Análise do processo de transição do IPv4 para o IPv6 na Universidade Federal de Juiz de Fora

Bruno Telles de Almeida

JUIZ DE FORA

JULHO, 2016

Análise do processo de transição do IPv4 para o IPv6 na Universidade Federal de Juiz de Fora

Bruno Telles de Almeida

Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

Departamento de Ciência da Computação

Bacharelado em Sistemas de Informação

Orientador: Eduardo Pagani Julio

JUIZ DE FORA

JULHO, 2016

Análise do processo de transição do IPv4 para o IPv6 na Universidade Federal de Juiz de Fora

Bruno Telles de Almeida

MONOGRAFIA SUBMETIDA AO CORPO DOCENTE DO INSTITUTO DE CIÊNCIAS EXATAS DA UNIVERSIDADE FEDERAL DE JUIZ DE FORA, COMO PARTE INTEGRANTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Aprovada por:

Eduardo Pagani Julio
Dr. em Computação

Eduardo Barrére
Dr. em Engenharia de Sistemas e Computação

Rafael Barra de Almeida
Ms. Ciência da Computação

JUIZ DE FORA

29 DE JULHO, 2016

Resumo

Em junho de 2012, o IPv6 passou a ser considerado o novo padrão da rede mundial de computadores, e a Universidade Federal de Juiz de Fora, a fim de adaptar-se a essa mudança, iniciou a implantação desse novo padrão. Tendo isso em vista, o presente trabalho busca analisar o processo de transição entre os protocolos da camada de rede, apontando quais foram as técnicas utilizadas (pilha dupla, tunelamento, tradução), o porquê da utilização dessas técnicas e as mudanças realizadas em infraestrutura e serviços essenciais. Ademais, testa a operacionalidade das principais funcionalidades do IPv6.

Palavras-chave: IPv6; IPv4; Pilha Dupla; Tunelamento; Tradução; Mecanismos de Transição, Implantação, Migração

Abstract

In June 2012, IPv6 came to be considered the new standard of the World Wide Web, and the Federal University of Juiz de Fora, in order to adapt to this change, began to implement this new standard. This paper aims to analyze the transition process between the network layer protocols, pointing out the techniques used (double stack, tunneling, translation), the reason for the use of these techniques and the changes made in infrastructure and essential services. In addition, it tests the operability of the main functionalities of IPv6.

Keywords: IPv6; IPv4; Dual Stack; Tunneling; Translation; Transition Mechanisms, Deployment, Migration

Agradecimentos

Agradeço primeiramente a minha família, sem eles essa conquista não seria possível. Aos amigos, que me apoiaram e incentivaram a perseguir esse sonho. Agradeço também aos colegas de curso, esses me mostraram que o trabalho em equipe permite atingir objetivos extremamente desafiadores. Não poderia esquecer de externar meu agradecimento a todos os professores que de alguma forma contribuíram para minha formação. Por fim, agradeço meu orientador Eduardo Pagani Júlio, pelo apoio, dedicação e por acreditar, desde o início, que a realização desse trabalho seria possível.

Conteúdo

Lista de Figuras

Lista de Tabelas

Lista de Abreviações

UFJF	Universidade Federal de Juiz de Fora
DARPA	*Defense Advanced Research Projects Agency*
ARPANET	*Advanced Research Projects Agency Network*
IP	*Internet protocol*
IPv4	*Internet protocol version 4*
IPv6	*Internet protocol version 6*
NIC.br	*Núcleo de Informação e Coordenação do Ponto BR*
DHCP	*Dynamic host configuration protocol*
NAT	*Network address translation*
TUBA	*TCP and UDP with Bigger Addresses*
MTU	*Maximum Transmission Unit*
CGCO	Centro de Gestão do Conhecimento Organizacional
SIPP	*Simple Internet Protocol Plus*
WEB	*World Wide Web*
QoS	*Quality of Service*
ICMPv6	*Internet Control Message Protocol Version 6*
ARP	*Address Resolution Protocol*
NDP	*Neighbor Discovery Protocol*
NS	*Neighbor Solicitation*
NA	*Neighbor Advertisement*
RS	*Router Solicitation*
RA	*Router Advertisement*
SIIT	*Stateless IP/ICMP Translation*
BIS	*Bump In the Stack*
BIA	*Bump in the API*
TRT	*Transport Relay Translation*
RFC	*Request for Comments*

1 Introdução

Data-se do final da década de 60 (1966) o surgimento do que seria conhecido hoje como a rede mundial de computadores ou a Internet. Inicialmente o projeto patrocinado pela DARPA (*Defense Advanced Research Projects Agency*) visava criar uma rede experimental, distribuída, que pudesse se adaptar a possíveis falhas nos diversos nós que a compunham. O corte nas comunicações era uma grande preocupação na época, visto que os EUA se encontrava no período de guerra fria com a extinta União Soviética e um ataque aos meios de comunicação americanos era bastante provável (Brito, 2013).

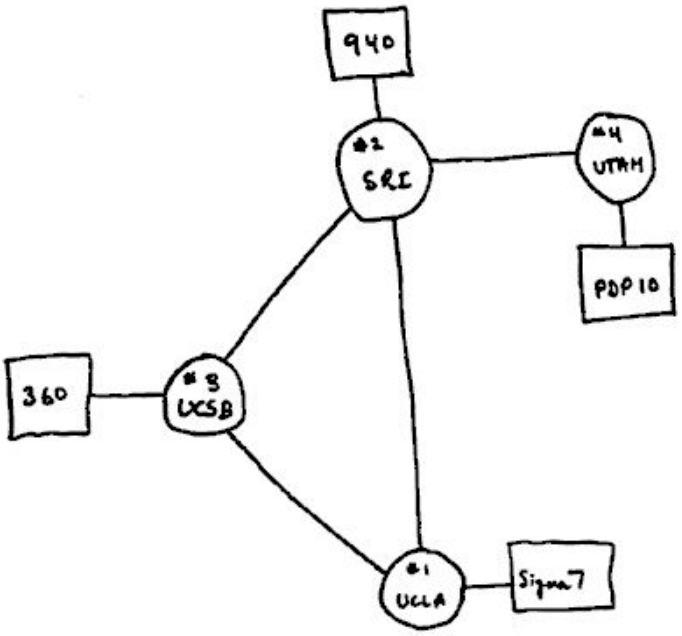

Figura 1.1: Mapa da ARPANET em 1969 (Abreu, 2014)

Conforme pode ser visto na Figura 1.1, primeiramente apenas quatro instituições foram contempladas pelo projeto que ficou conhecido como ARPANET (*Advanced Research Projects Agency Network*), eram elas: Universidade da Califórnia Em Los Angeles (UCLA), Universidade da Califórnia em Santa Bárbara (UCSB), Universidade de Utah e a Universidade de Standford (SRI). Em 1983 quando já possuía mais de 500 equipamentos conectados, a ARPANET evoluiu para o que conhecemos hoje como Internet, baseada em

padrões abertos como o TCP/IP (Brito, 2013).

O protocolo especificado na época não previa que com a liberação da Internet para fins comerciais nos anos 90, que sua popularização popularização atingiria níveis mundiais, saltando de aproximadamente 2.056.000 de *Hosts* em 1993, para mais de 26.000.00 em 1997. Nessa mesma época já começavam as especulações em relação ao esgotamento dos endereços IPv4 disponíveis (Moreiras *et al.*, 2012).

A fim de solucionar as limitações e falhas presentes no IPv4, iniciaram-se estudos relacionados ao desenvolvimento de um novo protocolo que pudesse substituí-lo. Em 1995 foram apresentadas as primeiras especificações do IPv6 sendo alteradas em 1998 por uma versão definitiva (Moreiras *et al.*, 2012).

1.1 Problema

As medidas paliativas que foram criadas ao longo do tempo, como o DHCP (*Dynamic host configuration protocol*) e o NAT (*Network address translation*) por exemplo, já não são mais capazes de frear a demanda por endereços. Logo, é importante que a transição entre protocolos ocorra de forma gradativa e comece o mais rápido possível, pois segundo o NIC.br (Núcleo de Informação e Coordenação do Ponto BR), em 10 de junho de 2014 o estoque de endereços IPv4 da América Latina se esgotou.

A organização supracitada (NIC.br), responsável no Brasil pela gerência de endereços IP (*Internet protocol*), iniciou a distribuição de blocos IPv6 para algumas instituições e empresas. A UFJF recebeu um bloco de endereços e ciente da criticidade dessa mudança, em parceria com os profissionais do CGCO (Centro de Gestão do Conhecimento Organizacional), começou a empregar técnicas de transição entre os protocolos nas redes internas da instituição.

Uma vez o que processo transição foi iniciado, é importante discutir quais técnicas foram utilizadas e quais as vantagens e limitações dessas técnicas. Além disso, destacar o que ainda precisa ser feito para que todos os setores estejam aptos a trocar informações através do novo protocolo. Por fim, identificar se os principais serviços e funcionalidades estão plenamente operacionais via IPv6.

1.2 Justificativa

É consensual que além de trazer inúmeros benefícios, a migração do IPv4 para o IPv6 é fundamental para o crescimento da rede mundial de computadores. Ela irá possibilitar a evolução para o que conhecemos hoje como Internet das Coisas (*Internet of Things*) (Melo, 2015). Nesse período uma infinidade de dispositivos (*Smartphones, Tablets*, carros, eletrodomésticos estarão aptos para trocar informações entre si e para tal precisarão de um endereço IP.

Apenas o fato de garantir a manutenção do crescimento já seria argumento bastante convincente para dar prosseguimento ao processo de implantação do novo protocolo. Mas ele vai muito além, permite de forma nativa a proveniência de segurança (autenticação, integridade e confidencialidade), ou seja, não transfere para camadas superiores essa responsabilidade. Implementa funcionalidades de Qualidade de serviço, classificando o tráfego e permitindo priorizar pacotes que sejam sensíveis ao atraso, como *Streaming* de vídeo e áudio por exemplo (Barreto, 2015).

A UFJF identificou essa necessidade em 2013 e criou um projeto de treinamento profissional com intuito de elaborar um documento que guiasse o processo de transição. Desde então, bolsistas e profissionais de rede, vem estudando materiais que apontem formas de realizar essa mudança, sabidamente necessária mas por muito tempo postergada, devido a aspectos econômicos intrínsecos a quaisquer mudanças de grande porte

1.3 Objetivos

1.3.1 Objetivos Gerais

Este trabalho visa analisar o modelo de transição entre os protocolos IPv4 e IPv6 adotado pela UFJF. Para tal pretende-se identificar quais medidas foram tomadas e quais ainda precisam ser colocadas em prática a fim de viabilizar que todos os setores troquem informações e possam acessar os principais serviços utilizando o IPv6.

1.3.2 Objetivos Específicos

Primeiramente são analisadas as técnicas de coexistência entre o IPv4 e IPv6, apontando suas vantagens e desvantagens.

Em um segundo momento, é feita uma análise do andamento do processo de transição na UFJF, apontando quais setores estão aptos para utilizar o novo protocolo e quais ainda não foram contemplados pela mudança.

Por fim, testa-se a comunicação através do IPv6, visando identificar se as principais funcionalidades estão sendo executadas corretamente. Testa-se também a acessibilidade e operacionalidade de serviços essenciais para este processo de implantação, como o DNS por exemplo.

1.4 Metodologia

E execução dessa monografia é de natureza qualitativa sendo apresentada na forma de um documento contendo uma análise do processo de transição entre os protocolos IPv4 e IPv6 na UFJF.

Para a composição deste documento foram realizadas entrevistas com os colaboradores do CGCO, que é o setor responsável pela administração da infraestrutura de rede da Universidade. Essas entrevistas visavam determinar o modelo de transição adotado nas redes internas da universidade, identificando os métodos utilizados, o que já foi implantado e o que ainda precisa ser feito a fim de permitir a utilização do IPv6 em toda a instituição.

O próximo passo foi através da análise da literatura disponível e de trabalhos que abordem formas de transição entre ambientes IPv4 / IPv6 realizar uma revisão da bibliografia, comparando os modelos existentes.

Por fim, foram realizados testes, adaptados a partir do trabalho Moreiras *et al.* (2015), na rede interna da UFJF, que tinham por objetivo comprovar a eficácia da adoção do IPv6.

