para conseguirem acesso à internet. Na concepção original da infraestrutura da internet, as mensagens entre os hosts origem e destino necessitam ter endereços IP válidos, ou seja, endereços que são roteáveis na internet. O NAT, portanto, age realizando a tradução dos endereços privados

[1] Coordenadoria de Gestão de Tecnologia da Informação, UTFPR, *Campus* Apucarana – Apucarana (PR) – Brasil
{fbarreto@utfpr.edu.br}

http://dx.doi.org/10.5335/rbca.2015.4455

em um ou mais endereços IP válidos para que assim os hosts consigam acessar a internet. A abordagem NAT, mesmo sendo amplamente utilizada atualmente, não possui grande escalabilidade, uma vez que afeta e até mesmo impede a operação de vários protocolos da pilha TCP/IP [5]. O VoIP é um exemplo, pois necessita de mecanismos de contorno do NAT, como STUN [6], TURN [7] ou ProxySIP Bridge [8], para disponibilizar algum endereço IP válido para que o protocolo SIP opere corretamente.

Em paralelo a essas abordagens temporárias, também na década de 1990, o documento intitulado *IP: Next Generation (IPng) White Paper Solicitation* [9] formalizou o início das pesquisas para desenvolver um novo protocolo IP, que culminou com o protocolo IP versão 6 (IPv6) [10]. O protocolo IPv6 utiliza 128 bits para endereços IP com o objetivo de resolver os problemas da falta de endereços IPv4. Esse novo endereço IPv6 é também hierárquico e com representação de prefixos de rede similar ao CIDR do IPv4. Além disso, tem um cabeçalho mais simples, fornece vários mecanismos nativos de segurança, mobilidade e autoconfiguração dos hosts. No entanto, o protocolo IPv6 não é compatível com o IPv4 criando várias barreiras para sua adoção natural, como a necessidade de pessoal capacitado, atualizações de firmware e aplicativos, sistemas operacionais, ou até mesmo da substituição de equipamentos. A não compatibilidade entre os protocolos também requer a adoção de alguma técnica de transição para viabilizar a comunicação entre as duas redes mundiais IPv4 e IPv6 [11] [12], até que a rede IPv4 seja substituída no futuro.

Mesmo com o protocolo IPv6 formalizado desde a década de 1990 e com um plano de transição do IPv4 para o IPv6 traçado [13], as abordagens temporárias IPv4 ainda permaneceram e são amplamente adotadas. Essas abordagens começaram a não atender a demanda acarretada pelo crescimento exponencial da internet, e a previsão de escassez de endereços IP se tornou uma realidade a partir do momento que a entidade mundial responsável por distribuir endereços IP (Internet Assigned Numbers Authority (IANA)), distribuiu as suas últimas 5 faixas de endereços IPv4 em 2011 [14]. Cada faixa foi alocada para uma entidade regional (Regional Internet Registry (RIR)) e algumas dessas entidades regionais já começaram a alocar endereços da última faixa que receberam [15]. A América Latina é atendida pela entidade regional Internet Address Registry for Latin America and the Caribbean (LACNIC), e o Brasil tem uma ramificação pelo Núcleo de Informação e Comunicação do Ponto BR (NIC.br). A LACNIC entrou na fase de esgotamento do IPv4 em junho de 2014 e aplica políticas restritivas na alocação da faixa final de endereços IPv4 [16]. Segundo o NIC.br, o esgotamento do IPv4 na LACNIC implica também no esgotamento do IPv4 no Brasil o que resulta em políticas restritivas de alocação para bloco IPv4 final [17], que estão sendo aplicadas pelo Registro.br [52]. Mesmo com esse cenário preocupante, observa-se em algumas estatísticas, como a do Google [18], que o Brasil ainda possui menos de 0,1% de usuários utilizando IPv6.

A escassez eminente de endereços IPv4 fará com que fornecedores de serviços/conexão com a Internet ou utilizem o protocolo IPv6 ou comecem a adotar abordagens temporárias cada vez mais complexas, como por exemplo as que se baseiam no Carrier Grade Nat (CGN) ou NAT444 [19] [21], que, além do NAT no escopo da rede do usuário, utilizam NAT também no provedor de serviço com uma faixa de endereços especial 100.64.0.0/10 (Shared Address Space) [21]. Da mesma forma que o NAT original, o NAT444 prejudica o desempenho ou cria mais barreiras na operação natural de vários aplicativos [22] [23], como VoIP, P2P, Jogos de console entre outros. Qualquer abordagem temporária que estenda o uso do protocolo IPv4 afeta diretamente a forma como a internet foi concebida, uma vez que interfere na concepção de comunicação fim a fim entre origem e destino, criando restrições no desenvolvimento de novas aplicações e podem até inviabiliza-las.

Com objetivo de acelerar a migração para o IPv6, a Anatel planeja acelerar a adoção do IPv6 em 2015, e revela que o grande problema das empresas de telecomunicação no Brasil é o custo da adequação e a falta de capacitação do pessoal técnico [80]. No entanto, o Comitê Gestor da Internet no Brasil (CGI) já havia começado a incentivar a adoção do protocolo IPv6 desde 2007 [14], com foco nos provedores de serviço Internet e nas operadoras de telecomunicações. Recentemente em 2013, o CGI aprovou a resolução CGI.br/RES/2013/033 [24], a qual recomenda a adoção urgente do protocolo IPv6, agora incluindo as universidades. Com base nessa resolução, o *campus* Apucarana da UTFPR começou a investigar e planejar a adoção do protocolo IPv6, sendo o pioneiro dentre todos os *campus* da UTFPR a adotar o IPv6.

Alguns trabalhos relacionados à experiência, à adoção, a melhores práticas do IPv6 em infraestruturas de rede foram encontrados, como [25], [2], [26] [27]. [28] [29], [30]. No entanto, tais trabalhos não apresentam características específicas de IPv6 e IPv4 com foco em administração de redes de *campus* e não apresentam experiências adquiridas no planejamento de uma infraestrutura IPv6. Este artigo tem por objetivo fornecer tais características e apresentar as dificuldades e soluções encontradas durante uma implementação de sucesso do protocolo IPv6 no *campus* Apucarana para auxiliar outras instituições no processo de adoção do IPv6.

Este trabalho apresenta na seção 2 um estudo comparativo entre IPv6 e IPv4 com foco na operação dos protocolos em uma infraestrutura de *campus* universitário. Na seção 3, apresenta-se um planejamento para iniciar a adoção do IPv6. Na seção 4 apresenta-se as experiências da implementação do mesmo no *campus*. Por fim, na seção 5, é apresentada uma síntese das lições aprendidas.

2 Características do IPv6 x IPv4

Pelo fato do IPv6 ser incompatível com o IPv4, um estudo do protocolo IPv6 foi elaborado para entender sua operação com foco nas particularidades da infraestrutura IPv4 existente no *campus* Apucarana. Em termos de cabeçalho, o IPv6 é mais simplificado em relação ao IPv4 e com alguns campos removidos ou renomeados [2]. A diferença principal encontra-se no endereçamento, onde o IPv6 utiliza endereços de 128 bits separados em 8 blocos de 16 bits com ":" representados em hexadecimal, enquanto IPv4 utiliza endereços de 32 bits representados em decimal e separados em 4 blocos de 8 bits com ".". Devido ao grande tamanho do endereço IPv6, é possível utilizar representações que omitem "0" à esquerda nos blocos e simplificam sequências de "0" para facilitar a sua escrita/leitura [31] [32]. Já a representação dos blocos de alocação de endereços IP em IPv6 (prefixos de rede e comprimento do prefixo) é similar ao adotado pelo IPv4, que se baseia na definição da CIDR. Detalhes mais específicos de comparação entre os cabeçalhos IPv6 e IPv4 estão fora do escopo deste trabalho e podem ser encontrados em [31] [2].

O tamanho necessário de Maximum Transmission Unit (MTU) para acomodar um datagrama IP é diferente no IPv6 e no IPv4. O tamanho padrão que um host IPv4 deve considerar é de 576 bytes [1]. Já o IPv6 define um tamanho mínimo de 1280 bytes [10]. Além disso, a especificação [10] fortemente recomenda que qualquer MTU da camada de enlace deva suportar um payload de no mínimo 1500 bytes em redes IPv6.

Além da diferença dos tamanhos de MTUs, o procedimento de fragmentação também apresenta diferenças, uma vez que, ao contrário do IPv4, os roteadores entre os hosts origem e destino não podem fragmentar datagramas IPv6 que excedem a MTU do enlace [10]. Fica, então, a cargo do host origem realizar a fragmentação antes de encapsular os dados nos pacotes IPv6. Para o host origem descobrir qual o tamanho do pacote IPv6, a especificação IPv6 fortemente recomenda o uso da abordagem Path MTU Discovery (PMTUD) [33] com o objetivo de conseguir usar MTU maiores que 1280 bytes na transmissão. No processo da PMTUD, o host considera inicialmente que a MTU inicial é a mesma do seu enlace (geralmente 1500 bytes dos enlaces Ethernet) e envia o pacote. Se houver algum enlace no caminho até o destino com MTU menor, o roteador adjacente a esse enlace descarta o pacote e envia um ICMPv6 Packet Too Big ao host para informar qual o tamanho de MTU a ser usado. Esse processo se repete até o pacote com tamanho ideal chegar ao destino. Consequentemente, a abordagem PMTUD deve ser considerada nas regras de filtragem de Firewall para permitir esse tipo de mensagem ICMPv6.

O PMTUD também existe em redes IPv4 [34], mas fica condicionado ao host origem marcar o bit Don´t Fragment dos pacotes para que os roteadores IPv4 (que devem também suportar [34]) descartem o pacote e, assim, retornem um ICMP Destination Unreachable. Nessa mensagem de retorno, há o valor de MTU a ser usado pelo host origem. No entanto, essa abordagem não é nativa do IPv4 e o uso comum e errôneo de filtros gerais de mensagens ICMP em implementações de Firewalls IPv4 [35] dificultam a adoção dessa abordagem. A filtragem geral e errônea de ICMP é comumente utilizada em redes IPv4, pois quase não influenciam na operação do protocolo IPv4 e acredita-se na redução de possíveis riscos, envolvendo ataques com mensagens ICMP.

Outra diferença entre IPv6 e IPv4 está relacionada com a quantidade mínima de endereços IP, além do endereço loopback, que um host ou roteador necessita para operar corretamente. Em redes IPv4, em sua forma nativa, necessita-se, para cada interface de rede, de um endereço IPv4 unicast hierarquizado e globalmente roteável (ou privado [4] se NAT), com comprimento do prefixo de rede (ou máscara) IPv4 definido. Cada interface pode ser configurada manualmente ou dinamicamente por um servidor Dynamic Host Configuration Protocol (DHCP) [36]. Nesse último caso, para obter um endereço IPv4 dinamicamente o host solicita por um servidor DHCP via broadcast, que ao receber a solicitação, responde ao host com uma mensagem contendo várias informações, e dentre elas o endereço IPv4 e a máscara IPv4 a serem utilizados por determinado momento.

Em redes IPv6, é necessário ter mais de um endereço IPv6 por interface devido à operação do protocolo e aos tipos de endereços IPv6 [37] [31]. Necessita-se de um endereço link-local unicast, pertencente ao prefixo fe80::0/64, por interface (sendo recomendável ter também um endereço global unicast com prefixo hierarquizado

e globalmente roteável pertencente ao prefixo 2000::/3) e atender aos endereços multicast reservados (em especial endereços All-Nodes multicast (ff02::1), Solicited-Node multicast (um para cada endereço link-local unicast e para cada endereço global unicast), e se for roteador, também ao endereço All-Routers multicast (ff02::2) [31]). O endereço link-local unicast é atribuído assim que a interface se tornar ativa e é gerado por um processo de autoconfiguração de endereços link-local [38]. Nesse processo, o endereço link-local é gerado a partir de um endereço de prefixo reservado fe80::0/64 com os últimos 64 bits obtidos a partir do endereço Media Access Control Address (MAC Address) modificado (Modified EUI-64 Format) [31] [39]. O endereço link-local unicast possui apenas validade no segmento de rede local a qual a interface do host se encontra, não sendo hierarquizado ou roteável. O endereço global unicast é atribuído manualmente ou por processo de autoconfiguração de endereços globais [38]. Nesse processo de autoconfiguração, utiliza-se informações contidas em mensagens Router Advertisement (RA) [40] [38], que são geradas por roteadores/gateways localizados no mesmo segmento de rede local. Essas mensagens são enviadas por multicast para o endereço All-Nodes multicast, sendo utilizadas para anunciar aos hosts um ou mais prefixos de endereços global unicast pertencentes ao segmento de rede local. O host, por sua vez, de posse de um prefixo de rede global unicast anunciado, consegue criar, de forma autônoma, seu endereço global unicast a partir desse prefixo e com os 64 bits gerados a partir do endereço MAC Address modificado. Tanto o processo de autoconfiguração de endereços link-local quanto de endereços global unicast são denominados stateless address autoconfiguration [38].

Ainda no processo de autoconfiguração de endereços global unicast, há flags na mensagem RA que podem sinalizar ao host se necessitam ou não de um servidor DHCPv6 para obter informações de configuração [38]. Ao sinalizar a necessidade de um servidor DHCPv6, duas abordagens são possíveis: stateless DHCPv6 [41] ou statefull DHCPv6 [42].

No caso da abordagem stateless DHCPv6, o host configura seu endereço IPv6 normalmente por meio do processo stateless address autoconfiguration e, com isso, obtém informações complementares de configuração através de um servidor DHCPv6, como serviço de DNS e demais serviços de rede [43]. Recentemente, uma extensão denominada Recursive DNS Server (RDNSS) foi padronizada [44] para adicionar informações de serviço de DNS já na mensagem RA. Dessa forma, o host consegue ter toda a informação básica necessária apenas no processo stateless address autoconfiguration, sem necessitar adotar a abordagem de stateless DHCPv6. Evitar o uso de um servidor DHCPv6 é preferível na maioria dos casos (acesso à Internet e serviços básicos de rede) quando não há necessidade de configurações individuais e específicas por host [45], pois toda a informação básica de configuração de host é obtida apenas pela mensagem RA.

No caso da abordagem statefull DHCPv6, o host é sinalizado pela mensagem RA para obter todas as informações de configuração (tanto endereçamento IPv6 quanto complementares) a partir de um servidor DHCPv6 (denominado statefull address autoconfiguration).

Para que qualquer processo de autoconfiguração ocorra corretamente, deve-se utilizar um tamanho de prefixo em cada segmento de rede de no máximo /64 [28]. Dessa forma, torna-se possível preencher os demais 64 bits restantes a partir do identificador de interface [31] [39], que em geral é o MAC Address modificado.

Em relação às redes IPv4 nativas o processo de autoconfiguração é inexistente. No entanto, esse recurso foi disponibilizado recentemente [46] ao definir uma faixa de endereços 169.254/16 a ser usada na geração de um endereço IPv4 para uma interface quando o host não localizar um servidor DHCP. Esse endereço é gerado de forma similar ao stateless address autoconfiguration do IPv6, e tem validade apenas para o segmento de rede local.

Além do endereçamento IP, os hosts geralmente necessitam de informações de roteamento para encaminhar mensagens destinadas aos hosts externos, ou seja, que não pertencem ao prefixo de rede do segmento de rede local do host. Essas informações significam que, no mínimo, um endereço IP de gateway deve ser configurado como next-hop para alcançar os hosts externos. Em redes IPv4, configura-se o endereço de gateway manualmente ou via informações obtidas por DHCP. Em redes IPv6, configura-se o endereço de gateway manualmente ou por meio do processo de autoconfiguração. Nesse último caso, a mensagem RA enviada por um roteador/gateway já indica que esse é um candidato a gateway, ou default router, se o campo Router Lifetime do RA contiver um valor maior que zero [40].

A operação do IPv6 para localizar hosts vizinhos em segmentos de redes locais (enlace local, domínio de broadcast em redes Ethernet ou segmento de Virtual LAN (VLAN)) possui também várias particularidades em relação à operação do IPv4. Em redes IPv4 cada host faz uso do protocolo Address Resolution Protocol (ARP) [47], que utiliza broadcast Ethernet para descobrir o MAC Address de um endereço IPv4 vizinho. No caso do

IPv6, utiliza-se o protocolo Neighbor Discovery Protocol (NDP) [40], o qual faz uso de mensagens multicast ICMP sobre multicast Ethernet no processo de resolução de endereço MAC a partir de um endereço IPv6. Nesse processo, é utilizada uma mensagem de Neighbor Solicitation para o endereço de destino Solicited-Node multicast. Todos os hosts IPv6 devem atender aos endereços multicast reservados IPv6, mas somente o host responsável por esse endereço Solicited-Node multicast responde com ICMP Neighbor Advertisement ao host origem. Esse, por sua vez, consegue então enviar uma mensagem IPv6 para o MAC Address de destino correto. Observa-se que, da mesma forma que no processo de autoconfiguração, o NDP também utiliza endereços multicast reservados para as mensagens ICMP, tornando-se necessário ter uma atenção extra na configuração de filtragem de Firewalls dos hosts e roteadores. É importante ressaltar que filtrar mensagens ICMP indiscriminadamente compromete o funcionamento do IPv6, tanto que recomendações de filtragem ICMP foram divulgadas [49] e que são fortemente recomendadas para serem seguidas. Há ainda um exemplo de configuração para ser usado como regras de Ip6Tables no Linux [49].