2 Fundamentação Teórica

Neste Capítulo são apontadas as principais diferenças do novo protocolo em relação ao seu antecessor, algumas funcionalidades e por fim quais são as técnicas disponíveis que permitem a coexistência de ambos.

2.1 O protocolo IPv6

A partir de estudos realizados na década de 90, foi constatado que o protocolo vigente na época (IPv4) não possuía capacidade de endereçamento suficiente para acompanhar o rápido aumento da demanda por endereços IP, estimando-se que os pouco mais de 4 bilhões de endereços possíveis não seriam capazes de suprir a demanda para os próximos anos (Brito, 2013).

Dada as limitações do IPv4, fez-se necessária a criação de um protocolo mais maduro e eficiente. Desde junho de 2012 o IPv6 passou a ser considerado o novo padrão adotado na rede mundial de computadores, ou seja, a partir dessa data todos os equipamentos fabricados deveriam ser compatíveis com este protocolo. Isso não significa que o IPv4 foi inutilizado ou vai ser em pouco tempo pois a fase de transição vai demandar alguns anos, em virtude de seu alto grau de disseminação (Brito, 2013).

Como pode ser observado na Figura 2.1, a versão final da especificação do IPv6 aproveitou ideias de outras propostas. Sendo basicamente uma versão revisada do SIPP (*Simple Internet Protocol Plus*) incorporando endereços de 128 bits, juntamente com os elementos de transição e autoconfiguração do TUBA (*TCP and UDP with Bigger Addresses*), o endereçamento baseado no CIDR e os cabeçalhos de extensão (Moreiras *et al.*, 2012).

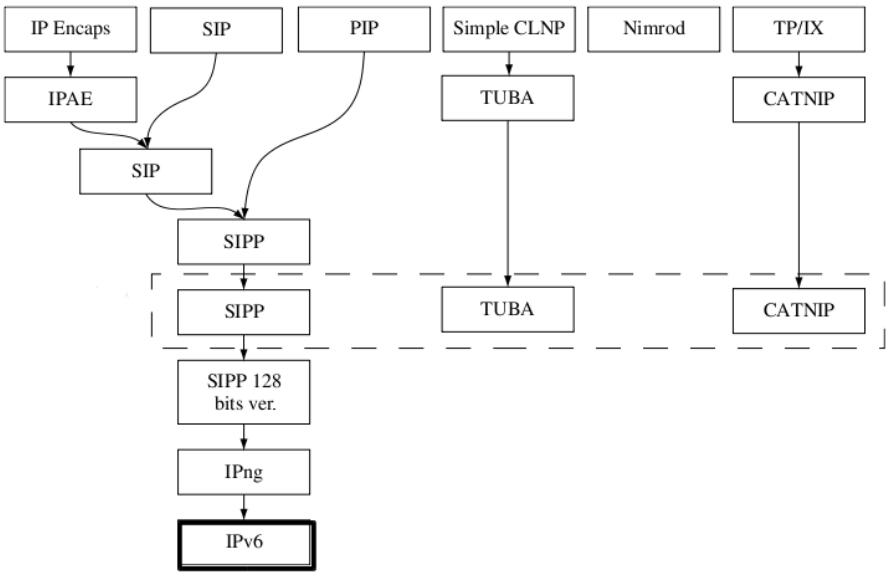

Figura 2.1: Criação do IPv6 (Abreu, 2014)

2.2 Características do IPv6

2.2.1 Principais diferenças entre o IPv4 e IPv6

As principais diferenças do IPv6 em relação ao IPv4 estão listadas a seguir:

- *Capacidade de endereçamento*: O IPv6 utiliza 128 bits para identificação de endereços, o IPv4, apenas 32 bits;
- *Formato do cabeçalho*: Mesmo possuindo capacidade de endereçamento superior em relação ao IPv4, o cabeçalho do IPv6 é mais simples, sendo permitida a adição de cabeçalhos de extensão;
- *Roteamento*: Pode ser especificado previamente o caminho a ser percorrido pelos pacotes, reduzindo-se o processamento nos roteadores;
- *Classificação de fluxos*: É possível priorizar a entrega de pacotes sensíveis ao atraso por meio de cabeçalhos de extensão, o que não estava presente no IPv4;
- *Suporte à autenticação e privacidade*: O IPv6 suporta de forma obrigatória mecanismos que permitem a autenticação de remetentes, além de garantirem a confiabilidade e integridade dos dados transmitidos.

2.2.2 Capacidade de endereçamento

O IPV6 tem como principal objetivo solucionar de forma definitiva o problema de escassez de endereços IP públicos disponíveis na Internet. No seu antecessor eram utilizados 32 bits apenas para o esquema de endereçamento, o que permitia a alocação de aproximadamente 4 bilhões de nós. Já no novo protocolo são utilizados 128 bits, permitindo que 340.282.366.920.938.463.374.607.431.768.211.456 (340 undecilhões) de nós públicos sejam alocados, equivalente a 79 trilhões de vezes a quantidade de endereços IPv4 (Brito, 2013).

No IPv4 um endereço é representado por valores decimais separado por pontos. Os endereços IPv6 são representados por dígitos hexadecimais (0-F) concatenados em oito grupos de dezesseis bits separados por dois pontos, como por exemplo: 2001:2014:abcd:3712:45b5:a78f:ab12:3454 (Neto, 2011).

Existem basicamente três tipos de endereços IPv6, eles podem ser classificados da seguinte forma:

- Endereço *Unicast*: Identifica um único *host* na rede, um pacote destinado a um endereço desse tipo é entregue diretamente à interface do equipamento que o possui. Um endereço do tipo *Unicast* pode ser subdivido em três categorias *Global Unicast*,*Link-local*, *Unique Local Address* (Gomes, 2012; Abreu, 2014):

  - *Global Unicast*: Representa aproximadamente treze porcento dos endereços IPv6 disponíveis. São globalmente roteáveis, acessíveis através da rede mundial de computadores, assim como os endereços IPv4 públicos. Atualmente é reservado o bloco de endereços IPv6 2000::/3, que corresponde a faixa de 2000:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff;
  - *Link-local*: É gerado a partir de alguns algoritmos, sendo o principal deles o IEEE EUI-64, com prefixo FE80::/64. Pode ser utilizado apenas no enlace em que a interface está conectada;
  - *Unique Local Address*: Utilizado apenas localmente, não deve ser roteável na Internet. É gerado com prefixo FC00::/7 e possui grande possibilidade de ser único globalmente, assim caso redes distintas sejam conectadas, provavelmente não acontecerão conflitos de endereços desse tipo.

- Endereço *Anycast*: Identifica um conjunto de interfaces pertencentes a *hosts* diferentes. Um pacote enviado a um endereço desse tipo é entregue à interface do equipamento mais próximo (Gomes, 2012);

- Endereço *Multicast*: Identifica um conjunto de interfaces pertencentes a um grupo de *hosts*, mas diferente do *Anycast*, os pacotes são entregues a todos os hosts identifcados pelo endereço. Endereços *Multicast* possuem prefixo FF00::/8 obrigatoriamente (Gomes, 2012).

2.2.3 Formato do cabeçalho

Um grande diferencial do IPv6 em relação ao IPv4 é seu cabeçalho. Mesmo possuindo uma capacidade de endereçamento superior, informações que antes estavam presentes obrigatoriamente passaram a ser opcionais. Assim o cabeçalho tornou-se mais simples, flexível e apto para ser adaptado a novas tecnologias (Martini Bogo, 2015).

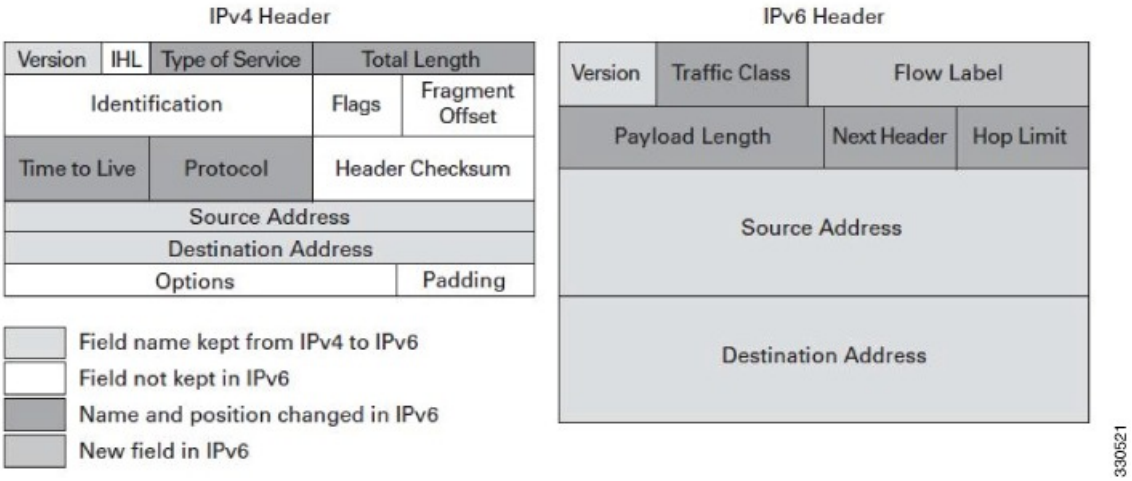

Figura 2.2: Formatos dos cabeçalhos IPv4 e IPv6 (Cisco, 2011)

A simplificação abordada, trouxe um aumento significativo na eficiência do roteamento de pacotes. O número de campos obrigatórios foi reduzido, padronizando-se um cabeçalho base simplificado e permitindo-se anexar cabeçalhos de extensão opcionais. Seguindo o formato de uma lista encadeada (Martini Bogo, 2015).

No IPv4 quando um datagrama é maior que a MTU ((*Maximum Transfer Unit*) da rede que está trafegando, ele é divido em datagramas menores e o conteúdo do

Figura 2.3: Cabeçalhos de Extensão do IPv6 (Martini Bogo, 2015)

cabeçalho original é copiado. Quando chegam em seu destino esses datagramas são remontados a fim de compor a informação originalmente enviada (Martini Bogo, 2015).

No IPV6 é utilizada uma técnica de descoberta do caminho, dessa forma a MTU até o destino pode ser identificada previamente. O *host* que está enviando a informação cria os datagramas de forma que os fragmentos tenham tamanho inferior a MTU identificada. Esse tipo de fragmentação é nomeada de fim-a-fim, pois será feita apenas pelo emissor, não sendo feitas operações adicionais nos roteadores intermediários (Martini Bogo, 2015).

2.2.4 Roteamento

O roteamento pode ser definido como o processo de encaminhamento de um datagrama de sua origem até seu destino final.

No IPv4 quando um *host* envia um datagrama pela rede, ele é encapsulado e enviado até o roteador com o menor ou melhor caminho. Chegando nesse roteador o datagrama é extraído, determina-se o próximo salto, encapsula-se novamente o datagrama, para ai sim enviá-lo para o próximo nó (Martini Bogo, 2015).

No IPv6 há a possibilidade de ser especificada previamente a rota que será seguida. Utiliza-se para esse fim os cabeçalhos de extensão. Dessa maneira o processamento nos roteadores é reduzido, aumentando a eficiência do roteamento e propiciando melhor controle do caminho a ser percorrido pelos pacotes (Martini Bogo, 2015).

2.2.5 Capacidade de classificação de fluxos ou QoS (*Quality of Service*)

De acordo com Reghini (2013) o IPv6 possui recursos que permitem identificar e priorizar a entrega de pacotes. Em seu cabeçalho há dois campos destinados ao QoS: Classe de

tráfego *(Traffic Class)* e etiqueta de fluxo *(Flow Label)*. Esses campos possibilitam a diferenciação dos pacotes a serem entregues.

Ainda segundo Reghini (2013):

> "O campo *Flow label* é responsável por "etiquetar" ou priorizar determinados fluxo de pacotes como voz sobre IP (VoIP) ou videoconferência, ambos os serviços dependem do tempo de entrega. Os novos campos do cabeçalho definem como o trafego é gerenciado e identificado, permitindo assim que os roteadores realizem um gerenciamento especial para cada tipo de pacote. Com a identificação do trafego no cabeçalho é possível dar suporte a QoS mesmo quando os pacotes estiverem utilizando IPSec" (Reghini, 2013).