O NDP também é utilizado na detecção de endereço IPv6 duplicado antes de realizar qualquer atribuição de endereço unicast a uma interface (automático ou manual). A detecção ocorre mediante uma consulta no segmento de rede, enviando uma mensagem Neighbor Solicitation destinada ao próprio endereço de destino Solicited-Node multicast. Se outro host responder a essa mensagem, então o endereço unicast em questão já foi alocado. Outros detalhes mais específicos sobre a operação do NDP podem ser encontrados em [40] e [38].

Ainda em relação à detecção prévia de endereços IP duplicados, esse processo não era realizado nativamente pelo protocolo ARP em redes IPv4, mas apenas recentemente uma expansão na operação do protocolo ARP foi padronizada para realizar tal tarefa [48].

A Tabela 1 sintetiza a comparação das principais características levantadas a respeito das características de operação do IPv4 x IPv6.

Tabela 1: Características principais IPv4 x IPv6

Características	IPv4	IPv6
Endereço IP	32 bits, organizado em 4 grupos de 8 bits no formato decimal e separados por ".". Ex: 192.168.0.10	128 bits, organizado em 8 grupos de 16 bits no formato hexadecimal e separados por ":". Pode-se simplificar "0" à esquerda e sequências de "0". Ex: a representação 2001:db8:1:0::a é a mesma que 2001:0db8:0001:0000:0000:0000:0000:000a
Tamanho da MTU usado pelo datagrama IP	576 bytes	1280 bytes
Fragmentação	Host origem e roteadores intermediários	Somente no host origem
Path MTU Discovery	Não é nativo	Fortemente Recomendado [10]
Quantidade mínima de Endereços IP necessários por interface (tanto host quanto roteador)	1 Endereço Hierárquico (privado ou global)	1 Endereço Link-Local unicast + 1 Endereço Global unicast + 1 Endereço All-Nodes multicast + Endereços Solicited-Node multicast (um para cada endereço unicast), e se for roteador, + 1 Endereço All-Routers multicast
Configuração Básica IP (Endereçamento, Rota Default/Gateway, DNS	Manualmente ou DHCP	Manualmente ou por Autoconfiguração (podendo utilizar stateless DHCPv6, statefull DHCPv6 ou RDNSS). Autoconfiguração requer um prefixo de rede de no máximo /64 [28]
Localizar hosts/ roteadores vizinhos no segmento de rede local	Protocolo ARP, utilizando broadcast Ethernet	Protocolo NDP, utilizando multicast ICMP (Endereços Multicast Reservados) e multicast Ethernet
Detecção de endereço IP duplicado	Não é nativo, mas é possível [48]	Fornecido pelo NDP antes de atribuir um endereço IPv6 para uma interface
Firewall ICMP	O bloqueio não afeta o funcionamento básico do IPv4	Deve ser considerado, pois afeta a funcionalidade básica do NDP e da autoconfiguração
NAT/Carrier Grade Nat	Comumente utilizado pela falta de endereços disponíveis. Utiliza endereços privados [4] e [21]	Não é necessário

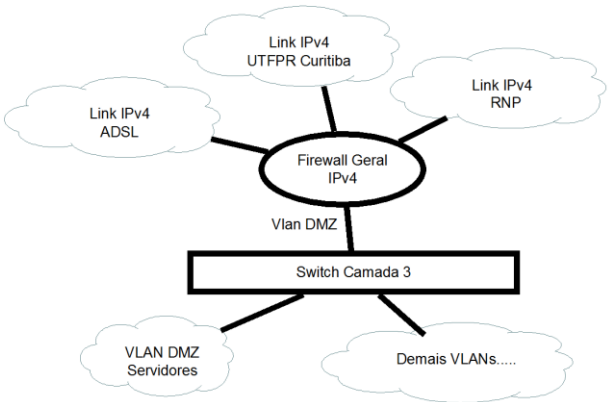
3 Planejando a implementação IPv6 em uma rede de *campus* universitário

Com as principais características do IPv6 apontadas, é necessário analisar a infraestrutura de rede IPv4 do *campus* para iniciar o planejamento da implementação do IPv6.

3.1 Infraestrutura IPv4 legada

A infraestrutura de rede IPv4 do *campus* Apucarana está composta na sua grande maioria por switches gerenciáveis de camada 2 e por um switch camada 3. Existem também pontos de acesso sem fio espalhados pelo *campus* e gerenciados por um switch controlador. Toda a infraestrutura utiliza VLANs com o padrão IEEE 802.1q gerenciados pelo switch camada 3, que separa logicamente todas as sub-redes IPv4 e realiza roteamento entre as mesmas mediante filtragem por Firewall no próprio switch. O endereçamento IPv4 utiliza endereços privados [4] com acesso à Internet via NAT, uma vez que o *campus* possui poucos endereços IPv4 válidos. Os equipamentos servidores estão organizados em máquinas virtuais e fornecem serviços básicos TCP/IP (DHCP, DNS), LDAP, proxy web, arquivos (protocolo SMB), sistema Web e ambiente Moodle. Dentre esses serviços, o proxy web, DNS, sistemas Web e ambiente Moodle situam-se na DeMilitarized Zone (DMZ). Utiliza-se também um Firewall geral implementado com Linux/IpTables para filtragem de tráfego das VLANs e DMZ para internet e vice-versa. O acesso à internet por meio de IPv4 é provido por 3 enlaces diferentes. O primeiro está conectado à infraestrutura de rede voltada para a comunidade brasileira de ensino e pesquisa, denominada Rede Ipê, fornecida pela Rede Nacional de Pesquisa (RNP). O segundo é um enlace fornecido pela própria UTFPR para acesso direto ao *campus* Curitiba da UTFPR. O terceiro é um acesso ADSL do Projeto Banda Larga nas Escolas [50]. A Figura 1 ilustra como está a infraestrutura de rede IPv4 no *campus* Apucarana.

Figura 1: Infraestrutura IPv4 legada



Os hosts conectados a essa infraestrutura do *campus* se classificam como desktops e dispositivos móveis via Wireless (notebooks, celulares, tablets). Os desktops são equipamentos do próprio *campus* e na sua maioria utilizam sistemas Windows, dividindo-se em 80% Windows 7, 18% Windows XP, e 2% Linux (Ubuntu). Os dispositivos móveis são na sua maioria laptops com Windows 7, 8 ou 8.1.

3.2 Conectividade com a rede mundial IPv6

O projeto Rede Ipê fornecido pela RNP já disponibiliza acesso nativo à rede mundial IPv6 [51]. Para conseguir tal acesso, basta a instituição ter algum vínculo com a RNP, conforme política dessa [51]. Como o *campus* Apucarana pertence à UTFPR que é uma instituição primária vinculada à RNP, tornou-se possível adquirir uma faixa de endereços IPv6 entrando em contato com o Ponto de Presença no Estado do Paraná (POP-PR) da RNP. A política para alocações dos blocos IPv6 são definidas de acordo com o órgão responsável. No caso, a LACNIC atribuiu a responsabilidade da alocação dos blocos IPv6 no Brasil para a NIC.br, que por sua vez delegou tal tarefa ao Registro.br. A política de alocação IPv6 adotada pelo Registro.br [52] informa que os provedores de serviços podem receber blocos /32, como é o caso do POP-PR (AS10881) que detém o bloco 2801:82::/32. Já os usuários finais (aqueles que utilizam os endereços IPv6 em suas próprias infraestruturas) conectados aos provedores de serviços, podem receber no mínimo um bloco /48 e no máximo um /32 conforme justificativa. Por conta dessas políticas, um bloco /48 foi alocado pelo POP-PR para o *campus* Apucarana da

UTFPR. É importante ressaltar que essa política de alocação teve como base recomendações da IETF [53] [28], no entanto pode ser modificada por uma recomendação recente da IETF [54], que sugere uma distribuição mais racional dos blocos IPv6 conforme a necessidade dos usuários finais (blocos /48 para usuários corporativos e /56 ou /64 para usuários domésticos). Tal recomendação também é sugerida pela equipe IPv6.br [55].

3.3 Verificação de equipamentos e softwares legados com suporte ao IPv6

É necessário que os equipamentos contenham firmwares com suporte ao IPv6 para poder adotá-lo. Atualmente, a grande maioria dos switches de médio e grande porte tem algum suporte. No caso do *campus* Apucarana, todos os switches gerenciáveis do *campus* foram verificados e todos os firmwares atualizados já apresentam suporte ao IPv6. Os softwares aplicativos utilizados nos equipamentos servidores do *campus* também têm suporte ao IPv6, bem como os sistemas operacionais de rede utilizados. Os softwares dos hosts clientes dependem basicamente do suporte do sistema operacional ao IPv6, uma vez que a maioria dos serviços utilizados está vinculado a navegadores Web (Firefox, Internet Explorer e Chrome), cujas versões instaladas já têm suporte ao IPv6. Em relação ao suporte do sistema operacional dos hosts, apenas o Windows XP necessita de no mínimo o Service Pack 2. Os demais sistemas Windows utilizados e Linux possuem suporte ao IPv6.

3.4 Sub-redes IPv6

A partir do bloco /48 alocado pelo POP-PR, é necessário realizar um planejamento do seu uso. Mesmo tendo uma gigantesca quantidade de endereços IPv6, existem algumas questões levantadas nas seções anteriores que precisam ser observadas para evitar problemas futuros. A primeira questão refere-se ao tamanho das sub-redes, que não devem ultrapassar o prefixo /64 por conta da atribuição automática de endereços IPv6 (tanto endereços link-local unicast quanto global unicast). Por conta dessa restrição, adota-se uma prática comum na gerência de endereços IPv6, que recomenda o planejamento de quantas sub-redes /64 pode-se gerenciar e não mais quantos endereços IPv6 estão disponíveis, como é realizado em redes IPv4 [2]. Nesse caso, a partir de um bloco /48 pode-se alocar no máximo 65536 sub-redes /64.

A segunda questão refere-se à organização das sub-redes IPv6 para evitar desperdício na alocação. Existem recomendações da IETF [28] [58] para organizar a separação das sub-redes IPv6 de forma a deixá-las escaláveis, com possibilidade de agregação de rotas e evitando assim uma futura reestruturação de sub-redes já atribuídas. Tal recomendação é parecida com a existente em redes IPv4 [59]. A última questão refere-se à infraestrutura já existente com IPv4 no *campus* Apucarana, que foi apresentada na Seção 3.1. Para manter a infraestrutura IPv4 operante, realizou-se a separação das sub-redes IPv6 em blocos /64 para essas VLANs planejando uma agregação de faixas dos blocos de endereços dos alunos, administrativos, professores, enlaces e DMZ para uma possível expansão ou segmentação futura. Sabe-se que o plano de sub-redes depende da necessidade e política de cada instituição, mas a título de exemplificação do que foi adotado, segue na Tabela 2 uma sugestão explicativa a partir de uma faixa 2001:db8:1:/48. O site do IPv6.br [78] disponibiliza um recurso para auxiliar a visualizar a alocação das sub-redes de acordo com a recomendação da IETF [58].

Tabela 2: Exemplo de um plano de sub-redes IPv6

Blocos principais	Descrição
2001:db8:1:0000:/52, com possibilidade de expansão até um /49 por conta do bit mais significativo do "0000"	Sub-redes /64 para: DMZ, Enlaces ponto a ponto entre equipamentos de interconexão (a ser usado /127 [60] de uma faixa /64), Administração de rede, VoIP, Impressoras, Wireless (administrativos / professores).
2001:db8:1:8000:/52, com possibilidade de expansão até um /49 por conta do bit mais significativo do "8000"	Todas essas sub-redes /64 com alocação de bits para permitir expansão (conforme recomendação [58]).

3.5 Técnicas de transição IPv4 para IPv6

Como a grande maioria dos serviços da internet ainda utiliza IPv4 [56] [57], esse acesso necessita ainda ser mantido. Faz-se necessário escolher alguma técnica de transição já consolidada dentre as disponíveis. Existem vários trabalhos que já apresentaram comparações aprofundadas entre essas técnicas, como [11] e [12],

e outras mais objetivas como a fornecida pelo material do IPv6.br [2]. Portanto, foge do escopo deste trabalho apresentar novamente essa comparação.

Pelo fato de o *campus* Apucarana já ter uma faixa de endereços IPv6 com acesso direto à rede mundial IPv6, optou-se por utilizar a técnica de transição de Pilha Dupla. Essa técnica é recomendada para ser usada sempre que for possível [2], e consiste em ter a implementações da pilha IPv4 e IPv6 operantes ao mesmo tempo em um host ou roteador. Isso torna o host ou roteador apto a enviar e receber pacotes usando IPv4 ou IPv6. Além disso, o uso da pilha dupla possibilita a adoção da abordagem Happy EyeBalls [77], o qual recomenda um algoritmo para as aplicações escolherem endereços IPv6 e IPv4 a partir do DNS de forma a melhorar a experiência do usuário no acesso a redes IPv6, quando disponível. Para utilizar Pilha Dupla, é necessário também configurar corretamente o serviço de DNS, Roteamento/Gateway, Firewalls e protocolos de roteamento da infraestrutura. Maiores detalhes são apresentados na Seção 4. É importante realçar que nesse planejamento para implementação, procurou-se deixar os mesmos serviços originais IPv4 também disponíveis em IPv6 para facilitar a migração gradual.

4 Experiências da implementação do IPv6 no *campus* Apucarana da UTFPR

Mesmos com os sistemas operacionais mencionando suporte nativo ao IPv6, foi detectado que esses possuem ou suporte parcial ou até mesmo incompleto em alguns casos, o que diverge das recomendações fornecidas pela IETF [79]. Todos os equipamentos servidores do *campus* foram definidos com endereços IPv6 manualmente e todos operaram corretamente conforme previsto pelo suporte dos softwares.

Em relação ao servidor de arquivos (protocolo SMB), detectou-se que o Windows XP não possui suporte nativo [61], necessitando obrigatoriamente da pilha IPv4 para acessar esse tipo de serviço. Os sistemas Windows 7 e Linux conseguem operar corretamente com SMB em IPv6.

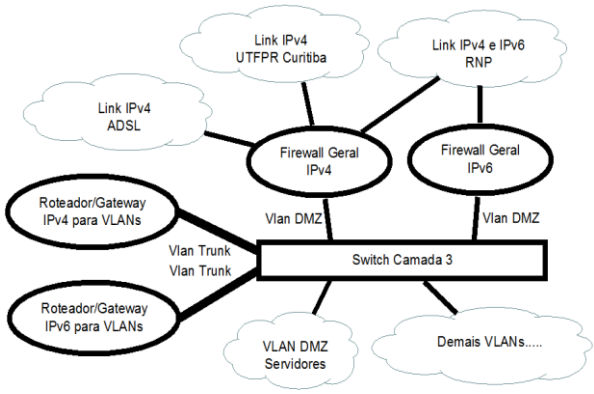
Em relação ao procedimento de autoconfiguração dos hosts clientes, tanto stateless DHCPv6 quanto statefull DHCPv6, detectou-se que não são suportados nativamente pelo Windows XP (mesmo com Service Pack 3), o que impede de obter informações do serviço de DNS a partir do DHCPv6. Essa restrição não atinge sistemas Windows 7 e Linux, e no caso do Windows XP, tal restrição está localizada no site da Microsoft [61]. Para contornar essa restrição no Windows XP, é necessário utilizar obrigatoriamente a pilha IPv4 para obter as informações do DNS por meio do serviço DHCP. Já o suporte nativo ao RDNSS é inexistente tanto no Windows XP, quanto Windows 7 e Linux. Em todos os casos, é possível contornar essas restrições por meio de softwares de terceiros [62], [63], [64], o que não é interessante para administradores de rede devido à dificuldade em realizar manutenções padronizadas das configurações de equipamentos do *campus*.