2.2.6 Suporte à autenticação e privacidade

IP Security (IPsec) fornece um canal de segurança a nível da camada de rede, garantindo uma comunicação segura entre pares de nós que estejam trocando informações. Além disso, é utilizado para autenticação de remetentes e também para garantir integridade e confiabilidade dos dados transmitidos. Para realizar suas funções, Utiliza dois cabeçalhos de extensão, *Authentication header (AH)* e *encapsulating security payload (ESP) header*. Sua criação foi baseada nos primeiros protocolos de segurança IP. O IPsec já estava presente no IPv4, mas de forma opcional. No IPv6 o suporte ao IPsec passou a ser obrigatório (Reghini, 2013).

2.3 Principais serviços e funcionalidades do IPv6

2.3.1 ICMPv6

ICMPv6 (*Internet Control Message Protocol Version 6*) é o nome utilizado para referenciar o protocolo ICMP no IPv6. Tem como principais objetivos informar características da rede, realizar diagnósticos e relatar erros. Seu cabeçalho é anexado a um datagrama IPv6 e identificado no campo Próximo Cabeçalho com valor 58. É precedido do cabeçalho base e possivelmente de outros de extensão (Heidrich, 2011).

ICPMv6 é de suma importância para o bom funcionamento do IPv6. Pois, é utilizado como protocolo auxiliar para a realização de uma série de funções essenciais, como por exemplo a descoberta de vizinhança, gerenciamento de grupos *multicast*, descoberta

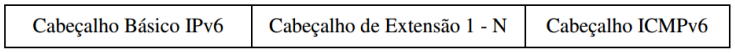

Figura 2.4: Posição do cabeçalho ICMPv6 (Heidrich, 2011)

do *path MTU*, mobilidade, autoconfiguração de endereços, dentre outras (Montibeller, 2011).

Existem basicamente dois tipos de mensagem ICMPv6, de erro e informativas. As de erro podem ser vistas na Tabela 2.1 e as informativas na 2.2 (Heidrich, 2011).

Tabela 2.1: Mensagens de Erros ICMPv6 (Heidrich, 2011).

Tipo	**Nome**	**Descrição**
1	*Destination Unreachable*	Indica que o destino para o qual um pacote foi enviado não está acessível ou há uma falha na transmissão.
2	*Packet Too Big*	Mensagem recebida quando o pacote excede o tamanho máximo da MTU do enlace.
3	*Time Exceeded*	Semelhante ao campo de tempo de vida da versão anterior, onde o limite máximo para os saltos nos enlaces ou o tempo de remontagem dos pacotes nos enlaces foi excedido.
4	*Parameter Problem*	Problemas de cabeçalhos, onde os parâmetros, tipos e tamanhos não foram reconhecidos pelo protocolo.

Tabela 2.2: Mensagens de Informações ICMPv6 (Heidrich, 2011).

Tipo	**Nome**	**Descrição**
128	*Echo Request*	Utilizadaspelo comando ping.
129	*Echo Reply*	
130	*Multicast Listener*	Para o gerenciamento de grupos multicast. Proprietárias do protocolo MLD.
131	*Multicast Listener Report*	
132	*Multicast Listener Done*	
133	*Router Solicitation (RS)*	Protocolo de Descoberta de Vizinhança.
134	*Router Advertisement (RA)*	
135	*Neighbor Solicitation (NS)*	
136	*Neighbor Advertisement (NA)*	
137	*Redirect Message*	
141	*InverseND Solicitation Message*	Utilizadas também na Descoberta de Vizinhança.
142	*Inverse ND Advertisement Message*	
151	*Multicast Router Advertisement*	Mensagens utilizadas nas descobertas dos roteadores vizinhos.
152	*Multicast Router Solicitacion*	
153	*Multicast Router Termination*	

2.3.2 NDP

O protocolo de descoberta de vizinhança ou *Neighbor Discovery Protocol* é definido pela RFC(Request for Comments) 4861 e sua principal função é intermediar a comunicação entre os nós de uma rede. No IPv4 essa função era parcialmente realizada pelo protocolo ARP em conjunto com o RARP e IGMP (Heidrich, 2011).

Segundo Heidrich (2011) as principais características do NDP são:

> "i) determinar o endereço de camada de enlace de dados do modelo OSI, denominada Controle de Acesso ao Meio – *Media Access Control* (MAC), mais conhecido por *MAC-Address*, representado no formato hexadecimal, sendo os três primeiros identificando o código do fabricante e os três últimos o equipamento; ii) encontrar roteadores diretamente conectados (vizinhos) e a acessibilidade dos mesmos; iii) determinar configurações de rede e autoconfiguração de endereços; e iv) alertar endereços de IP duplicados na mesma rede.".

A fim de realizar suas diversas funcionalidades o NDP se utiliza de algumas mensagens que são enviadas através do protocolo auxiliar ICMPv6 com numerações entre 133 e 137, descritas a seguir (Andrade Júnior, 2010; Abreu, 2014):

- *Router Solicitation* (RS): Requisita que os roteadores presentes na rede informem sua presença. A mensagem do tipo RS é enviada ao grupo *multicast all routers* (FE02::2);

- *Router Advertisement* (RA): Enviada por roteadores, a mensagem RA é enviada periodicamente ou em resposta a uma mensagem RS, utilizada para um roteador anunciar sua presença dentro de um enlace. O destino da mensagem depende do motivo que originou a mensagem. Quando é enviada periodicamente, o endereço é o grupo *multicast all-nodes*(FF02::1), caso seja em resposta a um RS, o endereço de destino será o endereço de origem do RS que é um *unicast link local*;

- *Neighbor Solicitation* (NS): Solicita, através de uma mensagem, que um vizinho se apresente e imediatamente envie uma resposta. Possui três funções básicas: detectar endereços duplicados na vizinhança, ter acessibilidade aos vizinhos do enlace e descobrir um endereço físico através de um endereço lógico;

- *Neighbor Advertisement* (NA): Enviada em resposta a um NS ou para anunciar alterações nas características de algum dispositivos da rede;

- *Redirect*: É utilizada pelo roteador para informar uma rota mais favorável para a comunicação com determinado destino.

2.3.3 PATH MTU Discovery

Quando um *host* IPv6 pretende enviar uma grande quantidade de dados, esses dados são divididos em uma série da pacotes menores ou datagramas. É recomendável que esses pacotes possuam o maior tamanho possível para que possam trafegar na rede sem que seja necessário haver nova fragmentação dos mesmos. (McCann *et al.*, 1996).

Segundo a RFC 1981 um *host* que pretende enviar um conjunto de dados através de uma rede IPv6, assume que o tamanho máximo do *PATH MTU* é o do primeiro salto que será realizado. Se em algum momento o datagrama enviado for grande demais para ser encaminhado para o próximo destino sem nova fragmentação, esse datagrama é descartado e o nó que descartou a informação dispara uma mensagem do tipo *ICMPv6 Packet Too Big*. Assim que recebe a mensagem, o nó emissor ajusta o valor do MTU de acordo com o que foi recebido e reenvia a informação pretendida (McCann *et al.*, 1996).

2.3.4 Autoconfiguração de Endereços

A autoconfiguração, configuração automática ou configuração *Stateless* tem como finalidade atribuir automaticamente um endereço para um *host* que pretende ingressar em uma rede IPv6, sem a necessidade de um servidor DHCP (Heidrich, 2011).

Para que seja possível a configuração de forma automática é utilizado um algoritmo que compõe o endereço IPv6 através do *MAC-Address* da interface juntamente com o prefixo da rede fornecido pelo roteador mais próximo. O algoritmo em questão é o *64-bits Extended Unique Identifier* (Heidrich, 2011).

2.3.5 Detecção de Endereços duplicados

Sempre que uma interface de rede recebe um novo endereço IPv6 é realizada a detecção de endereços duplicados. Essa afirmação é pertinente tanto para atribuições manuais quanto para configurações automáticas (Moreiras *et al.*, 2015).

É utilizado o mesmo procedimento da descoberta de vizinhança, a diferença é que

envia-se uma mensagem de *neighbor solicitation* para o mesmo endereço que está sendo configurado e caso alguém responda a essa mensagem com um *neighbor advertisement*, o nó interrompe o processo de configuração e o endereço pretendido não é utilizado (Moreiras *et al.*, 2015).

2.3.6 DNS

O DNS permite a tradução de nomes em endereços IP e também de endereços IP em nomes. Diferente de outras funcionalidades não trabalha como um serviço distinto para o IPv4 e seu sucessor, ou seja, um servidor DNS pode conter tantos os tradicionais registros A(IPv4) quanto os novos registros AAAA que são o novo padrão para o IPv6. Na verdade o servidor não necessita nem mesmo possuir um endereço IPv6 para poder traduzir nomes em registros A ou AAAA (Araújo, 2014).

Se no protocolo a ser substituído já era fácil notar a importância do DNS, uma vez que decorar endereços numéricos é consideravelmente mais desafiador do que nomes, o IPv6 onde os endereços são maiores, o DNS teve sua importância ainda mais acentuada.

2.4 Formas de transição entre protocolos

Conforme foi apontado anteriormente, devido ao alto grau de disseminação do IPv4, o processo de migração será bastante moroso. Nesse período os protocolos terão de coexistir e para tal foram desenvolvidas técnicas que viabilizam esse feito. Dentre elas, as principais serão explicadas a seguir: pilha dupla, tunelamento e tradução.

2.4.1 Pilha Dupla

A técnica mais simples que permite que nós IPv6 continuem compatíveis com nós IPv4 é a pilha dupla. Nós em pilha dupla possuem tanto o IPv4 quanto o IPv6 configurados em suas interfaces e são capazes de enviar e receber informações através de ambos os protocolos, ou seja, podem se comunicar com um *host* que implemente apenas o IPv6 ou apenas o IPv4 ou com outro que também esteja em pilha dupla (Nordmark Gilliganl, 2005).

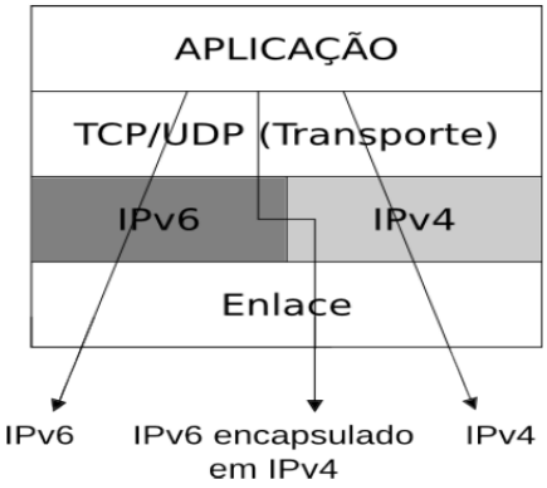

Figura 2.5: Funcionamento da pilha dupla (Moreiras *et al.*, 2012)

Como um nó deve suportar os dois protocolos, precisa receber um ou mais endereços para cada uma das pilhas. Para realizar a configuração do endereço IPv4, podem ser utilizados serviços como o DHCP ou a configuração de endereços manual. Para receber um IPv6 pode-se também recorrer ao DHCPv6 ou a mecanismos de autoconfiguração, lembrando que DHCP e DHCPv6 são serviços distintos (Nordmark Gilliganl, 2005).

2.4.2 Tunelamento

Ao longo do tempo infraestruturas de redes *IPv6-olny* ou as chamadas ilhas IPv6 serão desenvolvidas e precisão se comunicar com outras redes. Nesse período as redes legadas e que implementam apenas o IPv4 continuaram operacionais e podem ser utilizadas para trafegar fluxos de informações em IPv6. Para tal pode ser utilizado um mecanismo de transição chamado tunelamento (Nordmark Gilliganl, 2005).

Em um túnel, um *host* em pilha dupla encapsula um datagrama IPv6 em um IPv4 e o envia através da rede. Quando chega ao seu destino, esse datagrama é desencapsulado e enviado para a interface ou conjunto de interfaces que deve receber aquele pacote (Nordmark Gilliganl, 2005).