Para os hosts configurarem o IPv6 por autoconfiguração, é necessário ter ao menos um roteador/gateway IPv6 no segmento de rede do host que anuncie mensagens RA conforme descrito na Seção 2. Como as redes estão segmentadas em VLANs, existe um roteador/gateway IPv6 em cada VLAN para roteamento e filtragem de tráfego (Firewall). Optou-se, inicialmente, em utilizar o switch de camada 3, que já realizava tal tarefa na infraestrutura de rede IPv4. No entanto, verificou-se que o switch apresentava apenas suporte de mensagens RA para stateless address autoconfiguration (com flag para stateless DHCPv6 ou statefull DHCPv6), não possuindo suporte ao RDNSS. Além disso, as regras de filtragem IPv6 poderiam aumentar a carga de processamento no switch de camada 3 futuramente, uma vez que esse é de pequeno/médio porte e não possui um hardware dedicado para operar como um Firewall completo. Por conta dessas limitações, resolveu-se retirar a função de roteador/gateway e Firewall IPv6 desse. Dessa forma, implementou-se um roteador/gateway IPv6 com um sistema Linux/Ip6Tables para fornecer roteamento, Firewall e, com o aplicativo Router Advertisement Daemon (RADVD) [65], para o anúncio de mensagens RA com suporte ao RDNSS. Esse roteador/gateway tem várias interfaces de rede físicas configuradas com VLAN trunk (habilitadas para marcação de pacotes) e conectadas ao switch de camada 3 (também com trunk). Cada interface de rede física tem várias interfaces de rede virtuais, cada uma representando um roteador/gateway de uma VLAN. O RADVD é configurado para enviar mensagens RA com suporte ao RDNSS para cada prefixo de rede definido nas VLANs. Como os sistemas operacionais dos hosts, atualmente, não possuem suporte nativo ao RDNSS, anuncia-se também a opção de autoconfiguração stateless DHCPv6. Grande parte das configurações já existentes no Firewall IPv4 do switch de camada 3 foi migrado para o Firewall IPv6, fazendo as adaptações necessárias e também obedecendo às recomendações para o funcionamento de autoconfiguração, NDP e PMTUD, conforme apresentado na seção 2. Mantém-se dessa forma

um único serviço RADVD, roteamento e Firewall de pacotes entre as VLANs IPv6. Como esse sistema Linux foi inserido em uma máquina virtual, tem-se imagens backup para caso de substituição do equipamento servidor.

Como os hosts não têm ainda suporte ao RDNSS e foi utilizado a opção de autoconfiguração stateless DHCPv6, faz-se necessário ter um servidor DHCPv6 para fornecer as informações complementares de configuração IPv6 referentes ao serviço de DNS. Esse servidor DHCPv6 (utilizou-se o ISC DHCP [66]) está localizado no roteador/gateway IPv6 e configurado para cada VLAN definida. Além do serviço de DNS, o DHCPv6 pode oferecer informações aos hosts clientes sobre outros serviços como NTP, SIP, entre outros [43]. Por conta da configuração do roteador/gateway IPv6 e para ter uma maior facilidade de sua manutenção, o recurso de roteamento/firewall entre as VLANs IPv4 do switch de camada 3 foi removido para ser configurado em um roteador/gateway com Linux idêntico ao adotado na rede IPv6. Consegue-se, então, realizar tanto roteamento quanto filtragem por Firewall do tráfego IPv4 entre as VLANs sem utilizar recursos do switch de camada 3. A Figura 2 ilustra a nova infraestrutura IPv4 e IPv6 no *campus*.

Figura 2: Infraestrutura modificada IPv4 e IPv6



Por fim, em relação ao serviço de Proxy e DNS, foi necessária uma investigação mais rigorosa com detalhes, apresentados a seguir, para utilizar Pilha Dupla.

4.1 DNS

Da mesma forma que em redes IPv4, o serviço de DNS é importante em redes IPv6. No caso da técnica da Pilha Dupla, o DNS deve prover resolução de nomes direto e reverso para ambos IPv4 e IPv6, independente se a consulta por parte do host for feita por meio do IPv4 ou IPv6. Existem vários softwares que fornecem tal serviço, e no caso do *campus* Apucarana utiliza-se o BIND versão 9 [67], o qual já possui suporte nativo ao IPv6.

As configurações referentes ao IPv6 para resolução direta (de nome para endereço IP) são realizadas no mesmo arquivo de configuração do IPv4, uma vez que pertencem à mesma zona DNS do domínio do *campus* Apucarana. Os endereços IPv6 são definidos por entradas "IN AAAA" [68] e podem ser adicionadas em uma nova linha, após uma entrada "IN A" do endereço IPv4 já existente, não replicando o nome do host. Com essa abordagem, a resolução do nome de um host servidor pode ser tanto em endereço IPv4 quanto IPv6. Quem decide por qual entrada deve ser consultada é o host cliente que está realizando a consulta. Até o momento, foram configurados manualmente entradas IPv6 apenas para os servidores e equipamentos de interconexão do *campus*.

Para a configuração do reverso (de endereço IP para nome), cada rede, IPv4 e IPv6, possui a sua configuração em arquivos diferentes por serem blocos de endereços em zonas DNS reversas diferentes (cada um para uma faixa IP). O reverso do IPv6 utiliza domínio ip6.arpa e faz uso da notação em nibbles [68], ou seja, cada número hexadecimal do endereço IPv6 invertido separado por ".". Da mesma forma que na resolução direta, foram inseridas entradas manualmente de IPv6 reverso apenas para os servidores e equipamentos de interconexão do *campus*. Tanto o Dynamic DNS [69] e Domain Name System Security Extensions (DNSSEC) [70] não são abordados nesse trabalho por ainda estarem em fase de estudo no *campus* Apucarana.

4.2 Proxy Web

O serviço de proxy Web é utilizado no *campus* para atuar como intermediário nas requisições dos hosts e assim aplicar regras de filtragem de conteúdo acessado via Web bem como serviço de cache. Esse serviço é fornecido por meio do aplicativo Squid, que já possui suporte nativo ao IPv6 na versão 3.1 [71].

O serviço de proxy Web em redes IPv4 do *campus* é configurado nos hosts mediante duas abordagens: Web Proxy Autodiscovery Protocol (WPAD) [72] [73] e proxy web transparente [73]. A abordagem por WPAD opera com o mecanismo de autodetecção de proxy Web nos hosts, que está habilitado por padrão nos navegadores web homologados pelo *campus*. Nessa abordagem, os navegadores obtêm as informações do serviço de proxy Web a partir de um arquivo de script Proxy auto-config (PAC), que é localizado a partir de um URL específica. Essa URL pode ser obtida, ou através da opção 252 do serviço DHCP [72], ou a partir de uma consulta à URL "http://wpad.dominio/wpad.dat", onde wpad.dominio é resolvido por uma consulta DNS (servidor "wpad" localizado na zona DNS "domínio do *campus* Apucarana"). Maiores detalhes sobre o WPAD podem ser encontrados na IETF [72]. Já a abordagem de proxy Web transparente funciona através da interceptação de tráfego Web por parte do roteador/gateway, não dependendo de configurações nos hosts. Essa particularidade é ideal no caso de dispositivos móveis e notebooks, pois não se tem controle administrativo dos aplicativos desses hosts. Como o host envia qualquer tráfego Web com endereço destino diferente da sua rede local para o roteador/gateway, o mesmo realiza o reencaminhamento desse tráfego, através de Destination NAT (DNAT) com IpTables [74], para o servidor proxy Web localizado na rede DMZ.

Em um ambiente com Pilha Dupla, espera-se que o servidor de proxy Web atuante na rede IPv4 possa ser reutilizado em redes IPv6. Em relação ao procedimento de configuração dos hosts, apenas a abordagem WPAD por meio de DNS funcionou corretamente, uma vez que o DHCPv6 não possui suporte à opção 252 [43] existente no serviço DHCP de redes IPv4. Na abordagem de proxy Web transparente, não se consegue utilizar a mesma abordagem DNAT em redes IPv4, pois não se aplica NAT em IPv6. Nesse caso, adotou-se a abordagem TPROXY [75], que consiste de um módulo no kernel do Linux para realizar o reencaminhamento de pacotes marcados através do Ip6Tables. Ao contrário do DNAT, o TPROXY no Ip6Tables marca os pacotes e reencaminha ao localhost para o serviço Squid com TPROXY, que opera localmente no roteador/gateway IPv6. Como já existe um serviço de proxy Web no *campus*, utilizado tanto para rede IPv4 (abordagem WPAD e proxy Web transparente) quanto IPv6 (abordagem WPAD por DNS), o serviço Squid TPROXY é configurado para reutilizar o serviço de proxy Web já existente para efetuar a consulta à página Web requisitada pelo host. Essa estratégia é possível mediante uso de FrontEnds e BackEnds [76] configurados nos dois serviços de proxy Web (TPROXY (roteador/gateway) e proxy Web (servidor Squid)). Dessa forma, reutiliza-se o cache já existente no servidor de proxy Web e também as mesmas regras de filtragem de conteúdo Web para a rede IPv4 e IPv6.

4.3 Análise de Tráfego IPv6

Foi realizado uma análise de tráfego utilizando a ferramenta NTOP [81] durante o período de uma semana para identificar qual a porcentagem de tráfego IPv6 no acesso à Internet. A análise apontou que, no momento de escrita desse artigo, chegou a 20% do tráfego total acessado do *campus* para a Internet e os principais serviços IPv6 acessados pela instituição pertencem ao domínio Google (principalmente o serviço Gmail), Facebook e RNP. Essa simples análise demonstra que existe um leve avanço na adoção do IPv6, mas ainda é pouco por conta da escassez de endereços IPv4 já declarada pelas entidades responsáveis [14,15,16,17].

5 Lições aprendidas

Para qualquer instituição adotar o IPv6, é necessário compreender questões de operação desse e identificar experiências/soluções de implementação a fim de facilitar a sua adoção. É necessário também realizar um planejamento para tornar a migração transparente, que pode ser sintetizado da seguinte forma:

- Identificação dos softwares/hardwares pertencentes à infraestrutura de rede, e verificar qual o suporte IPv6 fornecido pelos fabricantes (procurando identificar implementações de IPv6 parciais, como exemplo, a falta de suporte ao RDNSS [44]);

- Levantamento dos softwares/hardwares (browsers, softwares corporativos, celulares, notebooks....) que fazem uso da infraestrutura de rede para identificar implementações parciais do IPv6 (como exemplo, tem-se o

Windows XP com implementação incompleta de IPv6, e o Windows 7 e Linux sem o suporte ao RDNSS nativo);

- Gerar um ambiente de testes para a operação dos serviços críticos da infraestrutura (DNS, Firewall, Roteadores, Proxy, softwares corporativos, dispositivos móveis, impressoras, etc...) com IPv6. Ainda nesse ambiente, verificar a possibilidade de usar a técnica de Pilha Dupla (devendo ser priorizada [2]) e é importante realizar vários testes para identificar possíveis problemas, pois o suporte ao IPv6 parcial e pouco documentado pode gerar alguma instabilidade em algumas operações de rede (por exemplo, o Windows XP necessita obrigatoriamente da pilha IPv4 ativa para que a sua implementação parcial de IPV6 consiga operar). É importante ressaltar que várias dificuldades apresentadas nesse trabalho foram identificadas/corrigidas durante o período de testes, não sendo localizadas na literatura ou na internet.

- Por conta da implementação IPv6 ser dependente da pilha IPv4, no Windows XP, torna-se impossível utilizar somente o protocolo IPv6 com Windows XP nativo.

- Para utilizar a técnica de Pilha Dupla conforme a descrita neste trabalho, deve-se solicitar um bloco IPv6 do provedor de serviços internet. Caso a instituição for uma universidade pública, pode-se conseguir mais rapidamente pelo fato de ter algum vínculo com a RNP. Caso não for utilizar a técnica de Pilha Dupla, recomenda-se analisar cada técnica em [2] para identificar qual a melhor para a instituição.

- Ao possuir um bloco IPv6, é importante planejar a geração das sub-redes a fim de ter escala de crescimento futuro, conforme seção 3.

- Ao usar a técnica de Pilha Dupla, pode-se organizar as VLANs a fim de acomodar tanto a rede IPv4 quanto IPv6 facilita a migração gradual além de permitir uma configuração da rede IPv6 com a rede IPv4 operante. Uma vez que não utilize mais a rede IPv4 no futuro, basta desabilitá-la dos hosts e equipamentos de rede.

- Os Roteadores/Gateways IPv4 e IPv6 devem ter acesso as VLANs, através de VLAN Trunk, para realizar roteamento/filtragem necessários entre as VLANs. Recomenda-se que as regras de filtragem estejam duplicadas, cada um com seus detalhes de configuração, devido ao funcionamento distinto das redes IPv4 e IPv6, principalmente em relação aos tipos de endereços IPv6 e funcionamento do NDP e do Path MTU Discovery (seções 2 e 4).

- Caso não for utilizar a técnica de Pilha Dupla, é importante investigar outras técnicas de transição e identificar qual a melhor para a instituição (ver [12] [13]). Realizar vários ambientes de testes é extremamente importante para detectar anomalias no funcionamento de algum serviço de rede por conta da técnica escolhida.

- Da mesma forma que o Roteador/Gateway IPv4 e IPv6 estão com as regras duplicadas, recomenda-se também duplicar as regras do Firewall Geral IPv4 e IPv6. Duplicar Roteador/Gateway e Firewalls Gerais acarretam o dobro de trabalho, mas permite organizar a infraestrutura de rede para facilitar futuramente a completa migração do IPv4 para o IPv6.

6 Conclusão

O protocolo IPv4 foi concebido para ser robusto e de fácil configuração, tendo um papel importante na disseminação da Internet. No entanto, a expansão exponencial da Internet atinge uma escassez de endereços IPv4. Várias abordagens temporárias e mais complexas, visando estender o uso do IPv4, continuam ainda sendo aplicadas, o que afeta a concepção inicial da Internet de comunicação entre os hosts. O protocolo IPv6 é o substituto do IPv4, o que eliminaria os problemas de escassez de endereços e das abordagens temporárias. Dada a incompatibilidade entre IPv4 e IPv6, a sua adoção se torna difícil por conta da falta de entendimento do protocolo IPv6 e das questões operacionais do mesmo. Este trabalho apresenta um estudo para facilitar o entendimento do IPv6 e apresenta as principais experiências adquiridas com as soluções para implementar o IPv6 na infraestrutura do *campus* Apucarana da UTFPR. A partir desse estudo e experiência, espera-se que outros *campus* universitários consigam mais facilmente iniciar a sua migração para o protocolo IPv6, para atenderem às solicitações do Comitê Gestor de Internet do Brasil.

Agradecimentos

As equipes de TI do *campus* Apucarana da UTFPR e do POP-PR pelo apoio na implementação IPv6.

Referências

[1] DARPA. Internet Protocol. *IETF Request for Comment 791*, 1981. Disponível em: <https://www.rfc-editor.org/rfc/rfc791.txt>. Acesso em: 28 out. 2015.

[2] SANTOS, R. R. et al. *Curso IPv6 Básico*. 2012. Disponível em: <http://ipv6.br/pagina/downloads>. Acesso em: 28 out. 2015.

[3] REKHTER, Y.; LI, T. An Architecture for IP Address Allocation with CIDR. *IETF Request for Comment 1518*, 1993. Disponível em: <https://www.rfc-editor.org/rfc/rfc1518.txt>. Acesso em: 28 out. 2015.

[4] REKHTER, Y. et al. Address Allocation for Private Internets. *IETF Request for Comment 1918*, 1996. Disponível em: <https://www.rfc-editor.org/rfc/rfc1918.txt>. Acesso em: 28 out. 2015.

[5] HOLDREGE, M.; SRISURESH, P. Protocol Complications with the IP Network Address Translator. *IETF Request for Comment 3027*, 2001. Disponível em: <https://www.rfc-editor.org/rfc/rfc3027.txt>. Acesso em: 28 out. 2015.

[6] ROSEMBERG, J. et al. Session Traversal Utilities for NAT (STUN). *IETF Request for Comment* 5389, 2008. Disponível em: <https://www.rfc-editor.org/rfc/rfc5389.txt>. Acesso em: 28 out. 2015.

[7] MAHY, R.; MATTHEWS, P.; ROSEMBERG, J. Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN). *IETF Request for Comment 5766*, 2010. Disponível em: <https://www.rfc-editor.org/rfc/rfc5766.txt>. Acesso em: 28 out. 2015.

[8] BARRETO, F. An improved B2BUAWM approach for VoIP infrastructure. In: LATIN AMERICAN NETWORK OPERATIONS AND MANAGEMENT SYMPOSIUM (LANOMS), 7. *Proceedings*... Quito: IEEE, 2011.

[9] BRADNER, S.; MANKIN, A. IP: Next Generation (Ipng) White Paper Solicitation. *IETF Request for Comment 1550*. 1993. Disponível em: <https://www.rfc-editor.org/rfc/rfc1550.txt>. Acesso em: 28 out. 2015.