Há várias técnicas de tunelamento disponíveis, dentre elas podem ser citadas a 6in4, ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*) e *Tunel Broker*. Além disso, um *Host* ou roteador pode realizar o tunelamento de diversas maneiras, algumas

delas são citadas a seguir (Nordmark Gilliganl, 2005):

- *Router-to-Router*: Roteadores em pilha dupla interconectados por uma infraestrutura IPv4 podem criar um túnel e trocar informações *IPv6-only* entre si;
- *Host-to-Router*: Um *host* em pilha dupla encapsula a informação em IPv6 criando o túnel e envia o datagrama encapsulado para um roteador intermediário que por sua vez envia o pacote a seu destino final;
- *Host-to-Host*: Hosts IPv6 interconectados por uma rede IPv4 trocam informações diretamente entre si encapsulando pacotes através de um túnel;
- *Router-to-Host*: Um roteado em pilha dupla pode encapsular os pacotes e enviá-los diretamente para o nó destino que deve receber a informação.

2.4.3 Tradução

O modelo de transição denomindao de tradução permite que nós que implementem apenas o IPv4 possam se comunicar com outros que implementem apenas o IPv6. Esse processo de comunicação é feito por meio da tradução de cabeçalhos e também da conversão de endereços IPv4 em IPv6 e vice-versa.

As principais técnicas de tradução são: SIIT (*Stateless IP/ICMP Translation*), BIS (*Bump In the Stack*), BIA (*Bump in the API*) e TRT (*Transport Relay Translation*). A utilização dessa técnica implica em uma série de malefícios que serão discutidos no Capítulo 3, impedindo que novas funcionalidades do IPv6 possam ser aproveitadas em sua totalidade (Pedrozo, 2014).

2.4.4 Conclusão

É possível notar, através da análise das principais características do IPv6 e das diferenças em relação ao IPv4, que o IPv6 foi projetado buscando-se torná-lo mais eficiente e livre das deficiências de seu antecessor.

No Capítulo 3, é feita uma revisão da bibliografia a fim de comparar os modelos de transição existentes e determinar quais são as vantagens e desvantagens de cada um

deles. Além disso, ainda por meio dessa revisão, determinar quais são recomendações e restrições para utilização desses modelos.

3 Revisão bibliográfica

Segundo a RFC 6180, a proposta de transição inicial recomendava a adoção da pilha dupla antes do esgotamento de endereços IPv4. A proposta em questão não foi amplamente adotada como o previsto, forçando que outros métodos (Turnelamento, Tradução) fossem desenvolvidos a fim de permitir a coexistência do IPv4 e IPv6 (Arkko Baker, 2007).

De acordo com os trabalhos que seguem: Araújo (2014), Manika (2014), Santos (2013), Junior (2014), Pedrozo (2014), Kaspary Cagliar (2014), Koller Mattos Becker (2012), Heidrich (2011), Carvalho (2006), Barreto (2015), Reghini (2013), Silva (2007), é de senso comum que o método mais recomendado para realizar a implantação do novo protocolo é através da pilha dupla. Esse método de transição facilita a adoção do IPv6 e permite que quando chegar o momento, a migração seja seja feita apenas desligando a pilha correspondente ao IPv4.

Além disso, Araújo (2014), Manika (2014), Santos (2013), Montibeller (2011), Pedrozo (2014), Barreto (2015), Pletsch (2012), Arkko Baker (2007), evidenciam a importância da adaptação de serviços como o DNS e *Firewall* para receber o IPv6. Já os autores Santos (2013), Araújo (2014), Koller Mattos Becker (2012), lembram que os protocolos de roteamento também devem ser adaptados, pois não são compatíveis com o IPv4 e IPv6 simultâneamente, sendo sugerida a adoção do OSPFv2 em paralelo ao OSPFv3.

Como pontos negativos relativos a implantação da pilha dupla, Junior (2014), Pedrozo (2014), Reghini (2013), Inagaki Hammerle (2010), Pletsch (2012) e Silva (2007), destacam o aumento do processamento e consumo de memória nos equipamentos que a adotam, pois estes tem de gerenciar pilhas com tabelas de roteamento distintas. Ainda em relação aos pontos negativos, segundo Santos (2013) e Barreto (2015), a adoção desse mecanismo de transição dificulta o gerenciamento da rede, uma vez que questões como a alocação de endereços, segurança e protocolos de roteamento devem ser tratadas para ambas as pilhas.

Em relação ao de Tunelamento, os autores Manika (2014) e Miotelli Casagrande (2014), sugerem que quando não é possível a adoção do método supracitado, seja pela in-

compatibilidade dos equipamentos envolvidos ou pela falta de endereços IPv4 disponíveis, que este deve ser utilizado. Manika (2014) sugere ainda que a adoção do tunelamento deve ser tratada como temporária, pois prolonga a vida útil do IPv4, retardando a migração por completo para o IPv6.

Assim como a pilha dupla, o tunelamento também possui problemas. Manika (2014), Inagaki Hammerle (2010) e Pletsch (2012), afirmam que sua utilização piora o desempenho da rede e aumenta o processamento nos roteadores, pois estes devem encapsular datagramas IPv6 para que possam trafegar em redes que estejam aptas para tratar apenas o IPv4.

Koller Mattos Becker (2012) ainda lembra que o Tunelamento tem a desvantagem de reduzir o MTU em 20 octetos, correspondentes ao cabeçalho do IPv4, além de dificultar a detecção de problemas na rede.

Em relação a tradução, segundo Manika (2014), esta é a pior das a técnicas de transição entre o IPv4 e IPv6. Os trabalhos Manika (2014), Junior (2014), Miotelli Casagrande (2014), Pedrozo (2014), Koller Mattos Becker (2012), Reghini (2013), Inagaki Hammerle (2010), Pletsch (2012), concordam que sua implantação é bastante complexa, ineficiente e por isso deve ser desencorajada.

Por fim, Miotelli Casagrande (2014) afirma que a tradução impõe limitações a utilização de novas funcionalidades do IPv6 (segurança fim-a-fim, classificação de fluxos), pois nem nem todos os campos do novo protocolo são passíveis de tradução.

3.1 Conclusão

Através da análise da bibliografia disponível, é possível notar uma consensualidade entre os autores que a pilha dupla é a mais indicada dentre as técnicas de transição disponíveis. Quando for o momento adequado, a migração será feita apenas removendo a pilha referente ao IPv4.

Quando não é possível a utilização da pilha dupla, o tunelamento é o modelo recomendado, mas deve ser tratado com uma solução temporária, evitando o prolongamento da vida útil do IPV4. A tradução só deve ser utilizada como forma de coexistência quando não for possível a adoção de outras técnicas.

O Capítulo 4 analisa o processo de transição entre os protocolos da camada de rede na UFJF, apontando o que foi feito, como foi feito e o que ainda deve ser colocado em prática de forma que toda a universidade esteja apta para utilizar o IPv6.

4 Análise do processo de Transição na UFJF

Neste capítulo é feita uma análise do processo de transição entre os protocolos da camada de rede na Universidade Federal de Juiz de Fora, explicando quais foram os métodos utilizados e o porque da utilização desses métodos.

Para o entendimento desse processo é importante conhecer a topologia da rede presente na Universidade. Pois, ela tem papel determinante na escolha das técnicas de transição. A Seção 5.1 aborda esse assunto de forma detalhada.

Além disso, na Seção 5.2, é mostrado como ficou a divisão do bloco de endereços recebido pela instituição. Em seguida, na Seção 5.3, são discutidos os fatores que influenciaram na escolha do modelo de transição utilizado pela UFJF.

A Seção 5.4 aborda a implementação da técnica de transição pilha dupla, apontando como foi feito o processo de implementação da pilha correspondente ao IPv6. Na sequência, Seção 5.5, são analisadas as principais mudanças em serviços essenciais, como o DNS por exemplo. Para finalizar, na Seção 5.6, são elencados os serviços que ainda não receberam o novo protocolo.

4.1 Topologia da Rede

A rede da UFJF segue um padrão conhecido como Estrela. Esse padrão é caracterizado pela existência de um elemento central interconectado com outros equipamentos (*Switches*), como pode ser visto na Figura 5.1.

Cada *Switch* é responsável por controlar o roteamento de pacotes em uma das trinta e uma unidades presentes ao longo do campus e a ele podem ser conectados equipamentos diversos, como computadores, impressoras e roteadores sem fio.

É importante salientar que os equipamentos envolvidos possuem suporte ao IPv6 e a seus possíveis protocolos de roteamento.

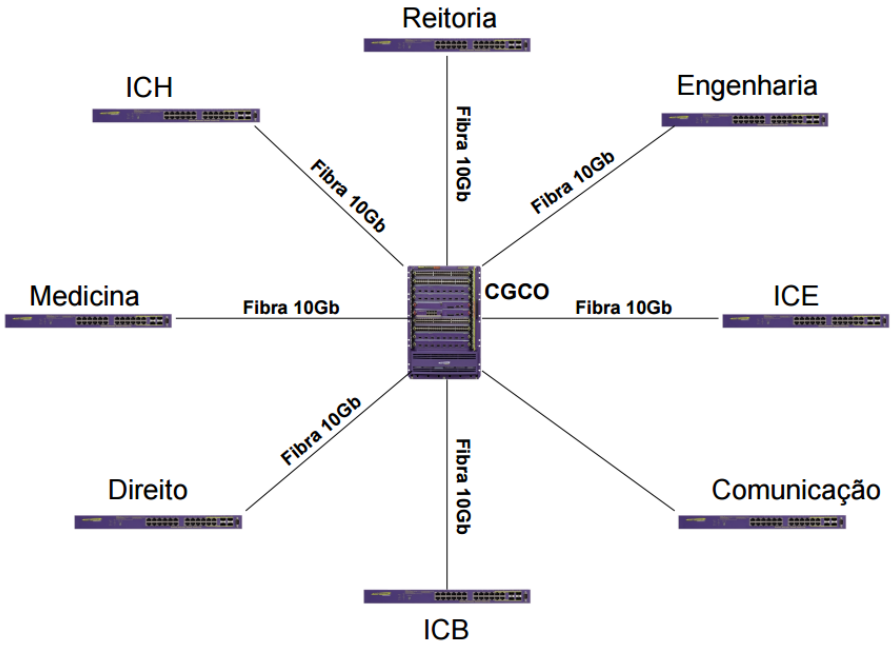

Figura 4.1: Topologia simplificada da rede em estrela na UFJF (Almeida, 2016)

4.2 Plano de endereçamento

O primeiro passo para a adoção do IPv6 é solicitar uma faixa de endereçamento. Um vez obtida essa faixa, deve ser criado um plano que atenda as necessidades atuais e futuras da instituição.

A UFJF fez a solicitação junto ao provedor de acesso e recebeu uma faixa de endereços com prefixo /48 (permite a criação de 256 subredes /56). A primeira proposta foi dividir esse bloco /48 em outros 256 blocos /56 (permite a criação de 256 subredes /64) e distribuir os 256 entre as 31 unidades existentes, ou seja, cada unidade iria receber 8 blocos, totalizando 248 alocações e ainda sobrando 8 para futuras expansões.

Após feita uma análise mais detalhada, concluiu-se que seria desnecessário distribuir todos os blocos /56 logo no início. Segundo a recomendação do NIC.br o ideal é que redes locais possuam prefixo /64 (permite a alocação de 18.446.744.073.709.551.616 dispositivos), dessa forma cada /56 ainda pode ser redividido em outras 256 redes /64.

Ao fim ficou decidido que cada unidade receberia um /56 ficando disponíveis ainda 225 blocos e mediante necessidades futuras as unidades poderiam requisitar outro bloco desse tipo.

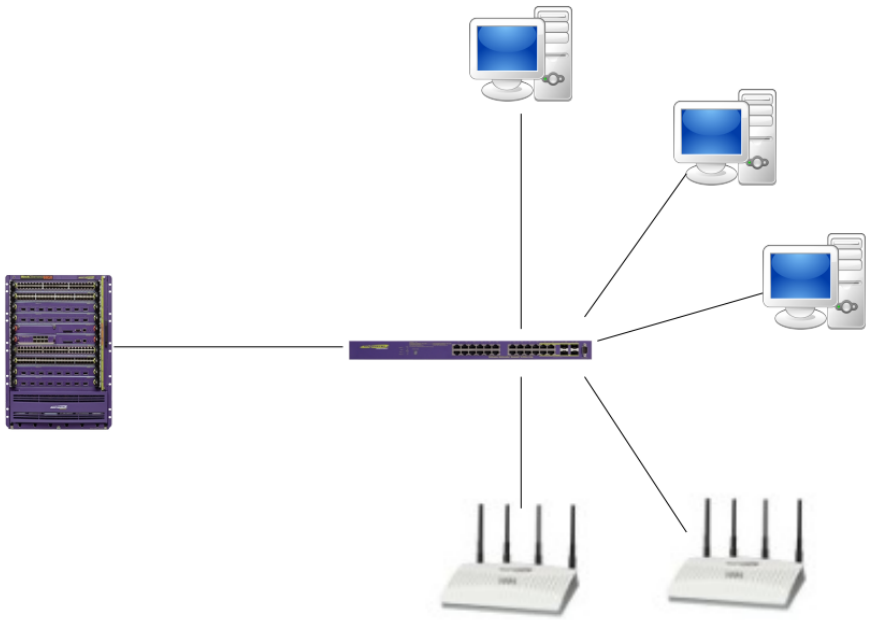

Figura 4.2: Exemplo simplificado de uma das 31 unidades(Almeida, 2016)

4.3 Técnicas de transição utilizadas

Assim que o plano de endereçamento foi criado, precisou-se determinar quais as técnicas de coexistência seriam empregas no processo de transição. Alguns fatores foram analisados na escolha das técnicas adequadas. Dentre eles podemos citar:

- Disponibilidade de endereços IPv4: Caso não haja mais endereços IPv4 disponíveis, é necessária a adoção de técnicas como o tunelamento ou a tradução, uma vez que não é possível a utilização da pilha dupla;
- Compatibilidade dos equipamentos com o IPv6: Outro fator que impede a utilização da pilha dupla é a incompatibilidade de equipamentos com o novo protocolo, forçando também a utilização do tunelamento ou da tradução.

A questão de disponibilidade de endereços IPv4 não foi um problema. Graças a utilização de técnicas como o NAT, a quantidade de endereços desse tipo ainda é suficiente para a demanda da instituição. Em relação a compatibilidade dos equipamentos, também não foram encontrados problemas, pois os roteadores, *Switches* e o *Firewall* são compatíveis tanto com o IPv4 quanto com o IPv6.

Feita essa análise inicial, conclui-se que a técnica mais adequada seria a pilha dupla, não sendo necessária a utilização de outras técnicas (tunelamento e tradução). Procedeu-se com o processo de implantação do IPv6 com base nessa forma de coexistência, onde todos os equipamentos presentes na rede podem trocar informações provenientes tanto do IPv4 quanto do IPv6.

4.4 Implementação da Pilha Dupla

Com o plano de endereçamento em mãos e a forma de implantação determinada, iniciou-se a implementação da pilha correspondente ao IPv6.

A nova pilha foi configurada primeiramente nos equipamentos presentes na borda da rede. Assim, o roteador mais externo, que é a porta de saída para a Internet na Universidade foi o primeiro a receber o IPv6. Em paralelo o *Firewall* também foi configurado para tratar o tráfego proveniente de ambos os protocolos.

Assim que os equipamentos da borda foram contemplados, os roteadores subjacentes começaram a receber a pilha correspondente ao IPv6. Hoje dos 31 equipamentos responsáveis por controlar o roteamento de pacotes nas unidades da UFJF todos estão aptos para conversar tanto via IPv4, quanto pelo IPv6.

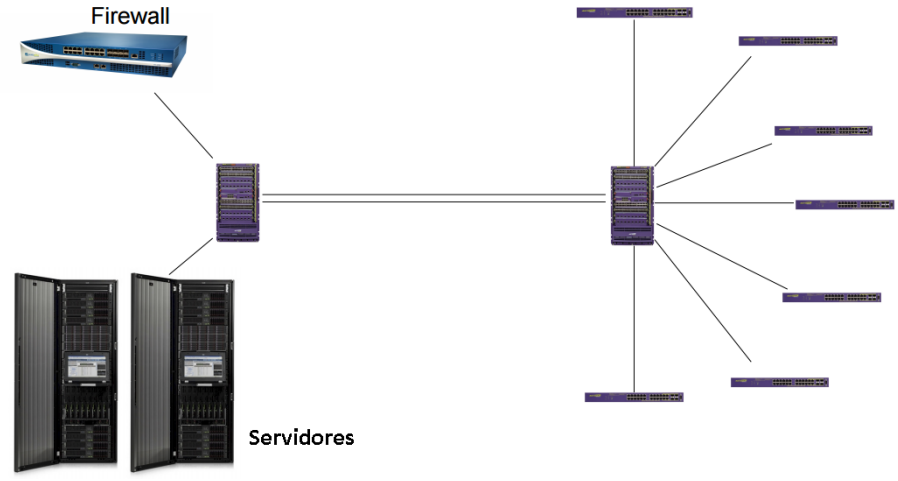

Figura 4.3: Roteadores de borda (Almeida, 2016)

Em seguida a DMZ (*Demilitarized Zone*) também teve o IPv6 habilitado e dessa forma serviços como o *Moodle*, Servidor de *Webmail* e o site institucional da UFJF passa-

ram a trabalhar com o IPv6. Por fim, as redes *Wireless* foram configuradas para distribuir endereços de ambas as pilhas.

4.5 Implementação de Serviços Essenciais

Para implementação de uma rede IPv6 alguns serviços que já existiam anteriormente precisam ser adaptados e outros, devido a incompatibilidade com o novo protocolo devem ser implementados do zero. As principais mudanças e novas implementações são discutidas a seguir.

4.5.1 DNS

Para que o IPv6 possa funcionar corretamente é essencial que o DNS possa resolver consultas de nomes do tipo AAAA. O servidor DNS principal e também os secundários foram configurados e hoje estão aptos a receber consultas de ambos os protocolos, conforme apresentado na Seção 6.5.

4.5.2 Configuração de endereços

Conforme foi abordado na Seção 2.2, o DHCP possui serviços distintos para o IPv4 e IPv6. Logo, o servidor DHCP ativo não pôde ser adaptado.

De maneira inicial ficou decidido que não será implementado um servidor DHCPv6. Dessa forma um equipamento que desejar receber um endereço IPv6 o fará de forma *Stateless*. Para que essa funcionalidade possa ser utilizada fez-se necessária a configuração dos roteadores para informar o prefixo da rede, esse combinado com o *MAC Address* do equipamento fornece um IPv6 do tipo *Global Unicast*.

4.5.3 Protocolo de roteamento

Assim como o DHCP, os protocolos de roteamento não são compatíveis entre si. Logo, foi preciso configurar os roteadores para utilizar o OSPFv3 em paralelo ao OSPF e assim realizar o roteamento de pacotes IPv6 e IPv4 respectivamente.

4.5.4 *Firewall*

Tanto no IPv4 quanto no seu sucessor é de vital importância que dados disponíveis na rede sejam protegidos de agentes maliciosos. Para fornecer essa proteção fez-se necessária a configuração do servidor de *Firewall* objetivando filtrar informações provenientes de ambos os protocolos. Para que isso fosse possível foi fundamental a adoção de um equipamento compatível com o IPv6.

4.6 Questões pendentes

Alguns serviços importantes estão alocados em uma Nuvem Privada. Essa nuvem utiliza o *Openstack* [1] para gerenciar recursos, possibilitando a criação de máquinas virtuais, adição de espaço em disco e gerenciamento de acessos. O problema é que a versão utilizada do *Openstack* não da suporte pleno ao IPv6, portanto, precisa ser atualizada para estar apta a receber o novo protocolo.

4.7 Conclusão

O processo de transição na UFJF foi realizado através da técnica Pilha Dupla, ou seja, nós presentes na rede estão aptos para trocar informações provenientes tanto do IPv4, quanto do IPv6.

Além disso, alguns serviços como o *Firewall* e o DNS, foram adaptados para comportar o IPv6. Outros serviços, que não são compatíveis com ambos os protocolos simultaneamente, precisaram ser implantados, dentre eles podemos destacar o protocolo de roteamento OSPFv3. O Capítulo 5 apresenta os testes que foram realizados objetivando comprovar a operacionalidade das principais funcionalidades do IPv6.

[1] https://www.openstack.org/

5 Testes realizados

Após entendido o atual estado do processo de transição, foram elaborados testes visando comprovar a eficácia da implementação do IPv6. Para cumprir esse objetivo, buscou-se monitorar a troca de mensagens e determinar se as principais funcionalidades estavam funcionando corretamente. Para captura do tráfego foi utilizada uma ferramenta específica para este fim cujo o nome é *Wireshark* [2]. Os testes que foram realizados estão listados a seguir:

- *Neighbor Solicitation* e *Neighbor Advertisement*: Verifica o funcionamento do mecanismo de descoberta de vizinhança;
- *Router Solicitation* e *Router Advertisement*: Verifica o funcionamento do mecanismo de descoberta de roteadores;
- Detecção de endereços duplicados: Testa, como o próprio nome diz, a impossibilidade de atribuição do mesmo endereço para dois equipamentos distintos em uma rede;
- *Path MTU Discovery*: Avalia o processo de descoberta do tamanho máximo do MTU da rota a ser percorrida por um datagrama;
- DNS: Testa a resolução de nomes em endereços IPv4 e IPv6;
- Conectividade do principal site da UFJF (ufjf.br): Verifica se o site ufjf.br está plenamente acessível via IPv6.

5.1 *Neighbor Solicitation* e *Neighbor Advertisement*

O objetivo desse teste é demonstrar o mecanismo de descoberta de vizinhos, realizado pelo NDP no IPv6. Para tal, dois nós se comunicam através do comando *ping6* presente na distribuição Ubuntu 16.04 do Linux. Iniciada a comunicação, é possível observar a

[2] https://www.wireshark.org/

troca de mensagens do tipo *Neighbor Solicitation* e *Neighbor Advertisement* utilizadas para mapear o endereço físico (MAC) e IP.

Na Figura 5.1, no campo endereço inet6, pode-se observar o endereço IPv6 da interface de rede, final 23d, do equipamento que iremos denominar *Host1*. Também pode ser observado no topo dessa Figura, o *ping6* sendo realizado para o endereço do equipamento denominado *Host2*, final cc53. Na Figura 5.2, no campo endereço inet6, é mostrado o endereço IPv6 do *Host2*.

Já na Figura 5.3, no campo *Type*, podemos visualizar a mensagem *Neighbor Solicitation* enviada pelo *Host1* ao *Host2* contendo seu enreço IP e também o MAC de sua interface de rede. Em contrapartida, na Figura 5.4, é possível identificar, também através do campo *Type*, a resposta na forma de uma mensagem *Neighbor Advertisement*, enviada do *Host2* para o *Host1*. Essa mensagem, da mesma forma que a anterior, informa o endereço da interface de rede (MAC).

```
bruno@brunoTelles:~$ ping6 2001:[redacted]:cc53
PING 2001:[redacted]:cc53(2001:[redacted]:cc53) 56 data bytes
64 bytes from 2001:[redacted]:cc53: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=2 ttl=64 time=0.758 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=3 ttl=64 time=0.760 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=4 ttl=64 time=0.741 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=5 ttl=64 time=0.793 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=6 ttl=64 time=0.790 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=7 ttl=64 time=0.768 ms
64 bytes from 2001:[redacted]:cc53: icmp_seq=8 ttl=64 time=0.364 ms
^C
--- 2001:12f0:614:300:27c7:3dd5:bbb0:cc53 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7006ms
rtt min/avg/max/mdev = 0.364/0.801/1.438/0.276 ms
bruno@brunoTelles:~$ ifconfig
enp0s3    Link encap:Ethernet  Endereço de HW 08:00:27:d2:6a:45
          inet end.: 10.[redacted].237  Bcast:10.[redacted].255  Masc:255.255.254.0
          endereço inet6: 2001:[redacted]:1742/64 Escopo:Global
          endereço inet6: 2001:[redacted]:23d/64 Escopo:Global
          endereço inet6: fe80::[redacted]:c6fb/64 Escopo:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
          pacotes RX:13161 erros:1 descartados:0 excesso:0 quadro:0
          Pacotes TX:198 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1000
          RX bytes:1167980 (1.1 MB) TX bytes:22787 (22.7 KB)
          IRQ:19 Endereço de E/S:0xd020

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACK RUNNING  MTU:65536  Métrica:1
          pacotes RX:110 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:110 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1
          RX bytes:11612 (11.6 KB) TX bytes:11612 (11.6 KB)
```