[10] DEERING, S.; HINDEN, R. Internet Protocol, Version 6 (IPv6) Specification. *IETF Request for Comment 2460*, 1998. Disponível em: <https://www.rfc-editor.org/rfc/rfc2460.txt>. Acesso em: 28 out. 2015.

[11] NORDMARK, E.; GILLIGAN, R. Basic Transition Mechanisms for IPv6 Hosts and Routers. *IETF Request for Comment 4213*, 2005. Disponível em: <https://www.rfc-editor.org/rfc/rfc4213.txt>. Acesso em: 28 out. 2015.

[12] WU, P. et al. Transition from IPv4 to IPv6: A State-of-the-Art Survey. *IEEE Communications Surveys & Tutorials*, IEEE, v. 15, n. 3, p. 1407–1424, 2013. ISSN 1553-877X.

[13] CURRAN, J. An Internet Transition Plan. *IETF Request for Comment 5211*, 2008. Disponível em: <https://www.rfc-editor.org/rfc/rfc5211.txt>. Acesso em: 28 out. 2015.

[14] NIC.BR. *Últimos blocos IPv4 são alocados pela IANA*. 2011. Disponível em: <http://nic.br/imprensa/releases/2011/rl-2011-04.htm>. Acesso em: 29 out. 2014.

[15] LACNIC. *Estado do IPv4 no final de 2012*. 2012. Disponível em: <http://portalipv6.lacnic.net/pt-br/estado-do-ipv4-final-de-2012/>. Acesso em: 29 out. 2014.

[16] LACNIC. *Não há mais endereços IPv4 na América Latina e no Caribe*. 2014. Disponível em: <http://portalipv6.lacnic.net/pt-br/nao-ha-mais-enderecos-ipv4-na-america-latina-e-o-caribe/>. Acesso em: 29 out. 2014.

[17] NIC.BR. *Termina o estoque de endereços IPv4 na América Latina*. 2014. Disponível em: <http://www.nic.br/imprensa/releases/2014/rl-2014-19.htm>. Acesso em: 29 out. 2014.

[18] GOOGLE. *Google IPv6 Statistics*. 2014. Disponível em: <http://www.google.com/ipv6/statistics.html#tab=per-country-ipv6-adoption>. Acesso em: 29 out. 2014.

[19] YAMAGATA, I.; SHIRASAKI, Y.; NAKAGAWA, A. NAT 444. *IETF Internet Draft draft-shirasaki-nat444-06.* 2012. Disponível em: <https://tools.ietf.org/id/draft-shirasaki-nat444-06.txt>. Acesso em: 28 out. 2015.

[20] JIANG, S; GUO, D.; CARPENTER, B. An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition. *IETF Request for Comment 6264*, 2011. Disponível em: <https://www.rfc-editor.org/rfc/rfc6264.txt>. Acesso em: 28 out. 2015.

[21] WEIL, J. et al. IANA-Reserved IPv4 Prefix for Shared Address Space. *IETF Request for Comment 6598*, 2012. Disponível em: <https://www.rfc-editor.org/rfc/rfc6598.txt>. Acesso em: 28 out. 2015.

[22] FORD, M.; BOUCADAIR, M.; DURAND, A. Issues with IP Address Sharing. *IETF Request for Comment 6269*, 2011. Disponível em: <https://www.rfc-editor.org/rfc/rfc6269.txt>. Acesso em: 28 out. 2015.

[23] DONLEY, C. et al. Assessing the Impact of Carrier-Grade NAT on Network Applications. *IETF Request for Comment 7021*, 2013. Disponível em: <https://www.rfc-editor.org/rfc/rfc7021.txt>. Acesso em: 28 out. 2015.

[24] CGI.BR. *Resolução CGI.br/RES/2013/033* – Ações para fomentar a adoção do IPv6. 2013. Disponível em: <http://www.cgi.br/regulamentacao/resolucao2013-033.htm>. Acesso em: 29 out. 2014.

[25] ARKKO, J.; KERANEN, A. Experiences from an IPv6-Only Network. *IETF Request for Comment 6586*, 2012. Disponível em: <https://www.rfc-editor.org/rfc/rfc6586.txt>. Acesso em: 28 out. 2015.

[26] PODERMANSKI, T.; GREGR, M.; SVEDA, M. *Deploying IPv6 – practical problems from the campus perspective*. 2012. Disponível em: <https://tnc2012.terena.org/core/presentation/49>. Acesso em: 28 out. 2015.

[27] 6NET. *An IPv6 Deployment Guide*. 2005. Disponível em: <http://www.6net.org/book/deployment-guide.pdf>. Acesso em: 29 out. 2014.

[28] VELDE, G. et al. IPv6 Unicast Address Assignment Considerations. *IETF Request for Comment 5375*, 2008. Disponível em: <https://www.rfc-editor.org/rfc/rfc5375.txt>. Acesso em: 28 out. 2015.

[29] CHITTIMANENI, K. et al. Enterprise IPv6 Deployment Guidelines. *IETF Internet Draft draft-ietf-v6ops-enterprise-incremental-ipv6-06*, 2014. Disponível em: <https://tools.ietf.org/id/draft-ietf-v6ops-enterprise-incremental-ipv6-06.txt>. Acesso em: 28 out. 2015.

[30] CONVERY, S.; MILLER, D. IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation. 2004. Disponível em: <http://www.seanconvery.com/v6-v4-threats.pdf>. Acesso em: 28 out. 2015.

[31] HINDEN, R.; DEERING, S. IP Version 6 Addressing Architecture. *IETF Request for Comment 4291*, 2006. Disponível em: <https://www.rfc-editor.org/rfc/rfc4291.txt>. Acesso em: 28 out. 2015.

[32] KAWAMURA, S.; KAWASHIMA, M. A Recommendation for IPv6 Address Text Representation. *IETF Request for Comment 5952*, 2010. Disponível em: <https://www.rfc-editor.org/rfc/rfc5952.txt>. Acesso em: 28 out. 2015.

[33] MCCANN, J.; DEERING, S.; MOGUL, J. Path MTU Discovery for IP version 6. *IETF Request for Comment 1981*, 1996. Disponível em: <https://www.rfc-editor.org/rfc/rfc1981.txt>. Acesso em: 28 out. 2015.

[34] MOGUL, J. Path MTU Discovery. *IETF Request for Comment 1191*, 1990. Disponível em: <https://www.rfc-editor.org/rfc/rfc1191.txt>. Acesso em: 28 out. 2015.

[35] WOOL, A. Quantitative Study of Firewall Configuration Errors. In: *IEEE Computer Society*, 2004, IEEE, v. 37, n. 6, p. 62–67, 2004. ISSN 0018-9162.

[36] DROMS, R. Dynamic Host Configuration Protocol. *IETF Request for Comment 2131*, 1997. Disponível em: <https://www.rfc-editor.org/rfc/rfc2131.txt>. Acesso em: 28 out. 2015.

[37] JANKIEWICZ, E.; LOUGHNEY, J; NARTEN, T. IPv6 Node Requirements. *IETF Request for Comment 6434*, 2011. Disponível em: <https://www.rfc-editor.org/rfc/rfc6434.txt>. Acesso em: 28 out. 2015.

[38] THOMSON, S.; NARTEN, T.; JINMEI, T. IPv6 Stateless Address Autoconfiguration. *IETF Request for Comment 4862*, 2007. Disponível em: <https://www.rfc-editor.org/rfc/rfc4862.txt>. Acesso em: 28 out. 2015.

[39] CRAWFORD, M. Transmission of IPv6 Packets over Ethernet Networks. *IETF Request for Comment 2464*, 1998. Disponível em: <https://www.rfc-editor.org/rfc/rfc2464.txt>. Acesso em: 28 out. 2015.

[40] NARTEN, T. et al. Neighbor Discovery for IP version 6 (IPv6). *IETF Request for Comment 4861*, 2007. Disponível em: <https://www.rfc-editor.org/rfc/rfc4861.txt>. Acesso em: 28 out. 2015.

[41] DROMS, R. Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6. *IETF Request for Comment 3736*, 2004. Disponível em: <https://www.rfc-editor.org/rfc/rfc3736.txt>. Acesso em: 28 out. 2015.

[42] BOUND, J. et al. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). *IETF Request for Comment 3315*, 2003. Disponível em: <https://www.rfc-editor.org/rfc/rfc3315.txt>. Acesso em: 28 out. 2015.

[43] IANA. DHCPv6 Option Codes. 2014. Disponível em: <http://www.iana.org/assignments/dhcpv6-parameters/dhcpv6-parameters.xhtml#dhcpv6-parameters-2>. Acesso em: 29 out. 2014.