Figura 5.1: Interface de rede do *host1* e ping6 sendo realizado para o *host2*

```
bruno@brunoTelles:~$ ifconfig
enp0s3    Link encap:Ethernet  Endereço de HW 08:00:27:9d:93:6e
          inet end.: 10.[redacted].244  Bcast:10.[redacted].255  Masc:255.255.254.0
          endereço inet6: 2001:[redacted]:cc53/64 Escopo:Global
          endereço inet6: 2001:[redacted]:1164/64 Escopo:Global
          endereço inet6: fe80::[redacted]:5291/64 Escopo:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
          pacotes RX:446 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:120 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1000
          RX bytes:41965 (41.9 KB) TX bytes:15585 (15.5 KB)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACK RUNNING  MTU:65536  Métrica:1
          pacotes RX:411 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:411 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1
          RX bytes:27037 (27.0 KB) TX bytes:27037 (27.0 KB)
```

Figura 5.2: Interface de rede do *host2*

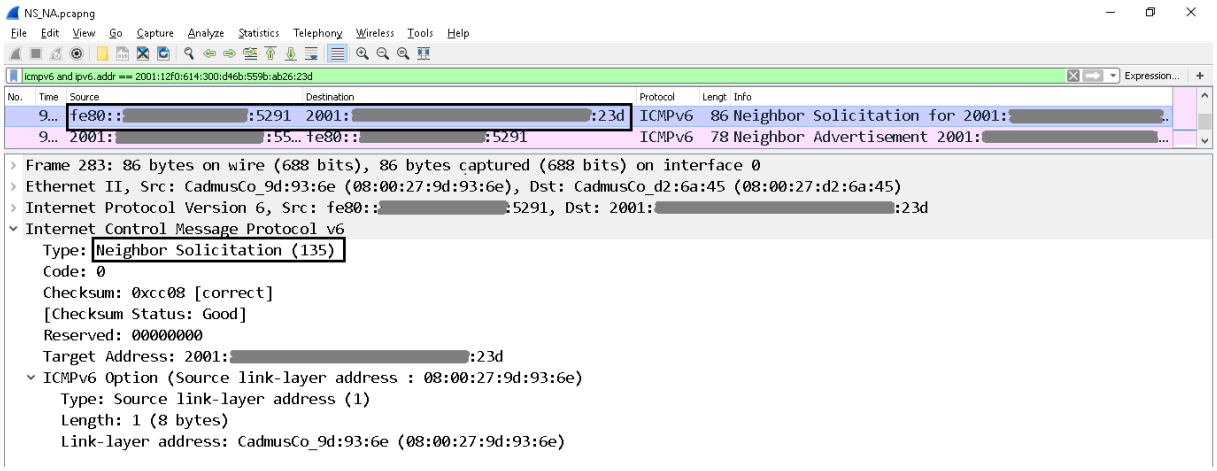

Figura 5.3: *Neighbor Solicitation* sendo disparada do *host1* para o *host2*

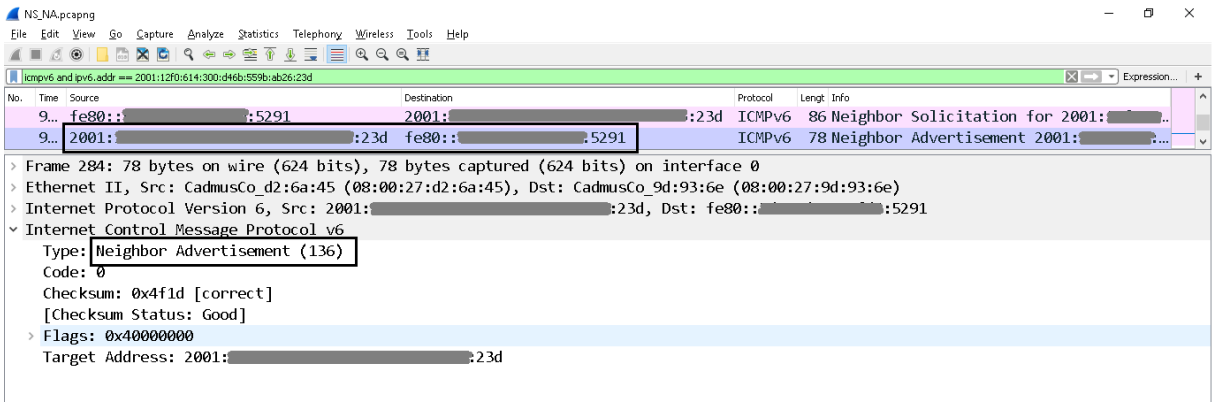

Figura 5.4: *Neighbor Advertisement* sendo disparada do *host2* para o *host1*

5.2 *Router Solicitation* e *Router Advertisement*

O objetivo desse teste é demonstrar o mecanismo de descoberta de roteadores, também realizado pelo NDP no IPv6. Quando um equipamento se conecta a uma rede, envia um mensagem do tipo *Router Solicitation* para o endereço de grupo *multicast all-routers* (ff02::2), informando o endereço físico (MAC) da interface de rede do equipamento. O roteador que recebe essa mensagem responde com uma outra do tipo *Router Advertisement*, informando as características da rede.

Na Figura 5.5, no campo *Type*, é possível identificar o envio da mensagem *Router Solicitation*, do equipamento com IPv6 final fffe para o endereço ff02::2, conforme foi informado anteriormente. Já na Figura 5.6 pode-se observar a resposta, assim como a anterior por meio do campo *Type,* através de uma mensagem *Router Advertisement* do roteador com IPv6 final 9547, informando as características da rede.

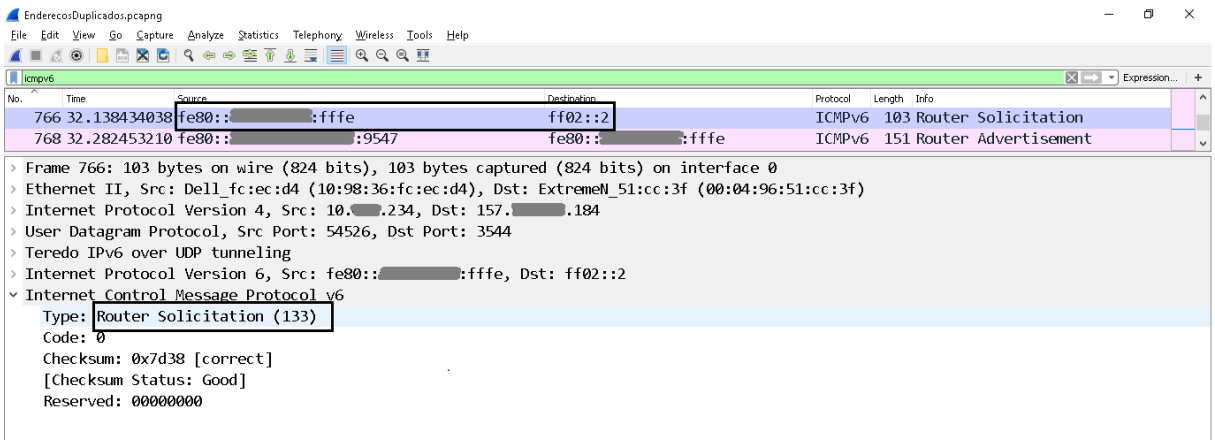

Figura 5.5: Mensagem de *Router Solicitation*

5.3 Detecção de endereços duplicados

Pretende-se identificar, através desse teste, o funcionamento do mecanismo de detecção de endereços duplicados. Para isto, foi feita uma tentativa de trocar o endereço IPv6 de um equipamento, denominado *Host1*, para um endereço já utilizado por outro equipamento, denominado *Host2*.

A Figura 5.7 destaca a falha na tentativa de inserir o IPv6, final cc53, no *Host1*. Pode ser visto também por meio dessa figura, que o *Host1* recebeu um outro endereço

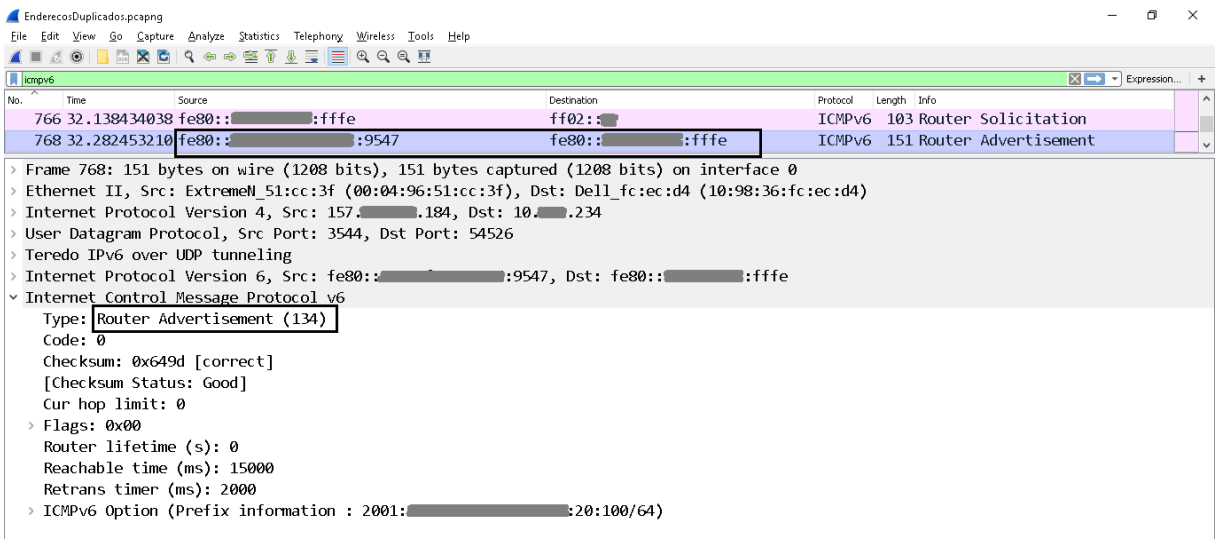

Figura 5.6: Mensagem de *Router Advertisement* em resposta a uma *Router Solicitation*

único, final 23d. Na Figura 5.8, no campo endereço inet6 em destaque, é possível visualizar o endereço IPv6 do *Host2*, final cc53.

Para realizar a detecção de endereços duplicados, o *Host1* envia uma mensagem do tipo *Neighbor Solicitation* para o endereço (final cc53) que pretende utilizar, como pode ser visto no campo *Type* da Figura 5.9. A Figura 5.10 mostra que a mensagem anterior obteve uma resposta, na forma de um *Neighbor Advertisement*, destacado também por meio do campo *Type*. Uma vez obtida essa resposta, o *Host1* identifica que o endereço está alocado para outro equipamento e portanto, não pode utilizá-lo.

5.4 *Path MTU Discovery*

Com a realização desse experimento, deseja-se demonstrar o funcionamento do mecanismo *Path MTU Discovery* do IPv6. Conforme foi abordado anteriormente, quando um *host* envia um datagrama pela rede, o faz, adotando-se o valor do MTU máximo do primeiro salto. Caso esse valor seja superior a algum dos enlaces em que esse datagrama vai trafegar, é enviada uma mensagem do tipo *Packet Too Big* contendo o valor limite do MTU para aquela rede.

A fim de permitir a visualização desse processo, forçou-se a comunicação entre dois equipamentos com um MTU sabidamente superior ao comportado pelos enlaces presentes entre eles. No topo da Figura 5.11, pode ser visto em destaque, a tentativa de comunicação

```
bruno@brunoTelles:~$ sudo ip addr add 2001:[redacted]:cc53/64 dev enp0s3
bruno@brunoTelles:~$ ip addr show dev enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 08:00:27:d2:6a:45 brd ff:ff:ff:ff:ff:ff
    inet 10.[redacted].237/23 brd 10.[redacted].255 scope global dynamic enp0s3
       valid_lft 5156sec preferred_lft 5156sec
    inet6 2001:[redacted]:cc53/64 scope global tentative dadfailed
       valid_lft forever preferred_lft forever
    inet6 2001:[redacted]:23d/64 scope global temporary dynamic
       valid_lft 604688sec preferred_lft 85688sec
    inet6 2001:[redacted]:5e5:1742/64 scope global mngtmpaddr noprefixroute dynamic
       valid_lft 2591966sec preferred_lft 604766sec
    inet6 fe80::[redacted]:e81d/64 scope link
       valid_lft forever preferred_lft forever
bruno@brunoTelles:~$ ifconfig
enp0s3    Link encap:Ethernet  Endereço de HW 08:00:27:d2:6a:45
          inet end.: 10.[redacted].237  Bcast:10.[redacted].255  Masc:255.255.254.0
          endereço inet6: 2001:[redacted]:1742/64 Escopo:Global
          endereço inet6: 2001:[redacted]:23d/64 Escopo:Global
          endereço inet6: fe80::[redacted]:e81d/64 Escopo:Link

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
          pacotes RX:25607 erros:2 descartados:0 excesso:0 quadro:0
          Pacotes TX:1027 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1000
          RX bytes:2624449 (2.6 MB) TX bytes:203163 (203.1 KB)
          IRQ:19 Endereço de E/S:0xd020

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACK RUNNING  MTU:65536  Métrica:1
          pacotes RX:236 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:236 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1
          RX bytes:26884 (26.8 KB) TX bytes:26884 (26.8 KB)
```

Figura 5.7: Tentativa sem sucesso de configurar o IPv6 do *host2* no *host1*

```
bruno@brunoTelles:~$ ifconfig
enp0s3    Link encap:Ethernet  Endereço de HW 08:00:27:9d:93:6e
          inet end.: 10.[redacted].244  Bcast:10.[redacted].255  Masc:255.255.254.0
          endereço inet6: 2001:[redacted]:cc53/64 Escopo:Global
          endereço inet6: 2001:[redacted]:1164/64 Escopo:Global
          endereço inet6: fe80::[redacted]:5291/64 Escopo:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
          pacotes RX:7534 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:370 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1000
          RX bytes:759148 (759.1 KB) TX bytes:42088 (42.0 KB)

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACK RUNNING  MTU:65536  Métrica:1
          pacotes RX:865 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:865 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1
          RX bytes:58760 (58.7 KB) TX bytes:58760 (58.7 KB)
```

Figura 5.8: Interface de Rede do *host2*

utilizando o *ping6* com parâmetro -s. Esse parâmetro permite informar o tamanho do pacote que será enviado, nesse caso o valor especificado foi 1500. Ainda nesse figura, pode ser visualizado no campo endereço inet6, o endereço do *host* que está iniciando a comunicação, IPv6 final 23d.

Na Figura 5.12 no campo *Type*, é destacada a mensagem *Packet Too Big*, enviada

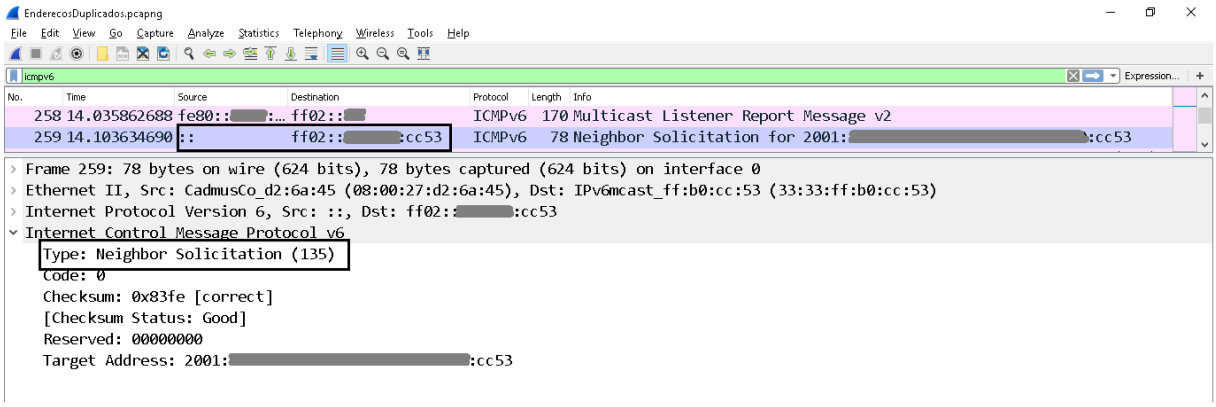

Figura 5.9: NS disparada na tentativa de localizar algum *host* com o endereço que está sendo configurado no *Host1*

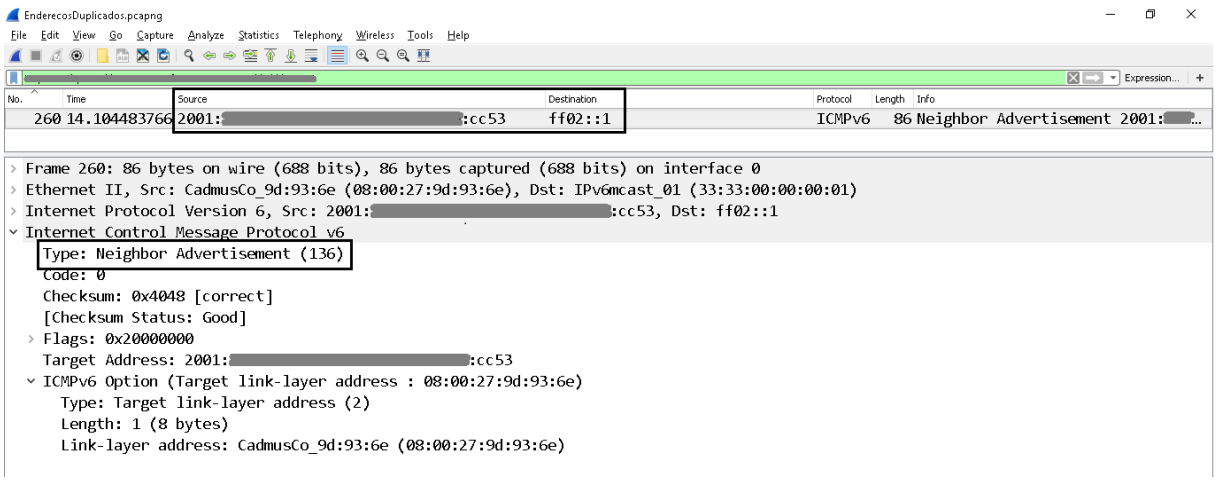

Figura 5.10: NA enviado pelo *host2* informando que o endereço pretendido está em uso

por algum dos roteadores ao longo do caminho percorrido pelos pacotes. É possível identificar, no campo MTU, que o MTU máximo para o enlace do roteador que disparou a mensagem é 1404, ou seja, o emissor deve ajustar o valor do MTU de acordo com o informado e disparar novamente a mensagem pretendida.

5.5 DNS

Um servidor DNS pode prover endereços IPv6 e IPv4 para um mesmo nome. Buscando comprovar o bom funcionamento do servidor DNS configurado na UFJF, serviço essencial para qualquer processo de implantação do IPv6, foram realizadas algumas consultas. Essas consultas foram feitas utilizando-se do comando *nslookup* presente no *prompt* de comando do sistema operacional Windows.

```
bruno@brunoTelles:~$ ping6 -s 1500 www.google.com
PING www.google.com(2800:3f0:4001:801::2004) 1500 data bytes
From 2001:[redacted]::5 icmp_seq=1 Packet too big: mtu=1404
^C
--- www.google.com ping statistics ---
4 packets transmitted, 0 received, +1 errors, 100% packet loss, time 3017ms

bruno@brunoTelles:~$ ifconfig
enp0s3    Link encap:Ethernet  Endereço de HW 08:00:27:d2:6a:45
          inet end.: 10.4.1.237  Bcast:10.4.1.255  Masc:255.255.254.0
          endereço inet6: 2001:[redacted]:1742/64 Escopo:Global
          endereço inet6: 2001:[redacted]:23d/64 Escopo:Global
          endereço inet6: fe80::[redacted]:e81d/64 Escopo:Link
          endereço inet6: 2001:[redacted]:cc53/64 Escopo:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
          pacotes RX:85638 erros:13 descartados:0 excesso:0 quadro:0
          Pacotes TX:9791 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1000
          RX bytes:21458360 (21.4 MB) TX bytes:3300388 (3.3 MB)
          IRQ:19 Endereço de E/S:0xd020

lo        Link encap:Loopback Local
          inet end.: 127.0.0.1  Masc:255.0.0.0
          endereço inet6: ::1/128 Escopo:Máquina
          UP LOOPBACK RUNNING  MTU:65536  Métrica:1
          pacotes RX:1254 erros:0 descartados:0 excesso:0 quadro:0
          Pacotes TX:1254 erros:0 descartados:0 excesso:0 portadora:0
          colisões:0 txqueuelen:1
          RX bytes:170714 (170.7 KB) TX bytes:170714 (170.7 KB)
```

Figura 5.11: Tentativa de ping com MTU 1500

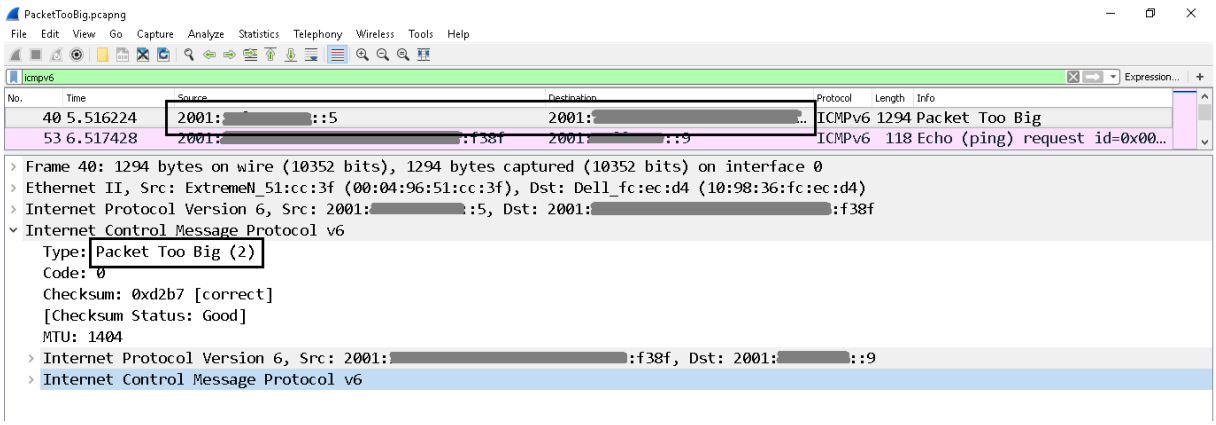

Figura 5.12: Menssagem de *Packet Too Big* em resposta a tentativa de ping com MTU superior ao limite da rede

A Figura 5.13 apresenta uma consulta realizada buscando identificar o endereço IP do site institucional da UFJF, o www.ufjf.br. Conforme pode ser visto no campo *Addresses*, o servidor resolve o nome corretamente, informando tanto os endereços IPv4 (finais 78 ou 79), quanto os endereços IPv6 (finais também 78 e 79). É também realizada uma consulta reversa, informando-se o IP e obtendo-se o nome desejado.

Já a Figura 5.14 mostra uma consulta, não autoritativa, ao site do *Google*, www.google.com. Da mesma forma que a anterior, também através do campo *Addresses*, são informados tanto o endereço IPv4 (final 36) quanto o IPv6 (final 2004). A consulta

reversa não encontrou um nome associado ao IP, possivelmente por não haver um registro reverso cadastrado no DNS responsável por essa zona.