[44] JEONG, J. et al. IPv6 Router Advertisement Options for DNS Configuration. *IETF Request for Comment 6106*, 2010. Disponível em: <https://www.rfc-editor.org/rfc/rfc6106.txt>. Acesso em: 28 out. 2015.

[45] JEONG, J. IPv6 Host Configuration of DNS Server Information Approaches. *IETF Request for Comment 4339*, 2006. Disponível em: <https://www.rfc-editor.org/rfc/rfc4339.txt>. Acesso em: 28 out. 2015.

[46] CHESHIRE, S.; ABOBA, B.; GUTTMAN, E. Dynamic Configuration of IPv4 Link-Local Addresses. *IETF Request for Comment 3927*, 2005. Disponível em: <https://www.rfc-editor.org/rfc/rfc3927.txt>. Acesso em: 28 out. 2015.

[47] PLUMMER, D. C. An Ethernet Address Resolution Protocol. *IETF Request for Comment 826*, 1982. Disponível em: <https://www.rfc-editor.org/rfc/rfc826.txt>. Acesso em: 28 out. 2015.

[48] CHESHIRE, S. IPv4 Address Conflict Detection. *IETF Request for Comment 5227*, 2008. Disponível em: <https://www.rfc-editor.org/rfc/rfc5227.txt>. Acesso em: 28 out. 2015.

[49] DAVIES, E.; MOHACSI, J. Recommendations for Filtering ICMPv6 Messages in Firewalls. *IETF Request for Comment 4890*, 2007. Disponível em: <https://www.rfc-editor.org/rfc/rfc4890.txt>. Acesso em: 28 out. 2015.

[50] BRASIL. Ministério da Educação. Programa Banda Larga nas Escolas. 2008. Disponível em: <http://www.educacao.gov.br/index.php?option=com_content&view=article&id=15808&Itemid=823>. Acesso em: 29 out. 2014.

[51] RNP. *IPv6 na RNP*. 2014. Disponível em: <http://www.rnp.br/ipv6/ipv6-rnp.html>. Acesso em: 29 out. 2014.

[52] REGISTRO.BR, *Políticas para distribuição de blocos IPv6*. 2014. Disponível em: <http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao#/num3>. Acesso em: 29 out. 2014.

[53] IAB. Recommendations on IPv6 Address Allocations to Sites. *IETF Request for Comment 3177*, 2001. Disponível em: <https://www.rfc-editor.org/rfc/rfc3177.txt>. Acesso em: 28 out. 2015.

[54] NARTEN, T.; HUSTON, G.; ROBERTS, L. IPv6 Address Assignment to End Sites. *IETF Request for Comment 6177*, 2011. Disponível em: <https://www.rfc-editor.org/rfc/rfc6177.txt>. Acesso em: 28 out. 2015.

[55] IPV6.BR. *Qual é o tamanho de bloco apropriado?* 2011. Disponível em: <http://ipv6.br/qual-e-o-tamanho-de-bloco-apropriado/>. Acesso em: 29 out. 2014.

[56] CAIDA. *IPv6 Evolution*. 2014. Disponível em: <http://www.caida.org/projects/ipv6_evolution/>. Acesso em: 29 out. 2014.

[57] WORDIPV6LAUNCH. *World IPv6 Launch*. 2014. Disponível em: <http://www.worldipv6launch.org/measurements/>. Acesso em: 29 out. 2014.

[58] BLANCHET, M. A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block. *IETF Request for Comment 3531*, 2003. Disponível em: <https://www.rfc-editor.org/rfc/rfc3531.txt>. Acesso em: 28 out. 2015.

[59] TSUCHIYA, P. On the Assignment of Subnet Numbers. *IETF Request for Comment 1219*, 1991. Disponível em: <https://www.rfc-editor.org/rfc/rfc1219.txt>. Acesso em: 28 out. 2015.

[60] GEORGE, W. RFC 3627 to Historic Status. *IETF Request for Comment 6547*, 2012. Disponível em: <https://www.rfc-editor.org/rfc/rfc6547.txt>. Acesso em: 28 out. 2015.

[61] MICROSOFT. *IPv6 for Microsoft Windows*: Frequently Asked Questions. 2011. Disponível em: <http://technet.microsoft.com/en-us/network/cc987595.aspx>. Acesso em: 29 out. 2014.

[62] IPV6INT.NET. *Dibbler DHCPv6*. 2009. Disponível em: <http://ipv6int.net/software/dibbler_dhcpv6.html>. Acesso em: 29 out. 2014.

[63] VINCENT, S. *RDNSSD-Win32*. 2014. Disponível em: <http://sourceforge.net/projects/rdnssd-win32/>. Acesso em: 29 out. 2014.

[64] NM. *Network Manager*. 2013. Disponível em: <https://wiki.debian.org/NetworkManager>. Acesso em: 29 out. 2014.

[65] LITECH. *Linux IPv6 Router Advertisement Daemon* (radvd). 2014. Disponível em: <http://www.litech.org/radvd/>. Acesso em: 29 out. 2014.

[66] ISC. ISC DHCP. Disponível em: <https://www.isc.org/downloads/dhcp/>. Acesso em: 29 out. 2014.

[67] ISC. BIND. Disponível em: <https://www.isc.org/downloads/bind/>. Acesso em: 29 out. 2014.

[68] THOMSON, S. et al. DNS Extensions to Support IP Version 6. *IETF Request for Comment 3596*, 2003. Disponível em: <https://www.rfc-editor.org/rfc/rfc3596.txt>. Acesso em: 28 out. 2015.

[69] THOMSON, S.; REKHTER, J.; BOUND, J. Dynamic Updates in the Domain Name System (DNS UPDATE). *IETF Request for Comment 2136*, 1997. Disponível em: <https://www.rfc-editor.org/rfc/rfc2136.txt>. Acesso em: 28 out. 2015.

[70] ARENDS, R. et al. DNS Security Introduction and Requirements. *IETF Request for Comment 4033*, 2005. Disponível em: <https://www.rfc-editor.org/rfc/rfc4033.txt>. Acesso em: 28 out. 2015.

[71] SQUID. *IPv6 in Squid*. 2012. Disponível em: <http://wiki.squid-cache.org/Features/IPv6>. Acesso em: 29 out. 2014.

[72] GAUTHIER, P. et al. Web Proxy Auto-Discovery Protocol. *IETF Internet Draft draft-ietf-wrec-wpad-01*, 1999. Disponível em <https://tools.ietf.org/id/draft-ietf-wrec-wpad-01.txt>. Acesso em: 28 out. 2015.

[73] COOPER, I.; MELVE, I.; TOMLINSON, G. Internet Web Replication and Caching Taxonomy. *IETF Request for Comment 3040*, 2001. Disponível em: <https://www.rfc-editor.org/rfc/rfc3040.txt>. Acesso em: 28 out. 2015.

[74] TLDP. *Transparent Proxy to a Remote Box*. 2002. Disponível em: <http://www.tldp.org/HOWTO/TransparentProxy-6.html>. Acesso em: 29 out. 2014.

[75] SQUID. TPROXYv4.1+ with full IPv4 and IPv6 transparent interception of HTTP. 2013. Disponível em: <http://wiki.squid-cache.org/Features/Tproxy4>. Acesso em: 29 out. 2014.

[76] SQUID. *MultiCpuSystem*. 2010. Disponível em: <http://wiki.squid-cache.org/ConfigExamples/MultiCpuSystem>. Acesso em: 29 out. 2014.

[77] WING, D.; YOURTCHENKO, A. Happy Eyeballs: Success with Dual-Stack Hosts. *IETF Request for Comment 6555*, 2012. Disponível em: <https://www.rfc-editor.org/rfc/rfc6555.txt>. Acesso em: 28 out. 2015.

[78] IPV6.BR. *Simulação RFC3531*. 2014. Disponível em: <http://ipv6.br/rfc3531demo/>. Acesso em: 29 out. 2014.

[79] GEORGE, W. et al. IPv6 Support Required for All IP-Capable Nodes. *IETF Request for Comment 6540*, 2012. Disponível em: <https://www.rfc-editor.org/rfc/rfc6540.txt>. Acesso em: 28 out. 2015.

[80] NIC.BR. *Anatel acelera discussão sobre certificação de equipamentos com IPv6*. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36382&sid=29>. Acesso em: 29 out. 2014.

[81] NTOP. *Network Monitoring*. Disponível em: <http://www.ntop.org>. Acesso em: 3 jun. 2015.