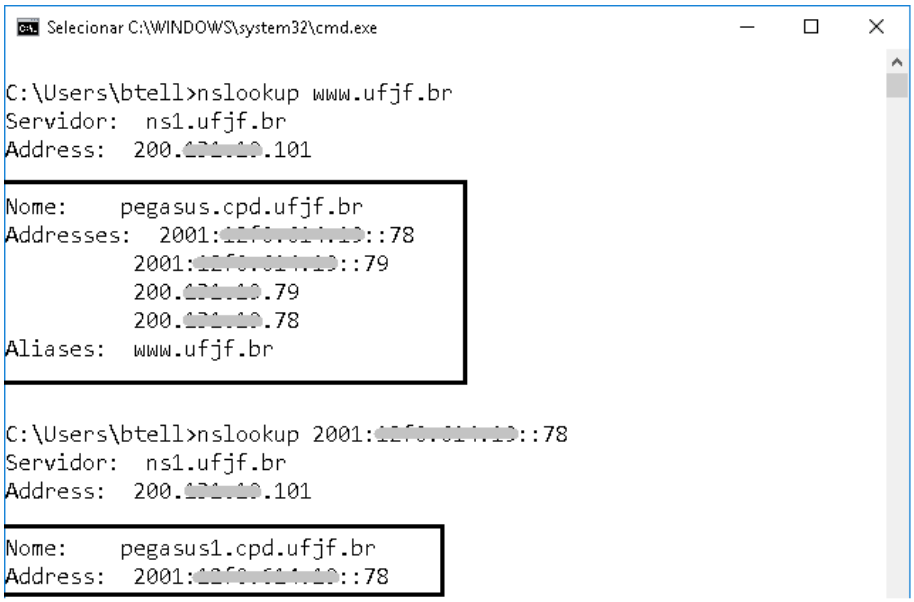

Figura 5.13: Consulta ao DNS da UFJF para o endereço ufjf.br

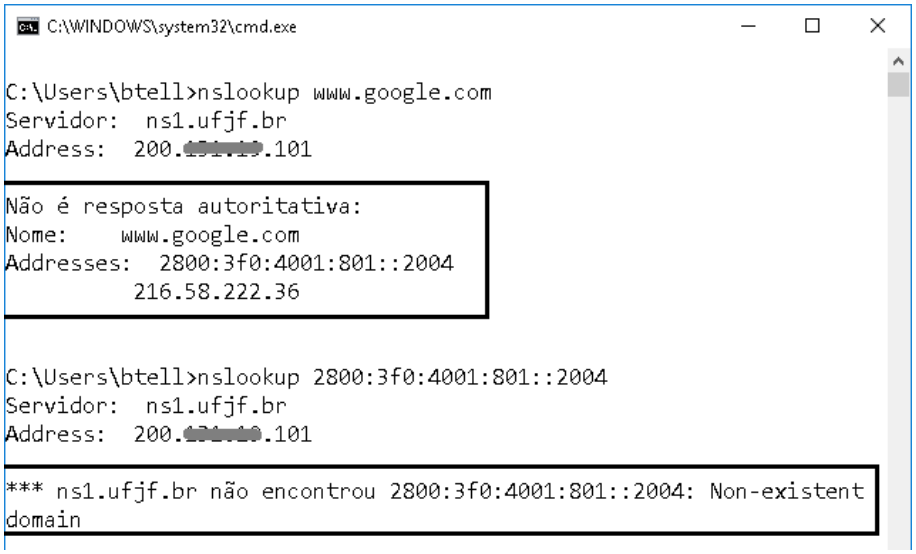

Figura 5.14: Consulta ao DNS da UFJF para o endereço www.google.com

5.6 Conectividade do principal site da UFJF (ufjf.br)

O último teste realizado, teve por objetivo, analisar a conectividade via IPv6 do site institucional da UFJF, www.ufjf.br e seus mais de 800 subdomínios. Para tal, foi utilizado

o comando *Wget* [3] presente na distribuição Ubuntu 16.04 do Linux.

O comando Wget permite realizar o Download, via chamadas HTTP e HTTPS, de um domínio especificado. Possui uma série de parâmetros que podem ser utilizados objetivando especificar alguns comportamentos. Os parâmetros utilizados juntamente com o comando *Wget* para realização desse teste são listados a seguir:

- *recursive*: Percorre de maneira recursiva a árvore de diretórios do domínio especificado;
- *prefer-family=IPv6*: Sempre que possível, dá preferência a comunicação através do IPv6, não sendo possível, utiliza o IPv4;
- *page-requisites*: Força o *Download* de todos os arquivos necessários para mostrar corretamente uma página HTML, como imagens e arquivos de estilo;
- *html-extension*: Arquivos baixados são salvos com extensão html.
- *domains* ufjf.br: O *Download*, ainda que recursivo, não segue domínios que estejam fora de ufjf.br;
- *convert-links*: Converte os links para que eles possam funcionar localmente.

Uma vez inciado o *Download*, monitorou-se, também através do *Wireshark*, as chamadas HTTP e HTTPS ao site da UFJF. Quaisquer chamadas através de endereços IPv4, seriam indicativos que o endereço www.ufjf.br não estaria acessível, em sua totalidade, através do novo protocolo.

Feito esse teste, foram recuperados 208 diretórios, 25134 arquivos, totalizando aproximadamente 1 *Gigabyte* de dados. Os *downloads* dos arquivos foram feitos exclusivamente através do IPv6, não sendo encontrada nenhuma chamada HTTP ou HTTPS através de endereços IPv4. Portanto, o site institucional da UFJF está plenamente acessível através do novo protocolo.

[3] https://www.gnu.org/software/wget/manual/wget.pdf

5.7 Conclusão

Os testes propostos visavam analisar a operacionalidade das principais funcionalidades do IPv6 e foram, em sua totalidade, realizados com sucesso. Logo, é possível constatar que o processo inicial de implantação do IPv6 na UFJF foi concluído com sucesso e a comunicação através do novo protocolo está funcional em todas as unidades da instituição. O Capítulo 6 analisa os resultados obtidos através desse trabalho e propõe alguns temas para realização de trabalhos futuros.

6 Conclusão

Através da análise da implantação do IPv6 na UFJF e revisão da bibliografia disponível, é possível afirmar que o processo de transição está de acordo com as recomendações da RFC 6180 [4] e de outros trabalhos semelhantes. Conforme foi abordado na Seção 2.3.3, essa RFC recomenda a adoção da pilha dupla como forma de coexistência entre protocolos da camada de rede.

A adoção da pilha dupla só foi possível graças a disponibilidade de endereços IPv4 para atual necessidade da instituição e a compatibilidade dos equipamentos envolvidos com o IPv6.

Os testes realizados permitiram comprovar que as principais funcionalidades do IPv6 (configuração de endereços *Stateless*, detecção de endereços duplicados, descoberta de vizinhos e roteadores, *Path MTU Discovery*) estão sendo executadas corretamente e sendo assim, a fase inicial de implementação foi realizada com sucesso.

O IPv6 trouxe outras funcionalidades que ainda precisam ser estudadas, implementadas, testadas e portanto, são oportunidades para realização de trabalhos futuros. Dentre essas funcionalidades podemos destacar a mobilidade em redes móveis, a utilização do IPsec para proveniência de segurança na camada de rede, utilização de grupos *multicast* e classificação de tráfego para priorização de pacotes sensíveis ao atraso.

Para finalizar, é importante salientar que o estoque de endereços IPv4 disponíveis na UFJF vai se esgotar com o tempo. Esse esgotamento de endereços irá forçar a implementação de outras técnicas de transição. Logo, há aqui uma outra oportunidade para realização de pesquisas futuras, que analisem e implementem essas técnicas (Tradução, tunelamento).

[4] https://tools.ietf.org/html/rfc6180

Bibliografia

Abreu, D. H. S. **Proposta de implantação do protocolo ipv6 na rede da universidade federal de lavras**. Lavras, Brasil, 2014.

de Almeida, R. B. **Rede da ufjf: Estrutura e tecnologias**. Juiz de Fora, Brasil, 2016.

Henrique de Oliveira Andrade, R. L. D. G. J. **Interligação da redunb ao br6bone**. Brasília, Brasil, 2010.

de Araújo, L. H. A. **Análise e simulação da técnica de pilha dupla para ipv6**. Curitiba, Brasil, 2014.

J. Arkko, F. B. **Guidelines for using ipv6 transition mechanisms during ipv6 deployment**. In: RFC 6180, 2007.

dos Santos Barreto, J. **Um modelo de migração de ambiente ipv4 para ipv6 em uma rede acadêmica heterogênea**. Brasília, Brasil, 2015.

Barreto, F. **Protocolo ipv6 com pilha dupla em um campus universitário**. In: Revista Brasileira de Computação Aplicada, volume 7, p. 2–16, Passo Fundo, Brasil, 2015.

Brito, S. H. B. **Ipv6 o novo protocolo da internet**. In: IPv6 O Novo Protocolo da Internet, São Paulo, Brasil, 2013. Novatec.

Carvalho, A. C. A. **Ipv6 - conceitos de migração**. Itatiba, Brasil, 2006.

Systems, C. **Routing and bridging guide cisco ace application control engine**. San Jose, *United States of America*, 2011.

Alexandre José Camilo Gomes, C. B. d. T. **Melhores práticas de migração de rede ipv4 para ipv6**. São Paulo, Brasil, 2012.

Heidrich, A. **Implementando um mecanismo de transição ipv4-ipv6**. Paraná, Brasil, 2011.

João Paulo Fernandes Inagaki, L. H. H. **Testes de comunicação em ipv6**. Curitiba, Brasil, 2010.

Junior, E. F. **Estratégia de migração para ipv6: Análise de implantação do dual stack**. Curitiba, Brasil, 2014.

Alexandre Hentges Kaspary, A. I. C. **Implantação do protocolo ipv6 em um laboratório de informática na fai faculdades**. In: Revista Conexão, número 3, Itapiranga, Brasil, 2014.

Leonardo Koller, Matheus Herbstrith de Mattos, R. B. **Implementação prática de tunelamento para transporte de pacotes ipv4 sobre redes ipv6**. In: Cippus, volume 1, p. 49–73, Porto Alegre, Brasil, 2012.

Manika, E. R. **Configuração de um ambiente de simulação de redes demonstrando o método de transição do protocolo ipv4 - ipv6: Pilha dupla e a configuração de um serviço dhcp em ambos os protocolos**. Curitiba, Brasil, 2014.

Fernando Zucuni Martini, M. B. **Análise e proposta de implantação de um ambiente de rede utilizando o protocolo ipv6**. In: Anais do V Encontro de Estudantes de Informática do Tocantins., p. 381–390, Palmas, Brasil, 2003.

J. McCann, S. Deering, J. M. **Path mtu discovery for ip version 6**. In: RFC 1981, 1996.

Melo, S. **Ipv6: Portas abertas para a era da "internet das coisas"**. São Paulo, Brasil, 2012.

Adilson Miotelli, R. A. C. **Estudo da transição entre protocolos de comunicação ipv4 e ipv6**. In: Anais SULCOMP, volume 2, Criciúma, Brasil, 2014.

Montibeller, R. **Implantação de uma rede ipv6 para validação dos protocolos envolvidos**. Blumenau, Brasil, 2011.

Antonio Marcos Moreiras, Edwin Santos Cordeiro, R. R. d. S. A. Y. H. E. B. M. H. d. S. G. T. J. N. R. M. C. T. T. **Ipv6 básico**. In: Curso IPv6 Básico, São Paulo, Brasil, 2012. Novatec.

Antônio Marcos Moreiras, Rodrigo Regis dos Santos, A. Y. H. E. S. C. T. J. N. E. B. M. H. d. S. G. R. M. C. G. B. L. **Laboratório de ipv6**. São Paulo, Brasil, 2015. Novatec Editora.

Neto, M. C. F. **Planejamento da implantação de ipv6 na rede corporativa da câmara dos deputados**. Brasília, Brasil, 2011.

E. Nordmark, R. G. **Basic transition mechanisms for ipv6 hosts and routers**. In: RFC 4213, 2005.

Pedrozo, R. M. **Implantação de uma rede utilizando os padrões do protocolo ipv6**. Santa Maria, Brasil, 2014.

Pletsch, V. **Transição para o protocolo ipv6: Um estudo de caso aplicado a uma provedora de serviços de comunicação multimídia**. Blumenau, Brasil, 2002.

REGHINI, E. C. **Técnicas de tunelamento para redes hibridas ip ipv6 trabalho de diplomação**. Medianeira, Brasil, 2013.

Santos, L. C. D. **Convergência entre ipv4 e ipv6**. Brasília, Brasil, 2013.

da Silva, G. F. **Tunelamento ipv6 / ipv4**. Goiás, Brasil, 2007.